UNIVERSIDADE DA BEIRA INTERIOR
Engenharia

Performance Evaluation of Cooperation Strategies for m-Health Services and Applications

Bruno Miguel Correia Silva

Tese para obtenção do Grau de Doutor em
Engenharia Informática
(3º ciclo de estudos)

Orientador: Prof. Doutor Joel José Puga Coelho Rodrigues

Covilhã, Fevereiro de 2015

This work has been also partially supported by *Instituto de Telecomunicações*, Next Generation Networks and Applications Group (NetGNA), Covilhã Delegation, by National Funding from the FCT - *Fundação para a Ciência e a Tecnologia* through the Pest-OE/EEI/LA0008/2013 Project, and by the AAL4ALL (Ambient Assisted Living for All), project co-financed by the European Community Fund (FEDER) through COMPETE - *Programa Operacional Factores de Competitividade*.

Dedicatória

Na minha vida
perdi madrugadas, venci caminhos
percorri trilhos, soltei muros
ultrapassei portões e barreiras
tive sempre um bom abrigo
a minha família esteve sempre comigo
tantas vezes
semeando o âmago de fútil quimera
nunca me senti isolado
eles sempre estiveram ao meu lado
abraçando a mais pura primavera
hoje
sinto-me feliz e orgulhoso
por ter uma família que sempre me apoiou
incentivou, deu, ajudou
e deixo lacrado, escrito, lavrado
esta poesia de amor
para todos eles
obrigado

de, António José Silva, Escritor, Poeta, Meu Pai.

Acknowledgments

First of all, I would like to thank Professor Joel José Puga Coelho Rodrigues for giving me the chance to join his research group, Next Generation Networks and Applications Group (Net-GNA), for all the constant words of encouragement and for supervising my PhD degree. Without his effort and encouragement, especially in the most difficult moments, none of this would have been possible.

I would also like to thank all my Lab colleagues, especially the ones that help me and collaborate with me, Ivo Lopes, Tiago Machado and Fabio De Longe.

I am most grateful to the University of Beira Interior, the Instituto de Telecomunicações, the Fundação para a Ciência e Tecnologia (FCT), and the Ambient Assisted Living for All (AAL4ALL) project, for all the support that was given to me.

Additionally, I'd like to thank to SAPO PT, especially to Benjamin Junior, for all the support and collaboration.

Last but not least, to my Mother, Father, Grandmothers and Wife, the most important people in my life. Thanks for all the support and help in all the hard times. They are the "pillars" of my "foundation", all that I am and all that I have, I owe to them.

Foreword

This thesis presents the research work performed during the 4-year doctoral research programme, including the main contributions and achieved conclusions. This doctoral programme and inherent research activities were carried at the Next Generation Networks and Applications Group (NetGNA) research group of the *Departamento de Informática*, University of Beira Interior, Covilhã, Portugal and *Instituto de Telecomunicações*, Covilhã Delegation, Portugal.

List of Publications

Articles included in the thesis resulting from this 4-year doctoral research programme

1. **Mobile Health: The Last Frontier on Healthcare Services and Applications**

   Bruno M.C. Silva, Joel J. P. C. Rodrigues, Isabel de la Torre Díez, Miguel López-Coronado

   Paper submitted for publication in an international journal, 2013.

2. **Cooperative Strategies for Challenged Networks and Applications: A Survey**

   Bruno M. C. Silva, Joel J. P. C. Rodrigues, Neeraj Kumar, Guangjie Han

   Paper submitted for publication in an international journal, 2014.

3. **A Novel Cooperation Strategy for Mobile Health Applications**

   Bruno M.C. Silva, Joel J. P. C. Rodrigues, Ivo M. C. Lopes, Tiago M. F. Machado, and Liang Zhou

   IEEE Journal of Selected Areas in Communications, IEEE, Vol. 31, Issue 9, pp. 28 - 36, September 2013.

   DOI: dx.doi.org/10.1109/JSAC.2013.SUP.0513003

4. **Towards a Cooperative Security System for Mobile-Health Applications**

   Bruno M.C. Silva, Joel J. P. C. Rodrigues, Fábio Canelo, Ivo M. C. Lopes and Jaime Lloret

   Journal of Electronic Commerce Research, Springer (in press).

5. **A Data Encryption Solution for Mobile Health Apps in Cooperation Environments: DE4MHA**

   Bruno M. Silva, Joel J. P. C. Rodrigues, Fábio Canelo, Ivo C. Lopes, and Liang Zhou

   Journal of Medical Internet Research, Vol. 13, Issue 4, April 2013.

   DOI: dx.doi.org/10.2196/jmir.2498

6. **MobiCoop: An incentive-based cooperation solution for mobile applications**

   Bruno M. C. Silva, Joel J. P. C. Rodrigues, Mario L. P. Junior, Guangjie Han

   Paper submitted for publication in an international journal, 2014.

Other publications resulting from this doctoral research programme not included in the thesis

1. **SapoFitness: A Mobile Health Application for Dietary Evaluation**

   Bruno M. C. Silva, Ivo C. Lopes, Pradeep Ray and Joel J. P. C. Rodrigues

   IEEE International Conference on E-health Networking, Application & Services (HEALTH-COM), Columbia, 13-15 June, 2011, pages: 375-380.

   DOI: dx.doi.org/10.1109/HEALTH.2011.6026782

2. **Pervasive and Mobile Healthcare Applications**

   Bruno M. C. Silva, Joel J. P. C. Rodrigues, and Ivo M. C. de M. Lopes

   Ambient Assisted Living (Re Visions: Critical Studies in the History and Theory of Art, CRC press Francis & Taylor Publishers, ISBN: 978-1-4398698-4-0, 1st Edition (in press).

3. **A New Mobile Ubiquitous Computing Application to Control Obesity: SapoFit**

   Joel J. P. C. Rodrigues, Ivo M. C. Lopes, Bruno M. C. Silva, and Isabel de la Torre

   Informatics for Health and Social Care, Informa Healthcare, Vol. 38, Issue 1, pp. 37-53, January 2013.

   DOI: dx.doi.org/10.3109/17538157.2012.674586

4. **A Mobile Health Application for Outpatients Medication Management**

   Bruno M. Silva, Ivo M. Lopes, Mickael B. Marques, Joel J.P.C. Rodrigues, and Mario L. Proença Jr.

   IEEE International Conference on Communications (IEEE ICC 2013) - Selected Areas in Communications Symposium – eHealth Track, Budapest, Hungary, June 09-13, 2013, ISBN: 978-1-4673-3122-7, pp. 2982-2986.

   DOI: dx.doi.org/10.1109/ICC.2013.6655256

5. **EmergenSIG: An Integrated Location-based System for Medical Emergencies**

   Bruno D. M. Santos, Joel J. P. C. Rodrigues, Bruno M. C. Silva, and Lei Shu

   The 9th International Conference on Multimedia Information Technology and Applications (MITA 2013), Bali, Indonesia, July 02-06, 2013.

6. **An Ambient Assisted Living Framework for Mobile Environments**

   Bruno M. Silva, Tiago Simões, , Sandra Sendra, and Jaime Lloret

   IEEE-EMBS International Conferences on Biomedical and Health Informatics (BHI 2014), Valencia, Spain, June 1-4, 2014, pp. 448-451.

   DOI: dx.doi.org/10.1109/BHI.2014.6864399

7. **A Mobile Healthcare Solution for Ambient Assisted Living Environments**

   Daniel F. M. Rodrigues, Edgar T. Horta, Bruno M. C. Silva, Fábio D. M. Guedes, and Joel J. P. C. Rodrigues

   16th International Conference on E-Health Networking, Applications and Services (IEEE Healthcom 2014), Natal, Brazil, October 15-18, 2014.

8. **Bruno M. C. Silva, Joel J. P. C. Rodrigues, Tiago M. F. Machado, "Método de cooperação de dados para aplicações e serviços em dispositivos móveis em redes sem fios", Pedido de Patente nº: PT 106891, Situação actual: Patent Pending.**

Resumo

A introdução de tecnologias e sistemas de informação na saúde trouxeram melhorias significativas para a vida dos pacientes, especialmente a pessoas com deficiências, idosos e doentes crónicos. As tecnologias de informação e comunicação têm evoluído rapidamente, juntamente com o conceito de Internet móvel e da ligação em qualquer lugar e a qualquer momento. Neste contexto, surgem as tecnologias móveis para a saúde (*mobile health* - m-Health) que se propõem fornecer serviços de saúde superando barreiras geográficas, temporais e até mesmo organizacionais. M-Health tem como objectivo responder a vários problemas emergentes nos serviços de saúde, incluindo o aumento do número de doenças crónicas relacionadas com os estilos de vida, os altos custos dos serviços de saúde nacionais existentes, a necessidade de capacitar os doentes e famílias para o auto-cuidado e a necessidade de fornecer acesso direto a serviços de saúde independentemente do tempo e do lugar. Sistemas e serviços m-Health incluem o uso de dispositivos móveis e aplicações que interagem com pacientes e cuidadores. No entanto, estes dispositivos têm várias limitações (como em termos de processador, energia e de armazenamento), afetando a qualidade de serviço e experiência do seu utilizador. Arquiteturas baseadas em dispositivos móveis e em comunicações sem fios apresentam vários problemas e constrangimentos, tais como a bateria e capacidade de armazenamento, limitações de transmissão, interferências, falhas de rede, ruídos, larguras de banda limitada e atrasos na rede. Neste sentido, estratégias de cooperação são apresentadas como uma solução para resolver estas limitações focando-se no aumento da ligação de rede, taxas de comunicação e fiabilidade. A cooperação é um importante tema de investigação que tem vindo a crescer nos últimos anos. Com a evolução das redes sem fios, estudos recentes apresentam os mecanismos e algoritmos de cooperação como uma solução para melhorar o seu desempenho. Na ausência de uma infraestrutura de rede estável, os dispositivos móveis devem cooperar entre si realizando todas as funcionalidades de rede. Por exemplo, um dispositivo (nó) intermédio pode suportar o encaminhamento de pacotes entre dois nós distantes.

A presente tese propõe uma estratégia de cooperação para serviços e aplicações de m-Health. Esta abordagem baseada em reputação usa um serviço Web para gerir todas as permissões e reputação dos nós da rede. O seu principal objetivo visa fornecer serviços de Internet a dispositivos móveis sem ligação de rede, através da cooperação com dispositivos vizinhos. Assim, propõe-se resolver os problemas de rede acima mencionados resultando numa melhoria para arquiteturas de rede m-Health. Este trabalho apresenta igualmente a avaliação do desempenho da proposta através de um protótipo num cenário de real com o objectivo de demonstrar e validar esta proposta utilizando uma aplicação m-Health real. Uma solução de criptografia para aplicações de m-Health em ambientes cooperativos, chamada DE4MHA, também é considerada e avaliada usando o mesmo cenário de rede e a mesma aplicação m-Health. Por fim, este trabalho propõe uma framework de aplicação cooperativa generalizada para qualquer aplicação móvel, chamada MobiCoop, baseada na abordagem cooperativa para aplicações m-Health. A avaliação do desempenho desta proposta também é apresentada por meio de um cenário real de rede a fim de demonstrar e validar o MobiCoop utilizando diferentes aplicações móveis.

Palavras-chave

Aplicações móveis para a saúde; Mobile Health; m-Health; Cooperação; Estratégias de Cooperação; Mecanismos de cooperação baseados em incentivos; Mecanismos de cooperação baseados em reputação

Resumo alargado

Enquadramento da Tese

Na última década, os sistemas de informação para a saúde (e-Health) e a telemedicina apresentaram inúmeros serviços e soluções com enorme qualidade e confiança. Estes serviços têm oferecido soluções de saúde mais acessíveis e disponíveis a pacientes que vivem em áreas rurais remotas, que viajam constantemente ou que são fisicamente incapacitados [1,2]. A introdução de tecnologias de informação e comunicação (TIC) como dispositivos médicos, medidores de pressão arterial, glicosímetros, balanças electrónicas e outros dispositivos que interagem com o paciente e médicos, são já casos de sucesso entre os cidadãos comuns. Os médicos podem facilmente fazer o *download* de registos médicos, resultados de laboratório, imagens e informações sobre medicamentos para dispositivos portáteis como assistentes pessoais digitais (PDAs) e *smartphones* ou *tablets*. Os pacientes podem facilmente conhecer o seu diagnóstico de controlo ou de doença e monitorização através de dispositivos móveis confortavelmente e em mobilidade. Estima-se que em 2010-2016 o mercado global de telemedicina deve crescer até cerca de 27,3 bilhões de dólares [3]. Um fator principal que contribui para este investimento do mercado é o aumento da monitorização remota de pacientes. Telemedicina consiste basicamente no uso de informação médica, também conhecido como registos electrónicos de saúde (EHR), trocados através de comunicações electrónicas, melhorando o estado de saúde dos pacientes. Nos EUA, o uso de EHR já é amplamente adotado. Estima-se que cerca de 150.000 profissionais de saúde usam plataformas de EHR [4]. Com a evolução das comunicações móveis suportadas em dispositivos móveis que usam as redes móveis 3G e 4G (e estima-se, para breve, o 5G) para o transporte de dados a computação móvel tem sido a principal atração das comunidades científicas e de negócios. Assim, oferecendo inúmeras oportunidades para criar soluções móveis eficientes para a saúde (m-Health). M-Health propõe-se a prestar e oferecer cuidados de saúde em qualquer lugar e a qualquer hora, superando barreiras geográficas, temporais e até mesmo organizacionais [5,6]. Sistemas m-Health, e as suas funcionalidades de mobilidade, têm um forte impacto sobre a monitorização típica de saúde e os sistemas de alerta, recolha de dados clínicos e administrativos, manutenção de registos, programas de prestação de cuidados de saúde, sistemas de detecção e prevenção de drogas, e até contrafação e roubo [7].

Arquiteturas de rede para serviços e aplicações móveis para a saúde utilizam os serviços Web e a Internet para proporcionar uma interação autêntica entre médicos e pacientes. Um médico ou um paciente pode facilmente aceder ao mesmo registo médico a qualquer hora e em qualquer lugar através do seu computador pessoal, tablet ou *smartphone*. O paciente pode entrar em contato com o médico em caso de emergência, ou mesmo ter acesso aos registos médicos ou compromissos, independentemente de tempo e lugar. Arquiteturas baseadas em dispositivos móveis e comunicações sem fios apresentam, no entanto, vários problemas e restrições, como, bateria e capacidade de armazenamento, as restrições de transmissão, interferências, desconexões, ruídos, larguras de banda limitada, e atrasos na rede. Neste sentido, as abordagens baseadas em cooperação são apresentadas como uma solução para resolver essas limitações, com foco na optimização de energia, aumento de ligações de rede, taxas de comunicação e fiabilidade.

Definição do Problema e Objectivos

O problema abordado nesta tese de doutoramento são as falhas e constrangimentos de redes sem fio e dos próprios dispositivos móveis (acima mencionados) que impedem e impossibilitam uma utilização constante e fiável de aplicações móveis para a saúde quer por parte de pacientes ou cuidadores. Aplicações móveis carecem de uma enorme dependência de uma ligação constante à *Internet* de forma a que consigam aceder a serviços específicos e a servidores. No entanto essas ligações não são sempre possíveis impossibilitando a utilização das mesmas aplicações. Por exemplo, um médico ou paciente que queira aceder aos seus registos médicos através do seu tablet necessita obrigatoriamente que este tenha ligação a uma rede.

Neste contexto, o objetivo principal deste trabalho é a construção e avaliação de uma estratégia de cooperação para serviços e aplicações móveis para a saúde. Esta proposta baseada em reputação, incentiva os utilizadores de dispositivos móveis a cooperar com outros dispositivos vizinhos, reencaminhando de pedidos e respostas e outros pedidos de serviços. Por exemplo, um médico ou paciente que queira aceder aos seus registos médicos através do seu tablet e não tenha ligação de rede, pode através de dispositivos móveis vizinhos, pedindo esses registos.

Para alcançar este objetivo, foram definidos os seguintes objectivos parciais:

- Revisão do estado da arte sobre tecnologias, serviços e aplicações móveis para a saúde existentes e sobre as estratégias e mecanismos de cooperação existentes para sistemas e-Health, redes sem fios, redes ad-hoc e redes com tolerância a falhas.
- Construção e avaliação do desempenho de uma aplicação móvel para a saúde que será usada para avaliar e validar a estratégia de cooperação proposta.
- Proposta e construção de uma nova estratégia de cooperação para serviços e aplicações móveis para a saúde.
- A avaliação do desempenho da estratégia de cooperação para aplicações móveis para a saúde através de um cenário de rede real envolvendo utilizadores reais com uma aplicação m-Health nos seus dispositivos móveis.
- Desenvolvimento e construção de uma solução de criptografia de dados para aplicações móveis para a saúde em ambientes de cooperação.
- A avaliação do desempenho da solução de criptografia de dados para aplicações móveis para a saúde em ambientes de cooperação através de um cenário de rede real envolvendo utilizadores reais.
- Proposta e avaliação de uma *framework* de aplicações generalizada e inter-operável baseada na abordagem cooperativa de incentivos para aplicações móveis.

Hipótese de investigação

Esta tese propõe uma estratégia de cooperação para aplicações móveis para a saúde com enfoque na transmissão e recepção de dados de/para dispositivos que não têm ligação direta com a *Internet*. Neste sentido, dispositivos sem ligação à *Internet* podem usar aplicações e serviços móveis para a saúde, sem problemas. Este trabalho foi portanto o resultado da seguinte hipótese de investigação:

Resumo alargado

Em primeiro lugar são estudadas as arquiteturas de redes em que aplicações e serviços móveis para a saúde são aplicadas, bem como os seus constrangimentos e limitações. De seguida são revistas e estudadas de forma detalhada as estratégias de cooperação que se enquadram nas arquitecturas de rede para aplicações móveis para a saúde. Após esse estudo, são depois analisados os desafios, limitações e problemas associados às estratégias de cooperação.

Baseado nos estudos realizados e nas contribuições retiradas das já existentes estratégias de cooperação, é proposta uma nova estratégia de cooperação para ambientes móveis para a saúde. Esta estratégia baseada em reputação, incentiva os utilizadores de dispositivos móveis a cooperar com outros dispositivos vizinhos, reencaminhando pedidos e respostas e outros pedidos de serviços. De forma a demonstrar a viabilidade e vantagens da proposta e a avaliar o seu desempenho, é usado um cenário real através de uma aplicação para controlo de peso e actividade física, chamada SapoFit [8]. Os resultados obtidos são usados para demonstrar a viabilidade e vantagens da nova estratégia de cooperação.

De seguida, a confidencialidade dos dados e informações pessoais e clinicas dos utilizadores de aplicações móveis para a saúde em ambientes cooperativos é tida em consideração. Assim, uma solução de encriptação de dados é construída e proposta especialmente para ser usada com a nova estratégia de cooperação. Esta solução criptográfica garante a confidencialidade, integridade e autenticidade dos dados trocados entre dispositivos móveis e em comunicações com o serviços *Web*. A avaliação de desempenho desta proposta é igualmente realizada através de um cenário real, usando a mesma aplicação móvel, SapoFit.

Por fim, é proposta uma *framework* de aplicações cooperativa generalizada, baseada na estratégia de cooperação para serviços e aplicações móveis para a saúde. Esta abordagem tem como principal objectivo generalizar a estratégia de cooperação para aplicações móveis para a saúde para quais queres aplicações móveis. A avaliação desta *framework* de aplicações cooperativa é avaliada através de duas aplicações móveis num cenário real. Os resultados obtidos são usados para demonstrar a viabilidade e vantagens desta proposta de cooperação.

Principais contribuições

A primeira contribuição desta tese é a revisão detalhada do estado da arte sobre tecnologias e aplicações para a saúde. Esta revisão analisa a fundo as arquiteturas e cenários de redes em que aplicações e serviços móveis para a saúde são aplicadas, bem como os seus constrangimentos e problemas associados. Este estudo está descrito com detalhe no capítulo 2, que consiste num artigo submetido para publicação numa revista internacional [9].

A segunda contribuição é o estudo exaustivo sobre estratégias de cooperação em redes sem fios, redes ad-hoc móveis (mobile ad-hoc networks - MANETs) e redes intermitentes (delay-tolerant networks - DTNs). Este estudo identifica as principais estratégias de cooperação aplicadas a cenários e constrangimentos de rede semelhantes aos identificados no estudo anterior. Esta contribuição está apresentada no capítulo 3 e consiste num artigo submetido para publicação em revista internacional [10].

A terceira contribuição é a proposta de uma nova estratégia de cooperação para serviços

e aplicações para a saúde. Esta contribuição apresenta uma abordagem baseada em reputação que incentiva os utilizadores de dispositivos móveis a cooperar com outros dispositivos vizinhos e, em função da sua disponibilidade para cooperar, ganham ou perdem reputação. Esta proposta veio resolver o problema identificado e o seu desempenho foi avaliado através de uma aplicação real para controlo de peso e actividade física, chamada SapoFit [8] que requer ligação à *Internet*. O cenário de testes envolveu 19 utilizadores todos com a aplicação SapoFit instalada num dispositivo móvel. Concluiu-se que através desta estratégia de cooperação os utilizadores sem acesso à Internet conseguiam aceder aos dados pedidos através de cooperação com dispositivos vizinhos. Esta contribuição está descrita com detalhe no capítulo 4, que consiste num artigo publicado na revista IEEE Jornal of Selected Areas and Communications [11].

A quarta contribuição inclui a proposta de uma solução de criptografia de dados para aplicações móveis para a saúde em ambientes de cooperação. Esta contribuição apresenta uma estratégia criptográfica que garante a autenticidade, integridade e confidencialidade de todos os pacotes trocados entre dispositivos durante os diversos procedimentos de cooperação. Esta solução de encriptação híbrida, usa algoritmos assíncronos e síncronos e foi especialmente concebida e pensada para aplicações móveis para a saúde em cenários cooperativos. Esta proposta é apresentada no capítulo 5, que consiste num artigo aceite para publicação na revista Journal of Electronic Commerce Research, Springer, num número especial intitulado ”Advances in Security and Privacy for Future Mobile Communications” [12].

A quinta contribuição desta tese é um estudo do comportamento e desempenho da solução de criptografia de dados para aplicações móveis para a saúde em ambientes de cooperação. Este estudo foi realizado através do uso da aplicação SapoFit envolvendo 35 utilizadores. Os testes e questionários concluíram que o desempenho quer da aplicação, quer da estratégia de cooperação não são afectados e que os utilizadores têm mais confiança em utilizar a aplicação sabendo que têm os seus dados protegidos. Este estudo é apresentado em detalhe no capítulo 6, num artigo publicado na revista Journal of Medical Internet Research (JMIR) [13].

A sexta e última contribuição desta tese, é a proposta de uma *framework* de aplicações cooperativa generalizada, baseada na estratégia de incentivos para serviços e aplicações móveis para a saúde anteriormente apresentada. Esta proposta foi construída, demonstrada e avaliada com duas aplicações móveis envolvendo 11 utilizadores e dispositivos reais. O estudo concluiu que os utilizadores sem acesso à Internet conseguiram utilizar com sucesso ambas as aplicações e que o desempenho da estratégia de cooperação se manteve positivo melhorando o próprio desempenho da rede. Esta contribuição é descrita com detalhe no capítulo 7, num artigo submetido para publicação numa revista internacional [14].

Serviços e Aplicações Móveis para a Saúde (M-Health)

O trabalho de investigação apresentado nesta tese inclui o estudo das tecnologias e aplicações móveis para a saúde (m-Health) existentes. Este estudo, descrito no capítulo 2, analisa a evolução destas tecnologias bem como os cenários aplicáveis e arquitecturas de rede, apontando constrangimentos e problemas em aberto em termos de investigação.

O termo m-Health (abreviatura de *mobile health*) foi definido por Laxminarayan e Iste-

panian pela primeira vez, em 2000, como *"unwired med-e"* [15]. Em 2003, o mesmo termo foi definido como comunicações móveis emergentes e tecnologias de rede para sistemas de saúde [16]. Em 2006, Laxminarayan *et al.* apresenta um estudo abrangente sobre o impacto da mobilidade nos sistemas de saúde já existentes. Esse estudo serviu como base para futuras tecnologias e serviços m-Health [17].

A 9 de janeiro de 2007, Steve Jobs, *CEO da Apple Inc.* [18], apresentou ao mundo o *iPhone 2G* e o sistema operativo (SO), *iOS* [19]. Este evento provocou uma evolução rápida dos *smartphones* e aplicações móveis, bem como o surgimento de novos sistemas operativos móveis. Claramente, o *Google Android* e o *iOS* da Apple dominam o mercado de sistemas operativos para dispositivos móveis. A qualidade de ambos é inquestionável e o sucesso das suas aplicações móveis é sustentado pelos respectivos mercados e lojas de aplicações *on-line*. Estas lojas estão abertas para programadores, permitindo-lhes desenvolver todo o tipo de aplicações para vender ou oferecer gratuitamente. Estes mercados abrem novas e potenciais áreas de investigação e desenvolvimento, tais como aplicações móveis para a saúde. No final de 2010, mais de 200 milhões de aplicações móveis para a saúde foram adquiridas e cerca de 70% dos cidadãos em todo o mundo têm interesse em ter acesso a pelo menos uma aplicação m-Health. Os navegadores da Web de *smartphones* igualmente melhoraram, facilitando a procura de aplicações gratuitas e informações [20]. Prevê-se que em 2017, mais de 1.7 biliões de pessoas adquiriram aplicações móveis relacionadas com a saúde, com uma receita de um total de 26 bilhões de dólares no mercado m-Health [21].

O estudo e desenvolvimento de serviços e aplicações móveis para a saúde tem sido um importante ponto de atenção por parte da comunidade científica. Várias áreas de investigação relacionadas com a saúde reuniram importantes descobertas e contribuições, tais como, cardiologia [22–26], diabetes [27–30], obesidade [31–34], tabagismo [35, 36], e cuidados a idosos e doenças crónicas [37, 38]. Estas diferentes especialidades médicas usam aplicações e serviços móveis para a saúde essencialmente para monitorização, prevenção e detecção de doenças e, em serviços mais avançados, apresentam diagnósticos básicos. Para além das aplicações médicas, serviços de m-Health são igualmente aplicáveis em sistemas de saúde em países em desenvolvimento onde as instalações e acesso a cuidados de saúde são difíceis e, por vezes, até inacessíveis [39, 40].

Cooperação entre serviços e aplicações móveis para a saúde apresenta-se como um desafio que precisa de um estudo mais abrangente. Pacientes ou médicos que utilizam os mesmos ou diferentes serviços devem cooperar a fim de alcançar objetivos comuns. Métodos de cooperação também visam uma melhor eficiência e desempenho de dispositivos móveis (por exemplo, bateria do dispositivo, armazenamento e rede). Numa arquitetura de rede típica para m-Health, dados sensíveis como os que são relacionados com saúde são trocados através de redes sem fios. A privacidade e segurança desses dados é uma questão importante na gestão da informação para as necessidades de saúde pública.

Um estudo relacionado com o impacto das tecnologias móveis para a saúde em pacientes e profissionais de saúde precisa de ser realizado. Este estudo deverá incluir questionários para recolha de dados relacionados com a influência de aplicações móveis para a saúde em utilizadores finais durante uma rotina diária. Outro estudo que importa igualmente realizar diz respeito ao modo como os serviços e aplicações móveis para a saúde podem reduzir os custos financeiros

tanto aos utilizadores em geral como aos sistemas privados/públicos de saúde.

Estratégias de Cooperação em Redes sem Fios, Redes Ad-hoc Móveis e Redes Intermitentes

Uma das fases iniciais do trabalho de investigação descrito nesta tese consistiu no estudo de mecanismos de cooperação em redes sem fios, redes ad-hoc móveis (MANETs) e redes intermitentes (DTNs). Os resultados desse estudo estão descritos no capítulo 3 e permitiram identificar abordagens e estratégias cooperativas que não resolvendo o problema abordado nesta tese, poderiam mesmo assim oferecer alguns contributos conceptuais.

A enorme evolução de redes sem fios com base em múltiplas, imprevisíveis e complexas interações exige que os nós da rede cooperem entre si para melhorar o desempenho geral da rede. Estratégias de cooperação em redes sem fios focam-se no aumento da eficiência energética, cobertura de rede, redução de probabilidade de falhas e outras restrições destas redes [41–44]. Além disso, os nós podem otimizar os seus recursos (por exemplo, a duração da bateria) e obter uma qualidade de serviço (*quaility of service* - QoS) equilibrada. Os mecanismos de cooperação diminuem igualmente a dependência das infra-estruturas de rede reduzindo os custos [45, 46].

Em redes móveis ad-hoc (MANETs) as abordagens de cooperação baseadas em incentivos estão divididas em dois grupos principais: sistemas baseados em moeda virtual e sistemas baseados em reputação [47, 48]. Sistemas de moeda virtual usam incentivos para estimular a cooperação entre dispositivos (os nós da rede), abordando o encaminhamento de pacotes como transações com preços e utilizando créditos virtuais como pagamentos. Estes pagamentos virtuais são normalmente atribuídos a nós de rede que cooperam ou executam outras operações de rede específicas. Vários sistemas baseados em moeda virtual têm sido apresentados e propostos [49–55]. Mecanismos de cooperação baseados em reputação observam os comportamentos dos nós da rede e utilizam a reputação para diminuir os comportamentos não cooperativos. Tipicamente, a reputação dos nós é obtida através de observação direta por nós vizinhos e todos os nós da rede conhecem a reputação dos outros nós. Estas estratégias de cooperação usam a reputação como um incentivo para motivar os nós a cooperar e assim, mitigar comportamentos egoístas. Várias importantes propostas baseadas em reputação foram apresentadas nos últimos anos [56–62].

Em redes intermitentes (DTN) [63], as restrições de rede (como a capacidade limitada de armazenamento, largura de banda e energia) afetam gravemente o seu desempenho. Além disso, o desempenho de uma DTN também é afetado por atrasos ou falhas, baixa densidade de nós, baixa fiabilidade de transmissão e mobilidade dos nós. Protocolos de encaminhamento para DTNs assumem geralmente um cenário de cooperação, no entanto, esta é uma assunção irrealista. Os nós podem não ser capazes de cooperar sempre, devido a limitações de recursos ou mesmo a comportamentos egoístas [64]. Por isso, na última década, vários estudos de cooperação e propostas para DTNs foram apresentados [65–70].

Estratégia de Cooperação para Serviços e Aplicações Móveis para a Saúde (M-Health)

A proposta de cooperação para serviços e aplicações móveis para a saúde, descrita no capítulo 4, vem responder aos problemas de rede estudados e ao problema identificado. Esta proposta é baseada em mecanismos de cooperação utilizando um sistema de reputação que consiste em três módulos: 1) a mensagem de controlo que é enviada (através de Bluetooth) para o dispositivo que pretende cooperação e contém o estado dos dispositivos vizinhos descobertos (identificação, estado da bateria, estado da ligação e estado da cooperação); 2) mensagem de controlo de acesso que contém a lista de todos os dispositivos que podem ou merecem cooperar através da sua reputação; 3) um serviço Web de cooperação que faz a gestão da cooperação entre dispositivos calculando e atribuindo a reputação a cada um deles.

1) A mensagem de controlo vai permitir que todos os dispositivos móveis conheçam o estado dos seus vizinhos. Desta forma, um dispositivo sabe qual o seu vizinho ou vizinhos que podem cooperar com ele. A mensagem de controlo, para além da identificação do dispositivo, estado da bateria e estado da ligação (se tem acesso à rede) contém também o estado da cooperação. Este estado informa se o dispositivo é cooperante ou não.

2) A mensagem de controlo de acesso é enviada sempre que a cooperação é estabelecida com outro dispositivo. Ela contém a identificação do dispositivo, o pedido de acesso (a que serviço de rede o dispositivo pretende aceder), uma lista atualizada de vizinhos ao seu alcance, a lista de reputação dos dispositivos na rede atualizada e o tempo de cooperação alcançado, que vai determinar quanto tempo o dispositivo demorou a conseguir o acesso à rede, determinando assim qual o melhor caminho para futuros acessos por cooperação. Este tempo serve também para terminar todos os pedidos de cooperação que alcancem o maior tempo determinado para cooperar (definido em 30 segundos).

3) O serviço Web de cooperação controla e gere toda a cooperação de rede. Através deste serviço é atribuída a reputação de cada dispositivo na rede. Este serviço avalia a condição do dispositivo (ex.: estado da bateria, ligação à Internet, etc.), se foi cooperativo ou não, e atribui um valor de reputação. Na Tabela I do artigo apresentado no capítulo 4 é apresentada a representação esquemática de como o serviço Web de cooperação calcula o valor de reputação considerando o estado da bateria do dispositivo que tem uma classificação que se distingue entre 'crítico', 'pobre', 'regular' e 'excelente'; a percentagem de bateria remanescente do dispositivo; a indicação se o dispositivo tem ligação à Internet; e se o dispositivo é cooperante ou não. Este valor de reputação dos dispositivos varia de $-\infty$ a $+\infty$, sendo que, de $-\infty$ até -1 é considerado egoísta; de -1 a 1, é considerado neutro; e de 1 a $+\infty$ é considerado cooperativo. Esta atribuição de reputação por parte de serviço Web determina os privilégios de acesso à rede. O facto de ser um serviço Web a gerir toda a cooperação da rede liberta e poupa recursos aos dispositivos e, igualmente, consegue que todos tenham acesso à lista de dispositivos na rede bem como à sua respectiva lista de reputação de uma forma mais rápida.

A avaliação do desempenho da proposta foi realizado e está descrito em detalhe na secção 4 do artigo apresentado no capítulo 4. Esta avaliação conclui que dispositivos sem ligação à rede, conseguiram aceder a serviços Web e receber dados através de cooperação com outros

dispositivos sem afectar o desempenho do próprio dispositivo e melhorando o desempenho do cenário de rede.

Solução de Criptografia para Aplicações Móveis para a Saúde: DE4MHA

A segurança foi considerada neste estudo sendo proposta uma solução criptográfica e adaptada especialmente à proposta de cooperação para serviços e aplicações móveis para a saúde. Esta solução, descrita detalhadamente no capítulo 5, intitulada como *Data Encryption Solution for M-Health Applications* (DE4MHA). Esta proposta usa o algoritmo Rivest, Shamir, Adleman (RSA) [71] para a encriptação e decriptação assimétrica das chaves criptográficas e usa o algoritmo Advanced Encryption Standard (AES) [72] para encriptação e decriptação simétrica dos dados. Para além de garantir confidencialidade, este método garante a integridade e autenticidade dos dados através da criação de um resumo da mensagem e de uma assinatura digital. O resumo da mensagem é igualmente encriptado usando a chave privada RSA. Para a segurança da comunicação entre dispositivos e o serviço Web, foi usado o protocolo Hypertext Transfer Protocol Secure (HTTPS) [73].

A avaliação do desempenho da solução de criptografia DE4MHA está descrita em detalhe no capítulo 6. Este estudo envolveu 35 utilizadores e os resultados apresentados na figura 6 do capítulo 6 mostram que a solução criptográfica não tem efeitos negativos no desempenho dos mecanismos de cooperação. Foi igualmente administrado um questionário aos utilizadores (apresentado na figura 4 do capítulo 6). Os utilizadores mostraram-se satisfeitos com o desempenho geral da aplicação e mais confiantes com o facto dos seus dados estarem protegidos durante a comunicação com outros dispositivos.

Framework de Aplicações Cooperativa Generalizada e Inter-operável para Aplicações Móveis: MobiCoop

O trabalho final de investigação desta tese foi a proposta de uma *framework* de aplicações cooperativa generalizada e inter-operável para aplicações móveis, chamada MobiCoop. Esta proposta esta apresentada no capítulo 7 e consiste numa *framework* de aplicações baseada na estratégia de cooperação para aplicações móveis para a saúde apresentada no capítulo 4. O objectivo principal do MobiCoop é apresentar uma *framework* para qualquer aplicação oferecendo uma biblioteca para que criadores de aplicações móveis possam facilmente incorporar e usufruir da estratégia de cooperação proposta.

Foram efectuadas diversas alterações conceptuais de forma a tornar o MobiCoop bastante fácil de incorporar e utilizar por parte dos criadores de aplicações. Além disso, pretende-se que seja o mais transparente possível para os utilizadores. A figura 1 do capítulo 7 apresenta a arquitetura do sistema onde são apresentados os 3 módulos principais do MobiCoop: 1) Modulo de tratamento de pedidos. Este módulo, atua quando o dispositivo não tem ligação à rede recebendo e tratando todos os pedidos realizados. É igualmente responsável pela gestão da ligação Bluetooth entre dispositivos e pelo envio da mensagem de controlo (conforme ilustrado na figura 2 do capítulo 7). Tal como é apresentado no algoritmo 1 (do capítulo 7), os criadores de aplicações têm apenas que incorporar um método de chamada ao módulo de tratamento de

pedidos; 2) Modulo de Cooperação. Este módulo é responsável pelos mecanismos e algoritmos de cooperação, tais como o envio da mensagem de controlo de acesso e o cálculo da reputação dos nós, conforme é apresentado na figura 3 do capítulo 7; e 3) Módulo de serviço Web cooperativo. É responsável por gerir um acesso justo aos serviços/dados pedidos (de forma inteligente) em função da reputação dos respectivos utilizadores/nós. As suas decisões têm como base as observações diretas e indiretas que recebe através das mensagem de controlo de acesso e da lista de reputação dos nós da rede.

A avaliação do desempenho desta proposta descreve-se em detalhe na secção 4 do artigo apresentado no capítulo 7. Esta avaliação envolveu 11 utilizadores reais e 2 aplicações móveis diferentes e o cenário esta ilustrado na figura 4 do capítulo 7. Os resultados desta avaliação apresentados nas figuras 5 e 6 mostram que em comparação com a proposta anterior os objectivos cooperativos foram igualmente alcançados sem deteriorar o desempenho dos dispositivos e da rede.

Principais Conclusões

A presente tese propõe uma nova estratégia de cooperação baseada em incentivos para serviços e aplicações móveis para a saúde. Para alcançar este objectivo o trabalho de investigação foi divido em quatro partes. Estas partes podem ser resumidas como se segue: a primeira foi dedicada ao estudo do tema da tese e à revisão do estado da arte para se identificar as principais tecnologias disponíveis e principais desafios de investigação em aberto; a segunda parte foi dedicada à proposta, construção e avaliação do desempenho de uma nova estratégia de cooperação para sistemas e aplicações móveis para a saúde; a terceira parte descreve e apresenta uma proposta de segurança através de criptografia de dados para aplicações móveis para a saúde em ambientes de cooperação; e, finalmente, a quarta parte foi dedicada à proposta e avaliação do desempenho de uma solução de cooperação generalizada e inter-operável para qualquer a aplicação móvel.

A primeira parte deste trabalho é descrita de forma detalhada nos capítulos 2 e 3 do presente documento. Foi realizado o estudo detalhado do tema da tese com o objectivo de compreender e analisar em profundidade o estado da arte. Em seguida, foi definido e delimitado o enfoque deste trabalho de investigação e foram descritos os principais objetivos. No capítulo 2 é apresentado um estudo abrangente sobre a evolução das tecnologias para a saúde, sobretudo, na área móvel. Através deste estudo foi possível identificar os principais constrangimentos e problemas em aberto neste tipo de arquiteturas de rede e aplicações. Foram igualmente identificados mecanismos de cooperação que apoiaram a proposta de uma solução viável para os problemas analisados. O capitulo 3 apresentou um estudo sobre o estado da arte em mecanismos e estratégias de cooperação em redes sem fios, redes móveis ad-hoc (MANETs) e redes intermitentes (DTNs). Através deste estudo foi possível recolher contribuições importantes para a concepção da nossa proposta. Depois de analisar e identificar as principais limitações das soluções existentes forma identificadas e discutidas algumas questões em aberto.

A segunda parte deste trabalho é apresentada no capítulo 4 e diz respeito ao objectivo principal desta tese, a proposta de uma nova estratégia de cooperação para serviços e aplicações móveis para a saúde. Esta proposta, baseada em mecanismos de reputação, incentiva os

utilizadores de dispositivos móveis a cooperar com outros dispositivos vizinhos, reencaminhando pedidos e respostas de informações médicas e outros pedidos de serviços sem aceder aos conteúdos das mensagens trocadas entre dispositivos. Esta estratégia de cooperação utiliza um serviço Web cooperativo para gerir o acesso a pedidos e a reputação de todos os nós de rede. Esta proposta foi integrada numa aplicação móvel chamada SapoFit. A avaliação do desempenho da proposta foi realizada através desta aplicação que requer ligação constante à Internet e a serviços Web envolvendo 19 utilizadores diferentes. As métricas utilizadas para a avaliação do desempenho dos mecanismos de cooperação foram a probabilidade de entrega de um pedido e o tempo médio de entrega de um pedido. O número de nós não cooperativos foi aumentando durante as experimentações, assumindo como pior caso um cenário com 9 nós não cooperativos. Os resultados foram bastante satisfatórios. Como resultado observou-se que dispositivos sem acesso à rede conseguiram aceder aos dados e ao respectivo serviço Web da aplicação através de cooperação com outros dispositivos. Para o pior caso, a probabilidade média de entrega de pedidos foi de 19% e o atraso máximo de entrega de um pedido foi de 83,7 segundos. De realçar que em números médios de nós não cooperativos (4 a 5) a probabilidade de entrega de pedidos ronda os 60% e a média de atraso de entrega de um pedido varia entre os 60 e os 70 segundos. Estes valores são todos influenciados por variações que resultam de perdas de ligação Bluetooth, variações de distâncias e diferentes especificações de hardware dos dispositivos móveis.

A terceira parte deste trabalho é descrita de forma detalhada nos capítulos 5 e 6 e diz respeito à construção e avaliação do desempenho de uma solução utilizando criptografia de dados para aplicações móveis para a saúde em ambientes de cooperação. O capítulo 5 apresenta a proposta utilizando criptografia híbrida que faz uso de algoritmos de encriptação simétricos e assimétricos para garantir a confidencialidade, integridade e autenticidade dos dados e informações trocadas durante a cooperação. O capítulo 6 apresenta a avaliação do desempenho da solução de criptografia DE4MHA. Esta avaliação envolveu 35 utilizadores que experimentaram a proposta através da aplicação SapoFit e no fim realizaram um breve questionário de satisfação. A avaliação do desempenho concluiu que a solução criptográfica não tem efeitos negativos no desempenho dos mecanismos de cooperação e na aplicação em si. A inclusão do DE4MHA na estratégia de cooperação tem um acréscimo quase insignificante nos tempos de entrega de dados, que ronda, em média, os 2% traduzindo-se em cerca de 0,003557 segundos. O questionário mostrou que os utilizadores ficaram satisfeitos, em geral, com o desempenho da aplicação e mais confiantes com o facto dos seus dados estarem protegidos durante a comunicação com outros dispositivos.

A quarta e última parte dos trabalhos desta tese é apresentada no capítulo 7 e diz respeito a uma proposta de uma *framework* de aplicações cooperativa generalizada e inter-operável para aplicações móveis, chamada MobiCoop. Esta proposta tem como principal objectivo oferecer uma *framework* para qualquer aplicação para que criadores/programadores de aplicações móveis possam facilmente incorporar e usufruir da estratégia de cooperação proposta. MobiCoop foi incorporado em duas aplicações móveis distintas: uma aplicação de mensagens instantâneas via Internet e uma aplicação de envio e recepção de mensagens de correio electrónico. Para a avaliação do desempenho desta proposta foram utilizadas as mesmas métricas num cenário real envolvendo 11 utilizadores. Porém e de forma a emular um cenário ainda mais real foram considerados dois tipos diferentes de utilizadores: utilizadores em mobilidade e utilizadores estáticos. O número de utilizadores não cooperativos variou e o pior caso foi assumido com 6 dispositivos não cooperantes (3 estáticos e 3 em mobilidade). Os resultados foram muito posi-

tivos, com o pior caso a apresentar 78.8 segundos como média de atraso de entrega de pedidos e 36% de probabilidade de entrega de pedidos.

O objectivo principal desta tese e todos os objectivos parciais foram totalmente cumpridos. A proposta de cooperação para serviços e aplicações móveis para a saúde possibilita a utilizadores com dispositivos sem acesso à rede que possam aceder a dados de um servidor e outros serviços Web, através da cooperação com outros dispositivos na vizinhança. Dada a sensibilidade dos dados e informação médica trocada em ambientes de cooperação, uma solução utilizando criptografia, chamada DE4MHA, foi proposta e avaliada com sucesso. Como extensão do trabalho realizado foi proposta uma *framework* de aplicações cooperativa generalizada para qualquer aplicação móvel. Essa proposta, chamada MobiCoop, foi construída e avaliada com sucesso.

Perspectivas de Trabalho Futuro

Uma das linhas de investigação que poderá ser abordada no futuro será o efeito da proposta de cooperação apresentada nesta tese em nós não cooperativos. Nesta tese, nós não cooperativos são incentivados a cooperar sob pena de perder reputação e como consequência não têm acesso a futuros pedidos. Mas pode-se questionar de que forma esses nós não cooperativos podem recuperar esse acesso. E de que forma é que a reputação dos nós vizinhos pode ser um estimulo para nós com baixa reputação tenham interesse em cooperar?

Outra análise futura pode considerar os dois tipos diferentes de utilizadores, com e sem mobilidade. Após a avaliação do desempenho do MobiCoop, apresentada no capítulo 7, foi claro que nós não cooperativos estáticos têm menos impacto que nós não cooperativos em mobilidade. Um estudo avaliando o impacto da mobilidade deve ser realizado com o objectivo de influenciar as pontuações de reputação a estes utilizadores conseguindo distinguir de forma ubíqua quais os que estão em mobilidade e quais os que são estáticos.

Uma outra abordagem futura poderá explorar o facto de que todos os dispositivos conhecem o estado dos dispositivos vizinhos, através da troca de mensagens de controlo. Assim, uma nova abordagem de cooperação pode explorar este facto e dispositivos com melhores condições de energia e processamento podem aceder à rede e servir de nós de encaminhamento para outros dispositivos em condições inferiores. Dispositivos podem-se organizar em grupos e alternadamente, consoante as suas disponibilidades, partilharem recursos e assim optimizar o desempenho da rede.

Referências

[1] B. L. Moullee and P. Ray, “Issues in e-health cost impact assessment,” in *World Congress on Medical Physics and Biomedical Engineering*, vol. 25, no. 12. Munich, Germany: Springer, September 2009, pp. 223–226.

[2] S. Akter, J. D’Ambra, and P. Ray, “User perceived service quality of mhealth services in developing countries,” in *European Conference on Information Systems*, Pretoria, Shouth Africa, June 2010, pp. 1–12.

[3] B. research, "Global markets for telemedicine technologies," 2012. [Online]. Available: http://www.bccresearch.com/market-research/healthcare/telemedicine-technologies-global-markets-hlc014e.html

[4] P. fusion, "150,000 medical professionals stay paperless with practice fusion," June 2013. [Online]. Available: http://www.practicefusion.com/pages/pr/practice-fusion-celebrates-earth-day-2013.html

[5] S. Akter and P. Ray, "mhealth - an ultimate platform to serve the unserved." *Yearb Med Inform*, pp. 94–100, 2010.

[6] S. Tachakra, X. Wang, R. S. Istepanian, and Y. Song, "Mobile e-health: The unwired evolution of telemedicine," *Telemedicine Journal and e-Health*, vol. 9, no. 3, pp. 247–257, 2003.

[7] P. Zuehlke, J. Li, A. Talaei-Khoei, and P. Ray, "A functional specification for mobile ehealth (mhealth) systems," in *11th International Conference on e-Health Networking, Applications and Services (Healthcom 2009)*, 2009, pp. 74–78.

[8] B. M. C. Silva, I. M. Lopes, P. Ray, and J. Rodrigues, "SapoFitness: A Mobile Health Application for Dietary Evaluation," in *IEEE HEALTHCOM 2011*, Columbia, MO, USA, June 13-15, 2011.

[9] B. M. Silva, J. J. P. C. Rodrigues, I. de la Torre Díez, and M. López-Coronado, "Mobile health: The last frontier on healthcare services and applications," *Paper submitted for publication in an international journal*, 2013.

[10] B. M. Silva, J. J. P. C. Rodrigues, N. Kumar, and G. Han, "Cooperative strategies for challenged networks and applications: A survey," *Paper submitted for publication in an international journal*, 2014.

[11] B. Silva, T. Machado, I. Lopes, J. Rodrigues, and L.Zhou, "A novel cooperation strategy for mobile health applications," *IEEE Journal of Selected Areas in Communications*, vol. 31, no. 9, pp. 28–36, September 2013.

[12] B. Silva, J. R. Rodrigues, F. C. Canelo, I. L. Lopes, and J. Lloret, "Towards a cooperative security system for mobile-health applications," *Journal of Electronic Commerce Research, Special Issue on Advances in Security and Privacy for Future Mobile Communications, Springer (in press)*, 2014.

[13] B. Silva, J. R. Rodrigues, F. C. Canelo, I. L. Lopes, and L. Z. Zhou, "A data encryption solution for mobile health applications in cooperation environments: De4mha," *Journal of Medical Internet Research (JMIR)*, vol. 15, no. 4, pp. 1–11, April 2013.

[14] B. M. Silva, J. J. P. C. Rodrigues, M. L. P. Junior, and G. Han, "Mobicoop: An incentive-based cooperation solution for mobile applications," *Paper submitted for publication in an international journal*, 2014.

[15] S. Laxminarayan and R. S. Istepanian, "UNWIRED E-MED: the next generation of wireless and internet telemedicine systems." *IEEE Transactions on Information Technology in Biomedicine*, vol. 4, no. 3, pp. 189–193, Sep. 2000.

[16] R. S. H. Istepanian and J. Lacal, "Emerging mobile communication technologies for health: some imperative notes on m-health," in *Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, vol. 2, 2003, pp. 1414–1416 Vol.2.

[17] R. Istepanian, S. Laxminarayan, and C. Pattichis, *M-Health: Emerging Mobile Health Systems*, ser. Topics in Biomedical Engineering. International Book Series. Springer, 2006.

[18] Apple. (2013) Apple. [Online]. Available: http://www.apple.com

[19] Apple iOS. (2013) Develop apps for ios. [Online]. Available: https://developer.apple.com/technologies/ios/

[20] Mobihealthnews, "The fastest growing and most successful health & medical apps," Mobihealthnews 2010 Report, Tech. Rep., 2010.

[21] research2guidance, "Global mobile health market report 2013-2017," 2013.

[22] D. Scherr, P. Kastner, A. Kollmann, A. Hallas, J. Auer, H. Krappinger, H. Schuchlenz, G. Stark, W. Grander, G. Jakl, G. Schreier, and M. F. a. Fruhwald, "Effect of home-based telemonitoring using mobile phone technology on the outcome of heart failure patients after an episode of acute decompensation: Randomized controlled trial," *Journal of Medical Internet Research*, vol. 11, no. 3, p. e34, Aug 2009. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/19687005

[23] J. Fayn and P. Rubel, "Toward a personal health society in cardiology." *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 2, pp. 401–409, 2010. [Online]. Available: http://dblp.uni-trier.de/db/journals/titb/titb14.html\#FaynR10

[24] C.-T. Lin, K.-C. Chang, C.-L. Lin, C.-C. Chiang, S.-W. Lu, S.-S. Chang, B.-S. Lin, H.-Y. Liang, R.-J. Chen, Y.-T. Lee, and L.-W. Ko, "An intelligent telecardiology system using a wearable and wireless ecg to detect atrial fibrillation." *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 3, pp. 726–733, 2010. [Online]. Available: http://dblp.uni-trier.de/db/journals/titb/titb14.html\#LinCLCLCLLCLK10

[25] M. Morris and F. Guilak, "Mobile heart health: Project highlight," *IEEE Pervasive Computing*, vol. 8, no. 2, pp. 57–61, 2009.

[26] B. Martínez-Pérez, I. de la Torre-Díez, M. López-Coronado, and J. Herreros-González, "Mobile apps in cardiology: Review," *JMIR Mhealth Uhealth*, vol. 1, no. 2, p. e15, Jul 2013. [Online]. Available: http://mhealth.jmir.org/2013/2/e15/

[27] S. G. Mougiakakou, C. S. Bartsocas, E. Bozas, N. Chaniotakis, D. Iliopoulou, I. N. Kouris, S. Pavlopoulos, A. Prountzou, M. Skevofilakas, A. Tsoukalis, K. Varotsis, A. Vazeou, K. Zarkogianni, and K. S. Nikita, "Smartdiab: a communication and information technology approach for the intelligent monitoring, management and follow-up of type 1 diabetes patients." *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 3, pp. 622–633, 2010. [Online]. Available: http://dblp.uni-trier.de/db/journals/titb/titb14.html\#MougiakakouBBCIKPPSTVVZN10

[28] J. C. Sieverdes, F. Treiber, and C. Jenkins, "Improving diabetes management with mobile health technology," *American Journal of the Medical Sciences*, vol. 345, no. 4, pp. 289–295, Apr 2013.

[29] M. Kirwan, C. Vandelanotte, A. Fenning, and J. M. Duncan, "Diabetes self-management smartphone application for adults with type 1 diabetes: Randomized controlled trial," *Journal of Medical Internet Research*, vol. 15, no. 11, p. e235, Nov 2013. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/24225149

[30] A. J. Cafazzo, M. Casselman, N. Hamming, K. D. Katzman, and R. M. Palmert, "Design of an mhealth app for the self-management of adolescent type 1 diabetes: A pilot study," *Journal of Medical Internet Research*, vol. 14, no. 3, p. e70, May 2012. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/22564332

[31] J. P. Pollak, G. Gay, S. Byrne, E. Wagner, D. Retelny, and L. Humphreys, "It's time to eat! using mobile games to promote healthy eating." *IEEE Pervasive Computing*, vol. 9, no. 3, pp. 21–27, 2010. [Online]. Available: http://dblp.uni-trier.de/db/journals/pervasive/pervasive9.html\#PollakGBWRH10

[32] H. Maamar, A. Boukerche, and E. Petriu, "3-d streaming supplying partner protocols for mobile collaborative exergaming for health," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 6, pp. 1079–1095, 2012.

[33] I. Lopes, B. Silva, J. Rodrigues, J. Lloret, and M. Proenca, "A mobile health monitoring solution for weight control," in *International Conference on Wireless Communications and Signal Processing (WCSP 2011)*, 2011, pp. 1–5.

[34] F. Zhu, M. Bosch, I. Woo, S. Kim, C. J. Boushey, D. S. Ebert, and E. J. Delp, "The use of mobile devices in aiding dietary assessment and evaluation." *Journal of Selected Topics in Signal Processing*, vol. 4, no. 4, pp. 756–766, 2010. [Online]. Available: http://dblp.uni-trier.de/db/journals/jstsp/jstsp4.html\#ZhuBWKBED10

[35] R. Whittaker, E. Dorey, D. Bramley, C. Bullen, S. Denny, R. C. Elley, R. Maddison, H. McRobbie, V. Parag, A. Rodgers, and P. Salmon, "A theory-based video messaging mobile phone intervention for smoking cessation: Randomized controlled trial," *Journal of Medical Internet Research*, vol. 13, no. 1, p. e10, Jan 2011. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/21371991

[36] J. Finkelstein and J. Wood, "Interactive mobile system for smoking cessation," in *35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC 2013)*, 2013, pp. 1169–1172.

[37] J. Fontecha, R. Hervás, J. Bravo, and J. F. Navarro, "A mobile and ubiquitous approach for supporting frailty assessment in elderly people," *Journal of Medical Internet Research*, vol. 15, no. 9, p. e197, Sep 2013. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/24004497

[38] G. Chiarini, P. Ray, S. Akter, C. Masella, and A. Ganz, "mhealth technologies for chronic diseases and elders: A systematic review," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 6–18, 2013.

[39] K. Källander, K. J. Tibenderana, J. O. Akpogheneta, L. D. Strachan, Z. Hill, A. A. H. ten Asbroek, L. Conteh, R. B. Kirkwood, and R. S. Meek, "Mobile health (mhealth) approaches and lessons for increased performance and retention of community health workers in low- and middle-income countries: A review," *Journal*

of Medical Internet Research, vol. 15, no. 1, p. e17, Jan 2013. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/23353680

[40] C. Déglise, S. L. Suggs, and P. Odermatt, "Short message service (sms) applications for disease prevention in developing countries," *Journal of Medical Internet Research*, vol. 14, no. 1, p. e3, Jan 2012. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/22262730

[41] Y. Li, X. Zhu, and W. Zhao, "Cooperation mode selection for maximizing throughput in wireless networks," in *Eighth International Conference on Wireless and Optical Communications Networks (WOCN 2011)*, May 2011, pp. 1–5.

[42] L. Al-Kanj and Z. Dawy, "Optimized energy efficient content distribution over wireless networks with mobile-to-mobile cooperation," in *IEEE 17th International Conference on Telecommunications (ICT 2010)*, April 2010, pp. 471–475.

[43] L. Lai, K. Liu, and H. El-Gamal, "The three-node wireless network: achievable rates and cooperation strategies," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 805–828, March 2006.

[44] S. Althunibat, G. Kibalya, and F. Granelli, "Energy-efficient network discovery mechanism by exploiting cooperation among terminals," in *IEEE 19th Symposium on Communications and Vehicular Technology in the Benelux (SCVT 2012)*, Nov 2012, pp. 1–5.

[45] B. Sirkeci-Mergen and A. Scaglione, "On the power efficiency of cooperative broadcast in dense wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 2, pp. 497–507, February 2007.

[46] P. Liu, Z. Tao, Z. Lin, E. Erkip, and S. Panwar, "Cooperative wireless communications: a cross-layer approach," *IEEE Wireless Communications*, vol. 13, no. 4, pp. 84–92, Aug 2006.

[47] M. H. L. Froushani, B. Khalaj, and S. Vakilinia, "A novel approach to incentive-based cooperation in wireless ad hoc networks," in *18th International Conference on Telecommunications (ICT)*, May 2011, pp. 78–83.

[48] H. Shen and Z. Li, "Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 8, pp. 1287–1303, 2012.

[49] L. Buttyan and J.-P. Hubaux, "Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks," Tech. Rep., 2001.

[50] S. Zhong, J. Chen, and Y. Yang, "Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications (INFOCOM 2003)*, vol. 3, March 2003, pp. 1987–1997 vol.3.

[51] M. Jakobsson, J.-P. Hubaux, and L. Buttyán, "A micropayment scheme encouraging collaboration in multi-hop cellular networks," in *Proc. Int'l Financial Cryptograph Conf.*, 2003.

[52] L. Buttyan and J.-P. Hubaux, "Enforcing service availability in mobile ad-hoc wans," in *First Annual Workshop on Mobile and Ad Hoc Networking and Computing (MobiHOC 2000)*, 2000, pp. 87–96.

[53] L. Buttyán and J.-P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," *ACM Mobile Networks and Applications*, vol. 8, no. 5, pp. 579–592, Oct. 2003. [Online]. Available: http://dx.doi.org/10.1023/A:1025146013151

[54] J. Crowcroft, R. Gibbens, F. Kelly, and S. Östring, "Modelling incentives for collaboration in mobile ad hoc networks," *Performance Evaluation Journal*, vol. 57, no. 4, pp. 427–439, Aug. 2004. [Online]. Available: http://dx.doi.org/10.1016/j.peva.2004.03.003

[55] L. Anderegg and S. Eidenbenz, "Ad hoc-vcg: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents," in *Proc. ACM MobiCom*, 2003, pp. 245–259.

[56] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking &Amp; Computing*, ser. MobiHoc '02. New York, NY, USA: ACM, 2002, pp. 226–236. [Online]. Available: http://doi.acm.org/10.1145/513800.513828

[57] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security*. Deventer, The Netherlands, The Netherlands: Kluwer, B.V., 2002, pp. 107–121. [Online]. Available: http://dl.acm.org/citation.cfm?id=647802.737297

[58] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," *CoRR*, vol. cs.NI/0307012, 2003. [Online]. Available: http://dblp.uni-trier.de/db/journals/corr/corr0307.html\#cs-NI-0307012

[59] Q. He, D. Wu, and P. Khosla, "Sori: a secure and objective reputation-based incentive scheme for ad-hoc networks," in *IEEE Wireless Communications and Networking Conference (WCNC 2004)*, vol. 2, March 2004, pp. 825–830 Vol.2.

[60] J. J. Jaramillo and R. Srikant, "Darwin: Distributed and adaptive reputation mechanism for wireless ad-hoc networks," in *Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '07. New York, NY, USA: ACM, 2007, pp. 87–98. [Online]. Available: http://doi.acm.org/10.1145/1287853.1287865

[61] J. Hu and M. Burmester, "Lars: A locally aware reputation system for mobile ad hoc networks," in *Proceedings of the 44th Annual Southeast Regional Conference*, ser. ACM-SE 44. New York, NY, USA: ACM, 2006, pp. 119–123. [Online]. Available: http://doi.acm.org/10.1145/1185448.1185475

[62] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in manets." *IEEE Transactions on Mobile Computing*, vol. 6, no. 5, pp. 536–550, 2007. [Online]. Available: http://dblp.uni-trier.de/db/journals/tmc/tmc6.html\#LiuDVB07

[63] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss, "Delay-Tolerant Networking Architecture," RFC 4838 (Informational), Internet Engineering Task Force, April 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4838.txt

[64] V. N. G. J. Soares and J. J. P. C. Rodrigues, *Cooperative Networking*. Wiley, 2011, ch. Cooperation in DTN-Based Network Architectures, pp. 101–115.

[65] U. Shevade, H. H. Song, L. Qiu, and Y. Zhang, "Incentive-aware routing in dtns," in *IEEE International Conference on Network Protocols (ICNP 2008)*, Oct 2008, pp. 238–247.

[66] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "Smart: A secure multilayer credit-based incentive scheme for delay-tolerant networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, pp. 4628–4639, Oct 2009.

[67] K. Srinivasan, S. Rajkumar, and P. Ramanathan, "Incentive schemes for data collaboration in disruption tolerant networks," in *IEEE Global Telecommunications Conference (GLOBECOM 2010)*, Dec 2010, pp. 1–5.

[68] X. Zhang, X. Wang, A. Liu, Q. Zhang, and C. Tang, "Cooperation enforcement scheme based on reputation for delay tolerant networks," in *International Conference on Computer Science and Network Technology (ICCSNT 2011)*, vol. 4, Dec 2011, pp. 2372–2376.

[69] M. Karaliopoulos, "Assessing the vulnerability of dtn data relaying schemes to node selfishness," *IEEE Communications Letters*, vol. 13, no. 12, pp. 923–925, December 2009.

[70] L. Wei, H. Zhu, Z. Cao, and X. S. Shen, "Mobiid: A user-centric and social-aware reputation based incentive scheme for delay/disruption tolerant networks." in *ADHOC-NOW*, ser. Lecture Notes in Computer Science, H. Frey, X. Li, and S. Rührup, Eds., vol. 6811. Springer, 2011, pp. 177–190. [Online]. Available: http://dblp.uni-trier.de/db/conf/adhoc-now/adhoc-now2011.html\#WeiZCS11

[71] J. Jonsson and B. Kaliski, "Public-key cryptography standards (pkcs) #1: Rsa cryptography specifications version 2.1," United States, 2003.

[72] K. Raeburn, "Advanced Encryption Standard (AES) Encryption for Kerberos 5," RFC 3962 (Proposed Standard), Internet Engineering Task Force, February 2005. [Online]. Available: http://www.ietf.org/rfc/rfc3962.txt

[73] R. E. and S. A., "The secure hypertext transfer protocol," August 1999. [Online]. Available: https://www.ietf.org/rfc/rfc2660.txt

[74] G. Kramer, I. Marić, and R. D. Yates, "Cooperative communications," *Found. Trends Netw.*, vol. 1, no. 3, pp. 271–425, Aug. 2006. [Online]. Available: http://dx.doi.org/10.1561/1300000004

Abstract

Health telematics are becoming a major improvement for patients' lives, especially for disabled, elderly, and chronically ill people. Information and communication technologies have rapidly grown along with the mobile Internet concept of anywhere and anytime connection. In this context, Mobile Health (m-Health) proposes healthcare services delivering, overcoming geographical, temporal and even organizational barriers. Pervasive and m-Health services aim to respond several emerging problems in health services, including the increasing number of chronic diseases related to lifestyle, high costs in existing national health services, the need to empower patients and families to self-care and manage their own healthcare, and the need to provide direct access to health services, regardless the time and place. Mobile Health (m-Health) systems include the use of mobile devices and applications that interact with patients and caretakers. However, mobile devices have several constraints (such as, processor, energy, and storage resource limitations), affecting the quality of service and user experience. Architectures based on mobile devices and wireless communications presents several challenged issues and constraints, such as, battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, and network delays. In this sense, cooperation-based approaches are presented as a solution to solve such limitations, focusing on increasing network connectivity, communication rates, and reliability. Cooperation is an important research topic that has been growing in recent years. With the advent of wireless networks, several recent studies present cooperation mechanisms and algorithms as a solution to improve wireless networks performance. In the absence of a stable network infrastructure, mobile nodes cooperate with each other performing all networking functionalities. For example, it can support intermediate nodes forwarding packets between two distant nodes.

This Thesis proposes a novel cooperation strategy for m-Health services and applications. This reputation-based scheme uses a Web-service to handle all the nodes reputation and networking permissions. Its main goal is to provide Internet services to mobile devices without network connectivity through cooperation with neighbor devices. Therefore resolving the above mentioned network problems and resulting in a major improvement for m-Health network architectures performances. A performance evaluation of this proposal through a real network scenario demonstrating and validating this cooperative scheme using a real m-Health application is presented. A cryptography solution for m-Health applications under cooperative environments, called DE4MHA, is also proposed and evaluated using the same real network scenario and the same m-Health application. Finally, this work proposes, a generalized cooperative application framework, called MobiCoop, that extends the incentive-based cooperative scheme for m-Health applications for all mobile applications. Its performance evaluation is also presented through a real network scenario demonstrating and validating MobiCoop using different mobile applications.

Keywords

Mobile Health; m-Health; Mobile computing; e-Health; Cooperation; Cooperation Strategies; Incentive-based cooperation scheme; Reputation based cooperative scheme

Contents

List of Figures

Chapter 2

Mobile Health: The Last Frontier on Healthcare Services and Applications

Chapter 3

Cooperative Strategies for Challenged Networks and Applications: A Survey

Chapter 4

A Novel Cooperation Strategy for Mobile Health Applications

Chapter 5

Towards a Cooperative Security System for Mobile-Health Applications

Chapter 6

A Data Encryption Solution for Mobile Health Apps in Cooperation Environments: DE4MHA

Chapter 7

MobiCoop: An incentive-based cooperation solution for mobile applications

List of Figures

List of Tables

Acronyms

3DES	Triple Data Encryption Standart
3G	Third-generation
4G	Fourth-generation
AES	Advanced Encryption Standart
AF	Amplify-and-forward
ANSI	American National Standards Institute
AP	Access Point
API	Application Programming Interface
BMI	Body Mass Index
BMR	Basal Metabolic Rate
CCS	Credit Clearance Service
CCS	Credit Clearance Service
CDMA	Code Division Multiple Access
CF	Compress-and-forward
CICC	Coordinate Interleaved Coded Cooperation
CMRC	Cooperative Maximum Ratio Combining
CONET	Cooperative Networking Protocol
CSCW	Computer Supported Cooperative Work
CUDA	Compute Unified Device Architecture
CWS	Cooperative Web Service
DARWIN	Distributed and Adaptative Reputation Mechanism for Wireless Networks
DES	Data Encryption Standart
DF	Decode-and-forward
DSA	Digital Signature Algorithm
DSR	Dynamic Source Routing Algorithm
DSTC	Distributed space-time Coding
DTN	Delay Tolerant Network
EC	European Commission
ECC	Elliptic Curve Cryptography
ECG	Electrocardiogram
EHR	Electronic Health Record
EMG	Electromyogram
FDA	U.S. Food and Drug Administration
FDASIA	FDA Safety and Innovation Act
FIPS	Federal Information Processing Standart
FTP	File Transfer Protocol
GBA	Generic Bootstrapping Architecture
GSM	Global System for Mobile Communications
HDE	Humanitarian Use Exception
HIV	Human Immunodeficiency Virus
HL7	Health Level seven
HTTP	HyperText Transfer Protocol

HTTPS	HyperText Transfer Protocol Secure
HUD	Humanitarian Use Devices
IBM	International Business Machines
ICT	information and communication technologies
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
JSP	Java Server Pages
KB	Kilobyte
KES	Knowledge Editing Service
LAN	Local Area Network
LARS	Locally Aware Reputation System
MAC	Media Access Control
MANET	Mobile ad-hoc network
MD5	Message Digest 5
MDD	Medical Devices Directive
MDF	Multipath Decode-and-forward
NBS	Nash Bargain Solution
NetGNA	Next Generation Networks and Applications Group
OS	Operating System
OSI	Open Systems Interconnection
P2P	Peer-to-peer
PAN	Personal Area Network
PC	Personal Computers
PDA	Personal Digital Assistant
PDF	Portal Document Format
PGP	Pretty Good Privacy
PHR	Personal Health Record
PKI	Public Key Infrastructure
PMA	Premarket approval
POP	Post Office Protocol
QoE	Quality of Experience
QoS	Quality of Service
RAM	Random Access Memory
REST	Representational State Transfer
RFID	Radio-Frequency IDentification
RS	Relay Stations
SAML	Secure Assertion Markup Language
SHA- 1	Secure Hash Algorithm
SOA	Service Oriented Architecture

Acronyms

SOAP	Simple Object Access Protocol
SoC	System-on-chip
SORI	Objective Reputation-based Incentive Scheme for Ad-Hoc Networks
SR	Selection Relaying
SSL	Secure Socket Layer
UBI	Universidade da Beira Interior
URL	Uniform Resource Locator
WBSN	Wireless Body Sensor Network
WEP	Wired Equivalent Privacy
WHO	World Health Organization
WLAN	Wireless Local Area Network
WS	Web Service
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

Chapter 1

Introduction

1.1 Motivation

In the last decade health telematics, also known as Electronic Health (e-Health), have presented a pletora of reliable health services. These services have offered patients that live in remote rural areas, that travel constantly or that are physically incapacitated, more accessible and affordable healthcare solutions [1, 2]. The introduction of information and communication technologies (ICTs) as home medical devices, such as blood pressure monitors, glucometers, scales and other devices that interact both with patient and their doctors, are already a success among common citizens. Physicians can easily download medical records, lab results, images, and drug information to handheld devices like personal digital assistants (PDAs) and smartphones. Patients could be aware of their diagnostic, disease control, and monitoring with comfortable mobile devices that accompany them everywhere. According to [3], from 2010 to 2016 the global telemedicine market is expected to grow from to nearly 27.3 billion dollars. One main factor that contributes to this market investment is the increased remote monitoring of patients. Telemedicine basically assents on the use of medical information, also known as Electronic Health Records (EHR), exchanged via electronic communications improving the patients□ health status. In the United States, the use of EHR technology is already widely adopted. It is estimated that 150.000 Medical professionals are using EHR platforms [4]. With the advent of mobile communications based on smart mobile devices that support 3G and 4G mobile networks for data transport, mobile computing has been the main attraction of research and business communities. Thus, offering innumerous opportunities to create efficient mobile health solutions. Mobile health (m-Health) is the new edge on healthcare innovation. It proposes to deliver healthcare anywhere and anytime, surpassing geographical, temporal, and even organizational barriers [5,6]. M-Health systems and its inherent mobility functionalities have a strong impact on typical healthcare monitoring and alerting systems, clinical and administrative data collection, record maintenance, healthcare delivery programs, medical information awareness, detection and prevention systems, drug-counterfeiting, and theft [7].

Typical m-Health services architectures (presented in Figure 1.1) use the Internet and Web services to provide an authentic pervasive interaction among doctors and patients. A physician or a patient can easily access the same medical record anytime and anywhere through his personal computer, tablet, or smartphone. A patient can contact a physician in case of an emergency, or even have access to medical registers or appointments regardless of time and place. Architectures based on mobile devices and wireless communications presents several challenged issues and constraints, such as, battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, and network delays. In this sense, cooperation-based approaches are presented as a solution to solve such limitations, focusing on increasing network connectivity, communication rates, and reliability.

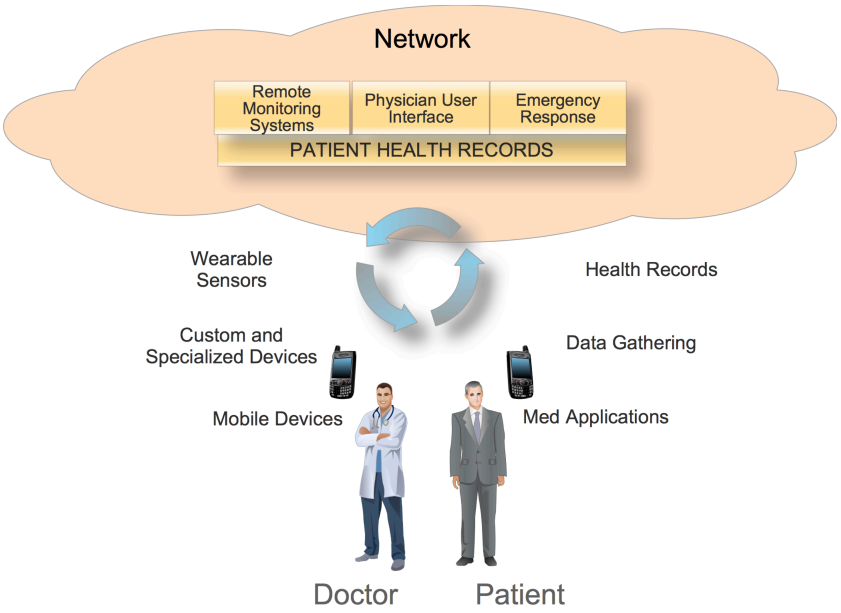


Figure 1.1: m-Health services typical arquitecture.

This research work presented on this thesis is focused in the challenges raised from wireless networks architectures based on Web services access and mobile devices that directly affects the quality of use of m-Health applications. Thus, this research work is dedicated to searching for solutions that can provide continuous use of m-Health services and applications to mobile devices under challenged wireless environments. The mechanisms studied and proposed in this thesis plays special attention to m-Health services and applications availability, mobile devices energy consumption and security of all forwarded health data.

1.2 Problem Definition and Research Objectives

Typical m-Health services and applications network architectures assent on mobile devices using the Internet and Web services. These architectures and wireless communications presents several challenged issues and constraints. Issues such as battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, and network delays, are often a limitation to m-Health applications that typically depends of Internet connection to have access to a data/information cloud storage or Web services. For example, a patient or a doctor that wants to have access to a patient EHR through a mobile device must have Internet or network connectivity. The research problem studied in this thesis addresses the constraints and issues of wireless networks architectures based on Web services access and mobile devices that directly affects the quality of use of m-Health applications.

Cooperation is an important research topic that has been growing in recent years. With the advent of wireless networks and mobile technologies, several recent proposals presented cooperative based schemes as a solution to improve wireless networks overall performance [74]. These cooperative strategies mainly focuses on increasing network connectivity, communication rates, reliability and energy efficiency. Therefore improving both network devices and network overall performance.

In this context, the main objective of this thesis is the proposal and performance evaluation of a novel cooperation strategy for mobile health services and applications. This proposal will enable mobile devices without Internet connectivity to access Web services requests through cooperation with neighbor mobile devices. This reputation based approach punishes un-cooperative behaviors focusing on forwarding and retrieving data to/from neighbor devices that have no direct connection to a m-Health application.

To reach this main goal, the following partial objectives were defined:

- Review the state of the art on available m-Health technologies, services, and applications and on existing cooperation strategies and mechanisms on e-Health, wireless networks, ad-hoc networks, and delay-tolerant networks. A comprehensive and meaningful study of the e-Health technologies and mobile health (m-Health) services and applications should be performed to understand in detail their characteristics, limitations, and challenges. Moreover, a detailed study on cooperation strategies and mechanisms should be performed in order to identify open issues and gathered contributions from the already existing cooperative approaches.
- Design and construction of a new cooperation strategy for m-Health services and applications. Based on the previous studies and the identified problems and open issues a novel cooperative-based strategy is proposed for m-Health services and applications. This proposal will focuses on enabling m-Health applications that are being used on mobile devices without Internet connectivity to access Web services requests through cooperation with neighbor mobile devices .
- Performance assessment of the cooperation solution for m-Health applications over a real testbed involving real users with an m-Health application on their mobile devices.
- Design and construction of a data encryption solution for mobile health applications under a cooperation environment. A cryptography proposal for the m-Health cooperation strategy that guaranties the health data/information confidentiality, integrity, and authenticity during cooperative processes.
- Performance assessment of the data encryption solution for mobile health applications under a cooperation environment involving real users with an m-Health application on their mobile devices.
- Proposal and performance evaluation of a generalized and interoperable incentive-based cooperative application framework for mobile applications. This proposal consists in a cooperative application framework for mobile applications, based on the cooperative strategy for m-Health services and applications. Its performance evaluation and demonstrations will be preformed though a real scenario using real mobile applications.

1.3 Research hypothesis

This thesis proposes a novel cooperation strategy for m-Health applications focusing on forwarding and retrieving data to/from nodes that have no direct connection to a m-Health application. In this sense, devices without Internet connection can use m-Health applications without problems. This cooperation approach presents a reputation-based strategy where a

Web service manages the access control and the cooperation among nodes along with their reputation. This work was the result of the following research hypothesis:

The evolution of e-Health technologies and mobile health (m-Health) services and applications is carefully studied. Through this study typical m-Health network architectures and their limitations and challenges are identified. Moreover, a detailed study on cooperative schemes applied to similar m-Health network scenarios is performed. This study presents several contributions that are used to the novel cooperation proposal for m-Health services and applications.

Based on the identified m-Health services and applications challenges and limitations and with the gathered contributions from the already existing cooperative approaches, a novel cooperative strategy for m-Health applications is proposed. This proposal is a cooperative reputation based approach that punishes un-cooperative behaviors focusing on forwarding and retrieving data to/from neighbor devices that have no direct connection to a m-Health application. This cooperation strategy assents on two main mechanisms: i) the direct observation of neighbor nodes, to detect un-cooperative behaviors; ii) a cooperative Web service that manages the access control and the cooperation among nodes along with their reputation. To demonstrate the advantages of this proposal and its performance evaluation a real scenario is used with a real m-Health application, called SapoFit [8].

The confidentiality of the user Health sensitive and personal information was also taken under consideration. A cryptography solution for m-Health applications under cooperative environments is constructed especially for m-Health applications that uses the proposed cooperative strategy. This proposal presents an encryption strategy that guaranties the confidentiality, integrity, and authenticity of health data/information during cooperative processes. To demonstrate de feasibility and performance evaluation a real scenario is used with the SapoFit m-Health application. Furthermore, a field survey was conducted with the application users, evaluating the experience satisfaction.

A generalized cooperative application framework for mobile applications, based on the cooperative strategy for m-Health services and applications is also presented. This proposal main goal is that developers can easily incorporate in their applications the early proposed cooperative strategy so that any user could easily use. The evaluation of this proposal was preformed through a real network scenario with two different mobile applications. The results obtained are used to demonstrate the feasibility and the advantages of using the proposed cooperative application framework.

The challenge in using real scenarios and real mobile applications in performance evaluations and demonstrations is that we must have in consideration that results may variate in unpredictable ways. This is in fact an advantage of real scenarios where mobile devices constrains, such as, mobility, loss of Bluetooth connection , distance variation, and different devices hardware specifications may cause unpredictable but more accurate results.

1.4 Main Contributions

This section briefly describes the main scientific contributions resulting from the research work presented in this thesis.

The first contribution of this thesis is the detailed survey of the state of the art on the evolution of e-Health technologies and mobile health (m-Health) services and applications. This study analyses the different scenarios and network architectures that sustain m-Health applications and services. Furthermore, it presents its typical network and devices constraints and open issues. This study is described in Chapter 2, which consists of a article submitted for publication in an international journal [9].

The second contribution is a comprehensive review of the state of the art on the available cooperation strategies on e-Health, wireless networks, ad-hoc networks, and delay-tolerant networks. This study identifies the main cooperative schemes and strategies applied to similar m-Health network scenarios. Furthermore, it points and describes several open issues and gathers important contributions for the upcoming cooperation proposal for m-Health services and applications. This contribution is presented in Chapter 3 as a article submitted for publication in an international journal [10]

The third contribution of this thesis includes the proposal and performance evaluation of the novel cooperation strategy for m-Health services and applications. It presents a cooperative reputation-based scheme that punishes un-cooperative behaviors promoting unselfish behaviors through reputation incentives. This cooperative strategy makes use of direct neighbor observation to detect and record un-cooperative behaviors and a a cooperative Web service that manages the access control and the cooperation among nodes along with their reputation. This proposal solved the early identified problem and it was evaluated through a real network scenario involving 19 users with a real m-Health application that requires constant network connection, called SapoFit [8]. This proposal is presented and described, in detail, in chapter 4 as an article published in IEEE Jornal of Selected Areas and Communications [11].

The next contribution of this thesis is the proposal of a cryptography solution for m-Health applications under cooperative environments, called, DE4MHA (Data Encryption Solution for M-Health Applications). This proposal presents an encryption strategy that guaranties the confidentiality, integrity, and authenticity of health data/information during cooperative processes. This solution uses both synchronous and asynchronous encryption algorithms and was especially design and implemented for the cooperative strategy for m-Health applications and services. This proposal is available in an article in press in Springer, Journal of Electronic Commerce Research [12]. This article composes the chapter 5 of this thesis.

The fifth contribution is the performance evaluation study and survey of the DE4MHA. This study was performed through a real network scenario involving 35 real users with the SapoFit application. The evaluation results prove that DE4MHA does not have negative impact on the performance of the cooperation strategy. Furthermore, a survey with the 35 users was conducted and concludes that users are more confidant in using m-Health applications knowing that their data/information is protected. This study is presented in chapter 6 and in a article published on Journal of Medical Internet Research [13].

The sixth and final contribution of this thesis is the proposal and performance evaluation of a generalized and interoperable incentive-based cooperative application framework for mobile applications, called MobiCoop. This proposal follows an incentive based approach for m-Health applications and it intends to be an application framework that developers can easily incorporate in their applications and users can easily use. The evaluation of this proposal was preformed through a real network scenario involving 11 users and two different mobile applications: an instant messaging application and a mail send/receiver application. This contribution is presented and described in chapter 7 as an article submitted for publication in an international journal [14].

1.5 Thesis Organization

This thesis is organized in eight chapters. Apart de current chapter, the Introduction, and the chapter with the conclusions and future work (Chapter 8), all the other chapters are composed by an article published in or submitted to an international journal. The rest of this document is organized as follows.

Chapter one describes the focus and the scope of this thesis as well as the problem definition and identification of the objectives to be accomplished. This chapter also includes the research hypothesis adopted in this thesis and summarizes its main contributions. Finally the organization and structure of the thesis is presented.

The second chapter presents a survey on the state of the art on m-Health technologies, services, and applications, entitled: *Mobile Health: The Last Frontier on Healthcare Services and Applications*. This study describes the evolution of e-Health technologies and mobile health (m-Health) services and applications and analyses the existing m-Health scenarios and network architectures.

Chapter three consist of an article that surveys the existing cooperation strategies and mechanisms on e-Health, wireless networks, ad-Hoc networks, and Delay Tolerant Networks, entitled: *Cooperative Strategies for Challenged Networks and Applications: A Survey*. This article identifies and gather contributions from the main cooperative schemes and strategies applied to similar m-Health network scenarios.

Chapter four presents the proposal for a novel cooperation strategy for m-Health services and applications, entitled: *A Novel Cooperation Strategy for Mobile Health Applications*. This chapter presents a cooperative reputation-based scheme that punishes un-cooperative behaviors promoting unselfish behaviors through reputation incentives. This reputation rating and fair access to requested services are controlled and managed by a cooperative Web service.

Chapter five consists of article that proposes a new cryptography strategy mobile health applications under cooperation environment, called DE4MHA. This article is entitled: *Towards a Cooperative Security System for Mobile-Health Applications*. Under cooperative environment, this proposal guaranties the confidentiality, integrity, and authenticity of health data/information.

Chapter six presents the performance evaluation of DE4MHA and a field survey of the proposed cryptography proposal, with real users. This article is entitled: *A Data Encryption Solution for Mobile Health Applications in Cooperation Environments: DE4MHA*.

Chapter seven describes the proposal and performance evaluation of a generalized and interoperable cooperative strategy, entitled: *MobiCoop: An incentive-based cooperation solution for mobile applications*. This strategy consists in a cooperative application framework, based on the cooperation strategy for m-Health applications. Its main goal is to be an framework for developers easily incorporate in their applications so that users can easily use.

Finally, chapter eight summarizes the main conclusions of the thesis drawn throughout the document and proposes several insights and suggestions for future work.

References

[1] B. L. Moullee and P. Ray, ”Issues in e-health cost impact assessment”, in *World Congress on Medical Physics and Biomedical Engineering*, vol. 25, no. 12. Munich, Germany: Springer, September 2009, pp. 223-226.

[2] S. Akter, J. D□Ambra, and P. Ray, ”User perceived service quality of mhealth services in developing countries,” in *European Conference on Information Systems*, Pretoria, Shouth Africa, June 2010, pp. 1-12.

[3] B. research, ”Global markets for telemedicine technologies,” 2012. [Online]. Available: http://www.bccresearch.com/market-research/healthcare/telemedicine-technologies-global-markets-hlc014e.html.

[4] P. fusion, ”150,000 medical professionals stay paperless with practice fusion,” June 2013. [Online]. Available: http://www.practicefusion.com/pages/pr/practice-fusion-celebrates-earth-day-2013.html.

[5] S. Akter and P. Ray, ”mhealth - an ultimate platform to serve the unserved.” *Yearb Med Inform*, pp. 94-100, 2010.

[6] S. Tachakra, X. Wang, R. S. Istepanian, and Y. Song, ”Mobile e-health: The unwired evolution of telemedicine,” *Telemedicine Journal and e-Health*, vol. 9, no. 3, pp. 247-257, 2003.

[7] P. Zuehlke, J. Li, A. Talaei-Khoei, and P.Ray, ”A functional specification for mobile ehealth (mhealth) systems,” in *11th International Conference on e-Health Networking, Applications and Services, Healthcom 2009.*, 2009, pp. 74-78.

[8] G. Kramer, I. Marić, and R. D. Yates, ”Cooperative communications,” *Found. Trends Netw.*, vol. 1, no. 3, pp. 271-425, Aug. 2006. [Online]. Available: http://dx.doi.org/10.1561/1300000004.

[9] L. Buttyán and J. P. Hubaux, ”Stimulating cooperation in self-organizing mobile ad hoc networks,” *ACM/Kluwer Mobile Networks and Applications (MONET)*, vol. 8, pp. 579-592, 2001.

[10] L. Bannon and J. Hughes, ”The context of cscw,” *Riso National Laboratory, Tech. Rep.*, 1993.

[11] V. Chan, P. Ray, and N. Parameswaran, ”Mobile e-health monitoring: an agent-based approach,” *IET Communications*, vol. 2, no. 2, pp. 223-230, 2008.

[12] Pradeep Ray, N. Parameswaran, V. Chan and W. Yu. ”Awareness modelling in collaborative mobile e-health,” *Journal of Telemedine and Telecare*, vol. 14, no. 7, pp. 381-5, 2008.

[13] B. M. C. Silva, I. M. Lopes, P. Ray, and J. Rodrigues, ”SapoFitness: A Mobile Health Application for Dietary Evaluation,” in *13th International Conference on e-Health Networking, Applications and Services (IEEE HealthCom 20011)*, Columbia, MO, USA, June 13-15, 2011.

[14] B. Silva, T. Machado, I. Lopes, J. Rodrigues, and L.Zhou, ”A novel cooperation strategy for mobile health applications,”*IEEE Journal of Selected Areas in Communications*, vol. 31, no. 9, pp. 28-36, September 2013.

[15] B. Silva, J. R. Rodrigues, F. C. Canelo, I. L. Lopes, and J. Lloret, ”Towards a cooperative security system for mobile-health applications,” *Journal of Electronic Commerce Research, Special Issue on Advances in Security and Privacy for Future Mobile Communications, Springer* (in press), 2014.

[16] B. Silva, J. R. Rodrigues, F. C. Canelo, I. L. Lopes, and L. Z. Zhou, ”A data encryption solution for mobile health applications in cooperation environments: DE4MHA,” *Journal of Medical Internet Research (JMIR)*, vol. 15, no. 4, pp. 1-11, April 2013.

[17] Bruno M.C. Silva, Joel J. P. C. Rodrigues, Isabel de la Torre Díez, and Miguel López-Coronado, ”Mobile Health: The Last Frontier on Healthcare Services and Applications,” *Paper submitted for publication in an international journal*, 2013.

[18] Bruno M.C. Silva, Joel J. P. C. Rodrigues, Neeraj Kumar and Guangjie Han, ”Cooperative Strategies for Challenged Networks and Applications: A Survey,” *Paper submitted for publication in an international journal*, 2014.

[19] Bruno M.C. Silva, Joel J. P. C. Rodrigues, Mario L. P. Junior and Guangjie Han, ”MobiCoop: An incentive-based cooperation solution for mobile applications,” *Paper submitted for publication in an international journal*, 2014.

Chapter 2

Mobile Health: The Last Frontier on Healthcare Services and Applications

This chapter consists of the following article:

Mobile Health: The Last Frontier on Healthcare Services and Applications

Bruno M. C. Silva, Joel J. P. C. Rodrigues, Isabel de la Torre Díez, and Miguel López-Coronado.

Article submitted for publication in an international journal.

Mobile Health: The Last Frontier on Healthcare Services and Applications

Bruno M.C. Silva[a], Joel J. P. C. Rodrigues[a,b], Isabel de la Torre Díez[c], Miguel López-Coronado[c]

[a]*Instituto de Telecomunicações, University of Beira Interior, Portugal, Rua Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal, Phone: +351 275 242 081; Fax: +351 275 319 899*
[b]*ITMO University, St. Petersburg, Russia, Kronverkskiy pr, 49; 197101, St.Petersburg, Russia, phone: +7 (812) 232-97-04, fax: +7 (812) 232-23-07*
[c]*Department of Signal Theory and Communications, University of Valladolid, Paseo de Belén, 15, 47011 - Valladolid, Spain Phone: +34 983423000 Ext. 3703; Fax: +34 983423667*

Abstract

Health telematics is a growing up issue that is becoming a major improvement on patient lives, especially in elderly, disabled, and chronically ill. In recent years, information and communication technologies improvements, along with mobile Internet, offering anywhere and anytime connectivity, play a key role on modern healthcare solutions. In this context, mobile health (m-Health) delivers healthcare services,overcoming geographical, temporal, and even organizational barriers. M-Health solutions address emerging problems on health services, including, the increasing number of chronic diseases related to lifestyle, high costs of existing national health services, the need to empower patients and families to self-care and handle their own healthcare, and the need to provide direct access to health services, regardless of time and place. Then, this paper presents a comprehensive review of the state of the art on m-Health services and applications. It surveys the most significant research work and presents a deep analysis of the top and novel m-Health services and applications proposed by industry. A discussion considering the European Union and United States

Email addresses: bruno.silva@it.ubi.pt (Bruno M.C. Silva), joeljr@ieee.org (Joel J. P. C. Rodrigues), isator@tel.uva.es (Isabel de la Torre Díez), miglop@tel.uva.es (Miguel López-Coronado)

approaches addressing the m-Health paradigm and directives already published is also considered. Open and challenging issues on emerging m-Health solutions are proposed for further works.

Keywords: e-Health; Health telematics; Healthcare; m-Health; Mobile Health; Telemedicine

1. Introduction

Last decade, health telematics, also known as Electronic Health (e-Health), have presented numerous and reliable health services. These services have offered patients that live in remote rural areas, that travel constantly or that are physically incapacitated, more accessible and affordable healthcare solutions [1, 2]. The introduction and interconnection of medical devices on information and communication technologies (ICTs), such as, blood pressure monitors, glucometers, scales, and other devices that interact both with patient and their medical doctors, are already a success among common citizens. Physicians can easily download medical records, lab results, medical images, and drug information to handheld devices like personal digital assistants (PDAs) and smartphones. Patients could be aware of their diagnostic, disease control, and monitoring with comfortable mobile devices that accompany them everywhere. According to [3], from 2010 to 2016 the global telemedicine market is expected to grow up to nearly 27.3 billion dollars. A key factor that contributes to this market investment is the increased remote monitoring of patients. Basically, telemedicine is based on the use of medical information, also known as Electronic Health Records (EHRs)[4], exchanged via electronic communications improving the patients health status. In United States, the use of EHR technology is already widely adopted. It is estimated that 55% of medical professionals are using EHR platforms [5].

With the advent of mobile communications using smart mobile devices that support 3G and 4G mobile networks for data transport, mobile computing has been the main attraction of research and business communities. It offers nu-

merous opportunities to create efficient mobile health (m-Health) solutions. M-Health is the new edge on healthcare innovation. It proposes to deliver healthcare anytime and anywhere, surpassing geographical, temporal, and even organizational barriers [6, 7]. M-Health systems and its corresponding mobility functionalities have a strong impact on typical healthcare monitoring and alerting systems, clinical and administrative data collection, record maintenance, healthcare delivery programs, medical information awareness, detection and prevention systems, drug-counterfeiting, and theft [8]. Typical m-Health services architectures (presented in Figure 1) use the Internet and Web services to provide an authentic pervasive interaction among doctors and patients. A physician or a patient can easily access the same medical record anytime and anywhere through his/her personal computer, tablet, or smartphone. The patient can contact the physician in case of an emergency, or even, have access to medical registers or appointments regardless of time and place.

This paper presents a comprehensive review of the state of the art on m-Health services and applications. It surveys the most significant research work and presents a deep analysis of the top and novel m-Health services and applications available in mobile markets and healthcare industry.

The main contributions of this paper are the following:

- An extensive review of the state of the art on m-Health and related approaches;
- A study of the scientific developments/break-through on m-Health;
- An analysis of the top mobile health applications in the top mobile markets;
- A discussion about current and open issues on m-Health services and technologies.

The reminder of this paper is organized as follows. Section II elaborates on the current state of the art on e-Health systems and how health institutions and agents are embracing the information and communication technologies. Section

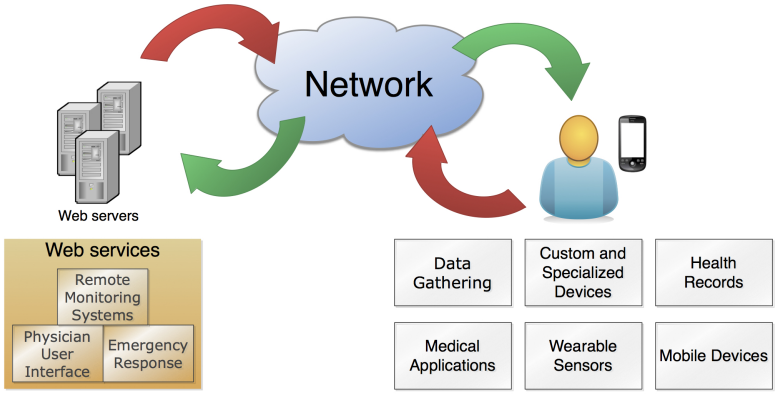


Figure 1: Illustration of a typical architecture of m-Health services.

III focuses on m-Health awareness and the use of m-Health services and applications. A discussion about current and open issues on m-Health technologies is presented in Section IV. Finally, the paper is concluded on Section V.

2. Healthcare and e-Health systems: The road so far

Health telematics had becoming a great topic in terms of medical informatics and healthcare. Currently, hospitals and health systems are relying on information and communication technology (ICT) as a mean for improving quality, safety, and productivity of health care services. E-Health connects medical informatics, public health, and business through associated technologies, such as the Internet. However, it has been suffered from a slow start due to the low priority given by Hospitals and health systems to ICT in the 90s. Nonetheless, the need to produce a standard for hospital information systems was crucial. In 1987, the International Health Level Seven (HL7) organization [9] was founded and, in 1994, it was accredited by the American National Standards Institute (ANSI). Its name is a reference to the seventh layer of the ISO Open Systems Interconnection (OSI) Reference model also known as the application layer.

Currently, the HL7 is adopted by ISO as a reference in terms of international standardization, publishing together several frameworks and related standards for exchange, integration, sharing, and retrieval of electronic health records (EHRs). In the beginning of the new century, between 1999 and 2002, e-Health services have finally awakened and rapidly increased. This growing was analogue to the rapid evolution of ICT infrastructures and access to patient data. The Web 2.0 concept and the emerging Web 3.0 have offered to healthcare professionals conditions that never had been given before [10]. They also enabled a key element in healthcare systems, the emergence of EHRs or Personal Health Records (PHRs). Usually, healthcare providers keep and handle patient health records. However, it is becoming more common that patients also request access to those data. Medical records (or health records) allow medical doctors to easily access a patient information without needing to ask them in person. E-health systems are typically sustained on EHRs [11]. An EHR-system is basically a repository of information regarding the health records of patient/consumer in a computer form [12]. The deployment of a public EHR-system can offer several advantages to a public healthcare system, for example, lower and more efficient management costs, more efficient management of high-volume patient data, and centralized medical patient records [13].

Public and private entities are embracing e-Health and the research community is continuously contributing with new better ICT solutions that can be applied to health services. Multimedia services, tools, and technologies offer new healthcare services. Healthcare professionals can now remotely monitoring patients more efficiently and with more affordable costs than never before.

A large number of telemedicine and e-Health systems are being widely and successfully produced delivering health care through different communication technologies. The World Health Organization (WHO) has identified a compendium of emerging health technologies, under development and already commercialized [14]. This report presents several health technologies that present the potential for being low-recourse solutions for unmet medical needs. Among these technologies, e-Health solutions are the dominant. Currently, the com-

mercialized and most relevant e-Health technologies include a fetal heart rate monitor, portable hemoglobin meter, self-powered pulse oximeter, medical data communication system, mobile technology to connect patients to remote doctors [15], and treatment response software application [14]. Considering the technologies under development, the authors identified, to the best of their knowledge, the most relevant ones.

Fetal heart rate monitor using a mobile phone [16]: A mobile application that analyses the fetal heartbeat and calculates the heart rate using a beat-to-beat accuracy algorithm. These data are sent and stored in a server, then a midwife can examine it through a Web browser.

Mobile health record system for pediatric HIV [14]: A Web based EHR system that uses an embedded comprehensive pediatric HIV knowledge base and clinical decision system. This system allows physicians to integrate clinical information to manage pediatric HIV at the point of care.

Mobile phone image transmission for diagnosis [17]: A mobile phone with camera functions as image transmission unit. This system allows a basic connection to more specialized health care facilities in remote areas in the field of medical image diagnostics. The images are sent as Multimedia Message system (MMS) via mobile phones. Mobile phone pulse oximeter [14]: A mobile phone combined with a pulse oximeter sensor analyses and displays the information received from a sensor placed on a finger. It can aid physicians to detecte clinical events and taking decisions. Portable telemedicine unit [18]: A portable telemedicine unit that combines a mobile telemedicine system with a computer server. Both can communicate among them via GSM, CDMA, Internet, and satellite. This device addresses healthcare services in rural or remote regions and can be used for several health services, such as recording and reporting, and tele-consultation.

Hossain et al. [19] present recent advancements and developments of multimedia services and technologies for e-Health, such as, health monitoring, ubiquitous solutions for healthcare, serious games for health, real-time access of medical services, medical assisted systems for elderly people, and medical data over

wireless body sensor networks (WBSN). For these topics the authors present the following studies and proposals. Two proposals considering the serious game paradigm are presented. The first, introduced by Chan et al. [20], is based on a serious game approach for learning ultrasound-guided needle placement skills. The ultrasound-guided needle placement techniques are often used for several radiological intervention procedures. The second serious game proposal, by Maamar et al. [21], discusses collaborative exergaming applications for child obesity epidemic. The authors present a new paradigm for mobile collaborative exergaming applications that are based on peer-to-peer (P2P) architectures. The main goal is that children can exercise as a team through the mobile application with more quality of 3-D streaming with low delays. Concerning bioelectric signal technology (e.g., electrocardiogram - ECG and electromyogram - EMG), Yang et al. [22] presents a hybrid solution of a biopatch for e-Health using low-power system-on-chip (SoC) sensor and paper-based inkjet printing technology. Regarding patient monitoring and localization technologies, an RFID-based system is presented by Shirehjini et al. [23]. This system aims to track the location of a mobile hospital equipment, minimizing positioning and orientation errors. Therefore, it improves the quality of care and reducing costs. Cognitive stimulation therapy through digital TV was also considered. A design, implementation, and validation of a cognitive stimulation system over interactive TV is presented in [24]. This service improves and provides better healthcare services to patients with cognitive disorders, such as, Alzheimer or mild cognitive impairment. Regarding the elderly people that constantly need support end health services, Hossain and Ahmed proposed a support system for caregivers in a assisted living environment [25]. This context-aware system, called ViCare, interprets the elderly activities based on data captured by several sensors placed in their environment and decides what health or other services should be provided. Zhang et al. [26] proposed a solution for WBSNs to preserve integrity, safety, and privacy of medical data over the network. The authors present a key agreement scheme in which neighbor nodes of wireless body sensor networks (WBSNs) share a common key generated by ECG signals. Efficient management of med-

ical multimedia data from various heterogeneous sources is addressed in [27]. Furthermore, a prototype for knowledge editing service (KES) is presented in [28]. This solution enables clinicians through an ICT platform to insert new knowledge for multisource data management in remote health monitoring. In [29], a cross layer design for a Wi-Max in order to deliver ultrasound video data through mobile devices is presented. Finally, a virtual reality-based surgical simulator for the mandibular angle reduction on a CUD-based platform is presented in [30]. This simulator provides stimulus and sensations for surgeons controlling instruments under different surgical situations and environments. These recent advances on e-Health services provide and improve patient care. However, the use of ICT solutions in healthcare services creates new potential health hazards [31].

A long road is still a head in many countries that continue adopting typical and old healthcare models based on the early 20th century. Nevertheless, the proportion of hospital income that is invested in ICT has doubled in recent years. Since the 1980s, investments in healthcare technologies and its growth have been a key factor, among others, for increasing healthcare spending among countries [32]. Currently, this spending growth is declining and technology is becoming an important factor to decrease healthcare costs. However, a new paradigm rises. Both patients and healthcare professionals are everyday embracing mobile technologies and mobile healthcare services. These services are having a great impact on healthcare industry and truly revolutionizing the healthcare delivery [33].

3. M-Health: The Healthcare Revolution

Laxminarayan and Istepanian [34] defined mobile health for the first time in the year 2000 as unwired e-med. In 2003, the term m-Health was defined as emerging mobile communications and network technologies for healthcare systems [35]. In 2006, Laxminarayan et al. present a comprehensive study about the impact of mobility on the existing e-Health commercial telemedical

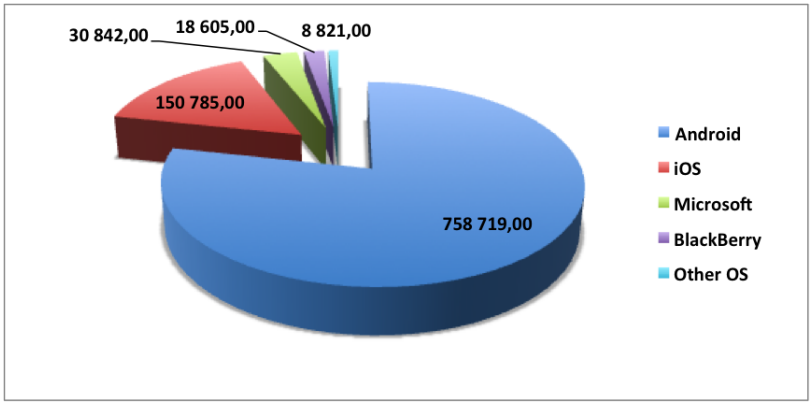


Figure 2: Worldwide smartphone sales to end users by operating systems in 2013 (Source: Gartner [39], 2013).

systems. Furthermore, it served as a basis for future m-Health technologies and services [36].

3.1. Mobile Health Awareness

In January 9, 2007, Steve Jobs, the CEO of Apple Inc. [37], presented to the world the iPhone 2G and its operating system (OS), the iOS [38]. This event triggered a rapidly evolution of smartphones and applications and also the emergence of new mobile platforms. Figure 2 presents the worldwide smartphone sales to end-users by operating systems in 2013.

Clearly, Google Android and Apple iOS dominate the OS market. The quality of both operating systems is unquestionable and both companies success in the mobile applications market is sustained by their online application markets (the Apps store). These online markets are open to developers allowing them to develop all kind off applications to sell or offer them for free. These markets open new and potential areas of research and development, such as, m-Health applications. At the end of 2010, more than 200 million m-Health applications were downloaded and about 70% of worldwide citizens were interested to access to, at least, one m-Health application. Overall, smartphone Web browsers

were improved becoming easier to find free applications and information [40]. It is predicted that, in 2017, more than 1.7 billion people will have downloaded health Apps with m-Health market revenue of a total of 26 billion dollars [41]. The market of mobile health applications is directed toward patients, clinicians, and healthcare professionals. These applications are mainly suited for diseases management, self-monitoring, and drug control as well as other clinical and educational applications. This raises several important and complex questions about these medical applications, such as, security, reliability, efficiency, and quality of service. Then, the following question should be raised: can they really perform a complete, secure, reliable, and efficient diagnosis? There are concerns related with this issue because several m-Health applications states claims, such as, this app will lower your blood pressure" or this app will help you to lose weight". Are these claims trustworthy? To protect users, the U.S. Food and Drug Administration (FDA), from the Department of Health & Human Services [42] enforces regulations on medical device approval and clearance. Devices manufacture must first register and notify FDA about their intent to market a medical device. This is known as 510(k) clearance and allows the FDA to determine if the device is valid and if it is equivalent to a device already placed in the market. The next step is the premarket approval (PMA). The PMA is the most rigorous approval of a request submitted to the FDA to market. This approval is based on the valid scientific evidence that assures that the proposed device is safe and effective for its intended use. FDA regulation also allows the submission of a Humanitarian Use Exception (HDE) approval. It applies to Humanitarian Use Devices (HUDs). HUDs are intended to care patients by treating or diagnosing a disease that affects less than 4,000 people in the U.S., per year. The HDE approval is very similar to the PMA, except the effectiveness requirements [42]. FDA also defines in the section 201(h) the term device as an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is [either] intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease,

in man or other animals [or] intended to affect the structure or any function of the body of man... The FDA regulations on devices are very clear. Analogously, the European Commission (EC) Medical Devices Directive (MDD) covers the regulatory requirements of the European Union for Medical Devices [43]. The MDD clears and places medical devices into one of four classes (I, IIa, IIb and III). These classes concern the device increasing risk to the patient according to their characteristics, functions, and intended purposes. The MDD includes 23 articles, 12 annexes, 18 classification rules, and it is considerably more complex to read and understand than the FDA regulation. For example, in 2010, an Ericsson m-Health framework [44] was certified in accordance to a Medical Device of Class IIa. Although several medical devices have already been certified, both FDA and EC regulations on m-Health software is yet to be well defined. Another important question that must be approved is the definition of medical device. A device plus a health-related application results in a medical device? If yes, it seems that smartphones can be considered medical devices because physicians already use them for numerous health purposes. Can they be classified as medical devices? To simplify the answer and the classification process, FDA recently proposes to amend its regulations governing classification and reclassification of medical devices to conform to provisions in the FDA Safety and Innovation Act (FDASIA) [45].

3.2. Mobile Health Applications and Services

The study and development of M-Health services and applications have been an important point of attention by the research community. Several research topics related to health have gathered important findings and contributions from m-Health, such as, cardiology [13], [46, 47, 48], diabetes [49, 50, 51], obesity [52, 53, 54], smoking cessation [55, 56], and elderly care and chronic diseases [57, 58]. These different medical specialties make use of m-Health essentially for monitoring, prevention, and detection of diseases, and in more advanced services present basic diagnosis. Besides all medical applications, m-Health services are even becoming popular in developing countries [59, 60] where healthcare facili-

ties are frequently remote and inaccessible. Mobile applications for healthcare systems are rapidly growing and evolving. Research interest in this topic is expanding every day, as well as the diversification of the impact areas. Fiordelli et al. [61] present a comprehensive view of the impact of mobile phones on health, in the last decade. The authors conducted a literature review of 117 articles published between 2002 and 2012, in 77 different journals. The results shown that between 2007 and 2008, the number of research articles almost doubled, exponentially growing every year. According to [62], only in the U.S. Apple iTunes store, there are available over 40.000 healthcare apps. Furthermore, this study presents the top healthcare apps categorized by therapy area and demographically: prevention/healthy lifestyles; finding a healthcare professional/facility; diagnosis/education; filling prescription; compliance; diabetes; mental health & behavioral disorders; musculoskeletal system and connective tissue; oncology; nervous system; womens health; childrens health. The IMS Health Appscore [62] was used to define which are the best applications based on functionality, patient reviews, and their potential to lower the cost of care services. The top m-Health applications in each therapy areas are presented in Table 1.

Table 1: Top m-Health applications by therapy area in 2013.

M-Health Applications	**Area**	**Description**
Calorie Counter and Diet Tracker [63]	Prevention/ Healthy Lifestyles	Diet application for calories counting, food tracking, exercise, and weight goals. Furthermore, it explores social aspects including links to friends as a motivation feature.
Calorie Counter PRO [64]	Prevention/ Healthy Lifestyles	Diet application for calorie counting, food tracking, and exercise using weight goals as a motivation aspect.

Continued on next page

Table 1 – *Top m-Health applications by therapy area in 2013.*

M-Health Applications	**Area**	**Description**
Chest Trainer [65]	Prevention/ Healthy Lifestyles	Weight training and fitness application that intents and claims to replace a personal trainer.
Healow [66]	Finding a healthcare professional/ facility	An application that allows patients communicating with their physicians office and also have access up-to-date health records. Furthermore, it also includes visit summaries and appointment reminders.
Vitals-Your top 10 doctors [67]	Finding a healthcare professional/ facility	This application provides a lists of local doctors rated by previous patients that also use this App. The search can be performed through symptom, condition, or medical specialty.
ZocDoc - Doctor Appointments Online! [68]	Finding a healthcare professional/ facility	An application that uses zip code searches to find and book doctors appointments.
HealthTap - free doctor answers to medical and health questions [69]	Diagnosis/ Education	An application that contains health answers and healthy tips on any symptom, condition, medication, health concern, or even wellness topics from 47,000 U.S. medical doctors.

Continued on next page

Table 1 – *Top m-Health applications by therapy area in 2013.*

M-Health Applications	**Area**	**Description**
iTriage [70]	Diagnosis/ Education	An application that contains information of several medical symptoms, diseases, conditions, procedures, medications, and drugs.
WebMD for iPad [71]	Diagnosis/ Education	An application that contains information of several medical symptoms, diseases, conditions, procedures, medications, and drugs. It includes WebMDs Symptom Checker.
GoodRx [72]	Filling Prescription	This application compares and provides prices for prescription drugs. Furthermore, it also provides coupons and savings tips for more than 6,000 drugs in several pharmacies in the U.S.
MyRefill Rx [73]	Filling Prescription	This application allows to order medications and get them delivered to a defined location. Moreover, it includes also medication and appointment reminders.
Walgreens [74]	Filling Prescription	An application that features medication prescriptions refill by Scan function, points for refills, pill reminders, transfer prescription feature and health references encyclopedia.
Dosecast [75]	Compliance	A medication reminder featuring a large drug database and the ability to support multiple users.

Continued on next page

Table 1 – *Top m-Health applications by therapy area in 2013.*

M-Health Applications	**Area**	**Description**
Pill Monitor Free Medication Reminders and Logs [76]	Compliance	A prescription reminder that features prescription alarms, reminder scheduling, setup reminders, and medication intake tracking.
RxmindMe Prescription / Medicine Reminder and Pill Tracker [77]	Compliance	A prescription reminder that features prescription alarms, reminder scheduling, setup reminders, and medication intake tracking.
Daily Carb - Carbohydrate, Glucose, Medication, Blood Pressure and Exercise Tracker [78]	Diabetes	An application that tracks daily nutrition intake of food, carbs, fiber, fat, tracks quantity of water intake, readings of glucose, HbA1c, blood pressure, heart rate, weight, exercise, medications, and insulin.

Continued on next page

Table 1 – *Top m-Health applications by therapy area in 2013.*

M-Health Applications	**Area**	**Description**
Glucose Buddy - Diabetes Logbook Manager w/syncing, Blood Pressure, Weight Tracking [79]	Diabetes	This application allows users to manually input glucose numbers, carbohydrate consumption, insulin dosages, and among other activities.
GoMeals [80]	Diabetes	This application is designed to aid the user in healthy lifestyle choices featuring food, activity, and glucose tracker.
ADHD Angel [81]	Mental health & behavioral disorders	An application that features reminders for medication intake, an updated health reports for physician visits, and advice on the 8 main ADHD 'Tipping Points'.
Live OCD Free [82]	Mental health & behavioral disorders	This application claims to reduce obsessive-compulsive disorder (OCD) symptoms by 34% in 8 weeks. It features video tutorials and extensive user guide.
T2 Mood Tracker [83]	Mental health & behavioral disorders	This application uses six pre-loaded mood scales (anxiety, stress, depression, brain injury, post-traumatic stress, general wellbeing) or custom scales to monitor and track a user mood.

Continued on next page

Table 1 – *Top m-Health applications by therapy area in 2013.*

M-Health Applications	**Area**	**Description**
Office-Fit [84]	Musculoskeletal system and connective tissue	An application that contains and offers several exercises against work-related pains and stress.
WebMD Pain Coach [85]	Musculoskeletal system and connective tissue	This application provides a complete approach to balancing lifestyle with chronic pain conditions, such as, back pain, neck pain, nerve pain, fibromyalgia, migraine, osteoarthritis, and rheumatoid arthritis.
Zimmer Arthritis 411 [86]	Musculoskeletal system and connective tissue	An application for people who suffer from osteoarthritis. It is an education tool that can be used at home to learn more about arthritis pain and treatment options.
Dr K's Breast Checker [87]	Oncology	An application designed to aid women keep track of change in breasts. Furthermore, it provides education information and reminders.
PCR Tracker [88]	Oncology	An application for Chronic myeloid leukemia (CML) patients that includes lab tests results tracking, treatment reminders, understand treatment milestones, and also features educational tools and videos.

Continued on next page

Table 1 – *Top m-Health applications by therapy area in 2013.*

M-Health Applications	**Area**	**Description**
SkinKeeper [89]	Oncology	This application allows users to monitor moles, capture important personal, and family skin cancer risk factors. Moreover, it allows a patient to share this information with their doctor.
Noteness (Multiple Sclerosis) [90]	Nervous system	A multiple sclerosis diary application that allows a user to track and monitor injections and symptoms.
Parkinson Diary [91]	Nervous system	An application for Parkinson patients and caregivers to record, reports, and reviews Parkinson symptoms.
Young Epilepsy [92]	Nervous system	An application for young people with epilepsy and also for their parents or carers. Contains a education portal, video, and a diary.
Ovulation Calendar Ladytimer Free [93]	Womens Health	An application to track and predict menstrual cycle days. It aids women to become pregnant or avoid pregnancy.
Period Diary (Period, Fertile & Ovulation Tracker) [94]	Womens Health	An application that monitors menstrual symptoms, body weight, temperature through a fully animated period, and ovulation tracker.

Continued on next page

Table 1 – *Top m-Health applications by therapy area in 2013.*

M-Health Applications	**Area**	**Description**
Pregnancy Tracker [95]	Womens Health	An application to aid women through pregnancy day-by-day. The women has access to personalized content and the latest parenting news and health information.
Baby Connect (Activity Logger) [96]	Childrens Health	A baby tracking application featuring graphical reports and trending charts, weekly averages, medicine, vaccine and growth tracking, timers, notifications, reminder alarms.
Baby Food Pee Poo Free [97]	Childrens Health	An application that features a baby logger/tracker, reminders (feeding, diaper change, and sleep), and a white noise recorder/player.
Total Baby [98]	Childrens Health	A complete baby tracking application that covers: Diapers, Nursing, Pumping, Bottles, Solids, Sleeping, Bath, and Other (timing and tracking), Diary, Milestones, Doctor Visits, Growth, Vaccines, and Allergies (logging).

4. Discussion and Open Issues

The advent of mobile technology and applications are transforming the way health information is accessed, delivered, and managed. Cloud computing is providing numerous benefits to healthcare industry distributing and accelerating deliverance of healthcare services. Healthcare industry's adherence to cloud computing is inevitable and it is already happening [99]. The fourth-generation

(4G) mobile communications system is the main responsible for enabling these advents. 4G technologies and networks empower new services and consumer usage models, reflected in corresponding m-Health services and applications [100]. These authors believe the future of this topic will pass by the transposition of services and applications based on the individual to services that involved groups and social networks. Nowadays, social networks are playing an important role on the people daily lives. M-Health solutions may enable social networking to promote healthy behaviors and awareness among patients involved in network groups and communities. Based on the above review of the state-of-the-art and market research on m-Health services and applications, mobile and ubiquitous paradigms raises important open issues. Cooperation between m-Health applications is a challenge that needs a more comprehensive study. Either patients or physicians that use the same or different services should cooperate in order to accomplish common objectives. Cooperation methods also aim a better efficiency and performance of mobile devices (for example, device battery, storage, and network). In an m-Health typical system architecture, sensitive health data is exchanged through wireless networks. Then, data privacy and security is a major issue on information management for public health needs. A study related with the impact of mobile communication technologies for health on patients and health professionals must be performed. This study should include questionnaires to collect data related to the influence of m-Health applications on end-users/patients daily routine. A study on how m-Health applications can reduce financial costs to end-users/patients and how the healthcare public and private systems are affected by m-Health.

5. Conclusion

M-Health services and applications propose healthcare delivery anytime and anywhere overcoming geographical, temporal, and even organizational barriers with low and affordable costs. This study reviewed the state-of-the-art on m-Health services and technologies. Furthermore, it presented the m-Health

technologies growth, its regulation, and legislation issues. Based on this compressive review, the authors believe that m-Health services and applications has already a very important and determinant role in restructuring the old healthcare services and systems that still based on the physical relationship between patient and physician. Moreover, m-Health applications have a strong impact on all healthcare services, such as, hospitals, care centers, and emergency attendance. Therefore, it aims to be a major improvement on patient lives, especially in elderly, disabled, and chronically ills.

Acknowledgments

This work has been partially supported by *Instituto de Telecomunicações*, Next Generation Networks and Applications Group (NetGNA), Covilhã Delegation, by Government of Russian Federation, Grant 074-U01, by National Funding from the FCT - *Fundação para a Ciência e a Tecnologia* through the Pest-OE/EEI/LA0008/2013 Project, and by the AAL4ALL (Ambient Assisted Living for All), project co-financed by the European Community Fund (FEDER) through COMPETE - *Programa Operacional Factores de Competitividade*.

References

[1] B. L. Moullee, P. Ray, Issues in e-health cost impact assessment, in: World Congress on Medical Physics and Biomedical Engineering, Vol. 25, Springer, Munich, Germany, 2009, pp. 223–226.

[2] S. Akter, J. D'Ambra, P. Ray, User perceived service quality of mhealth services in developing countries, in: European Conference on Information Systems, Pretoria, Shouth Africa, 2010, pp. 1–12.

[3] B. research, Global markets for telemedicine technologies (2012) [cited Online].
URL `http://www.bccresearch.com/market-research/healthcare/telemedicine-technologies-global-markets-hlc014e.html`

[4] M. Eichelberg, T. Aden, J. Riesmeier, A. Dogac, G. Laleci, Electronic health record standards - a brief overview, in: Information Communications Technology, 2006. ICICT '06. ITI 4th International Conference on, 2006, pp. 1–1. doi:10.1109/ITICT.2006.358222.

[5] N. S. Fleming, E. R. Becker, S. D. Culler, D. Cheng, R. McCorkle, B. d. Graca, D. J. Ballard, The Impact of Electronic Health Records on Workflow and Financial Measures in Primary Care Practices, Health Services Research 49 (1pt2) (2014) 405–420. doi:10.1111/1475-6773.12133.

[6] S. Akter, P. Ray, mhealth - an ultimate platform to serve the unserved., Yearb Med Inform (2010) 94–100.

[7] S. Tachakra, X. Wang, R. S. Istepanian, Y. Song, Mobile e-health: The unwired evolution of telemedicine, Telemedicine Journal and e-Health 9 (3) (2003) 247–257.

[8] P. Zuehlke, J. Li, A. Talaei-Khoei, P. Ray, A functional specification for mobile ehealth (mhealth) systems, in: e-Health Networking, Applications and Services, 2009. Healthcom 2009. 11th International Conference on, 2009, pp. 74–78.

[9] Health Level Seven International, Health Level Seven International (2013) [cited Online].
URL http://www.hl7.org

[10] S. Subramoniam, A. Saifullah Sadi, Healthcare 2.0, IT Professional 12 (6) (2010) 46–51. doi:10.1109/MITP.2010.66.

[11] J. Li, L. P. W. Land, P. Ray, S. Chattopadhyaya, E-health readiness framework from electronic health records perspective., International Journal of Internet and Enterprise Management (4) 326–348.
URL http://dblp.uni-trier.de/db/journals/ijiem/ijiem6.html#LiLRC10

[12] M. Eichelberg, T. Aden, J. Riesmeier, A. Dogac, G. B. Laleci, A survey and analysis of electronic healthcare record standards, ACM Comput. Surv. 37 (4) (2005) 277–315. doi:10.1145/1118890.1118891.
URL http://doi.acm.org/10.1145/1118890.1118891

[13] B. Martínez-Pérez, I. de la Torre-Díez, M. López-Coronado, J. Herreros-González, Mobile apps in cardiology: Review, JMIR Mhealth Uhealth 1 (2) (2013) e15. doi:10.2196/mhealth.2737.
URL http://mhealth.jmir.org/2013/2/e15/

[14] WHO, Compendium of new and emerging technologies (2011) [cited Online].
URL http://www.who.int/medical_devices/innovation/new_emerging_techs/en/

[15] ClickMedix, Clickmedix (2013) [cited online].
URL http://clickmedix.com

[16] C. S. Lee, M. Masek, C. P. Lam, K. T. Tan, Advances in fetal heart rate monitoring using smart phones, in: Proceedings of the 9th international conference on Communications and information technologies, ISCIT'09, IEEE Press, Piscataway, NJ, USA, 2009, pp. 735–740.
URL http://dl.acm.org/citation.cfm?id=1789954.1790134

[17] L. Bellina, E. Missoni, Mobile cell-phones (m-phones) in telemicroscopy: increasing connectivity of isolated laboratories, Diagnostic Pathology 4 (1) (2009) 19. doi:10.1186/1746-1596-4-19.
URL http://dx.doi.org/10.1186/1746-1596-4-19

[18] E. Sutjiredjeki, S. Soegijoko, T. L. R. Mengko, S. Tjondronegoro, Development of mobile telemedicine system with multi communication links to reduce maternal mortality rate, in: Proceedings of the Sixth IASTED International Conference on Biomedical Engineering, BioMED '08, ACTA Press, Anaheim, CA, USA, 2008, pp. 402–407.
URL http://dl.acm.org/citation.cfm?id=1713360.1713444

[19] M. Shamim Hossain, S. Goebel, A. El Saddik, Guest editorialmultimedia services and technologies for e-health (must-eh), Information Technology in Biomedicine, IEEE Transactions on 16 (6) (2012) 1005–1006. doi:10.1109/TITB.2012.2225260.

[20] W.-Y. Chan, J. Qin, Y.-P. Chui, P.-A. Heng, A serious game for learning ultrasound-guided needle placement skills, Information Technology in Biomedicine, IEEE Transactions on 16 (6) (2012) 1032–1042. doi:10.1109/TITB.2012.2204406.

[21] H. R. Maamar, A. Boukerche, E. M. Petriu, 3-d streaming supplying partner protocols for mobile collaborative exergaming for health., IEEE Transactions on Information Technology in Biomedicine 16 (6) (2012) 1079–1095.
URL http://dblp.uni-trier.de/db/journals/titb/titb16.html#MaamarBP12

[22] G. Yang, L. Xie, M. Mäntysalo, J. Chen, H. Tenhunen, L.-R. Zheng, Bio-patch design and implementation based on a low-power system-on-chip and paper-based inkjet printing technology., IEEE Transactions on Information Technology in Biomedicine 16 (6) (2012) 1043–1050.
URL http://dblp.uni-trier.de/db/journals/titb/titb16.html#YangXMCTZ12

[23] A. A. N. Shirehjini, A. Yassine, S. Shirmohammadi, Equipment location in hospitals using rfid-based positioning system., IEEE Transactions on Information Technology in Biomedicine 16 (6) (2012) 1058–1069.
URL http://dblp.uni-trier.de/db/journals/titb/titb16.html#ShirehjiniYS12

[24] C. G. Vázquez, E. M. Martínez, M. Á. V. Duboy, A. G. Oliva, Distributed system for cognitive stimulation over interactive tv., IEEE Transactions on Information Technology in Biomedicine 16 (6) (2012) 1115–1121.

URL http://dblp.uni-trier.de/db/journals/titb/titb16.html#VazquezMDO12

[25] M. Hossain, D. Ahmed, Virtual caregiver: An ambient-aware elderly monitoring system, Information Technology in Biomedicine, IEEE Transactions on 16 (6) (2012) 1024–1031. doi:10.1109/TITB.2012.2203313.

[26] Z. Zhang, H. Wang, A. Vasilakos, H. Fang, Ecg-cryptography and authentication in body area networks, Information Technology in Biomedicine, IEEE Transactions on 16 (6) (2012) 1070–1078. doi:10.1109/TITB.2012.2206115.

[27] M. Masud, M. S. Hossain, A. Alamri, Data interoperability and multimedia content management in e-health systems., IEEE Transactions on Information Technology in Biomedicine 16 (6) (2012) 1015–1023.
URL http://dblp.uni-trier.de/db/journals/titb/titb16.html#MasudHA12

[28] S. Colantonio, M. Esposito, M. Martinelli, G. De Pietro, O. Salvetti, A knowledge editing service for multisource data management in remote health monitoring, Information Technology in Biomedicine, IEEE Transactions on 16 (6) (2012) 1096–1104. doi:10.1109/TITB.2012.2215622.

[29] C. Debono, B. Micallef, N. Philip, A. Alinejad, R. S. H. Istepanian, N. Amso, Cross-layer design for optimized region of interest of ultrasound video data over mobile wimax, Information Technology in Biomedicine, IEEE Transactions on 16 (6) (2012) 1007–1014. doi:10.1109/TITB.2012.2201164.

[30] Q. Wang, H. Chen, W. Wu, H.-Y. Jin, P.-A. Heng, Real-time mandibular angle reduction surgical simulation with haptic rendering, Information Technology in Biomedicine, IEEE Transactions on 16 (6) (2012) 1105–1114. doi:10.1109/TITB.2012.2218114.

[31] ECRI, Ecri institute 2013 top 10 health technology hazards, Tech. rep., ECRI (August 2013) [cited Online].
URL https://www.ecri.org/Documents/Secure/Health_Devices_Top_10_Hazards_2013.pdf

[32] A. Chandra, J. S. Skinner, Technology growth and expenditure growth in health care, Working Paper 16953, National Bureau of Economic Research (April 2011).
URL http://www.nber.org/papers/w16953

[33] C. Free, G. Phillips, L. Watson, L. Galli, L. Felix, P. Edwards, V. Patel, A. Haines, The Effectiveness of Mobile-Health Technologies to Improve Health Care Service Delivery Processes: A Systematic Review and Meta-Analysis, PLoS Med 10 (1) (2013) e1001363. doi:10.1371/journal.pmed.1001363.

[34] S. Laxminarayan, R. S. Istepanian, UNWIRED E-MED: the next generation of wireless and internet telemedicine systems., IEEE Trans Inf Technol Biomed 4 (3) (2000) 189–193.

[35] R. S. H. Istepanian, J. Lacal, Emerging mobile communication technologies for health: some imperative notes on m-health, in: Engineering in Medicine and Biology Society, 2003. Proceedings of the 25th Annual International Conference of the IEEE, Vol. 2, 2003, pp. 1414–1416 Vol.2.

[36] R. Istepanian, S. Laxminarayan, C. Pattichis, M-Health: Emerging Mobile Health Systems, Topics in Biomedical Engineering. International Book Series, Springer, 2006.

[37] Apple, Apple (2013) [cited Online].
URL http://www.apple.com

[38] A. iOS, Develop apps for ios (2013) [cited Online].
URL https://developer.apple.com/technologies/ios/

[39] Gartner, Gartner (2014) [cited Online].
URL http://www.gartner.com/newsroom/id/2665715

[40] Mobihealthnews, The fastest growing and most successful health & medical apps, Tech. rep., Mobihealthnews 2010 Report (2010).

[41] research2guidance, Global mobile health market report 2013-2017 (2013) [cited Online].
URL http://www.research2guidance.com/the-market-for-mhealth-app-services-will-reach-26-billion-by-2017/

[42] U.S. Food and Drug Administration (2013) [cited Online]. [link].
URL http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/DeviceApprovalsandClearances/default.htm

[43] European Union for Medical Devices, Council directive 93/42/eec of june 14, 1993, concerning medical devices, Official Journal of the European Communities 36 (L169).

[44] Ericsson, Live smart mobile health (2013) [cited Online].
URL http://www.ericsson.com:80/hr/ict_solutions/e-health/emh/index.shtml

[45] U.S. Food and Drug Administration (2014) [cited Online]. [link].
URL http://www.fda.gov/RegulatoryInformation/Legislation/FederalFoodDrugandCosmeticActFDCAct/SignificantAmendmentstotheFDCAct/FDASIA

[46] I. Bisio, F. Lavagetto, M. Marchese, A. Sciarrone, A smartphone-centric platform for remote health monitoring of heart failure, International Journal of Communication Systems, (2014),doi:10.1002/dac.2778.

[47] J. Fayn, P. Rubel, Toward a personal health society in cardiology., IEEE Transactions on Information Technology in Biomedicine 14 (2) (2010)

401–409.
URL http://dblp.uni-trier.de/db/journals/titb/titb14.html#FaynR10

[48] C.-T. Lin, K.-C. Chang, C.-L. Lin, C.-C. Chiang, S.-W. Lu, S.-S. Chang, B.-S. Lin, H.-Y. Liang, R.-J. Chen, Y.-T. Lee, L.-W. Ko, An intelligent telecardiology system using a wearable and wireless ecg to detect atrial fibrillation., IEEE Transactions on Information Technology in Biomedicine 14 (3) (2010) 726–733.
URL http://dblp.uni-trier.de/db/journals/titb/titb14.html#LinCLCLCLLCLK10

[49] J. C. Sieverdes, F. Treiber, C. Jenkins, Improving diabetes management with mobile health technology, Am. J. Med. Sci. 345 (4) (2013) 289–295.

[50] M. Kirwan, C. Vandelanotte, A. Fenning, J. M. Duncan, Diabetes self-management smartphone application for adults with type 1 diabetes: Randomized controlled trial, J Med Internet Res 15 (11) (2013) e235. doi:10.2196/jmir.2588.
URL http://www.ncbi.nlm.nih.gov/pubmed/24225149

[51] A. J. Cafazzo, M. Casselman, N. Hamming, K. D. Katzman, R. M. Palmert, Design of an mhealth app for the self-management of adolescent type 1 diabetes: A pilot study, J Med Internet Res 14 (3) (2012) e70.
URL http://www.ncbi.nlm.nih.gov/pubmed/22564332

[52] H. Maamar, A. Boukerche, E. Petriu, 3-d streaming supplying partner protocols for mobile collaborative exergaming for health, Information Technology in Biomedicine, IEEE Transactions on 16 (6) (2012) 1079–1095. doi:10.1109/TITB.2012.2206116.

[53] I. Lopes, B. Silva, J. Rodrigues, J. Lloret, M. Proenca, A mobile health monitoring solution for weight control, in: Wireless Communications and Signal Processing (WCSP), 2011 International Conference on, 2011, pp. 1–5. doi:10.1109/WCSP.2011.6096926.

[54] F. Zhu, M. Bosch, I. Woo, S. Kim, C. J. Boushey, D. S. Ebert, E. J. Delp, The use of mobile devices in aiding dietary assessment and evaluation., J. Sel. Topics Signal Processing 4 (4) (2010) 756–766.
URL http://dblp.uni-trier.de/db/journals/jstsp/jstsp4.html#ZhuBWKBED10

[55] R. Whittaker, E. Dorey, D. Bramley, C. Bullen, S. Denny, R. C. Elley, R. Maddison, H. McRobbie, V. Parag, A. Rodgers, P. Salmon, A theory-based video messaging mobile phone intervention for smoking cessation: Randomized controlled trial, J Med Internet Res 13 (1) (2011) e10.
URL http://www.ncbi.nlm.nih.gov/pubmed/21371991

[56] J. Finkelstein, J. Wood, Interactive mobile system for smoking cessation, in: Engineering in Medicine and Biology Society (EMBC), 2013 35th Annual International Conference of the IEEE, 2013, pp. 1169–1172. doi:10.1109/EMBC.2013.6609714.

[57] J. Fontecha, R. Hervás, J. Bravo, J. F. Navarro, A mobile and ubiquitous approach for supporting frailty assessment in elderly people, J Med Internet Res 15 (9) (2013) e197. doi:10.2196/jmir.2529.
URL http://www.ncbi.nlm.nih.gov/pubmed/24004497

[58] G. Chiarini, P. Ray, S. Akter, C. Masella, A. Ganz, mhealth technologies for chronic diseases and elders: A systematic review, Selected Areas in Communications, IEEE Journal on 31 (9) (2013) 6–18. doi:10.1109/JSAC.2013.SUP.0513001.

[59] K. Källander, K. J. Tibenderana, J. O. Akpogheneta, L. D. Strachan, Z. Hill, A. A. H. ten Asbroek, L. Conteh, R. B. Kirkwood, R. S. Meek, Mobile health (mhealth) approaches and lessons for increased performance and retention of community health workers in low- and middle-income countries: A review, J Med Internet Res 15 (1) (2013) e17.
URL http://www.ncbi.nlm.nih.gov/pubmed/23353680

[60] C. Déglise, S. L. Suggs, P. Odermatt, Short message service (sms) applications for disease prevention in developing countries, J Med Internet Res 14 (1) (2012) e3. doi:10.2196/jmir.1823.
URL http://www.ncbi.nlm.nih.gov/pubmed/22262730

[61] M. Fiordelli, N. Diviani, P. J. Schulz, Mapping mHealth research: a decade of evolution, J. Med. Internet Res. 15 (5) (2013) e95.

[62] IMS Health, 2013 report: Patient apps for improved healthcare (2013) [cited Online].
URL http://www.imshealth.com/deployedfiles/imshealth/Global/Content/Corporate/IMS%20Health%20Institute/Reports/Patient_Apps/IIHI_Patient_Apps_Report.pdf

[63] MyFitnessPal, Calorie counter and diet tracker (2014) [cited Online].
URL https://itunes.apple.com/br/app/calorie-counter-diet-tracker/id488519281?mt=8

[64] MyNetDiary, Calorie counter pro (2014) [cited Online].
URL https://itunes.apple.com/us/app/calorie-counter-pro-by-mynetdiary/id352247139?mt=8

[65] Azumio Inc., Chest trainer (2014) [cited Online].
URL https://itunes.apple.com/ca/app/chest-trainer-100+-chest-exercises/id583620753?mt=8

[66] eClinicalWorks, Healow [cited Online].
URL https://itunes.apple.com/us/app/healow/id595012291?mt=8id595012291?mt=8https://itunes.apple.com/us/app/healow/id595012291?mt=8

[67] Vitals, Vitals - your top 10 doctors (2014) [cited Online].
URL https://itunes.apple.com/us/app/vitals-your-top-10-doctors!/id540384807?mt=8

[68] ZocDoc, Zocdoc – doctor appointments online! (2014) [cited Online].
URL https://itunes.apple.com/us/app/zocdoc-doctor-appointments/id391062219?mt=8

[69] HealthTap, Healthtap – free doctor answers to medical and health questions (2014) [cited Online].
URL https://itunes.apple.com/us/app/healthtap-free-doctor-answers/id466079030?mt=8

[70] Healthagen, itriage (2014) [cited Online].
URL https://itunes.apple.com/us/app/itriage-health-doctor-symptoms/id304696939?mt=8

[71] WebMed, Webmed (2014) [cited Online].
URL https://itunes.apple.com/us/app/webmd-for-ipad/id373185673?mt=8

[72] GoodRx, Goodrx (2014) [cited Online].
URL https://itunes.apple.com/us/app/goodrx-prescription-medicine/id485357017?mt=8

[73] I. C. Solutions, Myrefill (2014) [cited Online].
URL https://itunes.apple.com/us/app/myrefill-rx/id372376803?mt=8

[74] Walgreen, Walgreen (2014) [cited Online].
URL https://itunes.apple.com/us/app/walgreens/id335364882?mt=8

[75] Montuno, Dosecast (2014) [cited Online].
URL https://itunes.apple.com/us/app/dosecast/id365191644?mt=8

[76] M. Software, Pill monitor free (2014) [cited Online].
URL https://itunes.apple.com/us/app/pill-monitor-free-medication/id485247638?mt=8

[77] Walgreen, Rxmindme prescription / medicine reminder and pill tracker (2014) [cited Online].
URL https://itunes.apple.com/us/app/rxmindme-prescription-medicine/id379864173?mt=8

[78] M. Software, Daily carb - carbohydrate, glucose, medication, blood pressure and exercise tracker (2014) [cited Online].
URL https://itunes.apple.com/us/app/daily-carb-carbohydrate-glucose/id536425111?mt=8

[79] Azumio Inc., Glucose buddy - diabetes logbook manager w/syncing, blood pressure, weight tracking (2014) [cited Online].
URL https://itunes.apple.com/us/app/glucose-buddy-diabetes-logbook/id294754639?mt=8

[80] Sanofi-aventis, Gomeals (2014) [cited Online].
URL https://itunes.apple.com/us/app/gomeals/id336651139?mt=8

[81] Daniel Anderton, Adhd angel (2014) [cited Online].
URL https://itunes.apple.com/us/app/adhd-angel/id485821457?mt=8

[82] Pocket Therapist, Live ocd free (2014) [cited Online].
URL https://itunes.apple.com/us/app/live-ocd-free/id509337840?mt=8

[83] The National Center for Telehealth and Technology , T2 mood tracker (2014) [cited Online].
URL https://itunes.apple.com/us/app/t2-mood-tracker/id428373825?mt=8

[84] Office-fit (2014) [cited Online].
URL https://itunes.apple.com/bh/app/office-fit/id408838099?mt=8

[85] WebMD, Webmd pain coach (2014) [cited Online].
URL https://itunes.apple.com/us/app/webmd-pain-coach/id536303342?mt=8

[86] Zimmer Inc., Zimmer arthritis (2014) [cited Online].
URL https://itunes.apple.com/us/app/webmd-pain-coach/id536303342?mt=8

[87] Lingopal Holdings Pty, Dr k's breast checker (2014) [cited Online].
URL https://itunes.apple.com/us/app/dr-ks-breast-checker/id385045662?mt=8

[88] Pcr tracker (2014) [cited Online].
URL https://itunes.apple.com/ch/app/pcr-tracker/id592097118?l=en&mt=8

[89] Skinkeeper (2014) [cited Online].
URL https://itunes.apple.com/lv/app/skinkeeper/id486413797?mt=8

[90] Martin Hartl, Noteness (2014) [cited Online].
URL https://itunes.apple.com/us/app/noteness/id639289114?mt=8

[91] Health Wave Signals, Parkinson diary (2014) [cited Online].
URL https://itunes.apple.com/us/app/parkinson-diary/id507107180?mt=8

[92] Y. Epilepsy, Young epilepsy (2014) [cited Online].
URL https://itunes.apple.com/gb/app/young-epilepsy/id564205130?mt=8

[93] Vipo.com, Ovulation calendar ladytimer free (2014) [cited Online].
URL https://itunes.apple.com/us/app/ovulation-calendar-ladytimer/id406762826?mt=8

[94] nanobitsoftware.com, Period diary (period, fertile & ovulation tracker) (2014) [cited Online].
URL https://itunes.apple.com/au/app/period-diary-period-fertile/id436762566?mt=8

[95] Everyday Health Inc., Pregnancy & baby — what to expect (2014) [cited Online].
URL https://itunes.apple.com/us/app/pregnancy-baby-what-to-expect/id289560144?mt=8

[96] Seacloud Software, Baby connect (activity logger) (2014) [cited Online].
URL https://itunes.apple.com/us/app/baby-connect-activity-logger/id326574411?mt=8

[97] Colorful Drop, Baby food pee poo free (2014) [cited Online].
URL https://itunes.apple.com/us/app/baby-food-pee-poo-free/id486705853?mt=8

[98] ANDESigned, Total baby (2014) [cited Online].
URL https://itunes.apple.com/us/app/total-baby/id312198543?mt=8

[99] A. Bahga, V. Madisetti, A cloud-based approach for interoperable electronic health records (ehrs), Biomedical and Health Informatics, IEEE Journal of 17 (5) (2013) 894–906. doi:10.1109/JBHI.2013.2257818.

[100] R. S. H. Istepanaian, Y.-T. Zhang, Guest editorial introduction to the special section: 4g health - the long-term evolution of m-health., IEEE Transactions on Information Technology in Biomedicine 16 (1) (2012) 1–5.
URL http://dblp.uni-trier.de/db/journals/titb/titb16.html#IstepanaianZ12

Chapter 3

Cooperative Strategies for Challenged Networks and Applications: A Survey

This chapter consists of the following article:

Cooperative Strategies for Challenged Networks and Applications: A Survey

Bruno M. C. Silva, Joel J. P. C. Rodrigues, Neeraj Kumar, and Guangjie Han

Article submitted for publication in an international journal.

Cooperative Strategies for Challenged Networks and Applications: A Survey

Bruno M. C. Silva [1], Joel J. P. C. Rodrigues[2], Neeraj Kumar[3], Guangjie Han[4]

***Abstract*—Wireless ad-hoc networks use mobile devices to deliver services supported by high-speed network connections and high-speed data transmissions, in real time. These devices (network nodes) typically act as the network infrastructure to forward data to other nodes from a source to the destination. However, several constraints (e.g., processor, energy consumption, bandwidth, etc.) affect the overall network performance. Cooperation strategies have been considered as a solution to such network limitations and constraints. Recent studies present cooperation mechanisms as a solution to unstable network infrastructures where mobile nodes cooperate with each other forwarding data and performing all the networking functionalities. This paper presents a comprehensive review of the state of the art on cooperation strategies and algorithms for mobile ad-hoc networks (MANETs) and delay tolerant networks (DTNs). These challenged networks frequently comprise situations where traditional Internet protocols fail to provide effectively a desired or expected communication. This study focuses on cooperation incentive-based approaches for network architectures that support mobile devices and that are challenged by mobility constraints, such as, battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, and network delays. The surveyed approaches merits and weaknesses are discussed and open issues are identified. Finally, conclusions are detailed.**

***Index Terms*—Cooperation; Cooperation Mechanisms; Wireless networks, MANET, DTN, Mobile computing.**

I. Introduction

With the rapid proliferation of mobile devices and the evolution of wireless networks technologies, the mobile Internet has experienced exponential growth in recent years [1]. With mobile Internet, mobile devices have migrated to data transfer and Internet services through several wireless communication technologies such as third-generation (3G) and fourth-generation (4G) services. Currently, 5G is a research topic under intensive research. This technological evolution triggers a new era of anytime/anywhere access to information, multimedia applications, and multiple mobile services[2]. Mobile devices frequently use wireless networks, especially local area networks (LANs), to access Internet services and communicate directly among them. However, in the absence of an access point (AP), mobile devices can create a mobile ad-hoc network (MANETs) [3], creating a group or several groups of wireless network nodes in a temporary network without centralized infrastructure [4] where the devices perform all the network tasks to provide connectivity. Furthermore, for network scenarios characterized by long and variable propagation delays, low node density, low transmission reliability, node mobility, and disruption, the delay tolerant networking (DTN) [5] paradigm is also considered to solve such network issues. DTN routing protocols assume that network nodes store-and-forward data to other nodes until the communication reaches the destination node.

These network architectures based on mobile devices and wireless communications present several challenged issues and constraints, such as, battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, and network delays. The mobility paradigm of anytime/anywhere access to Internet services is constantly challenged by network and communication limitations, and the experience expected by users it is far to be perfect. In this sense, cooperative strategies appeared as a solution that focuses on increasing network connectivity, communication rates, reliability, and energy optimization. For instance, cooperation strategies are a key aspect in User-Centric Networks (UCN) to motivate users to share their resources and to avoid uncooperative nodes to prevent the usability of the entire system. These networks uses an high cooperative environment to enable Internet access to end-users, providing a better Internet connectivity or allowing the access to services without a reliable Internet connection [6], [7]. UCNs use cooperation incentive based approaches to promote cooperation between network agents [8]. Incentives, such as credit based mechanisms or reputation based mechanisms enforce cooperation and also to promote a trust management system and assure a fair network access [9], [10], [11].

Cooperation is a hot research topic that has been growing in recent years with the advent of wireless networks. Basically, in a challenged network scenario, in the presence of a situation where traditional Internet protocols fail, nodes cooperate with each other performing all the networking functionalities, such as, support intermediate nodes by forwarding packets between two distant nodes [12]. Recent studies propose cooperation mechanisms and algorithms as a solution to improve wireless networks performance [13].

This paper elaborates on an extensive review of the state of the art on cooperative strategies for wireless ad-hoc networks focusing on MANETs and DTNs. It considers the most significant cooperative based-approaches that present significant improvements to the most simple cooperation solutions. The main contributions of this paper are the following:

[1] Bruno M. C. Silva is with Instituto de Telecomunicações, University of Beira Interior, Rua Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal (bruno.silva@it.ubi.pt)

[2] Joel J. P. C. Rodrigues is with Instituto de Telecomunicações, University of Beira Interior, Rua Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal; and University ITMO, St. Petersburg, Russia (joeljr@ieee.org)

[3] Neeraj Kumar is with Department of Computer Science and Engineering, Thapar University, Patiala (Punjab), India (nehra04@yahoo.co.in)

[4] Guangjie Han is with Department of Information & Communication Systems, Hohai University, Changzhou, China (hanguangjie@gmail.com)

- A comprehensive review on cooperative game theoretical based approaches.
- A description of the most significant cooperative incentive-based approaches.
- A discussion and comparison of the most relevant cooperative approaches, pointing their most significant characteristics and open issues.

The reminder of this paper is organized as follows. Section II elaborates on the current state of the art on cooperative strategies for wireless networks while Section III focuses on the most recent cooperation-based approaches for MANETs. Section IV describes the most recent cooperation-based approaches for DTNs. A discussion on cooperative strategies and open issues are presented in Section V. Finally, the paper is concluded on Section VI.

II. Cooperative Strategies and Communication on Wireless Networks

The overwhelming evolution of the available wireless networks based on multiple, unpredictable, and complex interactions demands that network nodes cooperate with one another to improve the overall network performance (as illustrated in Figure 1). Cooperation strategies on wireless networks mainly focuses on increasing power efficiency, network coverage, outage probability reduction, and other wireless network constraints [14], [15], [16], [17]. Through cooperation, wireless networks increase the overall performance increasing data rates and network throughput. Furthermore, through relaying schemes nodes can optimize their resources (e.g. battery life) obtaining a balanced quality of service (QoS). Moreover, it decreases network infrastructure dependency reducing costs [18], [19].

Cooperative coding or relaying strategies, such as, amplify-and-forward (AF), classic multi-hop, compress-and-forward (CF), decode-and-forward (DF), multipath decode-and-forward (MDF), among others, have been presented as a solution to promote cooperative communication in wireless networks. These cooperative relaying schemes can be applied in both wired and wireless networks [20] and, in the last decade, have been served as basis to several proposals for cooperative strategies. This section considers the most relevant cooperation strategies proposals for wireless networks.

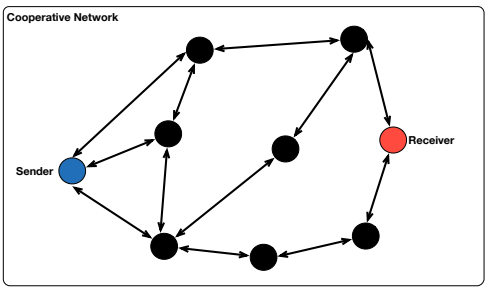


Fig. 1. Illustration of a cooperative network scenario.

Game theory techniques have been widely applied in cooperation strategies. Originally, these techniques were developed for economic issues. Game theory aims to model scenarios where several agents present mutual or may have conflict of interests. Therefore, wireless networks architectures fit perfectly in the game theory formulation [21]. In a typical cooperative game scheme, network agents cooperate to achieve network privileges/agreements so they can gain maximum benefits that would not be obtained without cooperation through selfish behaviors [22].

Wen *et al.* [23] present a game theory based approach for wireless cellular networks that promotes user cooperation to improve energy efficiency. The authors present a network scenario that considers a cellular framework where two mobile users request communication with a base station assuming a DF relaying scheme. The cooperative game approach is applied to solve decision problems (whether to cooperate or not) improving and maximizing, therefore, the overall network performance, mainly, the system payoff.

In [24], the authors present a cooperative strategy for wireless networks considering multi-user symmetrical cooperative communications networks. The paper presents an admission control algorithm to obtain maximum cooperation feasibility. The authors use the Nash bargain solution (NBS) from game theory approaches to optimize the bandwidth allocation during cooperation. Through the presented simulation results, the authors demonstrate this cooperation strategy improves the transmission rates effectively in comparison to non-cooperative strategies.

Gyarmati and Trinh [25] present an analysis and modeling of the access method selection on mobile devices under cooperation scenarios. The authors propose a model applying game theory analysis to obtain optimal cooperation in wireless technologies. Nash equilibrium strategies are presented for mobile devices using multiple access technologies to determine the devices optimal access method. The performance of the proposal was evaluated through simulation where the results were obtained for a case study quantifying the impact of the proposed model on payoff and energy usage.

Zetterberg *et al.* describe experimental results of an investigation on cooperative relaying schemes including AF, DF, cooperative maximum ratio combining (CMRC), and distributed space-time coding (DSTC) [26]. Furthermore, the authors include a novel relaying strategy called selection relaying (SR). SR considers that one of two relay nodes is selected based on path-loss. Results show that all cooperative schemes increase the coverage area compared with direct transmission and that antenna diversity improve the overall system performance.

In [27] the authors present a novel cooperative communication system that operates over wireless networks in real-time. The authors demonstrate through a performance evaluation study that using AF relays clearly benefits and improves the conditions of a realistic wireless network.

Korakis *et al.* [28] present an implementation of the above-described cooperative MAC protocol called CoopMAC [29]. It is based on two different approaches, one based on open source drivers and another based on software defined radio platform. Furthermore, the study compares and confirms that the cooperative MAC protocol outperforms the legacy (IEEE

802.11) MAC protocol, improving the overall network performance.

Laura Cottatellucci *et al.* [30] refer four articles that focus on cooperative transmission and analysis and optimization of cooperative protocols. These articles are presented and described bellow.

In [31] the authors propose a novel end-to-end outage probability approach of a cooperative diversity system based on exact integral expressions. In this proposal, a relay node assists in the communication between source and destination nodes. This paper also introduces insights and advantages on the impact of the multiple-access protocol on cooperation, presenting comparison results with non-cooperative approaches.

Vandendorpe *et al.* present a proposal for the optimization and minimization of the transmit-power for throughputs and link performances [32]. The authors consider a relay node that operates in a DF mode to assist between source and destination. Furthermore, the paper considers the use of two different protocols to compare and investigate the power allocation problem using two types of power constraints.

In [33] a proposal for cooperative systems that considers two-user coordination interleaved coded cooperation (CICC) scheme is presented. This proposal combines cooperative and modulation schemes whether users know the cooperation status or not. The CICC was proposed mainly to increase both bandwidth efficiency and diversity gains. The authors claim through a performance evaluation and comparison that this proposal outperforms the best space-time approaches used in cooperation systems.

In [34] the authors propose an end-to-end antenna selection (EEAS) strategy to maximize end-to-end mutual information and diversity gains for multiplexing gains in a multi-hop relay channel. This proposal considers the use of a subset of end-to-end joint antenas of each relay stage for source signal transmission to the destination. Therefore, amplifying and forwarding at each relay stage achieve maximum mutual information at the destination.

Cooperative strategies on wireless network commonly aim network efficiency improving the overall performance increasing data rates and network throughput. However, mobility scenarios are constantly challenged and unstable forcing network nodes to self-adapt to the network characteristics. Next section overviews the most important techniques to enforce cooperation in MANETs.

III. Cooperation Strategies for Mobile Ad-Hoc Networks

In a mobile ad-hoc network (MANET) mobile devices (network nodes) are continuously self-adapting/configuring to the network characteristics to receive and forward data [35]. Therefore, it is assumed that all network nodes must cooperate so that data can be forwarded or routed. However, this cooperative behavior is not followed by all the nodes that are called *un-cooperative nodes*. These nodes can be faulty or malicious, or/and selfish and may not always forward other nodes data or refuse to perform specific network operations [36]. Several cooperation strategies have been proposed to stimulate cooperative nodes and mitigate the detrimental effect of non-cooperative nodes. This section presents the most significant cooperation strategies and mechanisms proposed for MANETs.

A. Incentive-based cooperation strategies

Cooperative incentive-based approaches are divided in two main groups: virtual currency based schemes and reputation based schemes [37] [38]. Virtual currency schemes use incentives to enforce nodes cooperation by addressing packet forwarding services as priced transactions using virtual credits. These virtual payments are often given to nodes that cooperate and perform other specific network operations. Virtual currency schemes also assume that forwarding services have an inherent cost to network nodes. Therefore, non-cooperative nodes need incentives to forward packets of other nodes.

Nuglets [39] is a popular system that uses virtual currency schemes that address the problem of non-cooperative nodes in large MANETs for civilian applications. This system uses a virtual currency, called *nuglets*, to stimulate packet forwarding decreasing, therefore, node selfish behaviors without negative effects on the network overall performance.

Another popular credit-based system, called Sprite, is presented in [40]. This virtual currency approach consists in a cheat-proof system that stimulates cooperation among selfish nodes. Sprite does not need any tamper-proof hardware at any node and it uses a received/forwarded message *receipts* to validate and determine the charge and credit to each node involved in a transmission. Furthermore, Sprite includes a central credit clearance service (CCS) to manage the credit payments to cooperative nodes. Therefore, selfish nodes are motivated to cooperate and to report their actions (selfish or not) honestly using a game theory perspective.

Jakobsson *et al.* propose a micro-payment scheme to stimulate cooperation in multi-hop cellular networks [41]. This proposal uses micro-payments as a reward for packet forwarding and punishes selfish behaviors or other forms of abuse. In this proposal, the authors include a technique to determine the package forwarding destination, a mechanism for base stations to verify and validate if packets are accompanied by their respective payments, the aggregation of payments, and a method to detect and identify cheating behaviors.

In [42] the authors propose a mechanism to stimulate node cooperation and prevent network congestion addressing the problem of service availability in MANETs. They use the concept of money and service charges to motivate users to keep their devices turned on. For this purpose, the authors introduce a virtual-currency called *nuggets*. *Nuggets* have no monetary value and can only be used within the network. Basically, every time a node wants to send a message, it must pay in *nuggets* for this service. Therefore, it motivates nodes to perform cooperative behaviors to gain more *nuggets*.

Buttyán and Hubaux present a cooperation mechanism to stimulate nodes to perform packet forwarding [43]. The authors consider a scenario where users can modify the node behavior tampering with its software or hardware for selfish purposes (e.g., save battery power). This proposal includes

a *nuglet* (virtual currency) counter in each network node that must remain positive. This counter decreases when a node wants to send a packet and increases when a node forwards a packet. Furthermore, this mechanism is protected by a security module detecting and preventing fraud behaviors. This cooperation mechanism motivates users to maintain their devices turned on and, therefore, increasing packet forwarding.

In [44] Crocraft *et al.* propose a model to stimulate cooperation in MANETs that uses incentives to rewards users that act as relaying nodes on multi-hop paths. The proposed pricing mechanism uses a dual algorithm for traffic and pricing management within the network. Node resources used when forwarding traffic along multi-hop routes is rewarded and prices are based on their bandwidth and power usage. Furthermore, traffic routes are calculated and chosen to obtain minimal routing price. The authors demonstrate that motivating users to act as relaying nodes, cooperation is a natural consequence of this pricing mechanism proposal.

Anderegg and S. Eidenbenz present a network scenario with game-theoretic routing where nodes that are assumed to be selfish only forward packets if payments cover their communication costs [45]. The authors propose a routing protocol, called ad-hoc-VCG, for MANETs to mitigate selfish behaviors achieving cost-efficiency and truthfulness. This proposal guarantees that network agents reveal their true cost for forwarding data and that routing is performed along the most cost-efficient path.

In [46] the authors propose a credit-based cooperation mechanism, called Express, that makes use of hash chains on messages to avoid node cheating behaviors. Express does not rely on any tamper-proof hardware and makes use of several Sprite [40] main strengths, such as the above-mentioned CCS. This proposal uses hash chains instead of digital signatures reducing significantly operation processes and identifying more clearly cheating behaviors. Authors demonstrate that Express guarantees secure and rational cooperation providing rational incentives for packet forwarding.

Raghavan and Snoeren presented an incentive-based scheme that provides priority for packet forwarding to un-selfish nodes [47]. This pricing forwarding scheme assumes that a MANET provides two types of traffic: best-effort and priority. Network nodes are rewarded with priority to access the best-effort service. Selfish nodes are punished and deprived to access the best-effort service.

Cooperative reputation-based mechanisms monitor the network nodes behaviors using reputation to diminish selfishness and even to isolate misbehaving nodes. These cooperation strategies use reputation as an incentive to motivate nodes to cooperate and, therefore, mitigate selfish behaviors. Usually, in theses schemes, nodes reputation is obtained by neighbor monitoring/observation and all the network nodes know the reputation of the other nodes. This is the opposite of trust based systems that often produce a rating that let parties to rate each other. It goals that other parties decide in the future if they want to cooperate with un-trusty parties. Trust systems are also incentive-based systems and sometimes can be included in reputation systems, or vice-versa [48].

One of the early studies in the area of reputation-based schemes and, to the best of the authors knowledge, the first one, was presented in [49] by Marti *et al.*. The authors studied a reputation-based cooperation mechanism that used *Watchdog* and *Pathrater*, that are extensions of the Dynamic Source Routing algorithm (DSR) [50]. Its goal is to use *Watchdog* to identify misbehaving nodes and *Pathrater* to manage routing protocols to avoid these nodes. The authors shown through simulation results that with these techniques, in the presence of misbehaving nodes, the network ratio of overhead transmissions increase as well as the network throughput.

CONFIDANT [51] aims to detect and isolate selfish nodes compelling them to cooperate. These cooperative scheme assent on four components per node: *i*) the monitor, where nodes locally detect deviating behavior of other nodes by listening the transmission of the next node or observing route protocol behavior. This component sends ALARMs of misbehaving actions to the trust manager component; *ii*) The trust manager component receives these ALARMs and makes decisions about to whom must provide or accept route information; *iii*) The reputation system rates node reputation based on their behavior; and *iv*) The path manager that based the reputation rating defines the path ranking in order to avoid malicious nodes.

CORE [52] scheme uses collaborative monitoring and a reputation table to stimulate cooperation among nodes. In this reputation table, nodes that have a good reputation can use network services (i. e., packet forwarding or other specific network operation) while nodes with a bad reputation are deprived of network services. Basically, when a node forwards a packet, its table reputation value increases. Otherwise, if the node refuses to forward a packet, its reputation table value decreases. Furthermore, to calculate this node reputation value, CORE defines three types of reputation: *subjective reputation*, calculated based on direct observation; *indirect reputation*, calculated based on second hand information given by other nodes; and *functional reputation*, calculated by a function that uses a packet forwarding weight in function of its importance.

OCEAN [53] aims to detect and mitigate misleading routing behaviors in MANETs. This cooperation scheme focuses on trust-management issues by avoiding second-hand reputation information using only direct first-hand observations of nodes' behaviors. Furthermore, OCEAN is an hybrid solution that uses both reputation and incentives through micro-payments to enforce cooperation. These payments are given to only cooperative neighbor nodes and cannot be earned on other packets in different routing paths.

In [54] He *et al.* present a cooperation scheme called Secure and Objective Reputation-based Incentive Scheme for Ad-Hoc Networks (SORI). SORI addresses problems of non-cooperative ad-hoc networks were node's selfish behaviors degrades the overall network performance. Therefore, this scheme aims to encourage nodes to forward packets and so decreasing selfish actions. SORI reputation mechanism quantifies the node reputation in objective measures and its propagation is only performed by neighbor nodes through an one-way-hash chain based authentication scheme. Furthermore, SORI includes also a punishment scheme that penalizes selfish nodes that refuse packets forwarding.

DARWIN (Distributed and Adaptive Reputation mechanism for Wireless Networks) [55] is a cooperative scheme that detects and punishes selfish behaviors with collision resistance avoiding retaliation scenarios of nodes being wrongly perceived as selfish nodes. Therefore, DARWIN guarantees full cooperation among nodes solving with robustness imperfect behaviors measurements.

Milan *et al.* present a research on negative impact of packets collisions on hop-by-hop reputation-based mechanisms for networks with uniform random traffic [56]. The authors propose a game theory model based on the classic Prisoner's Dilemma [57] to perform this study characterizing the impact of selfish behaviors on the network capacity. Furthermore, this study also includes the proposal of two more severe punishment schemes, called, One-step Trigger and Grim Trigger.

In [58] the authors present a reputation scheme called LARS (Locally Aware Reputation System). This proposal deals with two types of node selfishness: selective selfishness and extreme selfishness. Node reputation is calculated only through direct observation. In selective selfishness, if a selfish node or selfish behavior is identified by its direct neighbors, the node reputation degrades. In case of extreme selfishness the routes that contain these selfish nodes are deleted and new routes are created excluding these nodes. Without being able to improve their reputation, these nodes may be eventually excluded from the network.

Liu *et al.* propose a solution for routing schemes to detect node misbehaviors, called 2ACK [59]. This proposal can be used as an add-on for routing protocols, such as, DSR for MANETs. This scheme basically proposes to send two-hop acknowledgment packets always in the routing path opposite direction. These packets are sent back by the receiver of the next-hop link. This way, 2ACK detects successfully, not the misbehaving single node, but misbehaving links. Therefore, it overcomes several issues, such as, ambiguous collisions, receiver collisions, and limited transmission powers.

B. Cooperation-based Approaches

This sub-section addresses cooperation-based approaches regardless of their incentive methods. These proposals improved the typical cooperative schemes, introducing innovative and single cooperation techniques, such as, the use of location aware services, cloud services, and clustering techniques.

Luo and Deters present a study on how cooperation schemes can improve the experience of mobile Web services consumers [60]. This study focuses on the use of cooperation between consumers and providers as an effective mean to improve the consumer experience and the QoS in a scenario where mobile devices (e.g., phones, smartphones, tablets) regularly request services from the Web. This cooperation model is based on a task prediction and uses two proxies, one in the server side and another in the client side (software model in the mobile device). The server proxy pre-fetches and pre-processes, pre-requests made by the client to the Web service. This way, through a task prediction, the system provides a client with choices and decisions rather than just provide stored information, therefore, improving the overall network performance.

In [61] the authors propose a distributed clustering protocol, called Cooperative Networking protocol (CONET) for energy saving in mobile devices with WLAN and Bluetooth interfaces. Figure 2 illustrates the CONET model presenting nodes organized by clusters. It dynamically auto-configures clusters of network nodes depending on their bandwidth requirements and their common activities. These clusters are arranged in Bluetooth personal area networks (PANs) and a cluster head node is elected to act as a gateway between the PAN and the WLAN access point. Therefore, enabling the clusters to access the WLAN infrastructure and also save energy since that they do not need to enable Wi-Fi in their devices.

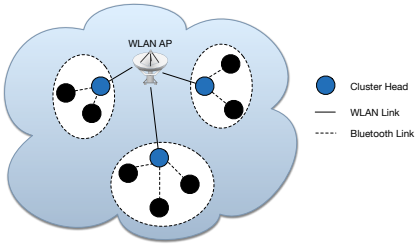


Fig. 2. Ilustration of CONET protocol with nodes organized in clusters.

Khalek and Dawy present a cooperative-based solution for video distribution over multi-hop networks to minimize the total of energy consumption in a real-time video broadcast scenario [62]. The proposed model includes a base station capable to transmit and relaying the video bit stream for mobile devices. The authors implemented two low complexity approximation algorithms achieving great energy consumption gains.

In [63] the authors proposed a cooperation-based strategy for wireless networks using relay stations to improve the throughput of the network balancing user traffic demand. This proposal, illustrated in Figure 3, uses a main base station for coordination instead of mobile relay nodes. Basically, it uses static relay stations (RSs) to optimize the network performance. The main base station distributes the requested content to the RSs forming a virtual antenna array and cooperatively transmitting the content to the mobile devices.

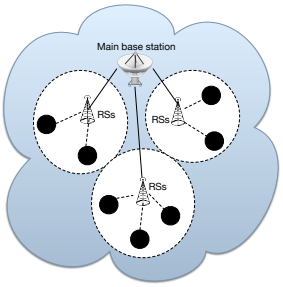


Fig. 3. Illustration of cooperation through relay stations.

Cooperation mechanisms have recently gained great relevance in localization and navigation systems especially in

wireless mobile networks. Several proposals have been elaborated where network agents estimate their positions through cooperative-based approaches [64] [65] [66]. Win *et al.* propose a research and description of cooperative-based approaches for localization and navigation from a theoretical perspective to applications covering used technologies, schemes, and algorithms [67].

Sammarco *et al.* present a location aware cooperation-based approach to improve localization tracking among mobile nodes through the information retrieved from a cellular network [68]. Each network node retrieves the location area code and the local network base station cell ID. Cooperative nodes within short links range (i.e., Bluetooth) request this information and send it to a server. The server compares the retrieved information and, through the Google Maps API [69], calculates a more accurate location position, retrieving it back to the mobile device.

In [70] authors overview cooperative localization approaches on wireless networks and study their performance on ultrawide bandwidth (UWB) wireless networks. Furthermore, the authors also present a novel localization algorithm, called SPAWN, that maps a graphical model directly onto the network topology. SPAWN can be deployed in several network scenarios requiring a minor communication overhead and achieves an accurate and robust localization.

IV. Cooperation Strategies for Delay Tolerant Networks

In a delay tolerant network (DTN) [71] scenario, network constraints (such as, limited storage capacity, limited network bandwidth, and limited energy) affect the network performance. Furthermore, the performance of a DTN is also affected by long or variable propagation delays, low node density, low transmission reliability, node mobility, and disruption. Several routing protocols were proposed for DTNs [72], [73], [74], [75], [76], [77], however, most of them only consider nodes mobility and no other behavior. DTN routing protocols usually assume a cooperative scenario, however, this is an unrealistic assumption. Nodes may not be able to always cooperate due to resources limitations or even to selfish behaviors [78]. Therefore, in the last decade, several cooperation studies and proposals for DTNs have been proposed in the literature.

A study on the impact of node misbehavior in DTN networks is presented in [79]. This work evaluates the impact o selfish nodes in several DTN routing protocols evaluating the delivery ratio, buffer time, hop count, latency, and overhead ratio. Results shown that different protocols are more resilient according to the number and type of misbehaviors. The authors main goal is to identify the best performance and select DTN routing protocols in the presence of misbehaving nodes.

In [80] a study that focuses on the performance of a DTN non-cooperative approach using three well known DTN routing protocols (Epidemic [74], Two-Hop, and Spray-and-Wait [75]) is presented. This performance evaluation study focuses on message delivery delay and the transmission overhead incurred until message delivery. Then, the authors modeled cooperation as a node probability to drop a message upon its reception or to forward it when encounters another node. Results shown that introducing a simple cooperation mechanism, the network performance considerably improved with all applied routing protocols.

Shevade *et al.* [81] present a study and demonstration of a DTN network overall performance degradation in the presence of nodes selfish behaviors. Furthermore, the authors propose an incentive-based strategy including the use of a simple Tit-for-Tat (TFT) mechanism to stimulate cooperation and mitigate node selfishness. This cooperative strategy assures through the TFT mechanism that every node forwards as much traffic as possible for a neighbor node as the neighbor also forwards traffic to it.

A cooperation scheme for Delay-Tolerant Vehicular Networks based on the cooperative ARQ (C-ARQ) is considered in [82]. This cooperation proposal reduces data losses in transmissions between fixed access points placed along the roads and passing by vehicles that buffer all the data. Basically, in areas that vehicles have no connectivity to access points, vehicles cooperate between them to increase the data delivery rate. Figure 4 illustrates a network scenario where nodes that failed to receive packets from an AP in their range, will eventually receive the same packets through cooperation with other vehicles in an area with no AP coverage.

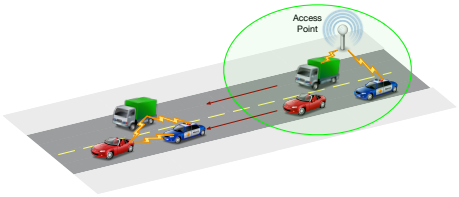


Fig. 4. Illustration of a network scenario for cooperation on DTNs.

A cooperative model, named Pay-for-Gain (PFG), is proposed in [83]. This proposal is based on game theory and loan-credit theory aiming to study the equilibrium point that maximizes the nodes own interests in cooperating with others. Furthermore, the authors present comparison results between a TFT strategy and PFG using Prophet [84] routing protocol using the ONE simulator [85]. Results shown that PFG mechanism is more effective than TFT algorithm in mitigating selfish node behaviors.

A game theoretical incentive scheme for DTN routing, called Multicent, is presented in [86]. This proposal encourages nodes to follow desired performance objectives, such as, minimal average delay, maximal hit rate, and minimal maximal delay by performing packet storage or forwarding. Furthermore, Multicent considers QoS of packet routing adjustable to specific sources, destinations, or source-destination pairs.

In [87] authors address the problem of cooperation additional costs on DTN multiple heterogeneous groups of nodes. The paper proposes a coalition game model for analyzing cooperation decisions within groups of nodes based on a tradeoff between performance gains and costs. This model was developed based on multidimensional absorbing Markov

chain. Basically, this cooperative model infers that none of the node communities can improve their payoffs while forming new coalitions.

Helgason *et al.* present a study on the performance of opportunistic content distribution under different levels of cooperation [88]. Authors consider three levels of cooperation: *i*) no cooperation; *ii*) un-limited cooperation; and *iii*) limited cooperation. In *i*) nodes do not cooperate and do not forward other nodes content. In *ii*) nodes cooperate without any restriction forwarding all desired contents and, in *iii*) nodes cooperate but contents are forwarding within a limit of time in order to save node resources (i.e., battery, CPU, link load). Performance results showed that cooperative approaches improve significantly the network performance.

MobiCent [89] is a credit-based incentive cooperative mechanism for DTNs to encourage cooperation among mobile nodes. This solution enables routing protocols to discover the most efficient paths minimizing the waste of transfer opportunities. Moreover, MobiCent detects and deters cheating nodes that create non-existing contacts to increase their rewards. It also provides different payment mechanisms that adapt to clients who want to minimize either payment or data delivery delay.

In [90] authors present a cooperative peer-to-peer file sharing technique for DTNs that aims to improve the accessibility of media contents from mobile devices. This technique distributes files taking advantage of the mobility of mobile device users or vehicles. As shown in Figure 5, the authors consider the DTN as an extension of the Internet, calling it as hybrid DTN. In this proposal, a single node downloads a file and afterwards shares it with other nodes.

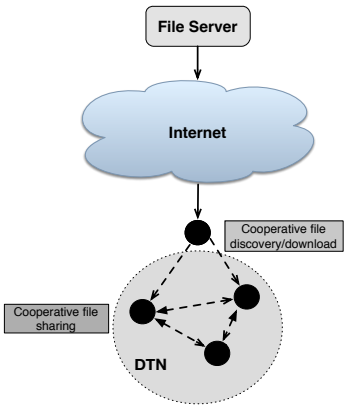


Fig. 5. Illustration of a hybrid DTN network architecture.

An incentive-based scheme for DTNs to stimulate bundle forwarding and cooperation among nodes, called SMART, is presented in [91]. SMART uses credits to encourage selfish nodes, charges and rewards DTN bundle forwarding. This scheme enables intermediate nodes to transfer/distribute credits without the involvement of the sender node. This feature is very important in a DTN network scenario since those sender nodes can predict forwarding paths and also due to possible delays that intermediate nodes may suffer from network constraints. Authors tested SMART compatibility with several DTN routing protocols and also proposed two efficiency-optimization methods for transmission and computation overhead.

In [92] the authors propose simple strategies that motivate data forwarding based on several cooperative incentive-based models for DTNs in publish-subscribe frameworks. These strategies are pull-based and discourage aggressive push framework. Therefore, they allow receivers to choose what messages they are willing to carry and forward. The proposed strategies encourage data forwarding mitigating selfish behaviors. Moreover, the authors demonstrate and study the performance of the deployed schemes through a real mobile platform testbed.

A cooperative reputation-based enforcement scheme for DTNs is proposed in [93]. This approach includes a protocol bundle propagation to detect and identify misbehaving nodes. This protocol is compatible with both single-copy and multi-copy DTN routing protocols. The reputation strategy features a reputation manager that motivates nodes to forward bundles in order to avoid punishments or even exclusion from the DTN.

Karaliopoulos presents a performance assessment of DTN unrestricted and two-hop relaying schemes in the presence of selfish nodes [94]. The author considers two types of selfishness, one when a node refuses to copy and store a third node data, and other when a node refuses to relay data to other nodes. Results shown that unrestricted routing has performance advantages over two-hop routing, decreasing the number of selfish nodes.

MobiID [95] is a *user-centric* and *social-aware* cooperative reputation-based scheme for DTNs. This scheme differs from the traditional reputation schemes that are based on neighbor direct observation. In MobiID, nodes are responsible to manage and update their reputation and only showing it for verification. The concept of self-check is included so that a node keeps its bundle forwarding evidence. The community-check concept is also included so that social-awareness of forwarding evidence is collected and checked by other network nodes.

Mei *et al.* present two forwarding protocols for DTN mobile wireless networks of selfish individuals called Give2Get Epidemic Forwarding and Give2Get Delegation Forwarding [96]. Authors assume that all network nodes are selfish and both protocols are Nash equilibria, which means that no node has interest to deviate. Through simulation, authors shown that both protocols improve the network performance by reducing the number of messages. In terms of delay both protocols introduce a small overhead.

V. Discussion and Open Issues

This section, presents a discussion on the above-surveyed cooperation techniques and describes the identified open issues. Table I and Table II provide a summary and offer a comparison analysis between the most significant cooperative solutions for MANETs and DTNs. Moreover, these tables highlight the classification of each solution into specific categories and cooperative approaches.

8

TABLE I: Summary of cooperation proposals for MANETs

Cooperation Strategy / Author's Name	**Cooperative based-aproach**	**Conceptual Characteristics**	**Proposal objectives/ Main goals**	**Key Aspects**
Nuglets [39]	Virtual currency based-approach	Uses virtual currency, called *nuglets*, to stimulate packet forwarding	Addresses the problem of non-cooperative nodes in large MANETs for civilian applications	Payments/rewards to nodes cooperative behaviors in the form of a virtual currency, called *nuglets*
Sprite [40]	Virtual currency based-approach	Uses a received/forwarded message *receipts* to validate and determine the charge and credit to each node. Includes a CCS to manage the credit payments	Stimulates cooperation among selfish nodes	Charge and/or credit virtual credits to a node depending on its behavior
Jakobsson *et al.* [41]	Virtual currency based-approach	Uses micro-payments as a reward for packet forwarding. Punishes selfish behaviors or other forms of abuse	Stimulates cooperation in multi-hop cellular networks	Micro-payments to nodes that forward packets
L. Buttyan and J.-P. Hubaux [42]	Virtual currency based-approach	Uses virtual currency, called *nuggets* and service charges to motivate users to keep their devices turned on and to cooperate	Prevent network congestion through cooperation, addressing the problem of service availability in MANETs	Payments/rewards to users in the form of a virtual currency, called *nuggets*
L. Buttyan and J.-P. Hubaux [43]	Virtual currency based-approach	Scenario where users can modify the node behavior tampering with its software or hardware for selfish proposes (e.g., save battery power). Uses a *nuglet* counter to motivate users to maintain their devices turned on	Stimulate nodes to cooperate increasing the network packet forwarding	Uses a *nuglet* counter, that must be positive, that motives users to cooperate
Crocraft *et al.* [44]	Virtual currency based-approach	Introduce incentives to rewards users that act as relaying nodes on multi-hop paths. Traffic routes are calculated and chosen to obtain minimal routing price	Stimulate cooperation in MANETs	Rewards users that act as relaying nodes and forward traffic. Rewards are based on their bandwidth and power usage
Anderegg and S. Eidenbenz [45]	Virtual currency based-approach	Proposes a routing protocol, called ad-hoc -VCG, for MANETs to mitigate selfish behaviors achieving cost-efficiency and truthfulness	Network agents reveal their true cost for forwarding data. Routing is performed along the most cost-efficient path.	Routing protocol to mitigate selfish behaviors on a network scenario of only selfish nodes
Express [46]	Virtual currency based-approach	Makes use of hash chains on messages to avoid node cheating behaviors	Guarantees secure and rational cooperation providing rational incentives for packet forwarding	Hash chains on messages has a security mechanism to prevent nodes cheating behaviors

TABLE I – *Summary of cooperation proposals for MANETs*

Cooperation Strategy / Author's Name	**Cooperative based-aproach**	**Conceptual Characteristics**	**Proposal objectives/ Main goals**	**Key Aspects**
Raghavan and Snoeren [47]	Virtual currency based-approach	Cooperative nodes are rewarded with priority to access network services. Selfish nodes are punished and deprived to access network services	Provides priority for packet forwarding to un-selfish nodes	Service access manager, that allows a fair access to a network service depending if the node is cooperative or not
CONFIDANT [51]	Reputation based-approach	Four components per node: i) the monitor ; ii) The trust manager; iii) The reputation system; and iv) the path manager	Aims to detect and isolate selfish nodes compelling them to cooperate	A reputation system that rates node reputation based on their behavior
CORE [52]	Reputation based-approach	Uses collaborative monitoring and reputation table to stimulate cooperation among nodes. When a node forwards a packet, its table reputation value increases. Otherwise, if the node refuses to forward a packet, its reputation table value decreases	Stimulate cooperation in MANETs	Reputation table to stimulate cooperation among nodes
OCEAN [53]	Reputation based-approach	Focuses on trust-management issues using only direct first-hand observations of nodes' behaviors	Aims to detect and mitigate misleading routing behaviors in MANETs	Hybrid solution that uses both reputation and incentives through micro-payments to enforce cooperation
SORI [54]	Reputation based-approach	Quantifies the node reputation in objective measures and its propagation is only performed by neighbor nodes through an one-way-hash chain based authentication scheme	The main goal is to encourage nodes to forward packets and so decreasing selfish actions	Includes a punishment scheme that penalizes selfish nodes, compelling them to cooperate
DARWIN [55]	Reputation based-approach	Detects and punishes selfish behaviors with collision resistance avoiding retaliation scenarios of nodes being wrongly perceived as selfish nodes	Guarantees full cooperation among nodes	Detects and punishes selfish behaviors guaranteeing full cooperation
LARS [58]	Reputation based-approach	Every-time that a selfish node or selfish behavior is identified by its direct neighbors, the node reputation degrades	Stimulate cooperation in MANETs	Node reputation is calculated only through direct observation
2ACK [59]	Reputation based-approach	Sends two-hop acknowledgment packets always in the routing path opposite direction sent back by the receiver of the next-hop link. This way, 2ACK detects successfully, not the misbehaving single node, but misbehaving links	Detects node misbehaviors and overcomes ambiguous collisions, receiver collisions, and limited transmission powers	Can be used as an add-on for typical MANET routing protocols

10

TABLE II: Summary of cooperation proposals for DTNs

Cooperation Strategy / Author's Name	**Cooperative based-aproach**	**Conceptual Characteristics**	**Proposal objectives/ Main goals**	**Key Aspects**
J. Pozo *et al.* [82]	Packet storage and forwarding cooperative approach	Based on the C-ARQ. Vehicles have no connectivity to access points, vehicles cooperate between them to increase the data delivery rate	Reduces data losses in transmissions between fixed access points placed along the roads and passing by vehicles that buffer all the data	Based on the cooperative ARQ (C-ARQ)
Liu *et al.* [90]	Packet storage and forwarding cooperative approach	Distributes files taking advantage of the mobility of mobile device users or vehicles	Aims to improve the accessibility of media contents from mobile devices	Cooperative nodes download contents to share it with other nodes later
Pay-for-Gain (PFG) [83].	Game theoretical approach	Use game theory and loan-credit theory presenting a comparison results between a TFT strategy and PFG	Study the equilibrium point that maximizes the nodes own interests in cooperate. Comparison results shown that PFG mechanism is more effective than TFT	Game theory and loan-credit theory based approach for DTNs
Multicent [86]	Game theoretical approach	Based on packet storage or forwarding. Considers QoS of packet routing	Aims to improve nodes minimal average delay, maximal hit rate, and minimal maximal delay	Encourages nodes to follow desired performance objectives by performing packet storage or forwarding
Niyato *et al.* [87]	Game theoretical approach	Proposes a coalition game model for analyzing cooperation decisions based on tradeoff between performance gains and costs	Addresses the problem of cooperation additional costs on DTN multiple heterogeneous groups of nodes	Based on multidimensional absorbing Markov chain. Infers that none of the node communities can improve their payoffs while forming new coalitions
Shevade *et al.* [81]	Incentive-based strategy	Includes a TFT mechanism to stimulate cooperation and mitigate node selfishness	Assures that every neighbor nodes forwards the same amount of network traffic as possible	Study and demonstration of degradation of a DTN network overall performance
MobiCent [89]	Virtual currency based-approach	Enables routing protocols to discover the most efficient paths minimizing the waste of transfer opportunities. Detects and deters cheating nodes	Encourage cooperation among mobile nodes in DTNs	Detects and deters cheating nodes that create non-existing contacts to increase their rewards
SMART [91]	Virtual currency based-approach	Enables intermediates nodes to transfer/distribute credits without the involvement of the sender node	Stimulate bundle forwarding and cooperation among nodes in a DTN	Uses credits to incentive selfish nodes, charges and rewards DTN bundle forwarding

TABLE II – *Summary of cooperation proposals for DTNs*

Cooperation Strategy / Author's Name	**Cooperative based-aproach**	**Conceptual Characteristics**	**Proposal objectives/ Main goals**	**Key Aspects**
Zhang *et al.* [93]	Reputation based-approach	Includes and use a protocol bundle propagation to detect and identify misbehaving nodes	Stimulate bundle forwarding and cooperation among nodes in a DTN	Features a reputation manager that motivates nodes to forward bundles
MobiID [95]	Reputation based-approach	Nodes are responsible to manage and update their reputation and only showing it when ever its necessary for verification. The community-check concept is also included so that social-awareness of forwarding evidence is collected and checked by other network nodes	Stimulate bundle forwarding and cooperation among nodes in a DTN	Differs from the traditional reputation schemes that are based on neighbor direct observation

After a detailed analysis of the above-presented cooperation techniques, cooperation design for mobile or wireless environments still presents several challenges and is considered an hot research topic [97]. These network environments often lack of standards that ensure all the devices have similar specifications. Furthermore, the fact that is impossible to guarantee the network homogeneity and guarantee its quality and stability creates unstable scenarios for cooperative schemes.

Mobile networks present several constraints, such as, mobile devices resources (e.g. processor power, storage capacity, battery life, network connections with limited bandwidth and/or with high latency) that turns cooperation mechanisms deployment in mobile environments a challenging task. In the above sections, these potential and open issues in cooperative schemes were presented. Moreover, they are inumered in [97], [98], [99] and can be summarized as follows:

- **Network low bandwidth and high latency issues.** Although cooperation mechanisms aim to solve such issues, they can also jeopardize network efficiency and effectiveness.
- **Synchronization, security, and trustfulness.** Often, cooperation systems require extra trust, security, and synchronization add-ons or systems. These extra cooperation efforts are often software/hardware based add-ons that are implemented and can be a difficult task to perform.
- **Complex relaying schedulers.** Networks with multiple nodes relaying information between each other often requires more sophisticated schedulers, adding complexity to the system.
- **Node discover/choice and routing paths.** Cooperation systems typically assume selfish nodes discovery in order to determinate the best node to cooperate and to achieve an optimum routing path. This might be the biggest contribution of cooperative schemes, however, it also can be the hardest one in the presence of unpredictable uncooperative nodes.
- **Mobile devices resources.** Low processor power, short amount of Random Access Memory (RAM), short battery life, and devices storage can present limitations to nodes cooperation. These issues definitively affect the node behavior and can induce selfishness.
- **Node heterogeneity.** Network nodes can have different hardware and/or software specifications. Therefore, cooperation schemes must assume the need to adapt and normalize node communication to achieve an optimal cooperation.
- **Fault-tolerance disconnection.** In mobility environments, communication fault/disconnections often occur during a relay situation. Therefore, it is necessary to identify the fault, recover the original message, and retransmit from the original node to the destination node. However, this assumption might not be always possible in a mobile scenario, being required to decide a new route for the request.

The creation and deployment of cooperation systems taking into account all the above-mentioned aspects is a key issue. Cooperation-based approaches should always consider an optimal quality of service (QoS) and quality of experience (QoE) with potential gains or without compromising or deteriorating the network performance.

Cooperative schemes in MANETs are usually divided in two types of approaches: credit based approaches and reputation-based approaches. As above-presented, reputation-based schemes have additional worrying issues in comparison with credit-based approaches [40], [46], [100]. In reputation-based systems nodes can more easily form communities/groups with faulty intentions to maximize their utility and, therefore, gain more reputation. Furthermore, the reliance of these schemes on wireless broadcast approaches is another weakness. Credit-based schemes are more reliable in these aspects, however, these schemes are always confronted with node's faulty or cheating behaviors. One weakness of these approaches comes from the fact that they often rely on tamper-proof hardware to assure security payments adding more complexity to the cooperative system. Although, several works tried to discard the hardware and credit-based approaches have more security complexity and issues in comparison to reputation-based approaches.

In DTNs, cooperative incentive based approaches are extraordinarily challenging due to these networks characteristics. Typical MANETs cooperation incentive-based schemes are not suitable for DTNs, mainly for two reasons: in DTNs the end-to-end path between source and the destination is unknown before data forwarding; and flooding or multi-copy forwarding is adopted often. Moreover, DTN reputation-based schemes face the fact that data forwarding cannot be observed during the store-carry-and-forward process. Efficiently node reputation propagation through the network is also another challenging issue. DTN credit-based incentive schemes regulate the store-carry-and-forward process and packet-forwarding through some form of virtual currency. However, the above-mentioned security issues are the same and in a DTN scenario it is more complex to solve due to the big lack of network infrastructures and device resources.

Cooperation based-approaches also aims a better efficiency and performance of mobile devices (for example, device battery, storage, and network). There are several network architectures that are supported by mobile devices, such as, general industry services where agents must cooperate and share information through mobile devices and Healthcare services where mobile health (m-Health) apps share medical information with patients and physicians. In these scenarios, especially in healthcare, cooperation between applications is a challenge that needs a more comprehensive study.

VI. Conclusion

Cooperation strategies have been proposed as a solution to unstable network infrastructures where mobile nodes cooperate with each other forwarding data and performing all networking functions. This paper elaborates a deep literature review on cooperation based approaches focusing on MANETs and DTNs. This study considered cooperative incentive-based schemes but also includes significant and important proposals on cooperative game theory based approaches. Furthermore,

this paper presented a discussion and open-issues of the above surveyed works presenting and discussing the main challenges, merits and weaknesses in the construction and design of cooperative solutions for MANETs and DTNs.

ACKNOWLEDGMENTS

This work has been partially supported by *Instituto de Telecomunicações*, Next Generation Networks and Applications Group (NetGNA), Covilhã Delegation, by Government of Russian Federation, Grant 074-U01, by National Funding from the FCT - *Fundação para a Ciência e a Tecnologia* in the scope of R&D Unit 50008, financed by the applicable financial framework (FCT/MEC through national funds and when applicable co- funded by FEDER - PT2020 partnership agreement), and by the AAL4ALL Project (Ambient Assisted Living for All), project co-financed by the European Community Fund (FEDER) through COMPETE - *Programa Operacional Factores de Competitividade*.

REFERENCES

[1] W. Jianping, L. Hewu, S. Wenqi, W. Qian, J. Zhuo, and Z. Wei, "Technology trends and architecture research for future mobile internet," *IEEE China Communications*, vol. 10, no. 6, pp. 14–27, June 2013.

[2] D. Raychaudhuri and N. B. Mandayam, "Frontiers of wireless and mobile communications," *Proceedings of the IEEE*, vol. 100, no. 4, pp. 824–840, April 2012.

[3] S. Corson and J. Macker, "Mobile Ad-hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC: 2501, 1999.

[4] N. Rama Suri, Y. Narahari, and D. Manjunath, "An efficient pricing based protocol for broadcasting in wireless ad hoc networks," in *Communication System Software and Middleware, 2006. Comsware 2006. First International Conference on*, 2006, pp. 1–7.

[5] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss, "Delay-Tolerant Networking Architecture," RFC 4838, April 2007.

[6] A. Bogliolo, P. Polidori, A. Aldini, W. Moreira, P. Mendes, M. Yildiz, C. Ballester, and J. Seigneur, "Virtual currency and reputation-based cooperation incentives in user-centric networks," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International*, Aug 2012, pp. 895–900.

[7] A. Aldini and A. Bogliolo, *User-Centric Networking: Future Perspectives*. Springer Publishing Company, Incorporated, 2014.

[8] M. Yildiz, M. Khan, F. Sivrikaya, and S. Albayrak, "Cooperation incentives based load balancing in ucn: A probabilistic approach," in *Global Communications Conference (GLOBECOM), 2012 IEEE*, Dec 2012, pp. 2746–2752.

[9] A. Fernandes, E. Kotsovinos, S. string, and B. Dragovic, "Pinocchio: Incentives for honest participation in distributed trust management," in *Trust Management*, ser. Lecture Notes in Computer Science, C. Jensen, S. Poslad, and T. Dimitrakos, Eds. Springer Berlin Heidelberg, 2004, vol. 2995, pp. 63–77.

[10] Y. Zhang, L. Lin, and J. Huai, "Balancing trust and incentive in peer-to-peer collaborative system." *I. J. Network Security*, vol. 5, no. 1, pp. 73–81, 2007.

[11] M. Yang, Q. Feng, Y. Dai, and Z. Zhang, "A multi-dimensional reputation system combined with trust and incentive mechanisms in p2p file sharing systems." in *ICDCS Workshops*. IEEE Computer Society, 2007, p. 29.

[12] L. Buttyán and J.-P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad hoc Networks," *Mobile Networks and Applications*, vol. 8, pp. 579–592, 2003.

[13] G. Kramer, I. Maric, and R. D. Yates, *Cooperative communications (Foundations and Trends in Networking)*. Now Publishers Inc., June 2007.

[14] Y. Li, X. Zhu, and W. Zhao, "Cooperation mode selection for maximizing throughput in wireless networks," in *Wireless and Optical Communications Networks (WOCN), 2011 Eighth International Conference on*, May 2011, pp. 1–5.

[15] L. Al-Kanj and Z. Dawy, "Optimized energy efficient content distribution over wireless networks with mobile-to-mobile cooperation," in *Telecommunications (ICT), 2010 IEEE 17th International Conference on*, April 2010, pp. 471–475.

[16] L. Lai, K. Liu, and H. El-Gamal, "The three-node wireless network: achievable rates and cooperation strategies," *Information Theory, IEEE Transactions on*, vol. 52, no. 3, pp. 805–828, March 2006.

[17] S. Althunibat, G. Kibalya, and F. Granelli, "Energy-efficient network discovery mechanism by exploiting cooperation among terminals," in *Communications and Vehicular Technology in the Benelux (SCVT), 2012 IEEE 19th Symposium on*, Nov 2012, pp. 1–5.

[18] B. Sirkeci-Mergen and A. Scaglione, "On the power efficiency of cooperative broadcast in dense wireless networks," *Selected Areas in Communications, IEEE Journal on*, vol. 25, no. 2, pp. 497–507, February 2007.

[19] P. Liu, Z. Tao, Z. Lin, E. Erkip, and S. Panwar, "Cooperative wireless communications: a cross-layer approach," *Wireless Communications, IEEE*, vol. 13, no. 4, pp. 84–92, Aug 2006.

[20] G. Kramer, I. Marić, and R. D. Yates, "Cooperative communications," *Found. Trends Netw.*, vol. 1, no. 3, pp. 271–425, Aug. 2006. [Online]. Available: http://dx.doi.org/10.1561/1300000004

[21] M. Felegyhazi and J.-P. Hubaux, "Game theory in wiress networks: A tutorial," EPFL, Tech. Rep., 2007.

[22] D. E. Charilas and A. D. Panagopoulos, "A survey on game theory applications in wireless networks," *Comput. Netw.*, vol. 54, no. 18, pp. 3421–3430, Dec. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2010.06.020

[23] S. Wen, B. Hu, A. B. Rad, X. Li, H. Lu, and J. Zhang, "Robust nash dynamic game strategy for user cooperation energy efficiency in wireless cellular networks," *Mathematical Problems in Engineering*, vol. 2012, 2012.

[24] M. Kai, G. Xinping, and Z. Bin, "Symmetrical cooperative strategies in wireless networks: A cooperative game approach," in *Control Conference (CCC), 2010 29th Chinese*, July 2010, pp. 4175–4179.

[25] L. Gyarmati and T. A. Trinh, "Cooperative strategies of wireless access technologies: A game-theoretic analysis." *Pervasive and Mobile Computing*, vol. 7, no. 5, pp. 545–568, 2011. [Online]. Available: http://dblp.uni-trier.de/db/journals/percom/percom7.html#GyarmatiT11

[26] P. Zetterberg, C. Mavrokefalidis, A. S. Lalos, and E. Matigakis, "Experimental investigation of cooperative schemes on a real-time dsp-based testbed." *EURASIP J. Wireless Comm. and Networking*, vol. 2009, 2009. [Online]. Available: http://dblp.uni-trier.de/db/journals/ejwcn/ejwcn2009.html#ZetterbergMLM09

[27] P. Murphy, A. Sabharwal, and B. Aazhang, "On building a cooperative communication system: Testbed implementation and first results." *EURASIP J. Wireless Comm. and Networking*, vol. 2009, 2009. [Online]. Available: http://dblp.uni-trier.de/db/journals/ejwcn/ejwcn2009.html#MurphySA09

[28] T. Korakis, Z. Tao, S. R. Singh, P. Liu, and S. S. Panwar, "Implementation of a cooperative mac protocol: Performance and challenges in a real environment." *EURASIP J. Wireless Comm. and Networking*, vol. 2009, 2009. [Online]. Available: http://dblp.uni-trier.de/db/journals/ejwcn/ejwcn2009.html#KorakisTSLP09

[29] P. Liu, Z. Tao, S. Narayanan, T. Korakis, and S. S. Panwar, "Coopmac: A cooperative mac for wireless lans." *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 2, pp. 340–354, 2007. [Online]. Available: http://dblp.uni-trier.de/db/journals/jsac/jsac25.html#LiuTNKP07

[30] L. Cottatellucci, X. Mestre, E. G. Larsson, and A. Ribeiro, "Cooperative communications in wireless networks." *EURASIP J. Wireless Comm. and Networking*, vol. 2009, 2009. [Online]. Available: http://dblp.uni-trier.de/db/journals/ejwcn/ejwcn2009.html#CottatelluccMLR09

[31] D. Skraparlis, V. K. Sakarellos, A. D. Panagopoulos, and J. D. Kanellopoulos, "Outage performance analysis of cooperative diversity with mrc and sc in correlated lognormal channels," *EURASIP J. Wirel. Commun. Netw.*, vol. 2009, pp. 5:1–5:7, Feb. 2009. [Online]. Available: http://dx.doi.org/10.1155/2009/707839

[32] L. Vandendorpe, J. Louveaux, O. Oguz, and A. Zaidi, "Rate-optimized power allocation for df-relayed ofdm transmission under sum and individual power constraints." *EURASIP J. Wireless Comm. and Networking*, vol. 2009, 2009. [Online]. Available: http://dblp.uni-trier.de/db/journals/ejwcn/ejwcn2009.html#VandendorpeLOZ09

[33] Ö. Oruç and Ü. Aygölü, "M-psk cooperative trellis codes for coordinate interleaved coded cooperation." *EURASIP J. Wireless Comm. and Networking*, vol. 2009, 2009. [Online]. Available: http://dblp.uni-trier.de/db/journals/ejwcn/ejwcn2009.html#OrucA09

[34] R. Vaze and R. W. H. Jr., "End-to-end joint antenna selection strategy and distributed compress and forward strategy for relay channels," *CoRR*, vol. abs/0905.2098, 2009. [Online]. Available: http://dblp.uni-trier.de/db/journals/corr/corr0905.html#abs-0905-2098

[35] S. Corson and J. Macker, "Mobile ad hoc networking (manet): Routing protocol performance issues and evaluation considerations," United States, 1999.

[36] J. Hu and M. Burmester, "Cooperation in mobile ad hoc networks," in *Guide to Wireless Ad Hoc Networks*, ser. Computer Communications and Networks, S. Misra, I. Woungang, and S. Chandra Misra, Eds. Springer London, 2009, pp. 43–57. [Online]. Available: http://dx.doi.org/10.1007/978-1-84800-328-6_3

[37] M. H. L. Froushani, B. Khalaj, and S. Vakilinia, "A novel approach to incentive-based cooperation in wireless ad hoc networks," in *18th International Conference on Telecommunications (ICT)*, May 2011, pp. 78–83.

[38] H. Shen and Z. Li, "Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 8, pp. 1287–1303, 2012.

[39] L. Buttyán and J.-P. Hubaux, "Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks," Tech. Rep., 2001.

[40] S. Zhong, J. Chen, and Y. Yang, "Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 3, March 2003, pp. 1987–1997 vol.3.

[41] M. Jakobsson, J.-P. Hubaux, and L. Buttyán, "A micropayment scheme encouraging collaboration in multi-hop cellular networks," in *Proc. Int'l Financial Cryptograph Conf.*, 2003.

[42] L. Buttyan and J.-P. Hubaux, "Enforcing service availability in mobile ad-hoc wans," in *Mobile and Ad Hoc Networking and Computing, 2000. MobiHOC. 2000 First Annual Workshop on*, 2000, pp. 87–96.

[43] L. Buttyán and J.-P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," *ACM Mob. Netw. Appl.*, vol. 8, no. 5, pp. 579–592, Oct. 2003. [Online]. Available: http://dx.doi.org/10.1023/A:1025146013151

[44] J. Crowcroft, R. Gibbens, F. Kelly, and S. Östring, "Modelling incentives for collaboration in mobile ad hoc networks," *Perform. Eval.*, vol. 57, no. 4, pp. 427–439, Aug. 2004. [Online]. Available: http://dx.doi.org/10.1016/j.peva.2004.03.003

[45] L. Anderegg and S. Eidenbenz, "Ad hoc-vcg: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents," in *Proc. ACM MobiCom*, 2003, pp. 245–259.

[46] H. Janzadeh, K. Fayazbakhsh, M. Dehghan, and M. S. Fallah, "A secure credit-based cooperation stimulating mechanism for manets using hash chains," *Future Gener. Comput. Syst.*, vol. 25, no. 8, pp. 926–934, Sep. 2009. [Online]. Available: http://dx.doi.org/10.1016/j.future.2008.12.002

[47] B. Raghavan and A. C. Snoeren, "Priority forwarding in ad hoc networks with self-interested parties," in *In Workshop on Economics of Peer-to-Peer Systems*, 2003.

[48] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decis. Support Syst.*, vol. 43, no. 2, pp. 618–644, Mar. 2007.

[49] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '00. New York, NY, USA: ACM, 2000, pp. 255–265. [Online]. Available: http://doi.acm.org/10.1145/345910.345955

[50] D. B. Johnson, D. A. Maltz, and J. Broch, "Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks," in *In Ad Hoc Networking, edited by Charles E. Perkins, Chapter 5*. Addison-Wesley, 2001, pp. 139–172.

[51] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking &Amp; Computing*, ser. MobiHoc '02. New York, NY, USA: ACM, 2002, pp. 226–236. [Online]. Available: http://doi.acm.org/10.1145/513800.513828

[52] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security*. Deventer, The Netherlands, The Netherlands: Kluwer, B.V., 2002, pp. 107–121. [Online]. Available: http://dl.acm.org/citation.cfm?id=647802.737297

[53] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," *CoRR*, vol. cs.NI/0307012, 2003. [Online]. Available: http://dblp.uni-trier.de/db/journals/corr/corr0307.html#cs-NI-0307012

[54] Q. He, D. Wu, and P. Khosla, "Sori: a secure and objective reputation-based incentive scheme for ad-hoc networks," in *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE*, vol. 2, March 2004, pp. 825–830 Vol.2.

[55] J. J. Jaramillo and R. Srikant, "Darwin: Distributed and adaptive reputation mechanism for wireless ad-hoc networks," in *Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '07. New York, NY, USA: ACM, 2007, pp. 87–98. [Online]. Available: http://doi.acm.org/10.1145/1287853.1287865

[56] F. Milan, J. J. Jaramillo, and R. Srikant, "Achieving cooperation in multihop wireless networks of selfish nodes," in *Proceeding from the 2006 Workshop on Game Theory for Communications and Networks*, ser. GameNets '06. New York, NY, USA: ACM, 2006. [Online]. Available: http://doi.acm.org/10.1145/1190195.1190197

[57] R. Axelrod, "Effective Choice in the Prisoner's Dilemma," *Journal of Conflict Resolution*, vol. 24, no. 1, pp. 3–25, Mar. 1980. [Online]. Available: http://dx.doi.org/10.1177/002200278002400101

[58] J. Hu and M. Burmester, "Lars: A locally aware reputation system for mobile ad hoc networks," in *Proceedings of the 44th Annual Southeast Regional Conference*, ser. ACM-SE 44. New York, NY, USA: ACM, 2006, pp. 119–123. [Online]. Available: http://doi.acm.org/10.1145/1185448.1185475

[59] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in manets." *IEEE Trans. Mob. Comput.*, vol. 6, no. 5, pp. 536–550, 2007. [Online]. Available: http://dblp.uni-trier.de/db/journals/tmc/tmc6.html#LiuDVB07

[60] Y. Luo and R. Deters, "Using cooperation to improve the experience of mobile web services consumers," in *Services Computing Conference, 2009. APSCC 2009. IEEE Asia-Pacific*, Dec 2009, pp. 213–218.

[61] J.-W. Yoo and K. H. Park, "A cooperative clustering protocol for energy saving of mobile devices with wlan and bluetooth interfaces," *IEEE Transactions on Mobile Computing*, vol. 10, no. 4, pp. 491–504, Apr. 2011. [Online]. Available: http://dx.doi.org/10.1109/TMC.2010.161

[62] A. A. Khalek and Z. Dawy, "Energy-efficient cooperative video distribution with statistical qos provisions over wireless networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 7, pp. 1223–1236, 2012.

[63] H.-C. Lu and W. Liao, "Cooperative strategies in wireless relay networks," *Selected Areas in Communications, IEEE Journal on*, vol. 30, no. 2, pp. 323–330, February 2012.

[64] N. Patwari, J. Ash, S. Kyperountas, A. Hero, R. Moses, and N. Correal, "Locating the nodes: cooperative localization in wireless sensor networks," *Signal Processing Magazine, IEEE*, vol. 22, no. 4, pp. 54–69, July 2005.

[65] Y. Shen, H. Wymeersch, and M. Z. Win, "Fundamental limits of wideband localization - part ii: Cooperative networks," *CoRR*, vol. abs/1006.0890, 2010. [Online]. Available: http://dblp.uni-trier.de/db/journals/corr/corr1006.html#abs-1006-0890

[66] U. Khan, S. Kar, and J. Moura, "Distributed sensor localization in random environments using minimal number of anchor nodes," *Signal Processing, IEEE Transactions on*, vol. 57, no. 5, pp. 2000–2016, May 2009.

[67] M. Win, A. Conti, S. Mazuelas, Y. Shen, W. Gifford, D. Dardari, and M. Chiani, "Network localization and navigation via cooperation," *Communications Magazine, IEEE*, vol. 49, no. 5, pp. 56–62, May 2011.

[68] C. Sammarco, F. Fitzek, G. Perrucci, A. Iera, and A. Molinaro, "Localization information retrieval exploiting cooperation among mobile devices," in *Communications Workshops, 2008. ICC Workshops '08. IEEE International Conference on*, May 2008, pp. 149–153.

[69] Google, "Google maps api." [Online]. Available: https://developers.google.com/maps/

[70] H. Wymeersch, J. Lien, and M. Win, "Cooperative localization in wireless networks," *Proceedings of the IEEE*, vol. 97, no. 2, pp. 427–450, Feb 2009.

[71] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss, "Delay-Tolerant Networking Architecture," RFC 4838 (Informational), Internet Engineering Task Force, April 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4838.txt

[72] T. Spyropoulos, K. Psounis, and C. Raghavendra, "Single-copy routing in intermittently connected mobile networks," in *Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First*

Annual IEEE Communications Society Conference on, Oct 2004, pp. 235–244.

[73] J. Byers and G. Nasser, "Utility-based decision-making in wireless sensor networks," in *Mobile and Ad Hoc Networking and Computing, 2000. MobiHOC. 2000 First Annual Workshop on*, 2000, pp. 143–144.

[74] A. Vahdat and D. Becker, "Epidemic Routing for Partially Connected Ad Hoc Networks," 2000. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.34.6151

[75] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: An efficient routing scheme for intermittently connected mobile networks," in *Proceedings of the 2005 ACM SIGCOMM Workshop on Delay-tolerant Networking*, ser. WDTN '05. New York, NY, USA: ACM, 2005, pp. 252–259. [Online]. Available: http://doi.acm.org/10.1145/1080139.1080143

[76] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for vehicle-based disruption-tolerant networks," in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, April 2006, pp. 1–11.

[77] A. Balasubramanian, B. Levine, and A. Venkataramani, "Dtn routing as a resource allocation problem," *SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 4, pp. 373–384, Aug. 2007. [Online]. Available: http://doi.acm.org/10.1145/1282427.1282422

[78] V. N. G. J. Soares and J. J. P. C. Rodrigues, *Cooperative Networking*. Wiley, 2011, ch. Cooperation in DTN-Based Network Architectures, pp. 101–115.

[79] N. Magaia, P. Rogerio Pereira, and M. Correia, "Selfish and malicious behavior in delay-tolerant networks," in *Future Network and Mobile Summit (FutureNetworkSummit), 2013*, July 2013, pp. 1–10.

[80] A. Panagakis, A. Vaios, and I. Stavrakakis, "On the effects of cooperation in dtns," in *Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd International Conference on*, Jan 2007, pp. 1–6.

[81] U. Shevade, H. H. Song, L. Qiu, and Y. Zhang, "Incentive-aware routing in dtns," in *Network Protocols, 2008. ICNP 2008. IEEE International Conference on*, Oct 2008, pp. 238–247.

[82] J. Pozo, O. Trullols, J. Barcelo, and J. Vidal, "A cooperative arq for delay-tolerant vehicular networks," in *Distributed Computing Systems Workshops, 2008. ICDCS '08. 28th International Conference on*, June 2008, pp. 192–197.

[83] L. Yin, H. mei Lu, Y.-D. Cao, and J. min Gao, "Cooperation in delay tolerant networks," in *Signal Processing Systems (ICSPS), 2010 2nd International Conference on*, vol. 1, July 2010, pp. V1–202–V1–205.

[84] A. Lindgren, A. Doria, and O. Schelén, "Probabilistic routing in intermittently connected networks," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 7, no. 3, pp. 19–20, Jul. 2003. [Online]. Available: http://doi.acm.org/10.1145/961268.961272

[85] A. Keränen, J. Ott, and T. Kärkkäinen, "The one simulator for dtn protocol evaluation," in *Proceedings of the 2Nd International Conference on Simulation Tools and Techniques*, ser. Simutools '09. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009, pp. 55:1–55:10. [Online]. Available: http://dx.doi.org/10.4108/ICST.SIMUTOOLS2009.5674

[86] K. Chen and H. Shen, "Multicent: A multifunctional incentive scheme adaptive to diverse performance objectives for dtn routing," in *Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2013 10th Annual IEEE Communications Society Conference on*, June 2013, pp. 532–540.

[87] D. Niyato, P. Wang, W. Saad, and A. Hjorungnes, "Coalition formation games for improving data delivery in delay tolerant networks," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, Dec 2010, pp. 1–5.

[88] O. Helgason, F. Legendre, V. Lenders, M. May, and G. Karlsson, "Performance of opportunistic content distribution under different levels of cooperation," in *Wireless Conference (EW), 2010 European*, April 2010, pp. 903–910.

[89] B. Chen and M. C. Chan, "Mobicent: a credit-based incentive system for disruption tolerant network," in *INFOCOM, 2010 Proceedings IEEE*, March 2010, pp. 1–9.

[90] C. Liu, J. Wu, X. Guan, and L. Chen, "Cooperative file sharing in hybrid delay tolerant networks," in *Proceedings of the 2011 31st International Conference on Distributed Computing Systems Workshops*, ser. ICDCSW '11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 339–344. [Online]. Available: http://dx.doi.org/10.1109/ICDCSW.2011.68

[91] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "Smart: A secure multilayer credit-based incentive scheme for delay-tolerant networks," *Vehicular Technology, IEEE Transactions on*, vol. 58, no. 8, pp. 4628–4639, Oct 2009.

[92] K. Srinivasan, S. Rajkumar, and P. Ramanathan, "Incentive schemes for data collaboration in disruption tolerant networks," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, Dec 2010, pp. 1–5.

[93] X. Zhang, X. Wang, A. Liu, Q. Zhang, and C. Tang, "Cooperation enforcement scheme based on reputation for delay tolerant networks," in *Computer Science and Network Technology (ICCSNT), 2011 International Conference on*, vol. 4, Dec 2011, pp. 2372–2376.

[94] M. Karaliopoulos, "Assessing the vulnerability of dtn data relaying schemes to node selfishness," *Communications Letters, IEEE*, vol. 13, no. 12, pp. 923–925, December 2009.

[95] L. Wei, H. Zhu, Z. Cao, and X. S. Shen, "Mobiid: A user-centric and social-aware reputation based incentive scheme for delay/disruption tolerant networks." in *ADHOC-NOW*, ser. Lecture Notes in Computer Science, H. Frey, X. Li, and S. Rhrup, Eds., vol. 6811. Springer, 2011, pp. 177–190. [Online]. Available: http://dblp.uni-trier.de/db/conf/adhoc-now/adhoc-now2011.html#WeiZCS11

[96] A. Mei and J. Stefa, "Give2get: Forwarding in social mobile wireless networks of selfish individuals," in *Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on*, June 2010, pp. 488–497.

[97] D. Zhang, M. Li, and L. Hu, "Challenges to mobile ad hoc cooperation design," in *Computer Supported Cooperative Work in Design, 2004. Proceedings. The 8th International Conference on*, vol. 1, May 2004, pp. 517–520 Vol.1.

[98] M. Dohler and Y. Li, *Cooperative Communications: Hardware, Channel and PHY*. Wiley, 2010. [Online]. Available: http://books.google.pt/books?id=YWj0PrnD78AC

[99] A. Hinze and G. Buchanan, "The challenge of creating cooperating mobile services: Experiences and lessons learned," in *Proceedings of the 29th Australasian Computer Science Conference - Volume 48*, ser. ACSC '06. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2006, pp. 207–215. [Online]. Available: http://dl.acm.org/citation.cfm?id=1151699.1151723

[100] M. Stemm and R. H. Katz, "Vertical handoffs in wireless overlay networks," *Mob. Netw. Appl.*, vol. 3, no. 4, pp. 335–350, Dec. 1998. [Online]. Available: http://dx.doi.org/10.1023/A:1019197320544

Bruno M. C. Silva received his BsC degree (licentiate) in 2008 in Informatics Engineering from University of Beira Interior. In 2010 he received his MsC degree in Informatics Engineering from University of Beira Interior. He is currently a PhD student on Informatics Engineering at the University of Beira Interior under supervision of Prof. Joel J. P. C. Rodrigues. He is also a PhD student member of the Instituto de Telecomunicações, Portugal. His current research areas are Delay Tolerant Networks, Vehicular Networks, Mobile Computing, Ubiquitous Computing, e-Health but especially in mobile Health. He authors or co-authors 12 international conference papers and 4 International Journal publications.

Chapter 4

A Novel Cooperation Strategy for Mobile Health Applications

This chapter consists of the following article:

A Novel Cooperation Strategy for Mobile Health Applications

Bruno M. C. Silva, Joel J. P. C. Rodrigues, Ivo M. C. Lopes, Tiago M. F. Machado, and Liang Zhou

IEEE Journal on Selected Areas in Communtications, 31(9): Article 3, 28-36, 2013.

DOI: dx.doi.org/10.1109/JSAC.2013.SUP.0513003

Receive the 2013 Best Paper Award of the IEEE Communications Society, Thecnical Committe on e-Health

According to 2013 Journal Citation Reports published by Thomson Reuters in 2014, this journal scored ISI journal performance metrics as follows:

ISI Impact Factor (2013): 4.138

ISI Article InfluenceScore (2013): 2.395

Journal Ranking (2013): 14/247 (Engineering, Electrical & Electronic)

Journal Ranking (2013): 4/78 (Telecommunications)

28 IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS/SUPPLEMENT, VOL. 31, NO. 9, SEPTEMBER 2013

A Novel Cooperation Strategy for Mobile Health Applications

Bruno M. C. Silva, Joel J. P. C. Rodrigues, *Senior Member, IEEE,*
Ivo M. C. Lopes, Tiago M. F. Machado, and Liang Zhou, *Member, IEEE*

***Abstract*—Mobile Health (m-Health) systems include the use of mobile devices and applications that interact with patients and caretakers. However, mobile devices have several constraints (such as, processor, energy, and storage resource limitations), affecting the quality of service and user experience. This paper proposes a novel cooperation strategy for m-Health services and applications. This contribution addresses two related limitations to m-Health applications with service-oriented architectures, namely the network infrastructure and Internet connectivity dependency. It follows a reputation-based approach as an incentive method for cooperation, which includes a Web service to manage all the network cooperation. It is responsible for verifying the cooperation status of neighbor nodes and to provide relay nodes the required data in order to perform a full data request. A performance evaluation study in a real scenario is presented, using an available m-Health application, called SapoFit. For performance evaluation purposes, an analytical model is also considered in order to compare the obtained experiment results. It is clearly shown that referred dependencies are relevantly decreased, providing mobile nodes without Internet connectivity a free of charge and suitable alternative to access its remotely stored health information. It also improves the service delivery probability while increasing the overall network throughput.**

***Index Terms*—Mobile health; m-health; mobile computing; e-health; cooperation**

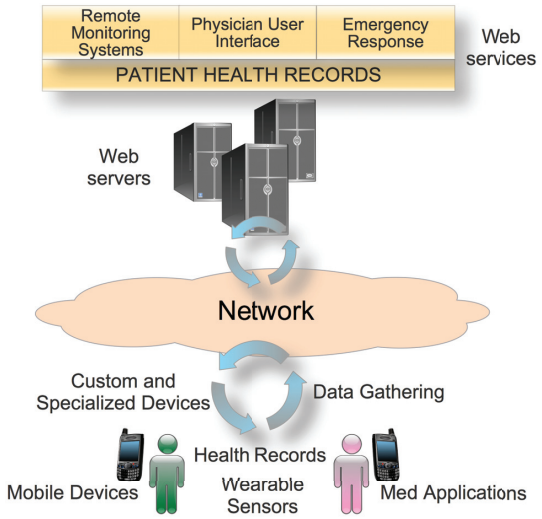


Fig. 1. Illustration of an m-Health application framework based on Web services.

I. Introduction

MOBILE health (m-Health) is considered the strongest contribution for the next generation e-Health systems and it is already changing typical healthcare services [1], [2]. The study and development of m-Health services and applications have been an important point of attention in the last years. Several research topics related to health have gathered important findings and contributions from m-Health, such as, cardiology [3], [4], [5], diabetes [6], [7] obesity [8], [9], [10], smoking cessation [11], among others. In the above-mentioned medical issues, m-Health applications are applied for health monitoring, diseases prevention and detection, and, in more advanced services, also provides basic diagnosis. M-Health services are also becoming popular in developing countries [12], [13], where healthcare facilities are frequently remote and inaccessible. Figure 1 illustrates a typical m-Health service architecture supported by Web services (WS). These WS are hosted on Web servers and can be used through network connectivity, including the Internet. Caretakers use several devices and technologies, such as mobile devices, sensors, and specialized health devices.

Architectures based on mobile devices and wireless communications presents several challenged issues and constraints, such as, battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, and network delays. In this sense, cooperation-based approaches are presented as a solution to solve such limitations, focusing on increasing network connectivity, communication rates, and reliability. Cooperation is an important research topic that has been growing in recent years. With the advent of wireless networks, several recent studies present cooperation mechanisms and algorithms as a solution to improve wireless networks performance [14]. In the absence of a stable network infrastructure, mobile nodes cooperate with each other performing all networking functionalities. For example, it can support intermediate nodes forwarding packets between two distant nodes [15]. To the best of our knowledge, there are no cooperative solutions for m-Health services and applications. However, cooperative work in the mobile e-Health context has been studied concluding that through cooperation health-care

Manuscript received February 15, 2012; revised July 14, 2012.

B. M. C. Silva, J. J. P. C. Rodrigues, I. M. C. Lopes, and T. M. F. Machado are with the Instituto de Telecomunicações, University of Beira Interior, Covilhã, Portugal (e-mail: {bruno.silva, ivo.lopes, tiago.machado}@it.ubi.pt, joeljr@ieee.org).

L. Zhou is with the Nanjing University of Posts and Telecommunications, Nanjing, China (e-mail: liang.zhou@ieee.org).

Digital Object Identifier 10.1109/JSAC.2013.SUP.0513003

professionals can improve their work. Computer-supported cooperative work (CSCW) is typically associated to tasks from e-Mail and instant messaging to wireless information sharing through broadband and telecommunication networks [16]. In healthcare context, CSCW enables patients and health professionals for working together especially from remote locations [17], [18].

This paper proposes a novel cooperation strategy for m-Health applications focusing on forwarding and retrieving data to/from nodes that have no direct connection to an m-Health application. In this sense, devices without Internet connection can use m-Health applications without problems. This cooperation approach presents a reputation-based strategy where a Web service manages the access control and the cooperation among nodes along with their reputation. It considers three main components: a *node control message*, a r*equester control message*, and a *cooperative Web service* (CWS). Both control messages are used to manage a local cooperation between two or more nodes. The CWS includes a reputation table for all the nodes and decides which nodes can have access to the requested services. The performance assessment and validation of the proposal is also considered. It proves the feasibility of this approach and also studies the impact of the cooperation strategy on the performance of an m-Health application taking into account different number of uncooperative nodes. The cooperation proposal is deployed and evaluated in an m-Health application for obesity prevention and control, called *SapoFit* [19], [20], [21]. Results show that mobile nodes without Internet connectivity can use the application continuously with success. It also shows the improvement of the service delivery probability and service average delay, increasing the overall network performance.

The remainder of this paper is organized as follows. Section II elaborates on related work about the topic focusing on cooperation techniques that contribute to the proposed cooperation solution, including wireless, mobile ad-hoc, and delay-tolerant networks (DTNs). Section III describes the proposed m-Health cooperation strategy, while its performance evaluation and validation through a prototype with an m-Health application is presented in Section IV. This section also includes an analytical model and these results are compared with those from the real experiments. Finally, Section V concludes the paper and points out further research works.

II. Related Work

Cooperative mechanisms have proven to be a promising solution for several network constraints in wireless networks and important solutions have been presented in the literature [22], [23], [24], [25]. Due to the overall characteristics of m-Health architectures, this study mainly focuses on wireless and mobile ad-hoc networks (MANETs). The delay tolerant network (DTN) paradigm is also considered to solve network disconnection problems. The proposed solution for m-Health applications gathered contributions from these available approaches.

A. Cooperation in wireless and mobile ad-hoc networks

Energy saving is a major concern in the context of wireless networks with limited energy resources. Al-Kanj and Dawy [26] present an optimized energy efficient content distribution and cooperation strategy for wireless ad-hoc networks. This proposal assents on a centralized base station that manages all network optimizations and minimizes energy consumptions of mobile terminals. At the same time, this cooperation strategy guaranties a quality of service (QoS) level where mobile terminals can either use unicast or multicast to receive content from the base station. Luo and Deters [27] investigate the use of cooperation on mobile Web services consumers. The authors propose a cooperation approach to improve the responsiveness of the Web service to mobile clients. This proposal includes two proxies to support cooperation. The server-proxy helps the server to improve the responsiveness. The client-proxy also benefits mobile clients to cooperate with the service provider by sharing workflow for pre-processing. Furthermore, to improve the performance of the mobile client a simple caching component and a prediction model are also included.

In a MANET [28] it is typically assumed that all network nodes must cooperate. Without cooperation no packet can be forwarded or route can be established [29]. However, neither all the nodes forward other nodes messages - called *uncooperative nodes*. Uncooperative nodes can be *faulty* or *malicious*, or/and *selfish*. *Faulty* or *malicious* nodes cannot follow a protocol or can be intentionally malicious to the network. *Selfish* nodes are non-cooperative in several or specific network operations [30]. Several cooperation schemes have been proposed for stimulate cooperation and mitigate the detrimental effect of non-cooperative nodes. Basically, two types of strategies are classified, *virtual currency based schemes* and *reputation based schemes*.

Virtual currency schemes use incentives to enforce nodes cooperation. These incentives are often given to nodes that cooperate and, then, use these incentives to gain privileged services from the network. Non-cooperative nodes that have no incentives will not get any service from the network. Virtual currency schemes assume that forwarding a message incurs in a cost to a node. Therefore, a non-cooperative node needs an incentive in order to forward messages of other nodes. *Nuglets* [31] and *Sprite* [32] are examples of popular systems that use virtual currency schemes. These systems use virtual payments to incentive nodes to forward messages and the payment is deducted from the sender or destination node.

Reputation schemes use the node reputation to diminish selfish behavior. All network nodes maintain the reputation of other nodes. Reputation is assessed by neighbor monitoring/observation or the exchange of reputation messages between nodes. Two popular reputation based schemes are the following: CONFIDANT [33] and CORE [34]. CONFIDANT detects and isolates non-cooperative nodes, compelling them to cooperate. Through passive observation nodes know all the packets within a single-hop neighbor node. CONFIDANT scheme assents on four components per node: a *monitor*, where nodes locally monitor deviating behavior; a *trust manager* that makes decisions about providing or accepting route information; a *reputation system* that is basically the node reputation rating; and a *path manager* that according to the reputation system defining the paths to avoid malicious nodes.

CORE scheme uses collaborative monitoring and reputation

mechanisms to stimulate cooperation among nodes. Basically, nodes that have a good reputation can use network services while nodes with a bad reputation, due to non-cooperative behaviors, do not have access to network services. For calculating a node reputation value, CORE defines three types of reputation: *subjective reputation*, calculated based on direct observation; *indirect reputation* which is calculated according to a second hand of information given by other nodes; and *functional reputation* that is calculated through a function that uses a weight in function of its importance.

B. Delay Tolerant Networks Paradigm and Cooperation techniques

In a delay tolerant network (DTN) [35] scenario, network constraints (such as, limited storage capacity, limited network bandwidth, and limited energy) affect the network performance. Furthermore, the performance of a DTN is also affected by long or variable propagation delays, low node density, low transmission reliability, node mobility, and disruption. In such scenarios, node cooperation is a key issue to success. Nodes can cooperate with each other storing and forwarding interested data for all the network nodes. DTN routing protocols usually assume a fully cooperative scenario. However, this is an unrealistic assumption. Nodes may not be able to always cooperate, due to resources limitations or even to a selfish behavior [36]. Therefore, several cooperation studies and proposals for DTNs have been presented and also offer contributions for the current proposal.

Shevade *et al.* [37] studies and demonstrates the degradation of a DTN performance due to selfish node behavior. The authors propose the use of practical and simple tit-for-tat (TFT) mechanism as an incentive strategy to stimulate cooperation. Through the TFT inclusion, the proposal assumes and guaranties that every node forwards as much traffic as possible for a neighbor node since the neighbor also forwards to it.

Morillo-Pozo et al. [38] proposes a cooperation scheme for DTNs based on the cooperative ARQ (C-ARQ). This cooperation proposal reduces data losses in transmissions between fixed access points placed along the roads and passing by vehicles that buffer all the data. Basically, in areas that vehicles have no connectivity to access points, vehicles cooperate between them to increase the data delivery rate.

The cooperation mechanism proposed in this paper gathered contributions from the above-described strategies in wireless, mobile ad-hoc, and delay tolerant networks.

III. Cooperation Strategy for Mobile Health Applications

This section describes, in detail, the cooperation approach for m-Health applications, specifically with service oriented architectures (SOAs) where Internet connectivity is required in order to fetch the information. Thus, this approach is suitable for mobile applications, and therefore, for mobile devices. It is based on two mobile modules and one remote module: i) the *node control message*, ii) the *requester control message* and iii) the *cooperative Web service* (CWS).

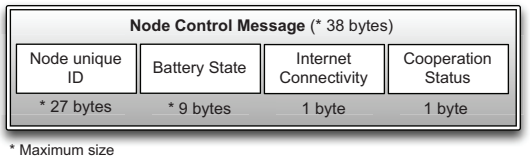


Fig. 2. Structure of the Node Control Message.

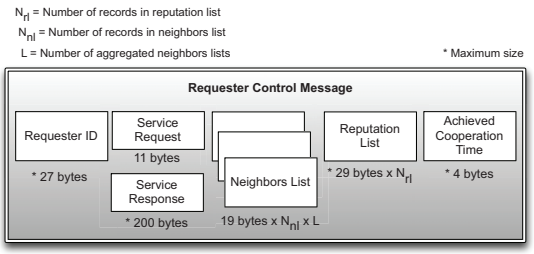


Fig. 3. Illustration of the Request Control Message.

A. Node Control Message (NCM)

Node Control Messages are sent from relay nodes to requester nodes and aim to provide an awareness of the relay node status, i.e., if the node is willing to cooperate and in what conditions. The structure of the node control message is presented in Figure 2.

The node control message contains the established node unique identifier, the battery state, the Internet connectivity status, and the cooperation status (i.e., if its cooperative or not). This status is achieved in the following manner: the application validates all the necessary requirements at application level in order to forward packets to other nodes. For instance, a third-party application, such as a Bluetooth firewall, can jeopardize the cooperation blocking Bluetooth communications. Thus, if a node connects to a relay node, which is publicly identified through its Bluetooth prefix name as mobile node with cooperation mechanisms, and does not receive any packets from it, it is assumed that the user is avoiding cooperation and therefore is considered as a selfish node.

B. Requester Control Message (RCM)

The requester control message is first sent by the initial requester node, and it comprises five main components: 1) **the requester ID**, the node unique identifier; 2) the **service request**, i.e., what the node is specifically requesting (e.g., the login token or its health profile); 3) the **neighbors list**; 4) the **reputation list**; and 5) the **achieved cooperation time** (ACT). An illustration of the RCM is presented at Figure 3. Its size can greatly change because it depends in the number of aggregated neighbors and reputation lists.

To prevent a request node to indefinitely wait for a request, it was defined a *maximum waiting period* (MWP). Therefore, when a node initiates a request and sends the requester control message, it will wait for the response until the MWP is lesser than 30 seconds. This value is defined in order to control the user quality of experience. When the MWP is achieved, the

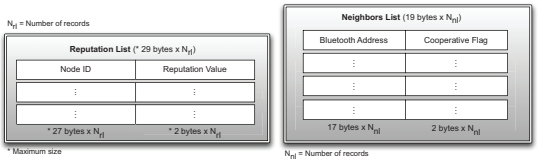


Fig. 4. Structure of the Reputation List and Neighbors List.

TABLE I
REPUTATION VALUE CALCULATION

Battery State	Internet Connectivity	Cooperation Status	Reputation Value
Critical	-	-	**-**
Poor	0	0	**0**
Poor	0	1	**+3**
Poor	1	0	**0**
Poor	1	1	**+3**
Regular	0	0	**-1**
Regular	0	1	**+2**
Regular	1	0	**-2**
Regular	1	1	**+2**
Excellent	0	0	**-2**
Excellent	0	1	**+1**
Excellent	1	0	**-3**
Excellent	1	1	**+1**

requester node cancels its request and starts searching and requesting cooperation to a different initial node. The ACT provides to all the nodes intervening in the cooperation process an awareness approach assuming they should stop cooperating and wasting resources finding a cooperative node with Internet connectivity.

In order to record relay nodes cooperative behavior, *reputation lists* (RLs) are used. The structure of the reputation list and neighbor list is presented in Figure 4.

The reputation list (RL) records are updated at every interaction with an intermediary node. They reside temporally in the mobile nodes side until its information is passed and updated definitely in the RL through the Web Service. The reputation value (RV) is calculated through a correlation of the relay node information received through the NCM, as may be seen in Table I.

The node status is based on its storage capacity and energy lifetime. A node has four types of status: *critical*, *poor*, *regular*, and *excellent*. While a node with a *critical* state of battery (below 15%) is neither compelled nor punished for non-cooperation, a node is *poor* when its available power energy is below 15%. The *regular* status occurs when its power energy is between 15% and 70%. A node has an *excellent* status when its available power energy is over 75%. The reputation value (R_v) ranges between -2 and +3. This interval is assumed to guarantee that non-cooperative nodes with a low number of nodes are punished. Cooperative nodes in a *poor* status have the highest R_v value (+3). The worst-case scenario for an uncooperative node is the one that is in *excellent* status with Internet connectivity and still refuses the cooperation. This node is punished with the worst R_v value (equal to -2).

When a node makes a request to another node, which does not have Internet connectivity, it is suitable that the intermediary node does not relay information and connects to a common neighbor of both, in order to achieve a better node discovery scope through Bluetooth. Also, when one or more malicious and uncooperative nodes are found during the request path, it is convenient that those nodes are avoided in the response packet route. Thus, *neighbors lists* (RLs), presented at Figure 4, are built before each request and sent within the *requester control message* in order to provide an awareness to the other relay nodes and a general perspective of the nodes in their proximities and their cooperative status.

C. Cooperative Web Service (CWS)

The proposed Web Service is responsible for performing a fair access control to data. Thus, according to the received reputation information, the Web Service holds the final reputation list in order to decide if a requester node should have access to the m-Health application Web service or not. The reputation list contains all registered network nodes with their identifier and their respective reputation value. The threshold value available at the reputation table for the node N is represented by R_v. When the WS receives reputation information upon a request, if performs its update, through $R_{v_{new}} = R_{v_{old}} + R_v$, where the initial R_v is equal to zero. The *reputation table* considers three status of reputation: *selfish*, *neutral*, or *cooperative*. As may be seen by the equation 1, these statuses are defined in order to provide a fair access to the Web Service, which truly considers the node cooperative behavior. Thus, an initial node with a reputation value equal to zero and, therefore, considered as *neutral*, can access directly the Web Service but cannot receive packets through cooperation. A *selfish* node with a negative value of reputation cannot access in any way to the information, being necessary to cooperate in order to reach a positive reputation value. Last, a *cooperative* node has full access to the WS. For networks with a small number of nodes it is extremely important that uncooperative nodes receive worst R_v, punishing and motivating them to cooperate.

$$Rep = \begin{cases} Selfish, R_v \in]-\infty, -1[\\ Neutral, R_v \in 0 \\ Cooperative, R_v \in [1, +\infty[\end{cases} \quad (1)$$

Figure 5 presents a multi-user interaction scenario for an m-Health application with the proposed cooperation approach. *User A* has network connection and cooperates, the status value is according to the battery status. *User B* has network connection and does not cooperate. Then, the status value will suffer a negative impact according with the battery status. *Users C* and *D* do not have network connectivity. *User C* queries *User A* for cooperation and receives a positive response and all the requested data. *User D* queries *User B* for cooperation and receives a negative response. Then, *User D* requests data from *User C* that sends it, getting positive status by cooperating.

A major concern in the proposal is the privacy issue of all forwarded and retrieved data. Privacy is a top priority

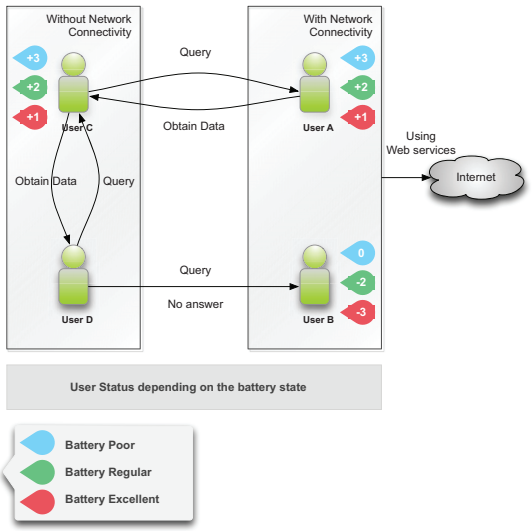


Fig. 5. Illustration of the interaction scenario for an m-Health application with the proposed cooperation approach for 4 users - *Users A* and *B* have network connectivity and *Users C* and *D* no.

issue in m-Health services and applications that deal with user sensitive information. On m-Health applications several security issues must be considered, such as, personal information management, secondary use of personal information, improper use of personal information, and errors with stored personal information. Therefore, cryptographic mechanisms can be seen as a solution to guarantied data confidentiality and protection [39], [40].

The presented cooperation strategy assumes secure data transactions among nodes using the Advanced Encryption Standard (AES) cipher algorithm used in Cipher Feedback Mode (CFB) with a key size of 128 bits [41]. This solution was used taking into account the common small computing power of mobile devices, the need for a relative lightweight cypher algorithm, and therefore keeping a good balance between performance and security.

IV. Performance Evaluation

This section focuses on the performance evaluation and validation of the m-Health cooperation approach proposed in this paper. Although the approach can be applied to mobile applications with different categories (e.g., social networking applications), and/or extended to other platforms, allowing cross-platform cooperation, it was chosen the Google Android Operating System. Besides the platform itself, hardware requirements comprise the Bluetooth hardware, Wi-Fi and/or GSM/CDMA data modules. First, the service-oriented m-Health application (*SapoFit*) and corresponding network scenario used to evaluate and demonstrate the solution is introduced. Afterwards, the system validation and results are discussed. The performance metrics used in the study are the *service requests delivery probability* and *service average delay*. These metrics are the network challenges that proposed approach tries to improve.

Fig. 6. Illustration of three activities of SapoFit with Login, Food Plans, and User Profile Screenshots.

A. SapoFit application

SapoFit is a weight control mobile application that allows users to keep track of weight in a healthier and more practical way. SapoFit allows users to control their weight, body mass index (BMI), basal metabolic rate (BMR), sports activity, and the possibility to follow food plans based on their needed calories. In this m-Health application all the users must be registered in a Web service. Figure 6 presents three activities screenshots of SapoFit application: *Login*, *Plans*, and *User Profile*. At the *Login* window the user enters his/her e-Mail address and corresponding password for authentication. After login, the application communicates with the Web service to obtain the personal user data (name, height, age, sex, weight, etc.). After loading all the data, they are displayed in a *Profile* window, which is the main window of SapoFit. At the *Plans* option, the calories factor that depends on the user target weight are presented. For the performance evaluation of the m-Health cooperation proposal, a user without Internet connection requesting access to the *Login* and *Plans* services is considered. Therefore, the user *Profile* will be fully obtained through cooperation among nodes.

B. M-Health network scenario

The real m-Health network scenario used for the performance evaluation study of the cooperative proposal may be seen in Figure 7. Nineteen (19) users use *SapoFit* with the embedded cooperation mechanisms. For illustration purposes, the figure only presents eight mobile nodes (using SapoFit), assuming that three of them are uncooperative nodes. Node M is the single node with connection to the SapoFit Web services. Although an m-Health scenario presents high node mobility, for evaluation purposes, it is assumed the node positioned according to the presented network scenario. The activity diagram of a mobile node (for a mobile device with *SapoFit*) and its cooperation mechanisms are presented in Figure 8. From the given figure, node *A* (without Internet connection) tries to login *SapoFit* server application (authenticating at the SapoFit Web service too). The application starts searching for neighbor nodes using Bluetooth connection. Afterwards, the requester node receives the *node control message* from each neighbor node. According to theses messages, the *cooperative*

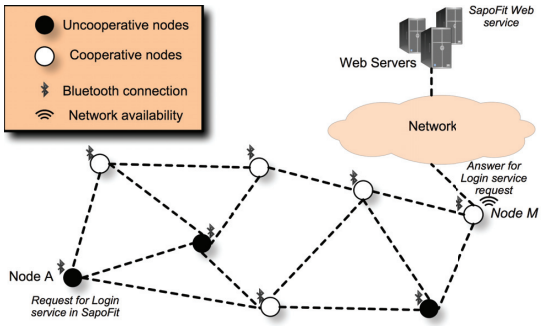


Fig. 7. Illustration of the m-Health network scenario used for the performance evaluation of the cooperation strategy.

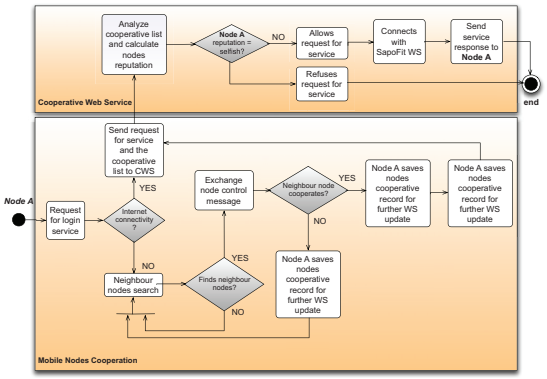


Fig. 8. Activity diagram of a mobile node representing a mobile device with SapoFit and its cooperation mechanisms.

list is updated and the request for *login* is sent together with the cooperative list to all the cooperative neighbor nodes. This process is repeated until finding a node (Node M) that is willing to cooperate and with Internet connectivity as well. When the request reaches a node in these conditions, the *cooperative Web service* will update the reputation table and evaluate the reputation of the requester node. If the node has a *selfish* reputation, the login request is discarded. If it has a cooperative reputation, the request is allowed without priority. If it has a super-cooperative reputation, the request is allowed with maximum priority over other sent answers. The same cooperation procedures are followed while retrieving the login service answer, but instead of searching a node with Internet connectivity, it searches for the requester node *id*.

C. Performance analysis

This section focuses on the performance analysis of the proposed cooperative strategy and its impact on the overall network performance. The study was performed through the above-described real prototype. The case study scenario included nineteen (19) users with the *SapoFit* application. Non-cooperative cases where controlled and measured to a maximum of nine to guarantee the minimum service performance. The first and perhaps the most important analysis refers to the case where without the cooperation strategy, all the devices with no Internet connectivity were unable to access the application Web services and therefore cannot use the m-Health application. Through cooperation all the devices can indeed use the m-Health application. However, uncooperative nodes affect directly the service delivery probability, service average delay, and the overall network performance. Performance metrics considered in this study are the service delivery probability (in percentage) and the service average delay (in seconds). The service delay is measured as the time between the request for the application service and its delivery. It was considered a worst-case scenario of nine uncooperative nodes. The service delivery probability and the service average delay as function of the number of uncooperative mobile nodes are presented in Figure 9. As may be seen, when the number of uncooperative nodes increases, the service delivery probability decreases. As expected, the service average delay also presents the same behavior. Increasing the number of uncooperative nodes the service average delay increases. The maximum service delay observed with nine uncooperative nodes was about 83.7 seconds.

Analyzing the service average delay results, an analytical model with two equations was used. Equations 2 and 3 calculate the maximum service delay and the service average delay, respectively.

$$\text{Maximum service delay} = (\alpha+\sigma+\varphi)\times T_c + (\alpha+\sigma)\times T_{uc} \quad (2)$$

$$\text{Service Average delay } = (\alpha+\sigma+\beta)\times T_{min} + (\alpha+\sigma)\times T_{uc} \quad (3)$$

where,

- α = Average connection establishment time = 3.6 seconds
- σ = Average node control message transfer time = 0.43 seconds
- φ = Average request for service+Cooperation List transfer time = 0.35 seconds
- β = Average service response delivery time = 0.28 seconds
- T_{min} = Minimum required nodes for cooperation = 3 nodes
- T_c = Total of cooperative nodes (variable)
- T_{uc} = Total of uncooperative nodes (variable)

The maximum service delay obtained by (2) was about 83.7 seconds, slightly below that one obtained by real experiments. A comparison between the service average delay results from the real experiments and the results obtained by (3) are depicted in Figure 10. As may be seen, the observed results show slightly variances that increase with the number of uncooperative nodes. These variances were mainly caused by mobile devices constrains, such as loss of Bluetooth connection between nodes, distance variation, and different devices hardware specifications. However, this comparison results are satisfactory, proving the feasibility of the obtained results from the real experiments that clearly follows the behavior provided by (3).

After the experiments, the users completed a survey evaluating their experience regarding the performance of the m-Health application with the embedded proposed cooperation

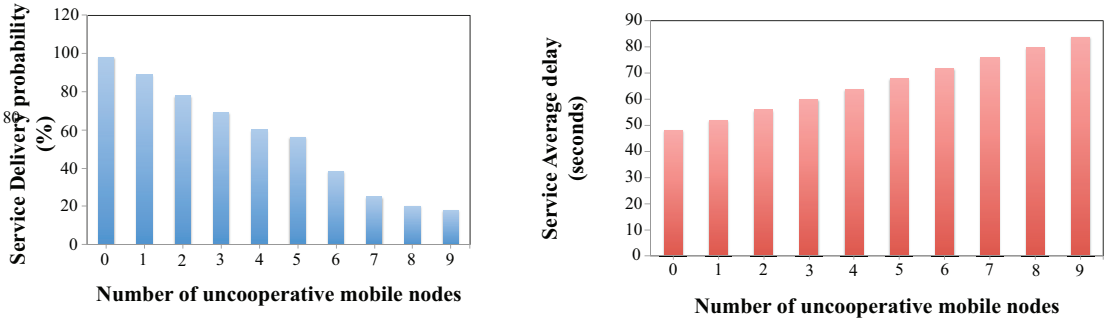


Fig. 9. Service delivery probability and service average delay as function of the number of uncooperative mobile nodes.

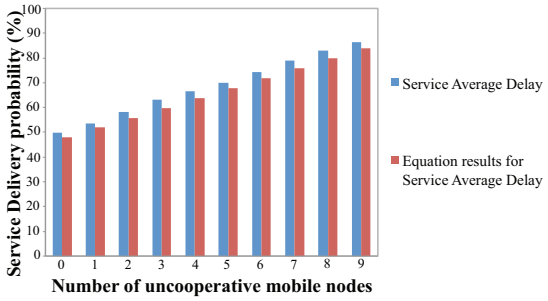


Fig. 10. Performance comparison of the service average delay as function of the number of uncooperative mobile nodes considering results obtained by experiments and by the equation (3).

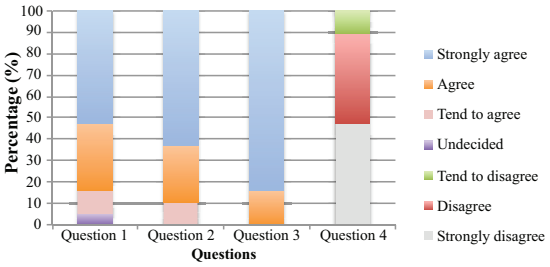


Fig. 11. Results of the survey to evaluate the user experience of the m-Health application with the proposed cooperation mechanisms.

TABLE II
SURVEY QUESTIONS

Question	Description
Q1	Without network connectivity, do you have always access to the required information?
Q2	Without network connectivity, do you received the required information in a comfortable time?
Q3	Are the cooperation mechanisms embedded on the application totally ubiquitous to the user?
Q4	Is the performance of the mobile device affected by the embedded cooperation mechanisms (broadband, battery, etc.)?

mechanisms. The questions are listed in Table II and the results may be seen in Figure 11. As can be observed, the results are very good the received feedback is very promised for this solution.

V. CONCLUSION AND FUTURE WORK

This paper proposed a cooperation strategy for m-Health applications following a service-oriented architecture. This approach presented a reputation-based strategy where a Web service manages all the network cooperation, along with the access control. It considers three main modules: a node control message, a requester control message that includes neighbors and reputation lists, among other components, as well as a cooperative Web service. The objective of providing an increased network infrastructure and Internet connectivity independency to m-Health applications with service-oriented architectures was fully accomplished. The proposed solution was evaluated, demonstrated, and validated through a real m-Health prototype using the SapoFit m-Health application. The service delivery probability and the service average delay performance metrics were considered. It was shown that the proposed approach provides network connectivity independency to m-Health clients when Internet connection is required and is not available. It was evaluated the influence of the number of uncooperative nodes on the network performance. The results confirm that when the number of uncooperative nodes increases, both the service delivery probability and the service average delay also increases, as expected. An analytical model confirmed these results. Through the network performance evaluation and its metrics results comparisons, it is possible to conclude that proposed cooperation solution have improved significantly the overall system performance and the quality of service (QoS) of the m-Health application. Despite some results variations, due to high mobility patterns and limited laboratory environment, cooperation mechanisms have shown significantly improvements on the QoS, namely, on the request for service delivery probability and its average delay, and hence improving the network performance due to the less number of server-side concurrency accesses. Refining the proposed strategy, including the treatment of sensitive and priority medical information that is handled in a given m-

Health application can be considered for future work. The performance evaluation of the m-Health cooperative proposal in more m-Health applications scenarios may also be considered.

ACKNOWLEDGMENTS

This work has been partially supported by *Instituto de Telecomunicações*, Next Generation Networks and Applications Group (NetGNA), Portugal, by National Funding from the FCT - *Fundação para a Ciência e a Tecnologia* through the PEst-OE/EEI/LA0008/2011 Project, and by the AAL4ALL (Ambient Assisted Living for All), project co-funded by COMPETE under FEDER via QREN Programme and by National Natural Science Foundation of China (Grant No. 61201165 and No. 61271240).

REFERENCES

[1] S. Akter and P. Ray, "mHealth - an Ultimate Platform to Serve the Unserved," *IMIA Yearbook Medical Informatics*, pp. 94–100, 2010.

[2] S. Tachakra, X. Wang, R. Istepanian, and Y. Song, "Mobile e-Health: The Unwired Evolution of Telemedicine," *Telemedicine J. e-Health*, vol. 9, pp. 247–257, 2003.

[3] G. Paré, K. M. K, G. Pineau, and C. St-Hilaire, "Clinical effects of home telemonitoring in the context of diabetes, asthma, heart failure and hypertension: A systematic review," *J. Medical Internet Research*, vol. 12, no. 2, 2010.

[4] J. Fayn and P. Rubel, "Toward a personal health society in cardiology," *IEEE Trans. Inf. Technol. Biomedicine*, vol. 14, no. 2, pp. 401–409, 2010.

[5] L. Chin-Teng, C. Kuan-Cheng, L. Chun-Ling, C. Chia-Cheng, L. Shao-Wei, C. Shih-Sheng *et al.*, "An intelligent telecardiology system using a wearable and wireless ECG to detect atrial fibrillation," *IEEE Trans. Inf. Technol. Biomedicine*, vol. 14, no. 3, pp. 726–733, 2010.

[6] A. Kollmann, M. Riedl, P. Kastner, G. Schreier, and B. Ludvik, "Feasibility of a mobile phone–based data service for functional insulin treatment of type 1 diabetes mellitus patients," *J. Medical Internet Research*, vol. 9, no. 5, 2007.

[7] S. G. Mougiakakou *et al.*, "SMARTDIAB: A communication and information technology approach for the intelligent monitoring, management and follow-up of type 1 diabetes patients," *IEEE Trans. Inf. Technol. Biomedicine*, vol. 14, no. 3, pp. 622–633, 2010.

[8] F. Zhu, M. Bosh, I. Woo, S. Kim, C. J. Boushey, D. S. Ebert *et al.*, "The use of mobile devices in aiding dietary assessment and evaluation," *IEEE J. Sel. Topics Signal Process.*, vol. 4, pp. 756–766, 2010.

[9] J. P. Pollak, G. Gay, S. Byrne, E. Wagner, D. Retelny, and L. Humphreys, "It's time to eat! - Using mobile games to promote healthy eating," *IEEE Pervasive Comput.*, vol. 9, pp. 21–27, 2010.

[10] K. Patrick *et al.*, "A text message–based intervention for weight loss: Randomized controlled trial," *J. Medical Internet Research*, vol. 11, no. 2, 2009.

[11] R. Whittaker, E. Dorey, D. Bramley, C. Bullen, S. Denny, C. R. Elley *et al.*, "A Theory-based video messaging mobile phone intervention for smoking cessation: Randomized controlled trial," *J. Medical Internet Research*, vol. 13, no. 1, 2011.

[12] S. Akter, J. D'Ambra, and P. Ray, "User perceived service quality of mhealth services in developing countries: Research paper," in *European Conf. Inf. Syst. (ECIS 2010)*, Pretoria, South Africa, 2010.

[13] D. Vatsalan *et al.*, "Mobile technologies for enhancing ehealth solutions in developing countries," in *Second International Conf. eHealth, Telemedicine, Social Medicine (eTELEMED)*, St. Maarten, Netherlands Antiles, 10-16 Feb. 2010, pp. 84–89.

[14] G. Kramer, I. Maric, and R. D. Yates, *Cooperative Communications (Foundations and Trends in Networking)*. Now Publishers Inc., June 2007.

[15] L. Buttyán and J.-P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," *Mobile Netw. Appl.*, vol. 8, pp. 579–592, 2003.

[16] L. Bannon and J. Hughes, "The context of CSCW," K. Schmidt (Ed.), Report of COST14 "CoTech". Working Group 4 (1991-1992), Denmark: Riso National Laboratory, Tech. Rep., 1993.

[17] P. Ray, N. Parameswaran, V. Chan, and W. Yu, "Awareness modelling in collaborative mobile e-health," *J. Telemedine Telecare*, vol. 14, no. 7, pp. 381–385, 2008.

[18] V. Chan, P. Ray, and N. Parameswaran, "Mobile e-Health monitoring: An agent-based approach," *IET Commun.*, vol. 2, no. 2, pp. 223–230, Feb. 2008.

[19] B. M. C. Silva, I. M. Lopes, P. Ray, and J. Rodrigues, "SapoFitness: A mobile health application for dietary evaluation," in *IEEE HEALTHCOM 2011*, Columbia, MO, USA, June 13-15, 2011.

[20] J. J. P. C. Rodrigues, I. M. C. Lopes, B. M. C. Silva, and I. Torre, "A new mobile ubiquitous computing application to control obesity: SapoFit," *Informatics Health Social Care, Informa Healthcare*, 2012 (in press).

[21] "SapoFit, [Online]. Available http://itunes.apple.com/pt/app/sapo-fit/id438487775?mt=8," Accessed in July 2012.

[22] I. Maric and R. D.Yates, "Cooperative multi-hop broadcast for wireless networks," *J. Sel. Areas Commun.*, vol. 22, no. 6, pp. 1080–1088, Aug. 2004.

[23] B. Sirkeci-Mergen and A. Scaglione, "On the power efficiency of cooperative broadcast in dense wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 2, pp. 497–507, Feb. 2007.

[24] G. Jakllari, S. V. Krishnamurthy, M. Faloutsos, and P. V. Krishnamurthy, "On broadcasting with cooperative diversity in multi-hop wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 2, pp. 489–496, Feb. 2007.

[25] Z. Han, Z. Ji, and K. J. R. Liu, "A cartel maintenance framework to enforce cooperation in wireless networks with selfish users," *IEEE Trans. Wireless Commun.*, vol. 7, no. 5, pp. 1889–1899, May 2008.

[26] L. Al-Kanj and Z. Dawy, "Optimized energy efficient content distribution over wireless networks with mobile-to-mobile cooperation," in *IEEE 17th International Conf. Telecommun., Doha, Qatar*, Apr. 4-7 2010, pp. 471–475.

[27] L. Yuting and R. Deters, "Using cooperation to improve the experience of mobile Web Services consumers," in *IEEE Asia-Pacific Services Comput. Conf., Singapore*, Dec. 7-11 2009, pp. 213–218.

[28] S. Corson and J. Macker, "Mobile Ad-hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC: 2501, 1999.

[29] L. Buttyán and J. P. Hubaux, "Stimulating cooperation in self-organizing mobile ad-hoc networks," vol. 8, 2003, pp. 579–592.

[30] J. Hu and M. Burmester, *Guide to Wireless Ad-Hoc Networks: Cooperation in Mobile ad-Hoc Networks*. Computer Communications and Networks, S. Misra, I. Woungang, S. C. Misra (Eds.), ISBN: 978-1-84800-327-9, ch. 3, pp. 43–57.

[31] L. Buttyan and J.-P. Hubaux, "Nuglets: A Virtual Currency to Stimulate Cooperation in Self Organized Mobile Ad Hoc Networks," Tech. Rep., No. DSC/2001.

[32] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, Cheat- proof, Credit-based System for Mobile Ad hoc Networks," in *IEEE Infocom 2003*, San Francisco, CA, USA, Mar. 30 - Apr. 3 2003.

[33] S. Buchegger and J. Y. L. Boudec, "Performance analysis of the CONFIDANT protocol," in *3rd ACM International Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc 2002)*, Lausanne, Switzerland, June 09-11 2002, pp. 226–236.

[34] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *6th IFIP TC6/TC11 Joint Working Conf. Commun. Multimedia Security*, Portoroz, Slovenia, Sept. 26-27 2002, pp. 107–121.

[35] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss, "Delay-Tolerant Networking Architecture," RFC 4838, Apr. 2007.

[36] V. N. G. J. Soares and J. J. P. C. Rodrigues, *Cooperative Networking*. S. Misra and M. Obaidat (Ed.s), ISBN: 978-0-470-74915-9, 2011, pp. 101-115.

[37] U. Shevade, H. H. Song, L. Qiu, and Y. Zhang, "Incentive-aware routing in dtns," in *16th IEEE International Conf. Netw. Protocols (ICNP 2008)*, Orlando, FL, USA, Oct. 19–22 2008, pp. 238–247.

[38] J. M. Pozo, O. Trullols, J. M. Barceló, and J. G. Vidal, "A Cooperative ARQ for Delay-Tolerant Vehicular Networks," in *28th International Conf. Distributed Comput. Syst. (ICDCS 2008)*, Beijing, China, June 17–20 2008, pp. 192–197.

[39] K. Raychaudhuri and P. Ray, "Privacy challenges in the use of eHealth SYSTEMS FOR PUBLIC HEALTH MANAGEment," *International J. e-Health Medical Commun., IGI-Global*, vol. 1, no. 2, pp. 12–23, 2010.

[40] L. Zhou and H.-C. Chao, "Multimedia traffic security architecture for internet of things," *IEEE Netw.*, vol. 25, no. 3, pp. 35–40, May/June 2001.

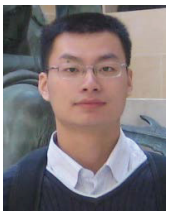
[41] U. Blumenthal, F. Maino, and K. McClohrie, "The Advance Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security model," RFC 3826, June 2004.

Bruno Silva received his BsC degree (licentiate) in 2008 in Informatics Engineering from University of Beira Interior. In 2010 he received his MsC degree in Informatics Engineering from University of Beira Interior. He is currently a PhD student on Informatics Engineering at the University of Beira Interior under supervision of Prof. Joel J. P. C. Rodrigues. He is also a PhD student member of the Instituto de Telecomunicações, Portugal. His current research areas are Delay Tolerant Networks, Vehicular Networks, Mobile Computing, Ubiquitous Computing, e-Health but especially in mobile Health. He authors or co-authors 12 international conference papers and 4 International Journal publications.

Joel Rodrigues is a professor in the Department of Informatics of the University of Beira Interior, Covilhã, Portugal, and researcher at the Instituto de Telecomunicações, Portugal. He received a PhD degree in informatics engineering, an MSc degree from the University of Beira Interior, and a five-year BSc degree (licentiate) in informatics engineering from the University of Coimbra, Portugal. His main research interests include sensor networks, e-health, e-learning, vehicular delay-tolerant networks, and mobile and ubiquitous computing. He is the leader of NetGNA Research Group (http://netgna.it.ubi.pt), the Vice-chair of the IEEE ComSoc Technical Committee on Communications Software, the Vice-Chair of the IEEE ComSoc Technical Committee on eHealth, and Member Representative of the IEEE Communications Society on the IEEE Biometrics Council. He is the editor-in-chief of the International Journal on E-Health and Medical Communications, the editor-in-chief of the Recent Patents on Telecommunications, and editorial board member of several journals. He has been general chair and TPC Chair of many international conferences. He is a member of many international TPCs and participated in several international conferences organization. He has authored or coauthored over 220 papers in refereed international journals and conferences, a book, and 2 patents. He had been awarded the Outstanding Leadership Award of IEEE GLOBECOM 2010 as CSSMA Symposium Co-Chair and several best papers awards. Prof. Rodrigues is a licensed professional engineer (as senior member), member of the Internet Society, an IARIA fellow, and a senior member of ACM and IEEE.

Ivo Lopes is a PhD student on Informatics Engineering at the University of Beira Interior, Covilhã Portugal, under supervision of Prof. Joel J. P. C. Rodrigues. He received his Master degree in Informatics Engineering from University of Beira Interior, 2011. His research interests include mobile and ubiquitous computing, eHealth, AAL, Web Services and sensor networks. Currently he is affiliated with Instituto de Telecomunicações, Portugal since March 2009. He has authored or co-authored of several papers in international journals, books and conferences.

Tiago Machado received his BSc degree (licentiate) in 2010 in Informatics Engineering from University of Beira Interior. In 2012 he received his MSc degree in Informatics Engineering from University of Beira Interior. He is a member of the Instituto de Telecomunicações, Portugal. His current research areas are Cooperation Mechanisms, Mobile Computing and Ubiquitous Computing. He authors or co-authors of one international conference paper and one journal publication.



Liang Zhou received his Ph.D. degree major at Electronic Engineering both from Ecole Normale Superieure (E.N.S.), Cachan, France and Shanghai Jiao Tong University, Shanghai, China in 2009. Now, he is a professor in Key Lab of Broadband Wireless Communication and Sensor Network Technology (Nanjing University of Posts and Telecommunications), Ministry of Education, China. His research interests are in the area of multimedia communications, in particular, resource allocation and scheduling, multimedia security, multimedia signal processing. E-mail: liang.zhou@ieee.org.

Chapter 5

Towards a Cooperative Security System for Mobile-Health Applications

This chapter consists of the following article:

Towards a Cooperative Security System for Mobile-Health Applications

Bruno M. C. Silva, Joel J. P. C. Rodrigues, Fábio Canelo, Ivo M. C. Lopes, and Jaime Lloret

Journal of Electronic Commerce Research, Special Issue on Advances in Security and Privacy for Future Mobile Communications, Springer, in press, 2014.

According to 2013 Journal Citation Reports published by Thomson Reuters in 2014, this journal scored ISI journal performance metrics as follows:

ISI Impact Factor (2013): 1.632

ISI Article InfluenceScore (2013): 0.267

Journal Ranking (2013): 50/110 (Business)

Journal Ranking (2013): 58/172 (Management)

Towards a Cooperative Security System for Mobile-Health Applications

Bruno M.C. Silva[1], Joel J. P. C. Rodrigues[1], Fábio Canelo[1] , Ivo M. C. Lopes [1] and Jaime Lloret[2]

[1]*Instituto de Telecomunicações, University of Beira Interior, Rua Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal*

[2] *Integrated Management Coastal Research Institute, Universidad Politécnica de Valencia, C/Paranimf, n° 1, 46730, Grao de Gandia, Spain*

E-mail: bruno.silva@it.ubi.pt, joeljr@ieee.org, {fabio.canelo; ivo.lopes}@it.ubi.pt, jlloret@dcom.upv.es

Abstract – Mobile Health (m-Health) system architectures are typically based on mobile and wireless communications, and use mobile devices with data exchange supported by Web Services (WS). Although m-Health systems offer mobility as a potential and precious resource they also present several challenged issues and constraints, such as, battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, and network delays. Furthermore, constant mobility and often-required Internet connectivity also exposes and compromises the privacy and confidentiality of the m-Health system information. This paper proposes a novel data encryption solution for mobile health systems, considering a novel and early-proposed cooperation strategy. This encryption solution, called data encryption for mobile health applications (DE4MHA), tries to guarantee the best confidentiality, integrity, and authenticity of m-health systems users data. The paper also presents a performance evaluation study comparing the performance an m-Health application with and without the DE4MHA.

Keywords: Mobile Health; m-Health; Mobile computing; e-Health; Cooperation; Cryptograph; Encryption; Security

1. Introduction

Mobile health (m-Health) is considered the future on Health telematics and a new edge on healthcare innovation. It proposes and aims to deliver healthcare anywhere and anytime,

surpassing geographical, temporal, and even organizational barriers [2,65]. It offers more accessible and affordable healthcare solutions to patients that live in remote rural areas, that travel constantly or that for some reason are physically incapacitated [40, 1]. In the last decade m-Health has been an important area of research gathering and innovating important findings and contributions to several health topics, such as, cardiology [47, 22, 40], diabetes [35, 44, 32], obesity [71, 49,48,67], smoking cessation [68], and healthcare services for developing countries [17], among others.

Typical m-Health services include mobile devices and wireless communications. Figure 1 illustrates a typical architecture of an m-Health system interacting with a Web service (WS) that delivers and provides several health services. However, these services and architectures present several challenging issues and constraints, such as, battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, and network delays.

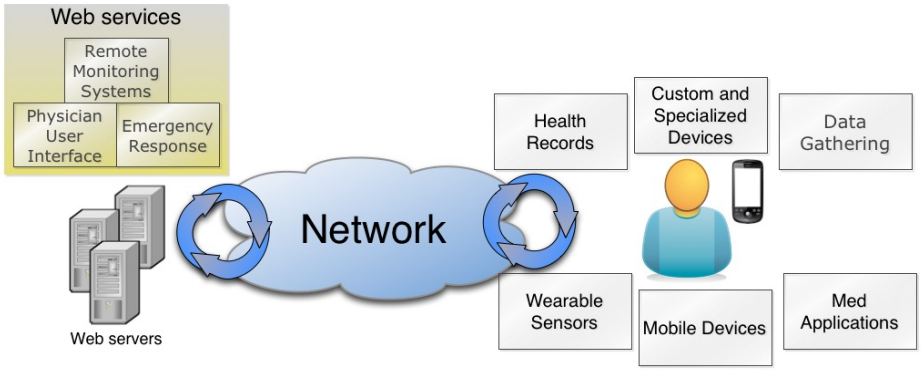


Figure 1. Illustration of a typical m-Health network architecture.

Several research studies present cooperation-based approaches as a solution to solve such limitations and also to improve wireless networks performance [34, 11]. In the healthcare context, cooperation among healthcare professionals has been studied and concluded that can improve their work and performance. Computer-supported cooperative work (CSCW) is usually used to share information through broadband and telecommunication networks (e-Mail or instant messaging) [5]. However, CSCW applied to healthcare information systems could enable patients and healthcare professionals to work together and share more efficiently health information even from remote locations [52,12].

Another challenging issue in m-Health services and applications is privacy and security. Moreover, security and privacy have been over the last year a point of interest in designing and

researching IT solutions [3,13,26,30,36]. M-Health applications often save or access to sensitive and personal information. A patient or a healthcare professional that manages such information must assure its confidentiality**,** integrity, and authenticity**.** Therefore, cryptographic mechanisms can be seen as an excellent solution to guaranty health information privacy and protection [53].

This paper proposes a data encryption solution for mobile health applications (DE4MHA) for an early-proposed cooperation strategy presented in [60] considering m-Health systems to assure data confidentiality, integrity, and authenticity. The cooperation strategy and the DE4MHA are deployed and evaluated in a real m-Health application for obesity prevention and control, called SapoFit [62,55,56]. The DE4MHA includes the use of the RSA algorithm [33] for asymmetric encryption/decryption to assure Key exchange confidentiality and the Advanced Encryption Standard (AES) algorithm [51] for symmetric encryption/decryption assuring data confidentiality. To ensure data integrity a message digest is created with the generation of a hash of the transmitted data. Digital signature is used for data authenticity, encrypting the previous hash message with the RSA private Key. The HTTPS protocol is used to secure the communication with the SapoFit Web service (WS). The network performance assessment and validation of the proposal is also presented. This evaluation proves its feasibility and also studies the impact of the DE4MHA over the cooperation strategy for m-Health applications.

The main contributions of the paper are the following:

- Study of encryption/decryption algorithms for typical m-Healh network architectures;
- Proposal of an encryption/decryption hybrid approach using symmetric and asymmetric encryption algorithms for typical m-Healh network architectures;
- Proposal of a data encryption solution for mobile health applications (DE4MHA) in cooperation environments.

The remainder of this paper is organized as follows. Section II elaborates on related work about the topic focusing on cryptography approaches suitable for e-Health and m-Health applications. Section III summarizes the early-proposed cooperation strategy where the DE4MHA was applied and the cryptography proposal and its conceptual design is presented in Section IV. The performance evaluation and assessment of DE4MHA is presented in Section V. Finally, Section VI concludes the paper and points out further research works.

2. Related Work

One of the most known and to the best of authors knowledge the first definition of m-health comes from Istepanian and Lacal [29] when, in 2003, defined mobile health as "emerging mobile communications and networks technologies for healthcare". In 2006, Laxminarayan *et al*. [39] presented an extensive study on the impact of mobility on the existing e-Health systems. In [16] authors define mobile health as "the provision of healthcare services through use of information and communication technologies (ICT) for mobile users". Mobile health services are present in a large scale in the applications available to users allowing them to obtain useful information about their health care serving as well as awareness prevention. M-Health systems and applications use the Internet and Web Services to provide an authentic pervasive interaction between physicians and patients. Any healthcare professional or a patient can easily access the same medical record anytime and anywhere through his personal computer, tablet, or smartphone. With the proliferation of mobile devices [55], innumerous m-health applications have been developed and turned available to the public through online markets [50] giving users the possibility of monitoring their own health state, allowing them to create and maintain their own health records, treatments alerts, health goals establishment, just to name few of them.

2.1 Challenges in m-Health systems design

The use and the design of mobile applications and systems include several challenges, such as, limited computing power, storage space, and battery lifetime, among others [27]. Therefore, a lightweight computing approach rather than an intensive and complex approach is desired in such context [14]. Furthermore, mobile devices face several security issues summarized as follows [70]:

- **Message interception and falsification** – By monitoring and analysing wireless traffic introducing then false packets to achieve network access compromising communications.
- **Impersonation, identity theft and fraud** – When using technical or social engineering techniques, credentials of legitimate users may be obtained.
- **Mobile virus and devices hijacking** – A device can be fully exposed to attacks if viruses, Trojans, or worms are installed in a disguised form.
- **Spamming** – Sending a huge amount of unsolicited SMS messages or Instant Messages to users.

- **Phishing** – Term usually used to define the process that involves sensitive information acquisition, like usernames, passwords or, e.g., credit card details through trust agent personification on electronic communication. It is often accomplished by redirecting users to fake Websites that look exactly as the one they expected.

When creating and designing m-Health services, it is extremely important to give the appropriated attention to all the above-mentioned issues to assure that health data is secure and not compromised. The most appropriate and ideal solution to handle such security issues is cryptography [25].

2.2 Cryptography approaches suitable for e-Health and m-Health services and applications

Cryptography may be defined as a set of techniques and algorithms to assure safe communication between two agents, on an open network channel. Moreover, it answers numerous issues of a communication process, such as, confidentiality**,** integrity, and authenticity [24]**.**

2.2.1 Confidentiality

Confidentiality assumes that data is unavailable or disclosed to unauthorized persons [41]. Therefore, referring confidentiality implies dealing with encryption algorithms. Encryption is the process of encoding messages so that only authorized agents should be able to read them. Hence, several algorithms were developed over the past decades to deal with the increasing need of assuring data confidentiality and they may be divided into two main groups, (1) symmetric algorithms where both encryption and decryption is accomplished using the same key and (2) asymmetric algorithms where one key is used for encryption (public key) and another one is used for decryption (private key) [46].

As above-mentioned, symmetric algorithms use the same key for encryption and decryption. In this section, several encryption algorithms that are suitable for m-Health applications are considered. A typical symmetric encryption algorithm workflow is presented in Figure 2. A number of well-known symmetric key encryption algorithms suitable for e-Health systems enumerated in [10] have been studied, namely, the following: DES, 3DES, AES, Blowfish, IDEA, and RC4.

Data Encryption Standard (DES) [23] is an algorithm developed by IBM, in 1975, that as been adopted and published as a Federal Information Processing Standard (FIPS) in 1977. The

algorithm operates on a 64 bits data block and a fixed key length of 56 bits size for 16 rounds. Nowadays, it is considered to be out-dated and it has been replaced by its successor 3DES.

TripleDES, or 3DES algorithm [28], was introduced in 1978 by IBM as an extension of DES. 3DES applies DES algorithm three times instead of just one, supporting 112 bits or 168 bits key length and a block size of 64 bits that operates on 48 rounds.

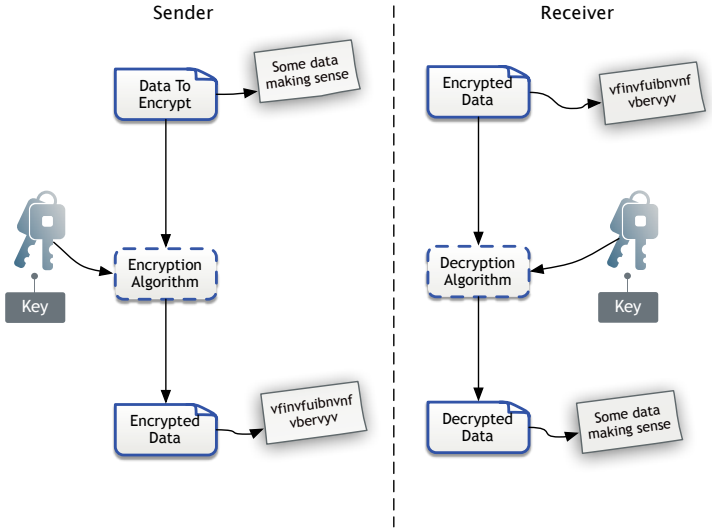


Figure 2. Illustration of a symmetric encryption algorithm workflow.

In 2001, in an open competition (known as Advanced Encryption Standard process), promoted by the National Institute of Standards and Technology (NIST), with the purpose of replacing the existing DES algorithm, two Belgian cryptographers proposed an algorithm originally named Rijndael that later became known as Advanced Encryption Standard (AES) [66]. It operates on a block cipher of 126 bits size and the key size is 128, 192, or 256 bits.

Another widely known symmetric algorithm is RC4 [31], also known as ARC4 or ARCFOUR and it was designed by Ron Rivest in 1987. This algorithm is applied to the Secure Socket Layer (SSL), WEP or PDF. It uses variable key length from 40 to 256 bits, as well as variable block sizes, changing its speed in encryption/decryption operations.

Blowfish [58] is another symmetric algorithm with worldwide acceptance and it was originally designed by Bruce Schneier, in 1993. The algorithm uses a variable key length between 32 and 448 bits (128 bits by default) and a 64 bits block size for operations on 16 rounds.

International Data Encryption Algorithm (IDEA) [7] is the best known for its use in Pretty Good Privacy (PGP) v2.0. It is an algorithm that operates on a 64 bits block size with a 128 bits key size.

Asymmetric cryptography, more known as public key cryptography, can be used to assure confidentiality. A typical asymmetric encryption algorithm workflow is presented in Figure 3. In this type of algorithms, two keys are required in order to operate. One key, known as public key, is used to encrypt the content of a message and the other one (private) key is used to decrypt it. These type of algorithms solve some of the faults of the symmetric algorithms, although they are considered to be at least 1000 times slower than symmetric ones [6] and keys size must be significantly bigger (for example, a 1024 bits key of an asymmetric algorithm corresponds approximately to a 128 bits key of a symmetric algorithm), and it is usually harder to handle key management. These types of algorithms are usually used for identification purposes or to session key exchange without requiring a trust agent [18].

RSA is an example of an asymmetric algorithm and its name stands for **R**ivest, **S**hamir and **A**dleman, the founders of the referred algorithm. It is widely known by being appropriated to encrypt/decrypt as well to perform digital signature. It was proposed in the late 70's but it is still used currently. Another example of asymmetric algorithm is Elgamal, described by Taher Elgamal in 1984 [21].

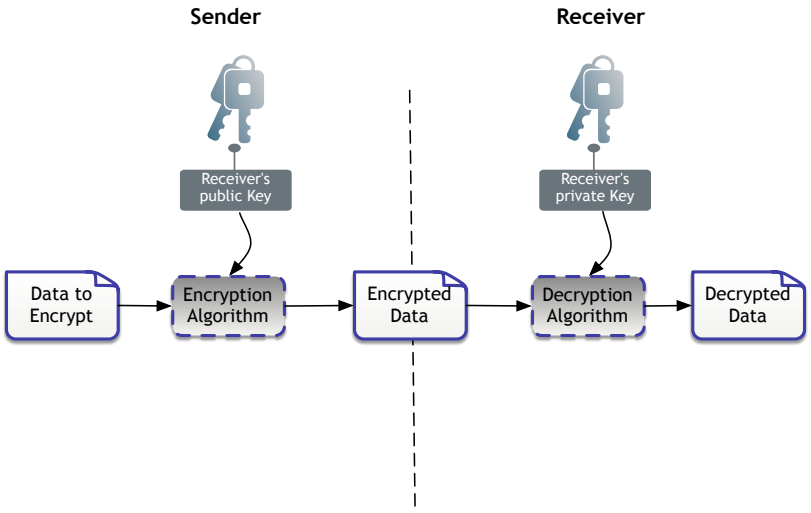


Figure 3. Illustration of asymmetric encryption algorithm workflow.

2.2.2 Integrity

Integrity is intended to provide users whether some data remains as it was when it was firstly created or if it has been changed [15, 59]. Health information is known as sensitive information in which a small change of the original information may have a negative outcome. Therefore, it is usually a good idea to use algorithms that can assure that users are handling unchanged and original information. Hence, cryptographic hash functions are used for that purpose.

As an example of a hash algorithm, Message Digest 5 can be named and it was designed by Ron Rivest, in 1991 [54], and it is largely used to check data integrity. It produces a 128-bit output, called message digest. In order to check data integrity, the same piece of data must always produce the same message digest as output, though in rare cases it may produce the same message digest for different piece of data [69]. For instance, given some data sent over the network, if it suffers any change when arriving at the end point, it will produce a different message digest, what makes possible to check data integrity.

Secure Hash Algorithm 1 (SHA-1) is an algorithm to assure data integrity, producing a 160 bit message digest. Both algorithms allow checking data integrity, by computing the message digest of a certain message. Any change of the message will almost certainly result in a different message digest, which allows to check if data integrity has been compromised or not [19].

2.2.3 Authenticity

Authenticity is another important concept when handling with security mechanisms. Nowadays, in every system, it is vital to assure that users send or receive information from the expected person or entity. Authenticity can be achieved using the above-mentioned RSA algorithm in combination with a hash function where the private key is used to encrypt the message digest. Then, the public key is used to decrypt the message digest and, when compared with the generated message digest on the sender side, both must be equal. Digital Signature Algorithm (DSA) [45] also provides digital signature capabilities. However, DSA can only sign and cannot encrypt information. Furthermore, it uses SHA-1 to generate the message digest as opposed to MD5 used by RSA. DSA was proposed by David Kravitz. In 1991, it was adopted by the National Institute of Standards and Technology (NIST).

2.3 Mobile health security approaches

Over the years securing e-Health data has been a matter with high importance, mainly due to the sensitivity data exchanged between users [64]. Many studies have been conducted in order to assure secure communications conveying e-Health data. In [63], a security model is presented focusing in identification, authentication, access control, integrity, confidentiality, and availability matters. For that purpose, cryptography has been widely used and studied in systems that share and transmit health data [9]. Furthermore, in [60], it is proposed an architecture that allows exchanging patients medical record in a secure way through the available infrastructure of mobile operators. Generic Bootstrapping Architecture (GBA) is used to enable user authentication while the other entity in the communication (service provider, hospital, and network operator) authenticates through the usage of Public Key Infrastructure (PKI). Finally, to guarantee secure communication, encryption and digital signature techniques are used. Although the use of standard security mechanisms of mobile networks and service providers present benefits, such as easy utilization and implementation of proven secure solutions, it clearly introduces some issues including the service provider and mobile network provider cooperation as well defining privacy and security policies concerning patient's private health data while transferred outside the source management. Since there are multiple mobile networks providers in each country and in order to turn health secure services available to all the potential users, it is clear that several agreements between multiple parties should be defined to turn this solution mobile operator dependent [60]. In

[42], the authors describe a new trend in security of e-Health data presenting XML security solutions describing some selected solutions in health data. eXtensible Access Control Markup Language (XACML) and Security Assertion Markup Language (SAML) languages are presented enabling authentication and authorization in a large network space. More specifically, SAML enables transmission of authentication data between parties, namely between an identity provider and a service provider. XACML defines access control policies as well as a processing model describing how to evaluate authorization requests according to the rules defined in the policies.

Lacuesta et al, presents in [38], a hybrid symmetric/asymmetric secure protocol for wireless ad hoc networks. This proposal also implements a trust scheme between users for data and secret key exchange. This scheme is based on the first visual contact between network nodes and its completely self-configured and able to create the entire network and exchange secure services.

3. Cooperation Strategy

This section describes, in detail, the early-proposed cooperation strategy for m-Healh applications [61]. This reputation-based strategy is based on the following three modules: *i*) *a node control message*, *ii*) a *cooperative list*, and *iii*) a *cooperative Web service* (*CWS*).

3.1. Nodes control message and cooperative list

The *node control message*, illustrated in Figure 4, contains a *node ID*, *node status* (storage capacity, energy, and Internet connectivity), and its *cooperation status* (cooperative or uncooperative). This *control message* is exchanged when a node establishes contact with a neighbor node. This *message* tries to provide an awareness control of all neighbor nodes knowing if they are willing to cooperate and in what conditions.

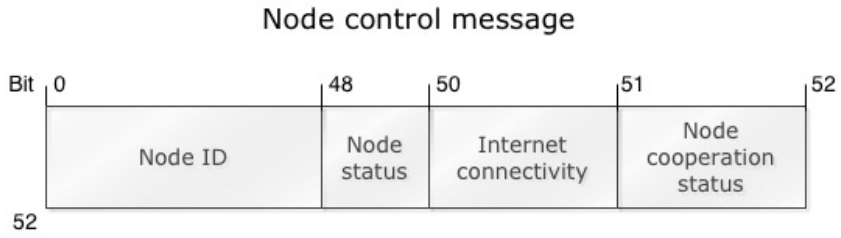


Figure 4. Node control message.

The *network cooperative list*, illustrated in Figure 5, registers all the cooperative and uncooperative network nodes throughout a service request. This *list* classifies all the neighbor nodes cooperative actions. It saves the *Node ID* and adds or subtracts a classification threshold according to the node *cooperation status*. When a service is requested from a node without Internet connectivity, all the nodes update their status in the *cooperative list*.

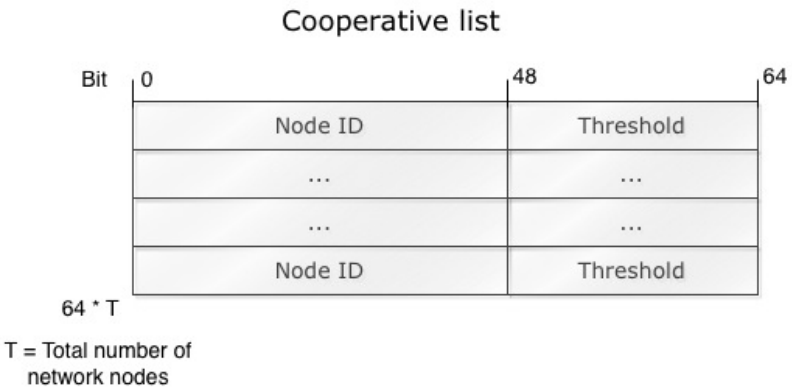


Figure 5. Node control message.

The *cooperative threshold list* (*CT*) influences directly the node reputation. The *list* starts at *0* (zero) and a unit (*1*) is added or subtracted according to the *node cooperation status* and *node status*. The correlation between the *node cooperation status*, the *node status*, its Internet connectivity, and the resultant CT is presented in Table I.

Table I. Correlation between the node cooperation status, the node status, its Internet connectivity, and the resultant CT classification.

Battery State		Internet Connectivity	Cooperation State	Reputation Value (RV)
Classification	0%-100%			
Critical	<15%	-	-	-
Poor	>= 15% and < 35%	0	0	-1
Poor		0	1	+3
Poor		1	0	-2
Poor		1	1	+4
Regular	>= 35% and < 70%	0	0	-2
Regular		0	1	+2
Regular		1	0	-3
Regular		1	1	+3

Excellent	>= 70%	0	0	-3
Excellent		0	1	+1
Excellent		1	0	-4
Excellent		1	1	+2

The node status is based on its storage capacity and energy lifetime. A node has three types of status: *poor*, *regular*, and *excellent*. A node with *poor* status occurs when the device storage capacity is over 95% or its available power energy is below 20%. The *regular* status comes when a node storage capacity is under 95% and its power energy is between 20% and 80%. A node is classified with an *excellent* status when the node storage capacity is under 95% and its available power energy is over 80%. The CT value guarantees that non-cooperative nodes are punished.

3.2 Cooperative Web service and reputation table

The *cooperative Web service* (*CWS*) includes and manages the *node reputation table*. To calculate nodes reputation, the *CWS* uses the *cooperative lists* deciding if the requesting node should have access to the m-Health application WS or not. Based on nodes reputation, the *CWS* will not grant access and release any resource from the WSs to *selfish* nodes. *Selfish* nodes are punished by the CWS with an order to cooperate until its reputation reaches a *cooperative* state. The CWS always release resources to *cooperative* nodes, however, *super-cooperative* nodes have a maximum priority in case of simultaneous requests. Figure 6 presents a user scenario of the m-Health cooperation approach. *User A* has network connectivity and cooperates, the status value is defined according to the battery status. *User B* has network connectivity and does not cooperate. Then, the status value will suffer a negative impact according to the battery status. *Users C* and *D* do not have network connectivity. *User C* queries *User A* for cooperation and receives a positive response and all the requested data. *User D* queries *User B* for cooperation and receives a negative response. Then, *User D* requests data from *User C* that answers this request, getting positive status by cooperating. Cooperating nodes have a better reputation, and have priority over selfish nodes to access the m-Health application services.

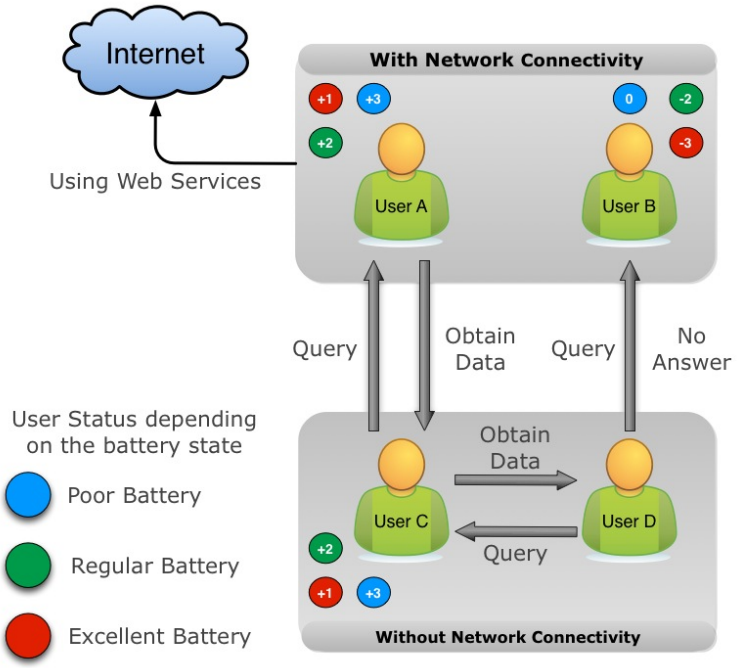


Figure 6. Illustration of the interaction for an m-Health application with the proposed cooperation approach for 4 users.

4. Data Encryption Mechanisms for Mobile Health Applications

This section presents the data encryption proposal for health applications (DE4MHA) in cooperation environments. The main goal aims to assure and guaranty m-Health data confidentiality, integrity, and authenticity in a cooperation environment where sensitive and personal data is exchanged through different agents. Figure 7 presents the use case diagram of the DE4MHA basic mechanisms and procedures.

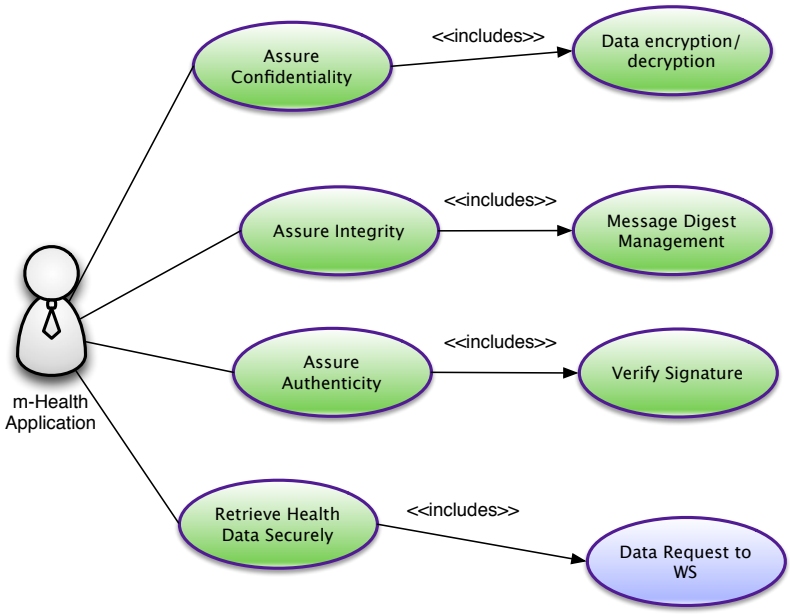


Figure 7. Use case diagram of the DE4MHA basic mechanisms and procedures.

Data confidentiality protects data that is exchanged through the network from unauthorized agents. There are two types of encryption algorithms to treat confidentiality: *i*) Symmetric Algorithms and *ii*) Asymmetric algorithms. Symmetric algorithms use the same key from encrypting and decrypting while asymmetric algorithms use one key for encryption (Public Key) and one for decryption (Private Key) [22]. Data confidentiality symmetric algorithms are widely used over asymmetric algorithms mainly because the last ones require a bigger encryption key that analogously increases the encryption time. In this paper, four distinct symmetric algorithms were considered to treat data confidentiality, namely, Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), RC4, and Blowfish. Working and studying encryption algorithms implies a comprehensive understanding of the encryption key procedure once the encrypted data strongly depends on key's size [4]. All the four experimented algorithms use 168 bits key length except for AES, which uses 128 bits key length (additionally, it is possible to use a 192 or 256 bits key length).

Concerning the asymmetric encryption, two algorithms were considered, RSA and Diffie-Hellman, although, Diffie-Hellman might not be considered an encryption algorithm but a key exchange protocol [8].

4.1 Encryption strategy

The first issue addressed on the construction of the DE4MHA was the exchange key problem [18]. Therefore, DE4MHA uses a hybrid approach using asymmetric algorithms for session key exchange and symmetric ones for encrypting data being transferred among network nodes.

The DE4MHA procedures (illustrated in the activity diagram shown in Figure 8) begins with a mobile node (a person using SapoFit), trying to access the SapoFit Web service (WS) that contains the user profile, weight measures, fitness, and diet indications. A SapoFit user (mobile requester node) without network connectivity and without access to the SapoFit WS will try to obtain the required health information through cooperation. Another user with network connectivity (mobile requested node) will forward the requested health information from the SapoFit WS. Both the requested and requester nodes will exchange (through Bluetooth) a Public Key Message (PKM). After the public key exchange, the requested node creates a session key, encrypting it with the requester node's public key. Then, a signature of the whole message is created and appended to the Session Key Message (SKM) that is sent to the requester node. When the message containing the session key is received, if its integrity and authenticity is verified, the requester node sends an acknowledgement (Ack) to the requested node. This method guaranties safe communication between nodes, otherwise, if the integrity and authenticity is not verified the communication between nodes is finished (aborted). A mobile node with network connectivity will access the cooperative WS to obtain the required health information. To secure all the communication with the WS, the Secure Socket Layer (SSL) over the HTTP (also known as HTTPs) is used. Therefore, granting confidentiality, integrity, and authenticity of all the retrieved health data from the WS.

Figure 9 illustrates the overall behaviour of DE4MHA and the most fundamental messages exchanged between two mobile nodes that requires safe communication establishment in order to exchange information through cooperation. The procedure begins when a requester node needs to obtain data through cooperation, performing the process of node discovery and further connection through Bluetooth to a mobile node willing to cooperate (1). When both nodes are connected through Bluetooth, both nodes will generate a RSA key pair, exchanging their public key, so that each mobile node will be able to encrypt messages for further exchange (2). As soon as the requested node receives the requester node's public key, it proceeds to generate an AES session key encrypting it through the requester node's public key, appending then a digital signature to assure data integrity as well as authenticity (3). Finally, if the previous message is received by the

requester node, its integrity and its authenticity will be checked and, if nothing wrong happened, the requester node will create a Ack message and a signature to guaranty that requested nodes know the requester node has received the session key (4). Therefore, all exchanged messages will be encrypted using the referred session key instead of the key pair used to exchange the session key, due to the superior time taken to encryption/decryption procedures by public key cryptography.

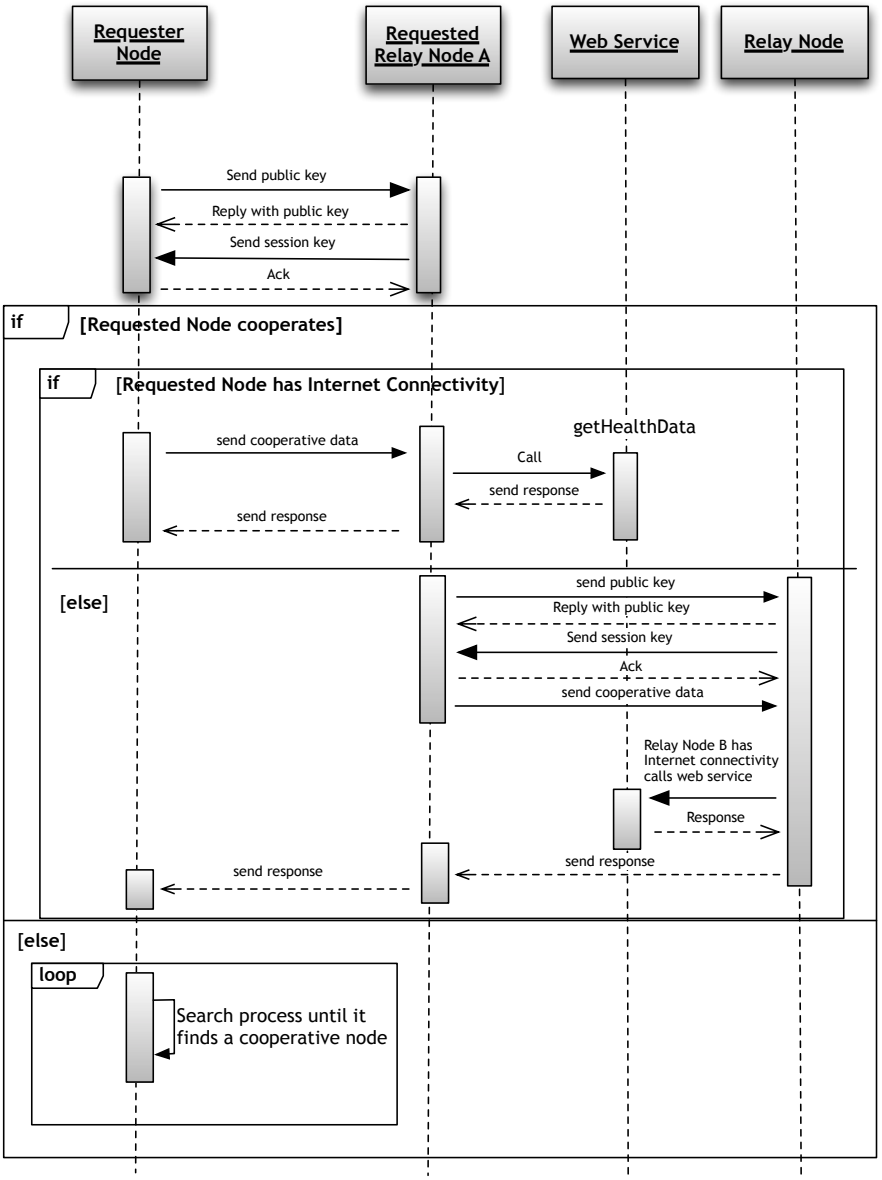


Figure 8. Activity diagram of the DE4MHA procedures.

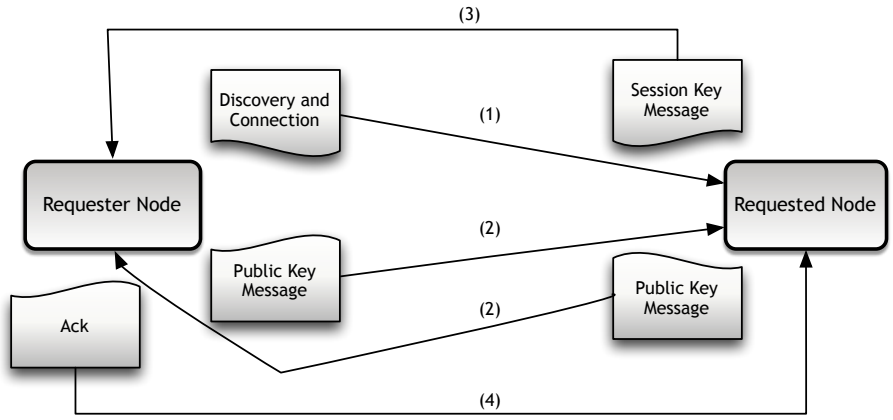


Figure 9. Data Exchange sequence

4.2 Public key message

Public key messages are sent from both requested and requester node, aiming to provide to each node their public key. In the future, this public key is used to encrypt a session key and it is used later to enable safe session key transfer.

Figure 10 illustrates a public key message. It has a maximum size of 119 bytes and the two following modules:

1. **Node unique ID:** This identifier is created through the aggregation of the mobile device Bluetooth mac address and the user unique identifier.
2. **Public Key:** This field will include the RSA public key previously generated along with the necessary private key.

These two elements comprise the public key message, which essentially enables safe public key exchange among mobile nodes on the network.

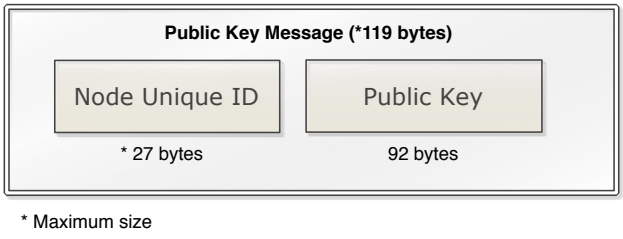


Figure 10. Public Key Message.

4.3 Session key message

The requested node is the one who sends the *session key message*, and it comprises three main components: *i*) the requested ID, *ii*) the session key, and *iii*) the signature. The three main components of the session key message are illustrated in Figure 11 and may be described as follows:

1. **Requested ID**: as above-mentioned, the requested ID results from the aggregation of the mobile device Bluetooth mac address and the user unique identifier.
2. **Session Key**: this field includes the session key used to encrypt and decrypt all the data exchanged among mobile nodes, assuring that all sensitive data is kept safe and its content remains unknown to unwanted threats (ensuring **confidentiality**).
3. **Signature**: To every message exchanged between mobile nodes an hash of that message is generated and encrypted with the node's private key creating a signature of the message. In this particular case, the requester node, to assure the message is exactly as it was when it was sent remains intact (preserving its **integrity**), and at the same time it assures the message was sent from the expected person (mobile node) guaranteeing **authenticity**.

When the requester node receives the session key message from the requested node, it verifies its integrity and authenticity. If the message has not been corrupted neither sent by someone else then expected, both the requester and requested nodes can safely communicate and exchange messages using the session key that only both possess.

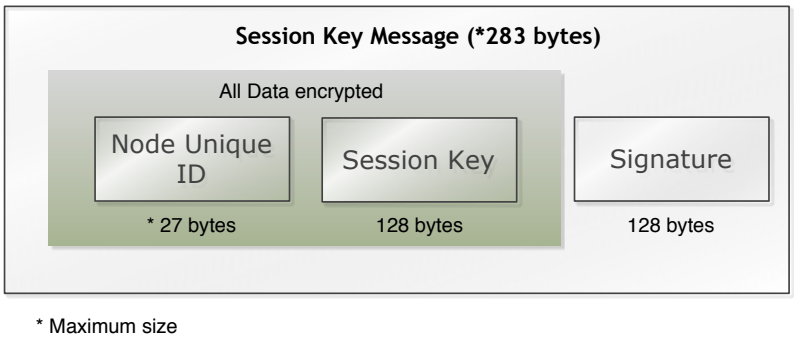


Figure 11. Session Key Message.

4.3 Symmetric and Asymmetric algorithm choice

In order to choose the most suitable symmetric encryption algorithm for DE4MHA, performance experiments were conducted using four different encryption algorithms, including AES, Triple Data Encryption Standard (3DES), RC4, and Blowfish. Given that DE4MHA aims any mobile health application in a cooperative environment, the amount of data that each application usually exchange is not known *a priori*. Therefore, in order to study several scenarios, different sizes of data that should be encrypted have been used as a performance metric.

Figure 12 presents the performance comparison of average encryption and decryption time as function of data size for the symmetric algorithms AES, 3DES, RC4, and Blowfish. As may be seen, results shown that when data size to encrypt increases, the encryption time (seconds) also increases, as expected. When comparing small amounts of data, all the four algorithms present similar results. However, AES algorithm presented better results, since the encryption time of bigger data tends to grow up very slowly. All the other three evaluated algorithms tend to grow up exponentially when data size to encrypt overcomes 1000 KB. The 3DES algorithm presented the maximum observed encryption time, encrypting 10,000 KB of data, which took on average 14.3 seconds. With the same amount of data, the AES encryption time was only about 0.0045 seconds. Regarding decryption process, the obtained results are nearly the same. AES algorithm decryption time is about 0.0038 seconds to decrypt 10,000 KB of data, in average. Given the observed results, AES algorithm was chosen for DE4MHA as a symmetric algorithm.

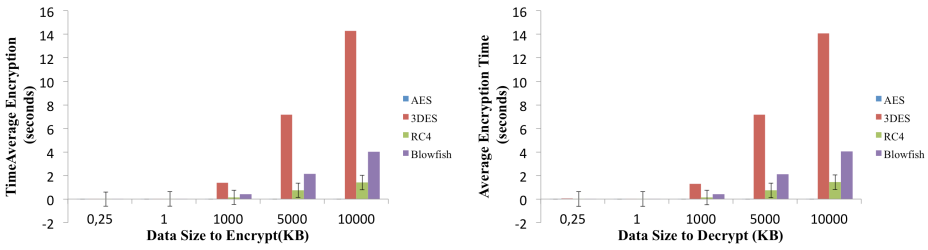


Figure 12. Performance comparison of average encryption and decryption time as function of data size for the symmetric algorithms AES, 3DES, RC4, and Blowfish.

Regarding the choice of an asymmetric algorithm to exchange session keys between mobile nodes, two options were considered, the RSA and the Diffie-Hellman algorithms. The RSA encrypts the

session key for delivery and the Diffie-Hellman allows users to share a secret, generating then a session key based on the shared secret.

Several experiments were performed with both algorithms. It was observed that RSA presents better encryption times than Diffie-Hellman, due to the high amount of computation needed by Diffie-Hellman and the low processing capacity of mobile devices.

4.4 Integrity and authenticity

In order to assure integrity, Message-Digest 5 (MD5) algorithm was chosen. It takes a message of arbitrary length as input and produces a 128-bit "hash" value or "message digest" as output. When this method is used multiple times with the exactly same message, it should always produce the same hash value. Then, if a message is modified or corrupted, generating a hash value and comparing it with the original one, it is possible to verify if the message maintains its integrity.

To guarantee authenticity, two approaches were considered, (1) using RSA algorithm to encrypt the hash value previously generated with MD5 and (2) using Digital Signature Algorithm (DSA). RSA can only sign a message but cannot encrypt information. Since a hybrid approach has been chosen when AES is used for symmetric encryption and RSA used for asymmetric encryption, the last one was chosen to perform digital signature, considering the fact that RSA will be used both for session key exchange and digital signature performance. Thus, the generation of a pair of keys to exchange session keys and another one for digital signature is unnecessary.

5. Performance Evaluation

This section focuses on the performance evaluation and validation of the security mechanisms embedded in an m-Health application with cooperation mechanisms. First, the m-Health application (SapoFit) and corresponding network scenario used to evaluate and demonstrate the solution is introduced. Afterwards, the system validation and results are discussed.

5.1 SapoFit, an m-Health application

SapoFit is a weight control mobile application that allows users to keep track of weight in a healthier and more practical way [56, 57, 62]. SapoFit allows users to control their weight, body mass index (BMI), basal metabolic rate (BMR), sports activity, and the possibility to follow food plans based on their needed calories. In this m-Health application all the users must be registered

in a Web service. Figure 13 presents the main activities screenshots of SapoFit application created for Android operating system.

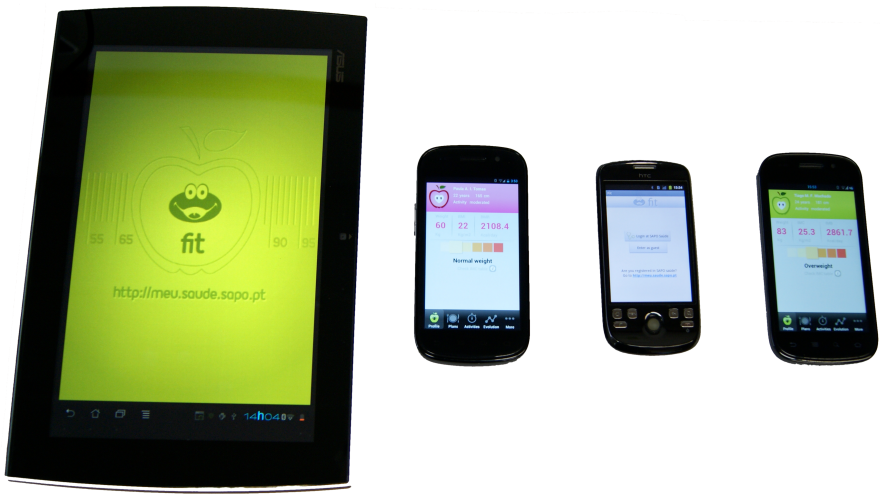


Figure 13. SapoFit Application.

The SapoFit application was used to evaluate and demonstrate DE4MHA and the cooperation strategy targets mobile devices running Google Android OS. The communication to the SapoFit Web service uses Simple Object Access protocol (SOAP) messages over Hypertext Transfer Protocol (HTTP). The information returns to the mobile application in JavaScript Object Notation (JSON) or Extensible Markup Language (XML).

5.2. Network scenario

Figure 14 presents the network scenario used to evaluate and demonstrate the proposed solution. It includes seven mobile devices with different hardware and software with SapoFit m-Health application. During five days, seven different users experimented the application. Non-cooperative cases where controlled and measured to a maximum of 4 to guarantee the minimum service performance. Through cooperation, all the devices can indeed use the m-Health application. However, uncooperative nodes affect directly the service delivery probability, service average delay, and the overall network performance. Performance metrics considered in this study are the request and response average time (in seconds). A performance comparison study of the m-Health application with and without the DE4MHA is presented.

In the presented scenario, all the devices carry Bluetooth class 2 modules, but only three devices have Internet connectivity. Users without Internet connectivity must use the integrated cooperation

mechanisms in order to obtain the requested health information. When the number of uncooperative nodes increases, the average time of any request or response also naturally increases.

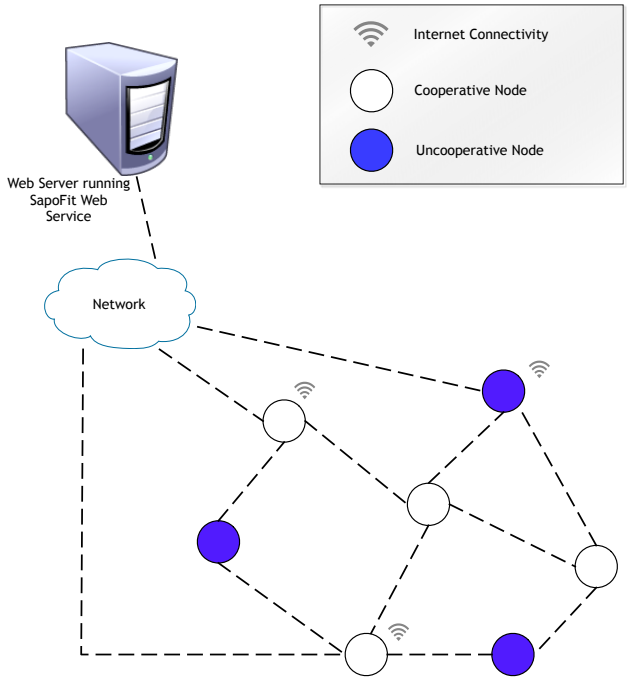


Figure 14. Network scenario of SapoFit in a cooperation enviorment.

Figure 15 shows how a request is handled when a mobile node desires to obtain determined health information. When a request is generated (required by the requester node), it initially checks if the device has Internet connectivity in order to obtain the desired information. In affirmative case, the requester node establishes a HTTPS connection (to assure data confidentiality) to the Web service that will try to obtain the information required by the device. On the other hand, when the requester node does not have Internet connectivity, a more complex scenario arises. In this scenario, in order to establish a secure channel through two mobile nodes, it is necessary to exchange public keys with the purpose of session key exchange assuring that nothing wrong happens in this procedure through authenticity and integrity properties. Thus, a message digest of the message to be sent is generated with MD5 algorithm, encrypting it with the receiver's public key and then appending it to the referred message (as previously referred). Hence, the receiver is able to generate a message digest of the received message using MD5 algorithm as well as comparing it with the message digest appended by the sender and decrypted with the receiver's private key, making it possible to check if the session key has not been modified and if it comes

from the expected source. Although this methodology has been exemplified with the session key message exchange case, it is actually applied in every message type that is exchanged between two mobile nodes.

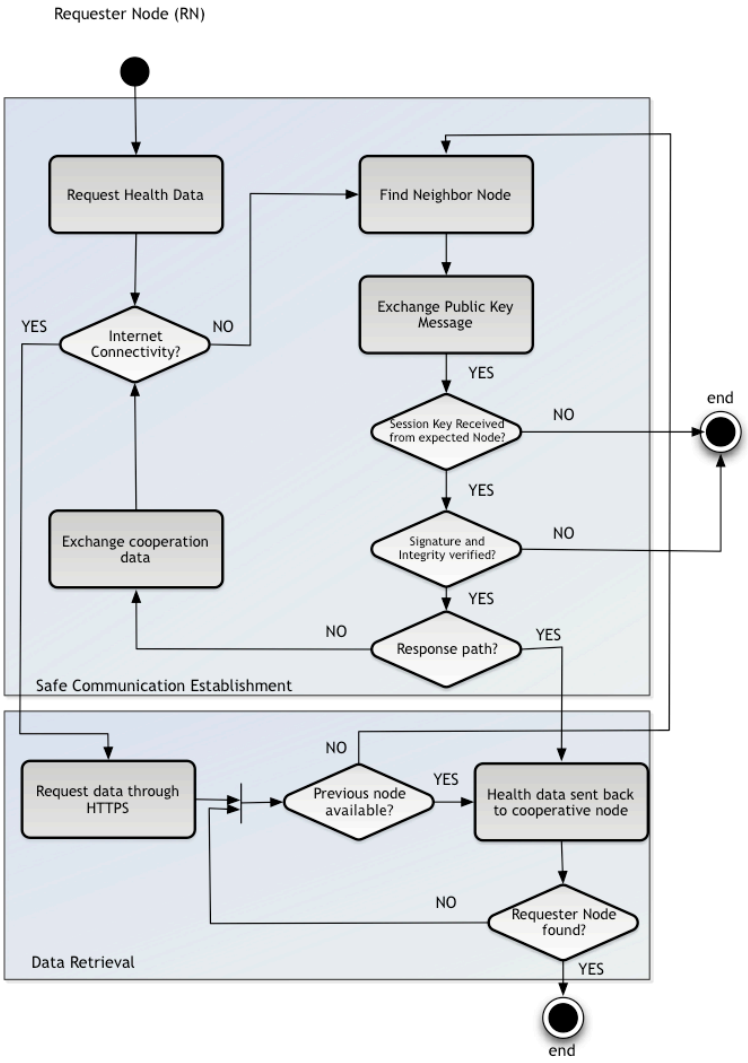


Figure 15 – Flowchart with request path activity.

At this moment, both mobile nodes might communicate safely, exchanging cooperative data so the requested node is aware of what the requester node desires to obtain. If the requested node has Internet connectivity and is willing to cooperate, it will establish a HTTPS connection to the cooperative Web service to obtain the required health data. Then, if the requester node is still within coverage, the health data is directly forwarded. If the requester is no longer within reach,

due to devices displacement, it tries to find an alternative mobile node with cooperation mechanisms embedded that is, at the same time, neighbor from both mobile nodes. Then, the common neighbor is able to deliver the message to its final destination, i.e., the requester node. Finally, when anything wrong happens, i.e., integrity or confidentiality is not verified, the communication between two mobile nodes is immediately ended (aborted) in order to avoid information leakage and system compromising.

5.3 Performance Analysis

This section focuses on the performance analysis of the proposed encryption strategy in the above-mentioned cooperative environment and its impact on the overall network performance. The study was performed with the above-mentioned real users. The study refers to the comparison of the m-Health application performance with and without the cryptography strategy embedded. Results show a minimal increase of the overall time taken to accomplish cooperation tasks when encryption mechanisms are present, not compromising the overall network performance. Hence, due to DE4MHA incorporation, the average time added with encryption/decryption tasks corresponds to approximately 0,003557 seconds, and if compared with the average time taken by cooperation mechanisms shown in [61], it corresponds to an increase of 2% of the overall time. In this sense, the extra time required is perfectly acceptable since privacy and security is a concerning issue and must be included in every m-Health applications. This analysis focuses on the response service average time and request delay (in seconds). The delay is measured as the time between the request for the application service and the time that a response is received. Figure 16 shows results of the average request and response time delay in function of the number of uncooperative mobile nodes with and without the DE4MHA. Taking into account both approaches, with and without DE4MHA, it is observed that DE4MHA presents a slightly worse result in both request and response average time delay. However, as may be seen, this delay increase is almost insignificant.

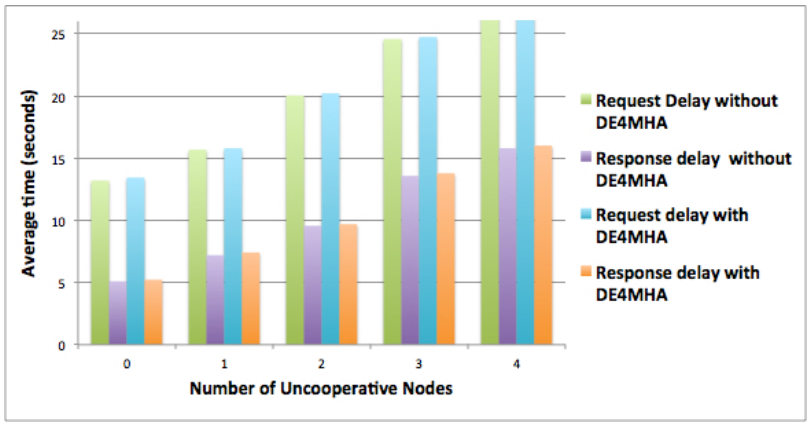


Figure 16. Average request and response time delay in function of the number of uncooperative mobile nodes with and without the DE4MHA.

6 – Conclusion and Future Work

This paper described, in detail, a data encryption solution for mobile health applications using a cooperation strategy proposed in [61], called DE4MHA. The data encryption algorithm DE4MHA with cooperation mechanisms embedded in mobile health applications allows users to safely obtain health information with data carried safely. DE4MHA uses a hybrid approach using symmetric and asymmetric encryption algorithms. From this study, it was concluded the most suited symmetric algorithm for m-Health network architecture is the AES algorithm. For the same network scenarios using typical m-Health architectures, this study concludes the most suited asymmetric algorithm is the RSA. For communication with Web services, the HTTPS protocol is the most suitable security mechanism.

The performance evaluation of this cryptography strategy shows that overall network and SapoFit performance was not degraded, maintaining slightly the same performance that without the encryption strategy. DE4MHA offers a robust and reliable increase of privacy, confidentiality, integrity, and authenticity on m-Health applications. Although it was experimented on a specific m-Health application, called SapoFit, both DE4MHA and the cooperation strategy can be deployed in a given m-Health application.

In future works we will test the impact of security attacks[36] in DE4MHA. Moreover, A performance evaluation study of DE4MHA in other m-Health applications to obtain comparison results with other health data types and length may be considered for further works. A comparison of a performance evaluation results obtained by simulation may also be considered.

Acknowledgments

This work has been partially supported by *Instituto de Telecomunicações,* Next Generation Networks and Applications Group (NetGNA), Portugal, by National Funding from the FCT - *Fundação para a Ciência e a Tecnologia* through the PEst-OE/EEI/LA0008/2011 Project, and by the AAL4ALL (Ambient Assisted Living for All), project co-funded by COMPETE under FEDER via QREN Programme.

References

[1] Akter, S., D'Ambra, J., and Ray, P. (2010). User Perceived Service Quality of mHealth Services in Developing Countries. European Conference on Information Systems (ECIS 2010). South Africa. 6-9 June 2010, pp 1-12.

[2] Akter, S. and Ray, P. (2010). mHealth - an Ultimate Platform to Serve the Unserved. IMIA Yearbook of Medical Informatics - Biomedical Informatics: Building Capacity Worldwide. Schattauer, Germany, pp 94-100.

[3] Antoniou, G., Batten, L. (2011). E-commerce: protecting purchaser privacy to enforce trust. Electronic Commerce Research, November 2011, Vol. 11, Issue 4, pp 421-456.

[4] Agrawal, M., and Mishra, P. (2012). A Comparative Survey on Symmetric Key Encryption Techniques. International Journal on Computer Science and Engineering, Vol. 4, pp 877–882.

[5] Bannon, L. and Hughes, J. (1993). The Context of CSCW. K. Schmidt (Ed.), Report of COST14 "CoTech". Working Group 4 (1991-1992).

[6] Batten, L. (2013). Public Key Cryptography: Wiley-IEEE Press.

[7] Biryukov A., Nakahara J., Preneel B., and Vandewalle J. (2002) New Weak Key Classes of IDEA. Lecture Notes In Computer Science. Vol. 2513, pp 315-326.

[8] Biswas, G. (2008) Diffie-Hellman technique: extended to multiple two-party keys and one multi-party key. IET Information Security. Vol. 2(1), pp 12-18.

[9] Bleumer, G. (1994). Security for decentralized health information systems. International Journal of Bio-Medical Computing. February 1994, pp 139-145

[10] Boonyarattaphan, A., Bai, Y., Chung , S. (2009) A security framework for e-Health service authentication and e-Health data transmission. 9th International Symposium on Communications and Information Technology (ISCIT 2009). 28-29 September, pp 1213-1218.

[11] Buttyán, L. and Hubaux , J.-P. (2003). Stimulating Cooperation in Self-Organizing Mobile Ad hoc Networks. Mobile Networks and Applications. Vol. 8(5), pp 579-592.

[12] Chan, V., Ray, P., and Parameswaran, N. (2008). Mobile e-Health monitoring: an agent-based approach. IET Communications. Vol. 2(2), pp 223-230.

[13] Chang, H. (2013). The security service rating design for IT convergence services. Electronic Commerce Research. Published Online: 15 May 2013. DOI: 10.1007/s10660-013-9115-2

[14] Chen, Y., and Ku, W. Self-encryption scheme for data security in mobile devices. Proceedings of the 6th IEEE Conference on Consumer Communications and Networking Conference, 850-854.

[15] Cochran, M. (2008). Cryptographic Hash Functions: ProQuest.

[16] Cubic, I., Markota, I., and Benc, I. (2010). Application of session initiation protocol in mobile health systems. Proceedings of the 33rd International Convention MIPRO. Opatija, Croatia, 24-28 May, pp 367–371.

[17] Déglise, C., Suggs, L., and Odermatt, P. (2012) Short message service (SMS) applications for disease prevention in developing countries. Journal of Medical Internet Research, Vol. 14(1), http://www.jmir.org/2012/1/e3/.

[18] Diffie, W. (1988). The first ten years of public-key cryptography. Proceedings of the IEEE. Vol. 76(5),pp 560-577.

[19] Eastlake, D., and Jones, P. (2001). US Secure Hash Algorithm 1. http://www.ietf.org/rfc/rfc3174.txt. Accessed 12 January 2013.

[20] Elminaam, D., Kader, H., and Hadhoud, M. (2010). Evaluating the performance of symmetric encryption algorithms. International Journal of Network Security. Vol. 10(3), pp 213–219.

[21] Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory. Vol. 31(4), pp 469- 472.

[22] Fayn, J., and Rubel, P. (2010). Towards a personal health society in cardiology. IEEE Transactions on Information Technology in Biomedicine. Vol. 14(2), pp 401-409.

[23] Federal Information Processing Standards Publication. Data Encryption Standard (Des). http://www.itl.nist.gov/fipspubs/fip46-2.htm. Accessed 12 January 2013.

[24] Ferguson, N., Schneier, B., and Kohno, T. (2012). Cryptography Engineering: Wiley. ISBN: 978-0-470-47424-2

[25] Goldreich, O. (2005). Foundations of Cryptography: Now Publishers Inc. ISBN 10: 1933019026.

[26] Gritzalis, S., Zhan, J., Z., Jeong, K. (2013). IT convergence and security. Electronic Commerce Research. Published Online: 9 May 2013. DOI: 10.1007/s10660-013-9114-3

[27] Gupta, A. (2008). Challenges of Mobile Computing. Proceedings of 2nd National Conference on Challenges and Opportunities in Information Technology. 29 March, pp 86-90.

[28] Housley, R. (2001). Triple-DES and RC2 Key Wrapping. http://www.ietf.org/rfc/rfc3217.txt. Accessed 12 January 2013.

[29] Istepanian, R., and Lacal, J. (2003). Emerging Mobile Communication Technologies for Health: Some Imperative notes on m-Health. Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society. Vol. 2, pp 1414-1416.

[30] Isaac, J. T., Zeadally, S., Cámara J., S. (2012). A lightweight secure mobile Payment protocol for vehicular ad-hoc networks (VANETs). Electronic Commerce Research. March 2012, Vol. 12(1), pp 97-123.

[31] Jaganathan, K., Zhu, L., and Brezak, J. (2006). The RC4-HMAC Kerberos Encryption Types. http://tools.ietf.org/html/rfc4757 /. Accessed 12 January 2013.

[32] Jara, A., Zamora, M., Skarmeta, A. (2011). An Internet of things-based personal device for diabetes therapy management in ambient assisted living (AAL). Personal and Ubiquitous Computing. Vol. 15(4), pp 431-440.

[33] Jonsson, J. and Kaliski, B. (2003). Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. http://tools.ietf.org/html/rfc3447. Accessed 12 January 2013.

[34] Kramer, G., Maric, I., and Yates, R. D. (2007). Cooperative communications (Foundations and Trends in Networking): Now Publishers Inc, ISBN-10: 1601980264.

[35] Kollmann, A., Riedl, M., Kastner, P., Schreier, G., and Ludvik, B. (2007). Feasibility of a mobile phone-based data service for functional insulin treatment of type 1 diabetes mellitus patients. Journal of Medical Internet Research. Vol. 9(5). http://www.jmir.org/2007/5/e36/.

[36] Koukopoulos, D., Styliaras, G. (2013). Design of trustworthy smartphone-based multimedia services in cultural environments. Electronic Commerce Research. May 2013, Vol. 13(2), pp 129-150.

[37] Kuncha Sahadevaiah and Prasad Reddy P.V.G.D. (2011). Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks, Network Protocols and Algorithms, Vol. 3(4), pp. 122-140.

[38] Lacuesta, R. Lloret, J. Garcia, M. Peñalver, L. (2013). A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation. IEEE Transactions on Parallel and Distributed Systems. Vol. 24(4), pp. 629-64. DOI:10.1109/TPDS.2012.168.

[39] Laxminarayan S., Istepanian R., and Pattichis C. S. (2006). M-Health: Emerging Mobile Health Systems: Springer. ISBN-10: 0387265589**.**

[40] Lin, C. T., Chang, K. C., Lin, C. L., Chiang C.C., Lu, S.W., Chang, S. S., et al. (2010). An intelligent telecardiology system using a wearable and wireless ECG to detect atrial fibrillation. IEEE Transactions On Information Technology in Biomedicine. Vol. 14(3), pp 726-733.

[41] Martin, K. (2012). Everyday Cryptography: OUP Oxford. ISBN-10**:** 0199695598.

[42] Moullee, B., and Ray, P. (2009). Issues in E-Health Cost Impact Assessment. In IFMBE Proceeding of the World Congress on Medical Physics and Biomedical Engineering. Berlin: Springer, pp. 223-226.

[43] Mirkovic, J., Bryhni, H., Ruland, C. (2011). Secure solution for mobile access to patient's health care record. 13th IEEE International Conference on e-Health Networking Applications and Services. 13-15 June. Columbia, USA, pp 296-303.

[44] Mougiakakou, S., Bartsocas, C., Bozas, E., Chaniotakis, N., Iliopoulou, D., Kouris, I., et al. (2010). SMARTDIAB: a communication and information technology approach for the intelligent monitoring, management and follow-up of type 1 diabetes patients. IEEE Transactions On Information Technology in Biomedicine. Vol. 14(3), pp 622-33.

[45] Paar, C., and Pelzl, J., (2010) The Data Encryption Standard (DES) and Alternatives. Understanding Cryptography, A Textbook for Students and Practitioners: Springer. pp 55-86.

[46] Pachghare, V. K. (2009). Cryptography And Information Security: PHI Learning Pvt. Ltd. ISBN: 978-81-203-3521-9.

[47] Pare, G., Moqadem, K., Pineau, G., and St-Hilaire, C. (2010) Clinical effects of home telemonitoring in the context of diabetes, asthma, heart failure and hypertension: a systematic review. Journal of Medical Internet Research. Vol. 12(2). http://www.jmir.org/2010/2/e21/.

[48] Patrick, K., Raab, F., Adams, M., Dillon, L., Zabinski, M., Rock, C., Griswold, W., and Norman, G. (2009). A text message-based intervention for weight loss: randomized controlled

trial. Journal of Medical Internet Research. Vol 11(1). http://www.jmir.org/article/citations/1100.

[49] Pollak, J., Gay, G., Byrne, S., Wagner, E., Retelny, D., and Humphreys, L. (2010). It's Time to Eat! Using Mobile Games to Promote Healthy Eating. IEEE Pervasive Computing. Vol. 9(2), pp 21-27.

[50] Qiang, Z., and Yamamichi, M. (2012). Mobile Applications for the Health Sector. http://siteresources.worldbank.org/INFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/mHealth_report.pdf. Accessed 12 January 2013.

[51] Raeburn K. (2005) Advanced Encryption Standard (AES) Encryption for Kerberos 5. http://www.ietf.org/rfc/rfc3962.txt. Accessed 12 January 2013.

[52] Ray, P., Parameswaran, N., Chan, V., and Yu, W. (2008). Awareness modeling in collaborative mobile e-health. Journal of Telemedine and Telecare. Vol. 14(7), pp 381-385.

[53] Raychaudhuri, K. and Ray, P. (2010) Privacy Challenges in the Use of eHealth Systems for Public Health Management. International Journal of e- Health and Medical Communications. Vol. 1(2), pp 12–23.

[54] Rivest, R. (1992). The MD5 Message-Digest Algorithm. http://www.ietf.org/rfc/rfc1321.txt. Accessed 12 January 2013.

[55] Rodrigues, J., Oliveira, M., and Vaidya B. (2010). New Trends on Ubiquitous Mobile Multimedia Applications. EURASIP Journal on Wireless Communications and Networking, Vol. 2010(10), pp 1-12.

[56] Rodrigues, J., Lopes I., Silva, B., and Torre, I. (2013) A new mobile ubiquitous computing application to control obesity: SapoFit. Informatics for Health and Social Care, Vol. 38(1), pp 37-53.

[57] SapoFit. http://itunes.apple.com/pt/app/sapo-fit/id438487775?mt=8. Accessed 12 January 2013.

[58] Schneier, B. (1994). The Blowfish encryption algorithm. Dr Dobb's Journal-Software Tools for the Professional Programmer. Vol. 19(4), pp 38-43.

[59] Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C: Join Wiley and Sons, Inc. ISBN-10: 0471117099

[60] Shanmugam M., Thiruvengadam, S., Khurat, A., and Maglogiannis, I. (2006). Enabling Secure Mobile Access for Electronic Health Care Applications. Pervasive Health Conference and Workshops. 29 November – 1 December. Innsbruck, Austria, pp 1-8.

[61] Silva, B., Rodrigues, J., Lopes, I., Machado, and T., Zhou, L. (2012). A Novel Cooperation Strategy for Mobile Health Applications. IEEE Journal on Selected Areas in Communications Special Issue on Emerging Technologies in Communications - eHealth, IEEE Communications Society (in press).

[62] Silva, B., Lopes, I., Rodrigues, J., and Ray, P. (2011) SapoFitness: A mobile health application for dietary evaluation. 13th IEEE International Conference on e-Health Networking Applications and Services (Healthcom 2011). 13-15 June. Columbia, Missouri, USA, pp 375-380.

[63] Smith, R. (2005). Introduction to multilevel security. Handbook of Information Security: Google Scholar.

[64] Sulaiman, R., Sharma, D., Ma, W., and Tran, D. (2008) A Security Architecture for e-Health Services. 10th International Conference on Advanced Communication Technology. Gangwon-Do, South Korea, Vol. 2, pp 99-104.

[65] Tachakra, S., Wang, X., Istepanian, R., and Song, Y. (2003) Mobile e-Health: the Unwired Evolution of Telemedicine. Telemedicine Journal and e- Health. Vol. 9(3), pp 247–257.

[66] Tillich, S., and Herbst, C. (2008) Attacking State-of-the-Art Software Countermeasures—A Case Study for AES. Proceedings of the 10th international workshop on Cryptographic Hardware and Embedded Systems. 10-13 August. Washington, D.C., USA, pp 228-243.

[67] Watson, A., Bickmore, T., Cange, A., Kulshreshtha, A., and Kvedar, J. (2012). An internet-based virtual coach to promote physical activity adherence in overweight adults: randomized controlled trial. Journal of Medical Internet Research. Vol. 14(1). http://www.jmir.org/2012/1/e1/.

[68] Whittaker, R., Dorey, E., Bramley, D., Bullen, C., Denny, S., Elley, C. et al. (2011). A theory-based video messaging mobile phone intervention for smoking cessation: randomized controlled trial. Journal of Medical Internet Research. Vol. 13(1). http://www.jmir.org/2011/1/e10/.

[69] Yong-Xia, Z. and Ge, Z. (2010). MD5 Research. Second International Conference on Multimedia and Information Technology. 24-25 April. Kaifeng, China, Vol. 2, pp 271-273.

[70] Zheng, P., and Ni, L. (2005). Smart Phone and Next Generation Mobile Computing: Morgan Kaufmann. ISBN-10: 0120885603.

[71] Zhu, F., Bosch, M., Woo, I., Kim, S., Boushey, C., Ebert, D., and Delp, E. (2010). The Use of Mobile Devices in Aiding Dietary Assessment and Evaluation. IEEE Journal of Selected Topics in Signal Processing. Vol. 4(4), pp 756-766.

Bruno Silva received his BsC degree (licentiate) in 2008 in Informatics Engineering from University of Beira Interior, Portugal. In 2010, he received his MsC degree in Informatics Engineering from University of Beira Interior. He is currently a PhD student on Informatics Engineering at the University of Beira Interior under supervision of Prof. Joel J. P. C. Rodrigues. He is also a PhD student member of the Instituto de Telecomunicações, Portugal. His current research interests include Delay Tolerant Networks, Vehicular Networks, Mobile Computing, Ubiquitous Computing, e-Health but especially in mobile Health. He authors or co-authors 12 international conference papers and 4 International Journal publications.

Joel Rodrigues is a professor in the Department of Informatics of the University of Beira Interior, Covilhã, Portugal, and researcher at the Instituto de Telecomunicações, Portugal. He received a PhD degree in informatics engineering, an MSc degree from the University of Beira Interior, and a five-year BSc degree (licentiate) in informatics engineering from the University of Coimbra, Portugal. His main research interests include sensor networks, e-health, e-learning, vehicular delay-tolerant networks, and mobile and ubiquitous computing. He is the leader of NetGNA Research Group (http://netgna.it.ubi.pt), the Chair of the IEEE ComSoc Technical Committee on Communications Software, the Vice-Chair of the IEEE ComSoc Technical Committee on eHealth, and Member Representative of the IEEE Communications Society on the IEEE Biometrics Council. He is the editor-in-chief of the International Journal on E-Health and Medical Communications, the editor-in-chief of the Recent Patents on Telecommunications, and editorial board member of several journals. He has been general chair and TPC Chair of many international conferences. He is a member of many international TPCs and participated in several international conferences organization. He has authored or coauthored over 250 papers in refereed international journals and conferences, a book, and 2 patents. He had been awarded the Outstanding Leadership Award of IEEE GLOBECOM 2010 as CSSMA Symposium Co-Chair and several best papers awards. Prof. Rodrigues is a licensed professional engineer (as senior member), member of the Internet Society, an IARIA fellow, and a senior member of ACM and IEEE.

Fábio Canelo received his BSc degree (licenciate) in 2011 in Information Systems and Technologies from University of Beira Interior, Portugal. Currently, he is concluding his MSc degree in Informatics Engineering also from the University of Beira Interior. He is a student member of the Instituto de Telecomunicações, Portugal. His current research topics include Security Mechanisms, Mobile Computing, and Ubiquitous Computing. He has co-authored one journal publication.

Ivo Lopes is a PhD student on Informatics Engineering at the University of Beira Interior, Covilhã Portugal, under supervision of Prof. Joel J. P. C. Rodrigues. He received his Master degree in Informatics Engineering from University of Beira Interior, 2011. His research interests include mobile and ubiquitous computing, e-Health, Ambient Assisted Living, Web Services, and sensor networks. Currently he is affiliated with Instituto de Telecomunicações, Portugal since March 2009. He has authored or co-authored of several papers in international journals, books, and conferences.

Jaime Lloret (jlloret@dcom.upv.es) received his M.Sc. in Physics in 1997, his M.Sc. in electronic Engineering in 2003 and his Ph.D. in telecommunication engineering (Dr. Ing.) in 2006. He is a Cisco Certified Network Professional Instructor. He is currently Associate Professor in the Polytechnic University of Valencia. He is the head of the research group "communications and remote sensing" of the Integrated Management Coastal Research Institute and he is the head of the "Active and collaborative techniques and use of technologic resources in the education (EITACURTE)" Innovation Group. He is the director of the University Expert Certificate “Redes y Comunicaciones de Ordenadores”, the University Expert Certificate “Tecnologías Web y Comercio Electrónico”, and the University Master "Digital Post Production". He is currently Vice-chair of the Internet Technical Committee (IEEE Communications Society and Internet society). He has authored 12 books and has more than 240 research papers published in national and international conferences, international journals (more than 70 with ISI Thomson Impact Factor). He has been the co-editor of 15 conference proceedings and guest editor of several international books and journals. He is editor-in-chief of the international journal "Networks Protocols and Algorithms", IARIA Journals Board Chair (8 Journals) and he is associate editor of several international journals. He has been involved in more than 200 Program committees of international conferences and in many organization and steering committees. He led many national and international projects. He is currently the chair of the Working Group for the Standard IEEE 1907.1. He has been the general chair (or co-chair) of 18 International conferences. He is IEEE Senior and IARIA Fellow.

Chapter 6

A Data Encryption Solution for Mobile Health Apps in Cooperation Environments: DE4MHA

This chapter consists of the following article:

A Data Encryption Solution for Mobile Health Apps in Cooperation Environments: DE4MHA

Bruno M. Silva, Joel J. P. C. Rodrigues, Fábio Canelo, Ivo M. C. Lopes, and Liang Zhou

Journal of Medical Internet Research, Volume 15, Issue 8: e66, August 2013.

DOI: dx.doi.org/10.2196/jmir.2498

According to 2013 Journal Citation Reports published by Thomson Reuters in 2014, this journal scored ISI journal performance metrics as follows:

ISI Impact Factor (2013): 4.669

ISI Article InfluenceScore (2013): 1.369

Journal Ranking (2013): 4/85 (Health Care Sciences & Services)

Journal Ranking (2013): 1/25 (Medical Informatics)

JOURNAL OF MEDICAL INTERNET RESEARCH Silva et al

Original Paper

A Data Encryption Solution for Mobile Health Applications in Cooperation Environments: DE4MHA

Bruno M Silva[1], B.Sc, MSc; Joel JPC Rodrigues[1], BSC, MSc, PhD; Fábio Canelo[1], BSC, Msc Candidate; Ivo C Lopes[1], BSC, MSc; Liang Zhou[2], BSC, MSc, PhD

[1]Instituto de Telecomunicações, University of Beira Interior, Covilhã, Portugal

[2]Nanjing University of Posts and Telecommunications, Nanjing, China

Corresponding Author:
Joel JPC Rodrigues, BSC, MSc, PhD
Instituto de Telecomunicações, University of Beira Interior
Rua Marques D'Avila e Bolama
Covilhã, 6201-001
Portugal
Phone: 351 275242081
Fax: 351 275319891
Email: joeljr@ieee.org

Abstract

Background: Mobile Health (mHealth) proposes health care delivering anytime and anywhere. It aims to answer several emerging problems in health services, including the increasing number of chronic diseases, high costs on national health services, and the need to provide direct access to health services, regardless of time and place. mHealth systems include the use of mobile devices and applications that interact with patients and caretakers. However, mobile devices present several constraints, such as processor, energy, and storage resource limitations. The constant mobility and often-required Internet connectivity also exposes and compromises the privacy and confidentiality of health information.

Objective: This paper presents a proposal, construction, performance evaluation, and validation of a data encryption solution for mobile health applications (DE4MHA), considering a novel and early-proposed cooperation strategy. The goal was to present a robust solution based on encryption algorithms that guarantee the best confidentiality, integrity, and authenticity of users health information. In this paper, we presented, explained, evaluated the performance, and discussed the cooperation mechanisms and the proposed encryption solution for mHealth applications.

Methods: First, we designed and deployed the DE4MHA. Then two studies were performed: (1) study and comparison of symmetric and asymmetric encryption/decryption algorithms in an mHealth application under a cooperation environment, and (2) performance evaluation of the DE4MHA. Its performance was evaluated through a prototype using an mHealth application for obesity prevention and cares, called SapoFit. We then conducted an evaluation study of the mHealth application with cooperation mechanisms and the DE4MHA using real users and a real cooperation scenario. In 5 days, 5 different groups of 7 students selected randomly agreed to use and experiment the SapoFit application using the 7 devices available for trials.

Results: There were 35 users of SapoFit that participated in this study. The performance evaluation of the application was done using 7 real mobile devices in 5 different days. The results showed that confidentiality and protection of the users' health information was guaranteed and SapoFit users were able to use the mHealth application with satisfactory quality. Results also showed that the application with the DE4MHA presented nearly the same results as the application without the DE4MHA. The performance evaluation results considered the probability that a request was successfully answered as a function of the number of uncooperative nodes in the network. The service delivery probability decreased with the increase of uncooperative mobile nodes. Using DE4MHA, it was observed that performance presented a slightly worse result. The service average was also slightly worse but practically insignificantly different than with DE4MHA, being considered negligible.

Conclusions: This paper proposed a data encryption solution for mobile health applications, called DE4MHA. The data encryption algorithm DE4MHA with cooperation mechanisms in mobile health allow users to safely obtain health information with the data being carried securely. These security mechanisms did not deteriorate the overall network performance and the application, maintaining similar performance levels as without the encryption. More importantly, it offers a robust and reliable increase of privacy, confidentiality, integrity, and authenticity of their health information. Although it was experimented on a specific mHealth application, SapoFit, both DE4MHA and the cooperation strategy can be deployed in other mHealth applications.

(J Med Internet Res 2013;15(3):e66) doi:10.2196/jmir.2498

KEYWORDS

mobile health; mHealth; mobile computing; eHealth; cooperation; encryption, security

Introduction

In the last decade, health telematics, also known as electronic health (eHealth), have offered patients major improvements in their lives by providing more accessible and affordable health care solutions [1,2]. This is particularly true for patients that live in remote rural areas, travel constantly, are physically incapacitated, elderly, or chronically ill. Telemedicine assumes the use of medical information, also known as electronic health records (EHRs), exchanged via electronic communications improving the patients' health status [3]. The rapid evolution of information and communication technology (ICT) infrastructures enables and provides rapid access to patient data. The Web 2.0 concept and the emerging Web 3.0 offer opportunities to health care professionals never seen before [4,5]. Now, physicians can perform many tasks through these modern technologies, such as (1) sharing medical videos, photos, and presentations (via YouTube, Flickr, and Slideshare, respectively), (2) use blogs to post medical cases and images, (3) share hospital management information, (4) use social networking to share medical ideas and tasks, and (5) use RSS feeds to keep track of alerts on specific medical interests.

With the advent of mobile communications using smart mobile devices that support 3G and 4G mobile networks for data transport, mobile computing has been the main attraction of research and business communities, thus offering innumerous opportunities to create efficient mobile health solutions. Mobile health (mHealth) is the new edge on health care innovations. It delivers health care anywhere and anytime, surpassing geographical, temporal, and even organizational barriers [6,7]. Laxminarayan and Istepanian defined mobile health for the first time in 2000, as "unwired e-med" [8]. In 2003, the term "mHealth" was defined as the "emerging mobile communications and network technologies for health care systems" [9]. Laxminarayan et al, in 2006, presented a comprehensive study on the impact of mobility on the existing eHealth commercial telemedical systems. They also presented other relevant computing and information technologies that will influence and offer the basis for the next generation of mHealth services [10]. Furthermore, this study served as the basis for future studies on mHealth technologies and services [11]. Several research topics related to health have gathered important findings and contributions using mHealth, such as cardiology [12,13], diabetes [14-16], obesity [17-20], and smoking cessation [21]. More specifically, mHealth applications were applied to health monitoring, disease prevention and detection, basic diagnosis, and in more advanced services. mHealth services are also becoming popular in developing countries where health care facilities are frequently remote and inaccessible [2,22].

Mobile devices and wireless communications present several challenging characteristics and constraints, such as battery and storage capacity, broadcasting constraints, signal interferences, disconnections, noises, limited bandwidths, and network delays. In this sense, cooperation-based approaches are presented as a solution to solve such limitations, focusing on increasing network connectivity, communication rates, and reliability.

In this paper, we present a data encryption solution for mHealth applications (DE4MHA) in cooperative environments guaranteeing data confidentiality, integrity, and authenticity. This novel and early-proposed cooperation strategy [23] for mHealth applications focuses on forwarding and retrieving data to and from nodes that have no direct connection to an mHealth service. In this way, devices without Internet connectivity can use mHealth applications without problems. This cooperation approach presents a reputation-based strategy where a Web service manages the access control and the cooperation among nodes along with their reputation. It considers the following three main components: a *node control message*, a *requester control message*, and a *cooperative Web service* (CWS). Both control messages are used to manage a local cooperation between two or more nodes. The CWS includes a reputation table for all the nodes and decides which nodes can have access to the requested services. The cooperation strategy and the DE4MHA was deployed and evaluated in an mHealth application for obesity prevention and control, called SapoFit [24-26]. To the best of our knowledge, there are no cooperative solutions thus far for mHealth services and applications considering this network scenario with constant network disconnection. DE4MHA uses symmetric and asymmetric encryption and decryption techniques. We used the Rivest, Shamir, Adleman (RSA) algorithm [27] for asymmetric encryption/decryption to ensure key exchange confidentiality, and the Advanced Encryption Standard (AES) [28] algorithm for symmetric encryption/decryption for data confidentiality. To ensure data integrity, we have created a message digest that creates a hash of transmitted data. For data authenticity, we used a digital signature. We encrypted the hash message with the RSA private key. To secure the communication with the SapoFit Web service (WS), we used the Hypertext Transfer Protocol Secure (HTTPS) protocol.

In this paper we report two studies that were performed to design and construct the DE4MHA algorithms: (1) a direct evaluation and comparison of several encryption algorithms, and (2) a series of trials evolving 35 people and 7 different mobile devices with SapoFit. The first study revealed what algorithms performed best in an mHealth application in cooperation environments. Overall, this study evaluated the performance of the DE4MHA over the cooperation mechanisms for mHealth applications. The second study revealed that real users experimenting on the SapoFit application trusted DE4MHA. More relevant, this study concluded that the performance of the application used was not affected by the inclusion of DE4MHA.

Methods

Overview

This study used an existing mHealth application, called SapoFit, to deploy, evaluate, and validate the proposed solution. This application uses a cooperation strategy that addresses two related limitations to mHealth applications with service-oriented architectures, namely the network infrastructure and Internet connectivity dependency. It follows a reputation-based approach as an incentive method for cooperation, which includes a Web service to manage all the network cooperation. It is responsible for verifying the cooperation status of neighbor nodes and to provide relay nodes the required data in order to perform a full data request.

Cooperation Strategy for mHealth Applications

The cooperation strategy for mHealth applications with service oriented architectures (SOAs) is based on the following two mobile modules and one remote module, respectively: (1) the *node control message*, (2) the *requester control message*, and (3) the *CWS*.

The mobile *nodes control messages* aim to provide an awareness of the relay node status, that is, if the node is willing to cooperate and in what conditions. It contains the established node unique identifier, the battery state, the Internet connectivity status, and the cooperation status (ie, if it is cooperative or not).

The *requester control message* is sent by the initial requester node first (the mobile device with mHealth application requesting health data), and it comprises the following five main components: (1) the requester ID, the node unique identifier, (2) the service request, that is, what the node is specifically requesting (eg, the login token or its health profile), (3) the neighbors list, (4) the reputation list, and (5) the achieved cooperation time (ACT).

The *CWS* is responsible for performing a fair access control to data. Thus, according to the received reputation information, the Web service holds the final reputation list in order to decide if a requester node should have access to the mHealth application Web service or not. The reputation list contains all registered network nodes with their identifier and their corresponding reputation value.

Figure 1 presents a user scenario of the mHealth cooperation approach. *User A* has network connectivity and cooperates. *User B* has network connectivity and does not cooperate. The status value is according to the battery status. Then, the status value will suffer a negative impact according to the battery status. *Users C* and *D* do not have network connectivity. *User C* queries *User A* for cooperation and receives a positive response and all the requested data. *User D* queries *User B* for cooperation and receives a negative response. Then, *User D* requests data from *User C* that answers this request, getting positive status by cooperating.

SapoFit Application

SapoFit is a weight control mobile application that allows users to keep track of weight in a healthier and more practical way. SapoFit allows users to control their weight, body mass index (BMI), basal metabolic rate (BMR), sports activity, and the possibility to follow food plans based on their needed calories. In this mHealth application, all the users must be registered in a Web service. Figure 2 presents screenshots of three main activities of the SapoFit application: *Login*, *Plans*, and *User Profile.*

Cooperating nodes have a better reputation, and have priority over selfish nodes to access the mHealth application services.

Figure 1. Illustration of the interaction for an mHealth application with the proposed cooperation approach for 4 users.

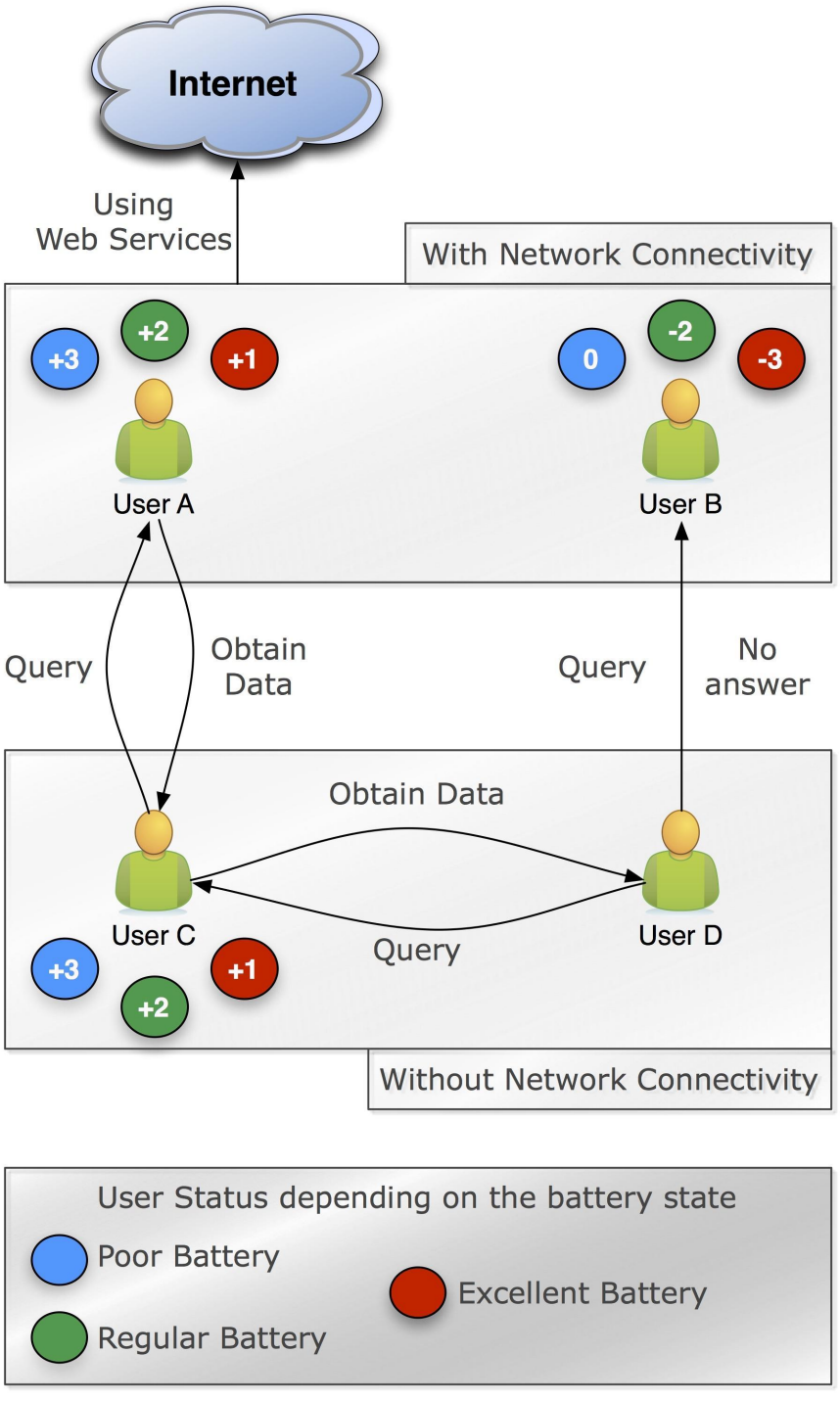


Figure 2. Screenshots of the three main activities of SapoFit application: Login, Plans, and User Profile.

Data Encryption Algorithm for Mobile Health Applications (DE4MHA)

The process begins with a mobile node (a person using SapoFit) trying to access the SapoFit Web Service that contains the user profile, weight measures, fitness, and diet indications.

A SapoFit user (mobile requester node) without network connectivity and therefore without access to the SapoFit WS obtains the required health information through cooperation. Another SapoFit user with network connectivity (mobile requested node) will forward the requested health information from the SapoFit Web service. Both the requested and requester nodes will create a pair of RSA keys and send public keys to both the requested and requester node through Bluetooth. After the public key exchange, the requested node creates an AES session key.

The next step is the creation of the digest message and its encryption using the private key. The Message Digest 5 (MD5) algorithm was used to create a 128-bit hash. For data authenticity, we used a digital signature. A digital signature is created for the message containing requested health information. This digital signature allows any node to verify that the message is the original one. By decrypting the digital signature with the public key, the original digest message is obtained. The receiver node then creates a new hash of the received message and compares it to the decrypted digest message to guarantee authenticity. The digital signature is then added to the message. When the message containing the session key is received, if its integrity and authenticity is verified, the requester node then sends an acknowledgement (*ack*) to the requested node. This method guaranties safe communication between nodes; if the integrity and authenticity is not verified, the communication between nodes is ended.

A mobile node with network connectivity will access the cooperative WS to obtain the required health information. To secure all communication with the WS the Secure Socket Layer (SSL) over the HTTP (also known as HTTPS) is used. Therefore, it grants confidentiality, integrity, and authenticity of all retrieved health data from the Web service.

Two studies were performed: (1) a study evaluating which symmetric and asymmetric algorithm present the best performance in SapoFit in cooperation environment, and (2) a series of trials involving 35 people and 7 different mobile devices with SapoFit. This study evaluated the performance of the DE4MHA over the cooperation mechanisms.

Study 1: Study of Cryptography Algorithms in an mHealth Application Under a Cooperation Environment

Symmetric Algorithm

In order to choose the best suited symmetric encryption algorithm for the SapoFit application, performance experiments were conducted using 4 different encryption algorithms, namely AES, Triple Data Encryption Standard (3DES) [29], Rivest Cypher 4 (RC4) [30], and Blowfish [31], using the data size encryption as a performance metric.

Asymmetric Algorithm

Two options were considered in selecting an asymmetric algorithm to exchange session keys between mobile nodes. We tested RSA, which enables encrypting the session key before sending it, and Diffie-Hellman [32], which allows users to first

share a secret, then generating a session key based on the shared secret. For our network scenario, these were the most suitable algorithms. Other encryption algorithms were considered in this study, such as the Elliptic Curve Cryptography (ECC) algorithm [33].

Study 2: Performance evaluation of the DE4MHA

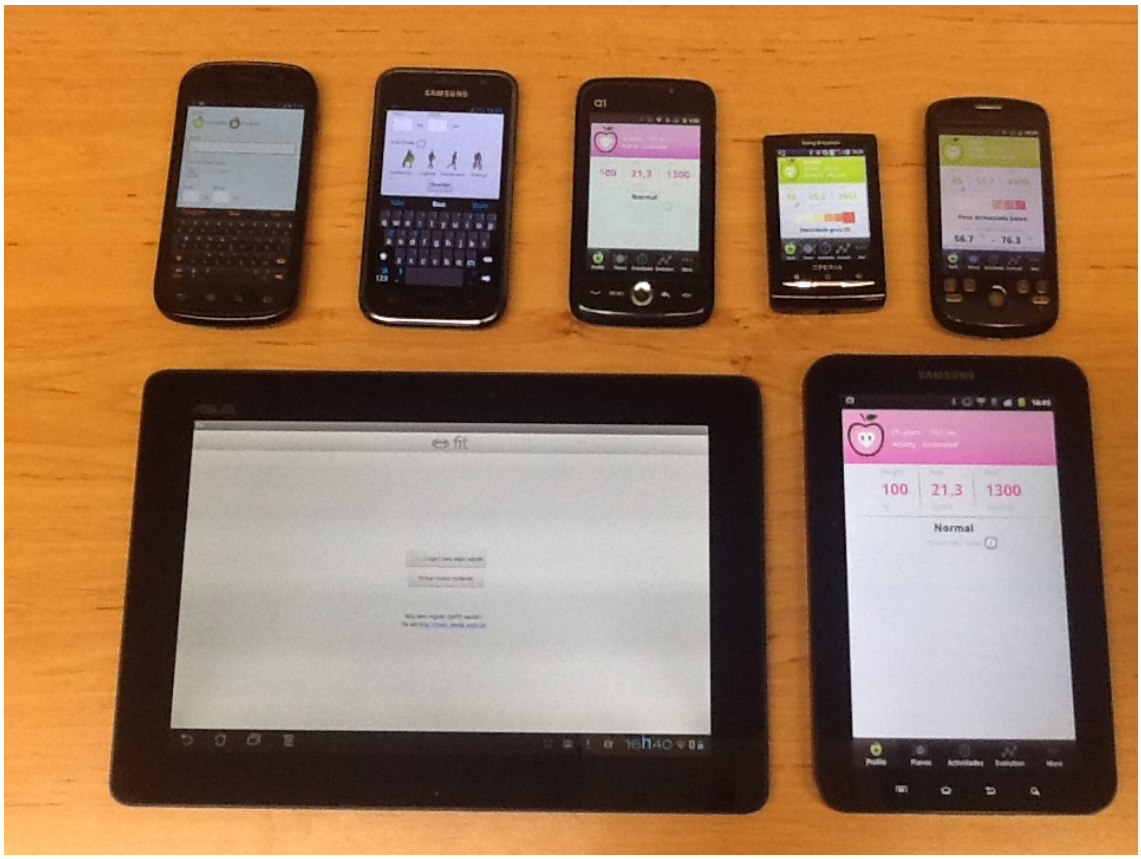
Performance Evaluation

The performance evaluation study was carried out using 7 real mobile devices, which were used 7 times in 5 different days with a total of 35 different users who successfully tested the application. Figure 3 presents the 7 different mobile devices with different hardware and software used with the SapoFit mHealth application.

Cooperative nodes without network connection cooperated with each other through Bluetooth. The communication with the CWS was obtained through the Wi-Fi or Edge/3.5G/4G modules of the device. The CWS was developed with the help of Java Server Pages (JSP) technology, using the Representational State Transfer (REST) architecture. To serve the WS, the Apache Tomcat Web Server was used.

Non-cooperative cases were controlled and measured to a maximum of 4 to guarantee the minimum service performance in order to guarantee cooperation among nodes. Through cooperation, all the devices could use the mHealth application. However, uncooperative nodes directly affect the service delivery probability, service average delay, and the overall network performance. Performance metrics considered in this study were the service delivery probability (as percentages) and the average service delay (in seconds). We present a comparison of the performance of the mHealth application with and without the DE4MHA.

Figure 3. Mobile devices used for trials with the SapoFit mHealth application.



User Trials Evaluation of DE4MHA in Cooperative Environments

User trials were conducted within the University informatics department using 7 devices available for trials. Within 5 days, 5 different groups of 7 students selected randomly agreed to use and experiment the SapoFit application using the 7 devices available for trials. Users were constantly moving far away from each other. This mobility was necessary to test the network scenario, forcing network delays and disconnections. The cooperative strategy and the DE4MHA was ubiquitous to its user. Throughout the trials, users only experienced and used the obesity prevention services that SapoFit offered without any constraints or perception of any cooperation mechanism or encryption algorithm that was embedded in the mHealth application.

While conducting the experiments, almost every users asked if their information was being kept secure or not, clearly showing that they did not wanted their health information to be available

or disclosed to unauthorized people, revealing privacy concerns. Another frequently raised question was the need to share Internet connectivity to other users.

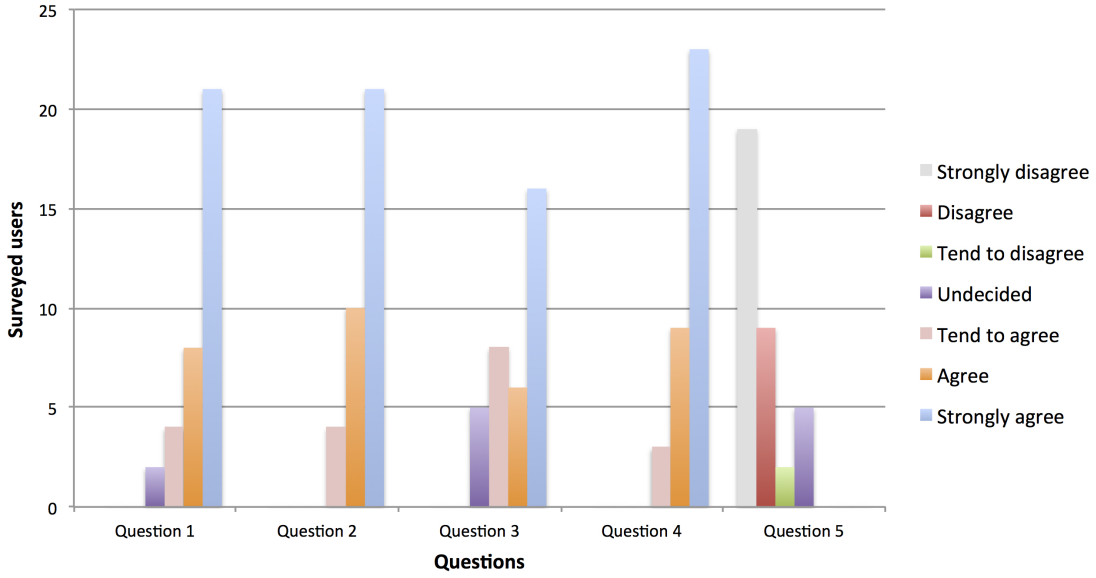
We explained and justified that sharing and cooperating with other users was essential to obtain a better reputation to gain cooperation privileges over other nodes with worse reputation. Furthermore we demonstrated to them that SapoFit was not intrusive with other users' personal data on the mobile device and only requested for SapoFit services.

After the experiments, the users completed a survey evaluating their experience. The questions are listed in Textbox 1and the results in Figure 4.

Textbox 1. Survey questions.

- Without network connectivity, do the user always gets the required information?
- Without network connectivity, does the required information get delivered in a comfortable time?
- Understanding the implemented cooperation strategy and its benefits, are you willing to cooperate and share the device/network resources with other users?
- With the encryption strategy applied to SapoFit, do you trust that your personal health information is secure?
- Was the mobile device affected by application cooperation and encryption mechanisms (eg, broadband, battery, etc)?

Figure 4. Results of the survey evaluating the main questions about the performance of the mHealth application with the proposed cooperation strategy and encryption solution.

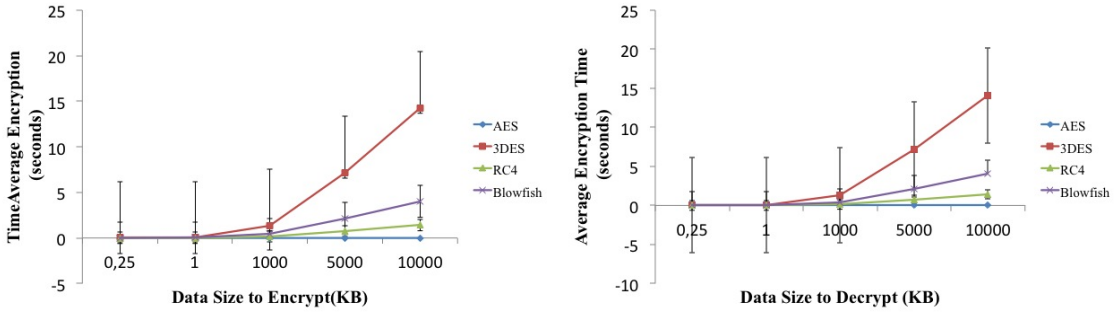


Results

Symmetric Algorithm

As seen in Figure 5, results showed that when the amount of data that needed to be encrypted increased, the encryption time (in seconds) also increased, as expected. When comparing small amounts of data, all 4 algorithms presented similar results. However, the AES algorithm presented better results, as there was a slower overall increase in encryption time in response to increased amount of data. The encryption time of the other three experimented algorithms grew exponentially when encryption data size exceeded 1000 kilobytes. The 3DES algorithm presented the worst encryption rate, encrypting 10,000KB of data in, on average, 14.3 seconds, presenting an average time of 4.58 seconds for multiple data size inputs (SD 6.17). With the same amount of data, the AES encryption time was only 0.0045 seconds, resulting in an average of 0.0035 seconds for the given data set (SD 0.00061 seconds). Decryption gave similar results (Figure 5). The average AES algorithm decryption time was 0.0038 seconds for 10,000KB of data and 0.0025 seconds on average for the working data-set (SD 0.001 seconds). Overall, the AES algorithm with a 128 bits key encryption was the most efficient algorithm for these network scenarios, when handling with both small and large amounts of data.

Figure 5. Comparison of encryption and decryption of symmetric algorithms (AES, 3DES, RC4, and Blowfish).



Asymmetric Algorithm

Two options were considered for an asymmetric algorithm in order to exchange session keys between mobile nodes—the RSA and the Diffie-Hellman algorithms. The RSA encrypts the session key first before it gets sent, and Diffie-Hellman allows users to first share a secret, then generates a session key based on the shared secret.

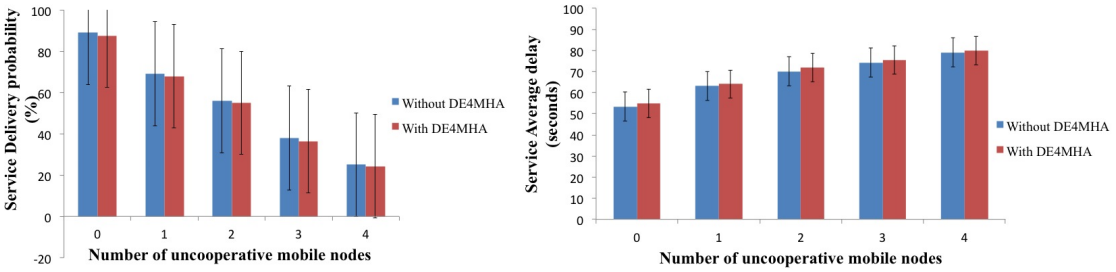
Several experiments were performed with both algorithms with RSA presenting better encryption times than Diffie-Hellman, due to the high amount of computation needed by Diffie-Hellman and the low processing capacity of mobile devices.

DE4MHA Performance Evaluation Results

In the presented scenario, all the devices had Bluetooth class 2 modules, but only 3 devices had Internet connectivity. Users without Internet connectivity had to use the integrated cooperation mechanisms in order to obtain the requested health information. When the number of uncooperative nodes increased, the service delivery probability decreased. The average service delay was also affected in the same mannor, as expected. Increased number of uncooperative nodes increased the average service delay.

Figure 6 shows the results of the service delivery probability and the average service delay as a function of the number of uncooperative mobile nodes with and without the DE4MHA. The probability that a request was successfully answered as a function of uncooperative nodes in the network decreased with the increase of uncooperative mobile nodes. Taking into account both approaches, with and without DE4MHA, it was observed that DE4MHA presented a slightly worse result. The average service delay also grew when the number of uncooperative mobile nodes increased, as expected. The results of the DE4MHA were also slightly worse but practically insignificant. As can be observed, with 4 uncooperative nodes, the service average delay, with and without DE4MHA, was about 30.78 and 29.77 seconds, respectively.

Figure 6. Service delivery probability and average service delay as a function of the number of uncooperative mobile nodes with and without the DE4MHA.



Discussion

Findings

Our main goal was to propose and construct a security encryption/decryption based solution in a cooperative environment for mHealth applications. We aimed to ensure data confidentiality, integrity, and authenticity. Privacy is a top priority issue in mHealth services and applications that deal with user sensitive information. On mHealth applications, several security issues must be considered, such as personal information management, secondary use of personal information, improper use of personal information, and errors with stored personal information. Therefore, cryptographic mechanisms can be seen as a solution to guarantied data confidentiality and protection [34].

In a mobility and cooperative environment with constant health data being forwarded and retrieved, studying and developing security mechanisms become crucial. Several experiments were conducted, involving 35 different users, to check if they could distinguish the application running with and without the DE4MHA embedded. Through the trials, we concluded that users could not tell which application had the DE4MHA embedded mainly because the time response taken to obtain the user health information was nearly the same as without DE4MHA. The DE4MHA was implemented in a ubiquitous

manner so users were able to keep using the application without noticing changes or presence of any cryptography mechanisms.

Limitations

There were several limitations to the study. The main limitation was applying security on mobile devices due to the low processor capacity compared with personal computers (PCs), though tremendous improvements in this area have been made, with a few mobile devices capable of competing with traditional PCs. This improvement allowed us to test several security algorithms to address the issues of confidentiality (AES, RC4, 3DES, and Blowfish), integrity (MD5 and SHA1), and authenticity (RSA with MD5 and DSA with SHA1) in order to verify which combination had a better performance in a mobile environment.

During the experiments, some users without Internet connectivity who wanted to obtain health information were in constantly moving further away from other users. Although the cooperation mechanism was embedded, users that were beyond the range of 10 meters (the maximum range for Bluetooth class 2 modules) could not obtain the desired health information. Another limitation, though not related to security, was with regard to the number of uncooperative nodes (mobile nodes that may not want to cooperate or they may not have cooperation mechanisms embedded), compromising service response probability.

Conclusion

This paper proposed a data encryption solution for mobile health applications, called DE4MHA. The data encryption algorithm DE4MHA with cooperation mechanisms in mobile health allow users to safely obtain health information with the data being carried securely. These security mechanisms did not deteriorate the overall network performance and the application, maintaining similar performance levels as without the encryption. More importantly, it offers a robust and reliable increase of privacy, confidentiality, integrity, and authenticity of their health information. Although it was experimented on a specific mHealth application, SapoFit, both DE4MHA and the cooperation strategy can be deployed in other mHealth applications.

Acknowledgments

This study was partially supported by Instituto de Telecomunicacões, Next Generation Networks and Applications Group (NetGNA) Portugal, National Funding from the FCT—Fundacão para a Ciência e a Tecnologia through the PEst-OE/EEI/LA0008/2011 Project, National Natural Science Foundation of China (Grant No. 61201165 and No. 61271240), and the AAL4ALL (Ambient Assisted Living for All), project co-funded by COMPETE under FEDER via QREN Programme.

Conflicts of Interest

None declared.

References

1. Le Moullee B, Ray P. Issues in E-Health Cost Impact Assessment. In: IFMBE Proceedings. 2009 Presented at: World Congress on Medical Physics and Biomedical Engineering; September 9-12, 2009; Munich, Germany p. 223-226. [doi: 10.1007/978-3-642-03893-8_63]
2. Akter S, D'Ambra J, Ray P. User Perceived Service Quality of mHealth Services in Developing Countries. 2010 Jun 09 Presented at: European Conference on Information Systems; June 6-9, 2010; Pretoria, South Africa.
3. United Nations Foundation, Vodafone Group Foundation, Telemedicine Society of India. mHealth and Mobile Telemedicine - an Overview. 2008 Aug 01. URL: http://ehealth-connection.org/content/mhealth-and-mobile-telemedicine-an-overview [accessed 2013-03-06] [WebCite Cache ID 6EvqsNn7K]
4. Subramoniam S, Sadi S. Healthcare 2.0. IT Professional 2010;12(6):46-51. [doi: 10.1109/MITP.2010.66]
5. epSOS – the European eHealth Project. URL: http://www.epsos.eu/ [accessed 2013-02-28] [WebCite Cache ID 6E0ipZcb2]
6. Akter S, Ray P. mHealth - an Ultimate Platform to Serve the Unserved. Yearb Med Inform 2010:94-100. [Medline: 20938579]
7. Tachakra S, Wang XH, Istepanian RS, Song YH. Mobile e-health: the unwired evolution of telemedicine. Telemed J E Health 2003;9(3):247-257. [doi: 10.1089/153056203322502632] [Medline: 14611692]
8. Laxminarayan S, Istepanian RS. UNWIRED E-MED: the next generation of wireless and internet telemedicine systems. IEEE Trans Inf Technol Biomed 2000 Sep;4(3):189-194. [Medline: 11026588]
9. Istepanian R, Lacal JC. Emerging mobile communication technologies for health: some imperative notes on m-health. : IEEE; 2003 Presented at: 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society; September 17-21; Cancun, Mexico p. 1414-1416. [doi: 10.1109/IEMBS.2003.1279581]
10. Istepanian R, Laxminarayan S, Pattichis CS. M-Health: Emerging Mobile Health Systems. In: M-health: emerging mobile health systems. New York, NY: Springer; 2006.
11. Paré G, Moqadem K, Pineau G, St-Hilaire C. Clinical effects of home telemonitoring in the context of diabetes, asthma, heart failure and hypertension: a systematic review. J Med Internet Res 2010 Jun;12(2):e21 [FREE Full text] [doi: 10.2196/jmir.1357] [Medline: 20554500]
12. Fayn J, Rubel P. Toward a personal health society in cardiology. IEEE Trans Inf Technol Biomed 2010 Mar;14(2):401-409. [doi: 10.1109/TITB.2009.2037616] [Medline: 20007033]

13. Lin CT, Chang KC, Lin CL, Chiang CC, Lu SW, Chang SS, et al. An intelligent telecardiology system using a wearable and wireless ECG to detect atrial fibrillation. IEEE Trans Inf Technol Biomed 2010 May;14(3):726-733. [doi: 10.1109/TITB.2010.2047401] [Medline: 20371411]
14. Kollmann A, Riedl M, Kastner P, Schreier G, Ludvik B. Feasibility of a mobile phone-based data service for functional insulin treatment of type 1 diabetes mellitus patients. J Med Internet Res 2007 Dec;9(5):e36 [FREE Full text] [doi: 10.2196/jmir.9.5.e36] [Medline: 18166525]
15. Mougiakakou SG, Bartsocas CS, Bozas E, Chaniotakis N, Iliopoulou D, Kouris I, et al. SMARTDIAB: a communication and information technology approach for the intelligent monitoring, management and follow-up of type 1 diabetes patients. IEEE Trans Inf Technol Biomed 2010 May;14(3):622-633. [doi: 10.1109/TITB.2009.2039711] [Medline: 20123578]
16. Jara AJ, Zamora MA, Skarmeta A. An internet of things–based personal device for diabetes therapy management in ambient assisted living (AAL). Pers Ubiquit Comput 2011 Jan 2011;15(4):431-440. [doi: 10.1007/s00779-010-0353-1]
17. Zhu F, Bosch M, Woo I, Kim S, Boushey CJ, Ebert DS, et al. The Use of Mobile Devices in Aiding Dietary Assessment and Evaluation. IEEE J Sel Top Signal Process 2010 Aug;4(4):756-766 [FREE Full text] [doi: 10.1109/JSTSP.2010.2051471] [Medline: 20862266]
18. Pollak J, Gay G, Byrne S, Wagner E, Retelny D, Humphreys L. It's Time to Eat! Using Mobile Games to Promote Healthy Eating. IEEE Pervasive Comput 2010 Jul 2010;9(3):21-27. [doi: 10.1109/MPRV.2010.41]
19. Patrick K, Raab F, Adams MA, Dillon L, Zabinski M, Rock CL, et al. A text message-based intervention for weight loss: randomized controlled trial. J Med Internet Res 2009;11(1):e1 [FREE Full text] [doi: 10.2196/jmir.1100] [Medline: 19141433]
20. Watson A, Bickmore T, Cange A, Kulshreshtha A, Kvedar J. An internet-based virtual coach to promote physical activity adherence in overweight adults: randomized controlled trial. J Med Internet Res 2012;14(1):e1 [FREE Full text] [doi: 10.2196/jmir.1629] [Medline: 22281837]
21. Whittaker R, Dorey E, Bramley D, Bullen C, Denny S, Elley CR, et al. A theory-based video messaging mobile phone intervention for smoking cessation: randomized controlled trial. J Med Internet Res 2011;13(1):e10 [FREE Full text] [doi: 10.2196/jmir.1553] [Medline: 21371991]
22. Déglise C, Suggs LS, Odermatt P. Short message service (SMS) applications for disease prevention in developing countries. J Med Internet Res 2012;14(1):e3 [FREE Full text] [doi: 10.2196/jmir.1823] [Medline: 22262730]
23. Silva B, Rodrigues JJPC, Lopes I, Machado T, Zhou L. A Novel Cooperation Strategy for Mobile Health Applications. IEEE Journal on Selected Areas in Communications Special Issue on Emerging Technologies in Communications - eHealth, IEEE Communications Society 2013:1-9 (forthcoming).
24. Silva B, Lopes I, Rodrigues J, Ray P. SapoFitness: A mobile health application for dietary evaluation. : IEEE; 2011 Presented at: 13th IEEE International Conference on e-Health Networking Applications and Services (IEEE HEALTHCOM 2011); June 13-15, 2011; Columbia, MO, USA p. 13-20. [doi: 10.1109/HEALTH.2011.6026782]
25. Rodrigues JJ, Lopes IM, Silva BM, de la Torre I. A new mobile ubiquitous computing application to control obesity: SapoFit. Inform Health Soc Care 2013 Jan;38(1):37-53. [doi: 10.3109/17538157.2012.674586] [Medline: 22657250]
26. SapoFit. URL: https://itunes.apple.com/pt/app/sapo-fit/id438487775?mt=8 [accessed 2013-02-15] [WebCite Cache ID 6Cw2BHsOA]
27. Jonsson J, Kaliski B. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. URL: http://www.rfc-editor.org/ [accessed 2013-02-15] [WebCite Cache ID 6Cw66XuiI]
28. Raeburn K. Advanced Encryption Standard (AES) Encryption for Kerberos 5. URL: http://www.rfc-editor.org/ [accessed 2013-02-15] [WebCite Cache ID 6Cw4IKbXi]
29. Housley R. Triple-DES and RC2 Key Wrapping. URL: http://www.rfc-editor.org/ [accessed 2013-02-15] [WebCite Cache ID 6Cw4ZXBdH]
30. Jaganathan K, Zhu L, Brezak J. The RC4-HMAC Kerberos Encryption Types. URL: http://www.rfc-editor.org/ [accessed 2013-02-15] [WebCite Cache ID 6Cw5Lwx1B]
31. Shirey R. Internet Security Glossary, Version 2. URL: http://www.rfc-editor.org/ [accessed 2013-02-15] [WebCite Cache ID 6Cw5pWnxS]
32. Rescorla E. Diffie-Hellman Key Agreement Method. URL: http://www.rfc-editor.org/ [accessed 2013-02-15] [WebCite Cache ID 6Cw6I1jk5]
33. McGrew D, Igoe M, Salter M. Fundamental Elliptic Curve Cryptography Algorithms. URL: http://www.rfc-editor.org/rfc/rfc6090.txt [accessed 2013-02-28] [WebCite Cache ID 6E0ktAxqb]
34. Raychaudhuri K, Ray P. Privacy Challenges in the Use of eHealth Systems for Public Health Management. International Journal of e-Health and Medical Communications, IGI-Global 2010;1(2):12-23. [doi: 10.4018/jehmc.2010040102]

Abbreviations

3DES: Triple Data Encryption Standard
ACT: achieved cooperation time
AES: Advanced Encryption Standard

BMI: body mass index
BMR: basal metabolic rate
CWS: cooperative Web service
DE4MHA: data encryption solution for mobile health applications
EHR: electronic health record
HTTPS: Hypertext Transfer Protocol Secure
ICT: information and communication technologies
JSP: Java Server Pages
RC4: Rivest Cipher 4
REST: Representational State Transfer
RSA: Rivest, Shamir, Adleman
SOAs: service oriented architectures
SSL: Secure Socket Layer
WS: Web service

Edited by G Eysenbach, A Jara, S Koch, P Ray; submitted 15.12.12; peer-reviewed by S Zeadally, C Verikoukis, A Vinel, P Lorenz, A Jara; comments to author 10.01.13; revised version received 22.01.13; accepted 09.02.13; published 14.03.13

Please cite as:
Silva BM, Rodrigues JJ, Canelo F, Lopes IC, Zhou L
A Data Encryption Solution for Mobile Health Applications in Cooperation Environments: DE4MHA
J Med Internet Res 2013;15(3):e66
URL: http://www.jmir.org/2013/3/e66/
doi:10.2196/jmir.2498
PMID:

Chapter 7

MobiCoop: An incentive-based cooperation solution for mobile applications

This chapter consists of the following article:

MobiCoop: An incentive-based cooperation solution for mobile applications

Bruno M. C. Silva, Joel J. P. C. Rodrigues, Mario L. Proença Jr., and Guangjie Han

Article submitted for publication in an international journal.

MobiCoop: An incentive-based cooperation solution for mobile applications

BRUNO M. C. SILVA, Instituto de Telecomunicações, University of Beira Interior
JOEL J. P. C. RODRIGUES, Instituto de Telecomunicações, University of Beira Interior; University ITMO
MARIO L. PROENÇA Jr, State University of Londrina
GUANGJIE HAN, Hohai university

Network architectures based on mobile devices and wireless communications presents several constraints (e.g. processor, energy storage, bandwidth, etc.) that affect the overall network performance. Cooperation strategies have been considered as a solution to such network limitations and constraints. In the presence of unstable network infrastructures mobile nodes cooperate with each other forwarding data and performing other specific networking functionalities. This paper proposes a generalized incentive-based cooperation solution for mobile services and applications, called MobiCoop. This reputation-based scheme includes a application framework for mobile applications that uses a Web-service to handle all the nodes reputation and networking permissions. The main goal of MobiCoop is to provide Internet services to mobile devices without network connectivity through cooperation with neighbor devices. A performance evaluation of MobiCoop in a real scenario demonstrating and validating this cooperative application framework using real mobile applications is presented. It was shown the proposed approach provides network connectivity independency to mobile apps users when Internet connection is unavailable. Then, it is concluded that MobiCoop improved significantly the overall system performance and the quality of service for a given mobile application.

Categories and Subject Descriptors: C.1.3 [**Processor Arquitectures**]: Other Architecture Styles; C.2.4 [**Computer-Communication Networks**]: Distributed Systems; H.5.3 [**Multimedia Information Systems**]: Group and Organization Interfaces

General Terms: Design, Cooperation, Performance

Additional Key Words and Phrases: Mobile computing; Mobile applications; Cooperation; Incentive-based cooperation; reputation-based cooperation

1. INTRODUCTION

The mobile communications and technological evolution based on mobile devices and Internet services aims to provide access to information, multimedia applications, and multiple mobile services anytime and anywhere [Jianping et al. 2013; Raychaudhuri and Mandayam 2012]. Mobile technologies and systems revolutionized the way people communicate and mobile applications offer new and single ways for communicating, shopping, organizing users lives, playing, and working under mobility environments [Mshvidobadze 2012]. It is foreseen that, in 2014, mobile applications stores surpasses the 130 billions downloads [Gartner 2013]. Today's mobile applications have a strong dependence of Internet services to access multimedia contents. These apps instantly share and/or retrieve from the Internet images, audio and video through

This work has been partially supported by *Instituto de Telecomunicações*, Next Generation Networks and Applications Group (NetGNA), Covilhã Delegation, by Government of Russian Federation, Grant 074-U01, by National Funding from the FCT - *Fundação para a Ciência e a Tecnologia* through the Pest-OE/EEI/LA0008/2013 Project, and by the AAL4ALL (Ambient Assisted Living for All), project co-financed by the European Community Fund (FEDER) through COMPETE - *Programa Operacional Factores de Competitividade*.
Author's addresses: Bruno M. C. Silva and Joel J. P. C. Rodrigues, Instituto de Telecomunicações, University of Beira Interior, Rua Marquês d'Ávila e Bolama, Covilhã, 6201-001, Portugal, (bruno.silva@it.ubi.pt, joeljr@ieee.org). Mario L. Proença Jr, Computer Science Department, State University of Londrina (UEL), Londrina, Brazil (proenca@uel.br). Guangjie Han, Department of Information & Communication Systems, Hohai University, Changzhou, China (hanguangjie@gmail.com).

mobile devices [Rowe 2013]. Therefore, the widely use of multimedia contents turn energy saving a priority concern to app developers, mobile devices users, and manufactures [Hoque et al. 2014a]. Mobile devices and their supporting wireless networks and communications are constantly challenged by different constraints, such as, battery and storage capacity, broadcast constraints, user interferences, disconnections, noises, limited bandwidths, and network delays [Lei et al. 2013; Hoque et al. 2014b]. These constraints can severely affect an user quality of experience. For instance, it can damage any ongoing mobile application process if its mobile device does not have network connectivity.

General industry services require that agents cooperate and share information through mobile devices. Healthcare services and mobile health (m-Health) applications are presenting new services and solutions every day, where patients and physicians, share common medical information. These scenarios, have different and complex network architectures that are based on mobile devices and Web services. Efficient cooperation between applications and devices is important to maintain and improve the quality of services as well as the overall network performance.

Cooperation strategies are emerging as a hot research topic that has been growing in recent years and focuses on increasing network connectivity, reliability, communication rates, and energy optimization [Kramer et al. 2007]. Cooperative schemes assume that nodes cooperate among them performing all the networking functionalities where intermediate nodes support the communication forwarding packets between two distant nodes (origin and destination) [Buttyán and Hubaux 2003]. This assumption fits perfectly as a solution to improve the performance of a mobile network scenario. Cooperation have been applied recently in different mobile network scenarios. Several proposals have been proposed to provide location-based services through cooperative-based strategies [Sammarco et al. 2008; Wymeersch et al. 2009; Win et al. 2011; Patwari et al. 2005]. Furthermore, cooperative schemes were also used to improve the performance of mobile Web services and multimedia contents distribution [Luo and Deters 2009; Yoo and Park 2011]. Basically, cooperative approaches can be classified in game theory and incentive-based techniques. In game theory schemes, network agents cooperate to achieve network privileges to gain maximum benefits that would not be obtained without cooperation [Liu et al. 2007; Charilas and Panagopoulos 2010; Felegyhazi and Hubaux 2007]. Cooperative incentive-based approaches are classified into two main groups: virtual currency based schemes and reputation based schemes [Froushani et al. 2011; Shen and Li 2012]. Virtual currency schemes use incentives in the form of virtual credits to enforce nodes cooperation. Reputation-based mechanisms observes the network nodes behaviors and uses reputation grades to diminish selfishness.

This paper proposes a cooperation solution for mobile services and applications, called MobiCoop. This application framework is a generalized soluction based on the evolution of an early cooperative strategy for mobile health applications, presented in [Silva et al. 2013b], to offer a cooperative solution for mobile applications. MobiCoop is a reputation-based scheme that aims to provide Internet connectivity or services to mobile devices through cooperation with neighbors. This solution is based on neighbor direct observation, however, it uses a Cooperative Web Service (CWS) that handles and gives reputation grades as an incentive to stimulate cooperation among mobile users. Furthermore, MobiCoop includes a secure module to secure communication between devices during cooperation, based on a novel cryptograph strategy presented in [Silva et al. 2013a]. This paper describes the main modules and components of MobiCoop along with its performance evaluation using different mobile applications. Furthermore, it presents an evaluation considering different types of user mobility and how it

affects the overall network performance. The main contributions of this paper are the following:

— A detailed review of the state-of-the-art on cooperation schemes for mobile ad-hoc networks (MANETs) and delay-tolerant networks (DTNs);
— The proposal of a novel and generalized incentive-based cooperation solution for mobile applications, called MobiCoop;
— The design and construction of two real mobile applications prototypes for performance evaluation of MobiCoop;
— The performance assessment and analysis of MobiCoop application framework through a real prototype, considering a real scenario and real users.

The remainder of the paper is organized as follows. Section II elaborates on related work about the topic focusing on cooperation techniques that contribute to the proposed solution, including mobile ad-hoc networks (MANETs) and delay-tolerant networks (DTNs). Section III describes the proposed cooperation solution while its performance evaluation and validation through different prototypes of mobile applications is presented in Section IV. Finally, Section V concludes the paper and suggests further research works.

2. RELATED WORK

Cooperation strategies on wireless networks mainly focuses on increasing power efficiency, network coverage, and outage probability reduction [Li et al. 2011; Al-Kanj and Dawy 2010; Lai et al. 2006; Althunibat et al. 2012]. Through cooperation schemes, network nodes can optimize their resources (e.g. battery life) obtaining a balanced Quality of Service (QoS). Cooperative coding or relaying strategies, such as, amplify-and-forward (AF), classic multi-hop, compress-and-forward (CF), decode-and-forward (DF), multipath decode-and-forward (MDF), among others, have been presented and served as a basis to several proposals for cooperative strategies in wireless networks [Kramer et al. 2006].

Game theory techniques have been widely applied in cooperative schemes. These techniques were developed originally for economic issues and aims to model scenarios where several agents present mutual or may have conflict of interests. Therefore, wireless networks architectures fit perfectly in the game theory formulation [Felegyhazi and Hubaux 2007]. In a typical cooperative-based game theory scheme, network agents cooperate to achieve network privileges/agreements so they can gain maximum benefits that would not be obtained without cooperation [Charilas and Panagopoulos 2010]. Several cooperative game theory based schemes have been recently proposed [Kai et al. 2010; Gyarmati and Trinh 2011; Wen et al. 2012; Zetterberg et al. 2009; Murphy et al. 2009; Korakis et al. 2009]. Although, these approaches does not belong to the focus of this study. Then, only the most significant and the ones that contributed to the presented cooperation proposal are surveyed.

Focusing on the main overall characteristics of a mobile network architecture supported by mobile devices and Web services, this study mainly addresses cooperation strategies for wireless and mobile ad-hoc networks (MANETs). The delay tolerant network (DTN) paradigm is also considered due to the network disconnection problems. The proposed cooperative solution gathered contributions from the available approaches for these networks.

2.1. Cooperation approaches in wireless and mobile ad-hoc networks

In a mobile ad-hoc network (MANET) it is assumed that all the network nodes should cooperate to assure that data is forwarded or routed to attain the destination node [Corson and Macker 1999]. However, this assumption is not always correct in the pres-

ence of *un-cooperative* nodes. These nodes can be faulty or malicious, or/and selfish, and do not always forward to other nodes the needed data or refuse to perform specific network operations [Hu and Burmester 2009]. Several cooperation proposals have been presented to stimulate cooperation and mitigate the detrimental effect of non-cooperative nodes. The most significant approaches that contributed to the presented proposal are described below.

Nuglets is a virtual currency cooperative scheme that addresses the problem of non-cooperative nodes in large MANETs for civilian applications. This system uses a virtual currency, called *nuglets*, to stimulate packet forwarding. Therefore, it decreases node selfish behaviors enhancing the overall network performance [Buttyán and Hubaux 2001].

Sprite is another popular virtual currency cooperative approach. It consists in a cheat-proof system that stimulates cooperative behaviors among selfish nodes. Sprite uses a received/forwarded message *receipts* to validate and determine the payment and credit to each node. This cooperative scheme includes a central credit clearance service (CCS) to manage the credit payments to cooperative nodes [Zhong et al. 2003].

CONFIDANT is a reputation-based scheme that detects and isolates selfish nodes compelling them to cooperate. These cooperative scheme includes four cooperative components per node: *i*) the monitor, responsible for detecting deviating behaviors of other nodes. The Monitor sends ALARMs of misbehaving actions to the trust manager component; *ii*) the trust manager component, that receives the ALARMs sent by the monitor, decides to whom should provide or accept route information; *iii*) the reputation system that rates the node reputation based on observed behaviors; and *iv*) the path manager, that is based on the reputation rating, defines the path raking in order to avoid malicious nodes [Buchegger and Le Boudec 2002] .

CORE is a reputation-based scheme that uses collaborative monitoring and a reputation table to stimulate cooperation among nodes. This reputation table defines, based on their reputation, the nodes can use network services (i. e., packet forwarding or other specific network operation). To calculate this reputation value, CORE defines three types of reputation: *subjective reputation*, based on direct observation; *indirect reputation*, based on second hand of information; and *functional reputation*, using a function which uses a packet forwarding weight in function of its importance [Michiardi and Molva 2002] .

Another popular reputation-based scheme, called OCEAN, is presented in [Bansal and Baker 2003]. The main goal of this cooperative approach tries to detect and mitigate misleading routing behaviors, in MANETs. This cooperation scheme uses only direct first-hand observations of node behaviors avoiding second-hand information due to trust-management issues. OCEAN is an hybrid solution that uses both reputation and virtual credit incentives through micro-payments to enforce cooperation.

SORI is a reputation-based scheme that addresses the problem of node's selfish behaviors that degrades the overall MANET performance. This approach goals to stimulate node packet forwarding and to decrease selfish actions. SORI reputation scheme quantifies the node reputation in objective measures and neighbor nodes and it is responsible for its propagation through an one-way-hash chain based authentication scheme. This solution also includes a punishment scheme that penalizes selfish node behaviors [He et al. 2004].

DARWIN is a cooperative scheme that aims the detection and punishment of selfish behaviors. It includes a collision resistance avoiding retaliation scenarios of nodes being wrongly perceived as selfish nodes. DARWIN guarantees full cooperation among nodes assuming to solve imperfect behaviors measurements [Jaramillo and Srikant 2007].

A reputation scheme, called LARS, is presented in [Hu and Burmester 2006]. Under this reputation-based approach, a node reputation is calculated only through direct observation and deals with two types of node selfishness: selective selfishness and extreme selfishness. In selective selfishness, If a selfish node or selfish behavior is identified by its direct neighbors, the node reputation degrades. In case of extreme selfishness, the routes that contain this selfish nodes are deleted and new routes are created excluding these nodes even from the network.

A study on how cooperation can improve the experience of mobile Web services consumers is presented in [Luo and Deters 2009]. This study focuses on the use of cooperation in a scenario where mobile devices (e.g., phones, smartphones, tablets) regularly request services from the Web. This cooperative approach is based on a task prediction model and uses two proxies, one in the server side and another in the client side. The server proxy pre-fetches and pre-processes, pre-requests made by the client to the Web service. The overall network performance is enhanced through the use of the task prediction model that enables the system to provide a client with choices and decisions rather than just provide stored information.

A distributed clustering protocol, called, Cooperative Networking protocol (CONET) for energy saving in mobile devices with WLAN and Bluetooth interfaces is proposed in [Yoo and Park 2011]. CONET scheme considers nodes organized by clusters that are dynamically auto-configured depending on their bandwidth requirements and their common activities. These clusters are arranged in Bluetooth personal area networks (PANs) and a cluster head node is elected to act as a gateway between the PAN and the WLAN access point. Therefore, this cooperative approach aims to enable node clusters to access the WLAN infrastructure and also save energy since they do not need to enable Wi-Fi in their devices.

Cooperative-based approaches have also been proposed for location and navigation systems especially in wireless mobile networks. Several location based systems have been proposed where network agents estimate their positions through cooperative schemes [Patwari et al. 2005; Shen et al. 2010; Khan et al. 2009]. A study of cooperative-based schemes for location and navigation from a theoretical perspective to applications covering used technologies, schemes, and algorithms is presented in [Win et al. 2011].

A location aware cooperative-based approach to improve location tracking among mobile nodes through the information retrieved from a cellular network is presented and described in [Sammarco et al. 2008]. Each network node retrieves the location area code and the local network base station cell ID. Cooperative nodes within short links range (i.e., Bluetooth) request this information and send it to a server. The server compares the retrieved information and, through the Google Maps API [Google], calculates a more accurate location position, retrieving it back to the mobile device.

Cooperative location approaches on wireless networks are overviewed in [Wymeersch et al. 2009]. This study presents a performance evaluation of cooperation mechanisms on ultra-wide bandwidth (UWB) wireless networks . Moreover, the authors also present a novel localization algorithm, called SPAWN, that maps a graphical model directly onto the network topology. SPAWN can be deployed in several network scenarios requiring a minor communication overhead and achieves an accurate and robust location.

2.2. Cooperation aproaches in Delay Tolerant Networks

In delay tolerant network (DTN) scenarios, variable propagation delays, low node density, low transmission reliability, node mobility, disruption, and other network constraints (such as, limited storage capacity, limited network bandwidth, and limited energy) affect the overall network performance [Cerf et al. 2007] . DTN routing proto-

cols usually assume a cooperative scenario, however, this is an unrealistic assumption due to the presence of *un-cooperative* nodes often [Soares and Rodrigues 2011]. Therefore, in the last decade, several cooperation studies and proposals for DTNs have been proposed in the literature that also offer contributions and insights for the current proposal.

Magaia *et al.* present a study focusing on the impact of a node misbehavior in DTNs [Magaia et al. 2013]. The authors describe and present an evaluation of the impact of selfish nodes using several DTN routing protocols. The metrics considered in this study are the delivery ratio, buffer time, hop count, latency, and overhead ratio. Obtained results shown that routing protocols are more resilient depending on the number and type of misbehaviors. This study main goal was to identify and select the best routing protocols performances in the presence of misbehaving nodes.

A DTN incentive-based strategy is presented in [Shevade et al. 2008]. This cooperative approach includes the use of a simple Tit-for-Tat (TFT) mechanism to stimulate cooperation. This proposal guaranties, through the TFT mechanism, that every node forwards as much traffic as possible for a neighbor node as the neighbor also forwards traffic to it.

A cooperation mechanism for DTNs based on the cooperative ARQ (C-ARQ) is proposed in [Pozo et al. 2008]. This cooperation proposal aims to reduce data losses in transmissions between fixed access points placed along the roads and passing by vehicles that buffer and forward all the data. The idea is that in areas that vehicles have no connectivity to access points, vehicles cooperate between them to increase the data delivery rate.

Pay-for-Gain (PFG) is a game theory and loan-credit theory proposed in [Yin et al. 2010]. This cooperation scheme aims to study the equilibrium point that maximizes the nodes own interests cooperating with others. This paper also presents results comparing TFT and PFG strategies. Results shown that PFG mechanism is more effective than TFT algorithm mitigating selfish node behaviors.

Multicent is a game theory incentive scheme for DTN routing. This proposal encourages nodes to follow their desired performance objectives, such as, minimal average delay, maximal hit rate, and minimal maximal delay by performing packet storage or forwarding [Chen and Shen 2013].

A study on the performance of opportunistic content distribution under different levels of cooperation in DTNs is presented in [Helgason et al. 2010]. This evaluation considers three degrees of cooperation: *i*) no cooperation; *ii*) un-limited cooperation; and *iii*) limited cooperation. In *i*) nodes do not forward content from other nodes and, therefore, do not cooperate. In *ii*), network nodes forward all requested contents, therefore cooperating without any limitation or rules, in *iii*), packets/contents are forwarded within a defined limit of time to optimize node resources (i.e., battery, CPU, link load). As expected, the obtained performance results shown that both cooperative approaches improve significantly the overall network performance.

A cooperative peer-to-peer file sharing technique for DTNs is presented in [Liu et al. 2011]. This technique addresses the accessibility optimization of media contents from mobile devices. The presented proposal takes advantage of the users mobile device or vehicles mobility for file distribution and sharing among nodes. For instance, a single node downloads a file and forwards it with other nodes. The network architecture is described as a hybrid DTN since that the authors consider the DTN as an extension of the Internet.

2.3. Considerations

The cooperation solution proposed in this paper gathered contributions from the above-described strategies in wireless, mobile ad-hoc, and delay tolerant networks. However,

the presented proposal took into account several open issues that are considered in the proposal.

As above-presented, most of the reputation-based systems rely only on direct neighbor observation. This aspect enables nodes to more easily form communities/groups with faulty intentions to maximize their utility and, therefore, gain more reputation rating. Moreover, the reliance of these approaches on wireless broadcast techniques is another weakness. In DTNs, incentive-based approaches are challenging due to their single characteristics. In DTNs, reputation-based schemes face an additional issue that data forwarding cannot be observed during the store-carry-and-forward process.

The presented proposal includes direct and second-hand observation, and propagation of all the nodes reputation through the network. Moreover, the reputation rating and access to requested data is controlled by a centralized Web service. This way, it reduces faulty node actions and eliminates the above-mentioned DTN issue.

3. MOBICOOP: A COOPERATIVE REPUTATION-BASED SOLUTION FOR MOBILE APPLICATIONS

This section describes, in detail, the MobiCoop system architecture, modules, and mechanisms. MobiCoop is an incentive-based cooperation solution that stimulates cooperation among users through a reputation scheme managed by a Web service. A previous version of this solution was early presented in [Silva et al. 2013b]. It was proposed and applied only to m-Health applications. In this paper, a generalized solution that any developer can easily incorporate within their mobile application is proposed. MobiCoop (illustrated in Figure 1) is an application framework for mobile applications that is based in 4 main modules: *i*) a request treatment module; *ii*) a cooperation module; *iii*) a security module; and *iv*) a cooperative Web service module. Next sub-sections presentes and describes the prosed modules.

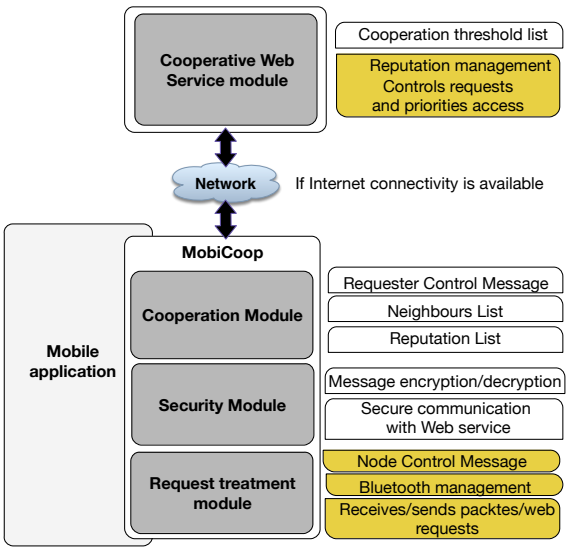


Fig. 1. Illustration of MobiCoop framework.

This cooperation solution was specifically designed and proposed for mobile applications with service oriented architectures (SOAs) where Internet connectivity is required in order to fetch the information. A mobile device without Internet connectivity uses Bluetooth communication to exchange messages between devices. Only a mobile device with Internet connectivity has access to the Cooperative Web Service.

The Bluetooth technology used for communication between devices was chosen due to the low energy consumption. Furthermore, MobiCoop shuts down the device Wi-Fi during the communication and the data exchange process between users. This process optimizes and saves the device precious battery life consumption.

3.1. Request treatment module

The request treatment module (RTM) (shown in Figure 2) initiates the cooperation process every time that a mobile application requests a service or data from the Internet/network and the connection is refused or inexistent. This module comprises a Bluetooth management component for communication with other devices and the Node Control Message (NCM) which is the first message that is exchanged between devices.

The Bluetooth management component searches for nearby neighbor users every time that cooperation is required. Moreover, it includes a process that keeps a cooperative mobile user listennig its neighbor users, expecting any contact requesting cooperation. This process and the device Bluetooth communication is a user choice and it is not forced by any MobiCoop method. However, if a user choose to turn off its Bluetooth communication while using the cooperative application it will affect negatively its reputation status.

A NCM is sent every time a nearby contact is discovered. Its main goal is to provide an awareness of the other mobile device (node) status, either if the node is willing to cooperate and in what conditions. It contains the established unique node identifier, the battery status, the Internet connectivity status, and the cooperation status (i.e., if its cooperative or not). Therefore, when a mobile application requests an Internet service or data, but the mobile device is unable to comply that request, the RTM captures the Internet application service or data request (such as, HTTP, FTP, POP, or others). Then, through the Bluetooth management component waits until nearby cooperative mobile users are announced. After receiving the neighbors NCMs it will identify the best user or users to cooperate and send its request. When these conditions are matched the Cooperative Module initiates its cooperative mechanisms.

3.2. Cooperative module

The Cooperative module (illustrated in Figure 3) begins a process when a pending request is captured by the request treatment module and a neighbor node is announced and identified as a suitable cooperative user. This module comprises tree components: i) a Requester Control Message (RCM); ii) a Neighbors List; and iii) a Reputation List.

The RCM is the first to be sent by the initial requester node to its neighbor or neighbors, and includes 1) the requester ID, the node unique identifier; 2) the pending service request, i.e., what node is specifically requesting; 3) the neighbors list that contains all the neighbor users and their cooperative status (if they are willing to cooperate); 4) the reputation list, that records cooperative or un-cooperative behaviors through the first hand observation; and 5) the achieved cooperation time (ACT).

The Neighbors Lists provide awareness to other nodes and a general perspective of the nodes in their proximities and their cooperative status. These lists allow nodes to avoid malicious and un-cooperative nodes in the response packet route. Furthermore, they enhance a better node discovery scope through the Bluetooth management.

Reputation lists are used to record first hand observations of node cooperative or un-cooperative behaviors. These lists are updated at any intervention with a neighbor

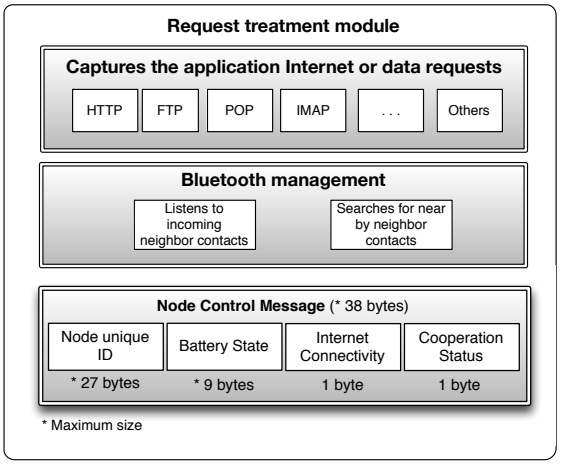


Fig. 2. Illustration of the Request treatment module and its components.

node and reside temporarily in the mobile devices until updated to the CWS. The reputation value of each node is calculated locally based on the information within the NCM. As shown in Table I, the reputation value is calculated through a correlation between the battery status, the Internet connectivity, and the node cooperation state. Every node has four types of battery state: *critical*, *poor*, *regular*, and *excellent*. It is considered that a node with a *critical* state of battery (below 15%) is neither compelled nor punished for non-cooperation. Its state is *poor* when its available power energy is between 15% and 35%. The *regular* status occurs when its power energy is between 35% and 70% and a node has an *excellent* status when its available power energy is over 70%. The worst punishment occurs when a node with *excellent* battery state has Internet connectivity but it is not willing to cooperate. The better reputation rewarded node is the one with *poor* battery state and Internet connectivity but it is willing to cooperate. Mobile devices without Internet connectivity could also increase its reputation by relaying packets on behalf of other requester nodes.

Table I. Reputation value calculation.

Battery State		Internet	Cooperation	Reputation
Classification	0%-100%	Connectivity	State	Value (RV)
Critical	<15%	-	-	-
Poor	>=15% and <35%	0	0	-1
Poor		0	1	+3
Poor		1	0	-2
Poor		1	1	+4
Regular	>=35% and <70%	0	0	-2
Regular		0	1	+2
Regular		1	0	-3
Regular		1	1	+3
Excellent	>=70%	0	0	-3
Excellent		0	1	+1
Excellent		1	0	-4
Excellent		1	1	+2

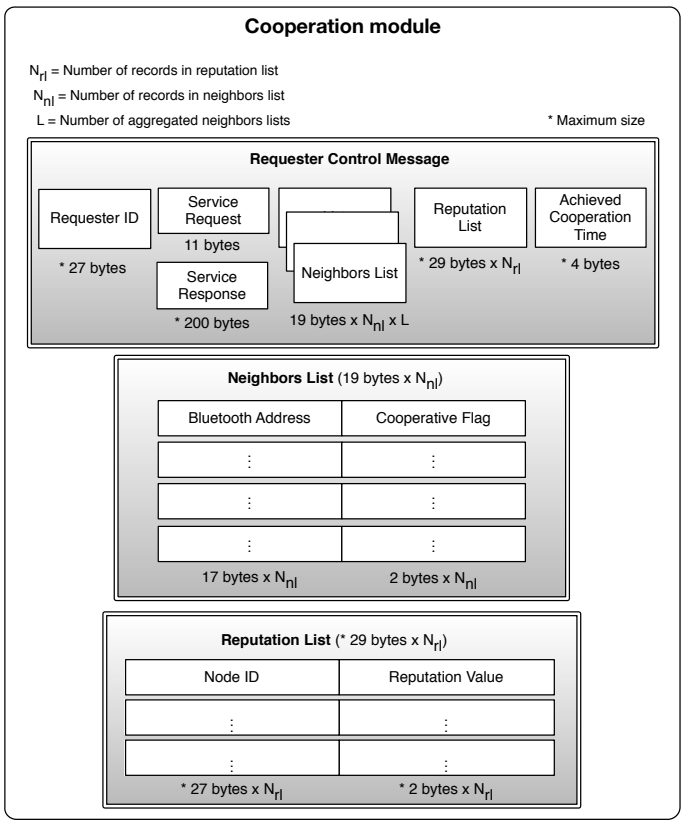


Fig. 3. Illustration of the Cooperation module and its components.

The ACT sent in the RCM provides an awareness when the cooperation process should stop and restart with a different neighbor cooperative user. A maximum waiting period (MWP) was defined to prevent a requester user to indefinitely wait for a request. When a node initiates a request and sends the RCM, the MWP is of 60 seconds. Otherwise, the requester user cancels its request and starts searching for another neighbor user that is willing to cooperate.

When a mobile device, receives or carries one or more pending requests (RCMs) has Internet connectivity it sends all of them to the CWS. The CWS will manage the updated reputation information and control the access to the requested services or data.

3.3. Cooperative Web Service

The CWS is responsible for performing a fair access control to requested services or data. It holds the final reputation list updated through the received reputation lists. The CWS reputation list contains all the registered network nodes with their identifier and their respective reputation value. The threshold value available at the reputation

table for the node N is represented by Rv. When the WS receives reputation information upon a request, if performs its update, through $Rvnew = Rvold + Rv$, where the initial Rv is equal to zero. The CWS reputation table considers three status of reputation: *selfish*, *neutral*, or *cooperative*. As may be seen by equation 1, these statuses are defined in order to provide a fair access to the requested service or data. An initial node with a reputation value equals to zero and, therefore, considered as *neutral*. A *selfish* node with a negative reputation value cannot access in any way to the requested service/data, being necessary to cooperate in order to reach a positive reputation value. Last, a *cooperative* node has full access to requested WS. For networks with a small number of nodes it is extremely important that un-cooperative nodes receive worst Rv, punishing and motivating them to cooperate.

$$Rep = \begin{cases} Selfish, R_v \in]-\infty, -1[\\ Neutral, R_v \in 0 \\ Cooperative, R_v \in [1, +\infty[\end{cases} \quad (1)$$

According to the node reputation status, the CWS will allow the node to have access to the requested services or data. Although the *neutral* status enables nodes to retrieve their requests, a node with a *cooperative* status has privilage and priority over a *neutral* node.

3.4. Security Module

A major concern in this solution is the privacy issue of all forwarded and retrieved data. Privacy is a top priority issue in mobile services and applications that deal with user sensitive information. Therefore, a cryptography solution that was proposed in [Silva et al. 2013a] for m-Heallth applications under cooperative environments, called DE4MHA (Data Encryption Solution for Mobile Health Applications) was adapted to this cooperative framework and incorporated into MobiCoop. DE4MHA is an hybrid cryptography solution that combines the use of the RSA [Jonsson and Kaliski 2003] algorithm for asymmetric encryption/decryption to guaranty key exchange confidentiality and the Advanced Encryption Standard (AES) algorithm for symmetric encryption/decryption for data confidentiality [Raeburn 2005] . This solution also ensures data integrity creating both message digest and an hash of the transmitted data. DE4MHA uses a digital signature for data authenticity, encrypting the previous hash message with the RSA private Key. The HTTPs protocol is used to secure the communication between any Web Service or other Internet service.

This cryptography solution was also included on the MobiCoop framework and generalized without any conceptual alteration for any mobile application. Figure 5) illustrates how the communication is protected between two nodes and between a node and the CWS by the MobiCoop security module.

This module assures a secure communication channel through two mobile users and between a mobile user and the CWS. The process starts by exchanging public keys, also with the purpose of session key exchange. This procedure will guarantee the message exchanged authenticity and integrity properties. The MD5 algorithm is used to generate a message digest of the exchange message that is encrypted with the received public key from the neighbor mobile user [Rivest 1992] . Simultaneously, a message digest of the exchange message is also generated and compared to the message digest previously created and exchanged between users. This message is decrypted using the users private key, enabling to check if the session key has not been modified and if its source is the expected one.

In case of a mobile user device has Internet connectivity the communication and message/data exchange is established through a Secure Socket Layer (SSL) over HTTP,

also known as HTTPs connection. Therefore, providing a data confidentiality mechanism for communication between the user and the CWS.

This methodology is not only applied to the session key message exchange. All messages or data exchange that uses MobiCoop cooperative processes during a communication are protected by this cryptography mechanisms.

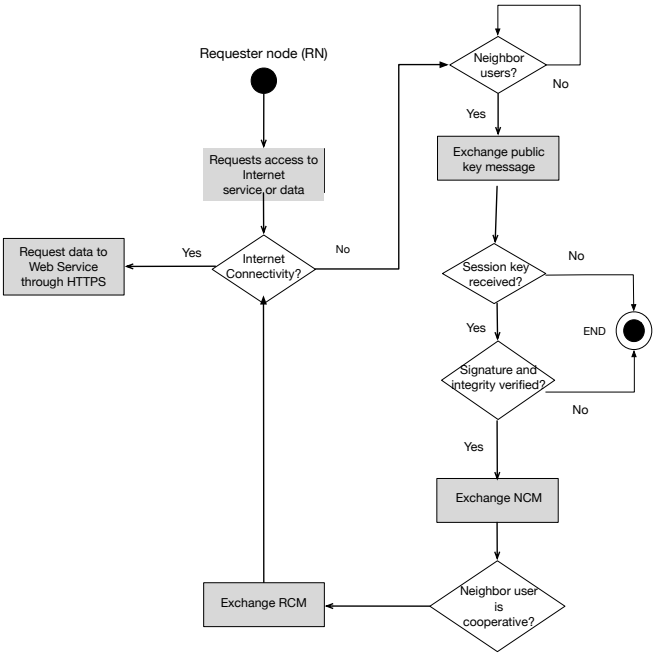


Fig. 4. Activity diagram illustrating the security mechanisms withim the cooperative process.

4. PERFORMANCE EVALUATION

This section focuses on the performance evaluation and validation of the cooperation solution proposed in this paper. MobiCoop was developed for Google Android Operating System and besides the platform itself, hardware requirements comprise the Bluetooth hardware, Wi-Fi and/or GSM/CDMA data modules. This solution is an application framework for mobile applications that is completely ubiquitous to the user, requiring only few setup configurations.

First, the service-oriented mobile applications and corresponding network scenarios used to evaluate and demonstrate MobiCoop are introduced. Afterwards, the system validation and results are discussed. The performance metrics used in the study are the *service requests delivery probability* and *service average delay* in the presence of network disconnections and/or Internet unavailability. These metrics are the network challenges that MobiCoop aims to improve and deliver.

The evaluation also considers the presence and variation of the number of uncooperative nodes in order to study how they affect the referred network metrics. Furthermore, two different user mobility behaviors are introduced. An user can be mobile

(i.e. the user is walking, moving along the scenario) and static (i.e. the user is fixed). It aims to study the mobility impact on the performance of MobiCoop.

4.1. Mobile Applications using MobiCoop

For evaluation of MobiCoop, two simple mobile applications (for Android OS) were developed: 1) an e-Mail client app; and 2) an instant message app for an internal corporative environment. The e-Mail client app allows users to send and receive e-Mails. For evaluation purposes it is assumed that the user has already an e-Mail account in the respective e-mail server. The instant message app allows any user/collaborator within the corporative environment to exchange instante messages with other users/collaborators. This app requires a register service to authenticate through a login and password. A user can send instant messages only after the respective Web service verifies his/her authentication.

The inclusion of the MobiCoop framework in both mobile apps is very simple. Developers only need to include the MobiCoop classes in the app package and, then, include the framework call method every-time the network connectivity fails sending the request to the *Request treatment module*. This procedure is presented in Algorithm 1.

ALGORITHM 1: MobiCoop call method: Request treatment module.

Input: The service or data requested and respective protocol: URL
Output: The URL is assigned to the *cooperative_requestment_module method*
repeat
  Access to service/data THREAD
  for *each attempt to request a service/data from Internet or external server* **do**
    ProtocolGet request = New ProtocolGet(URL);
    if *(Internet availability == Null;*
    then
      Request_treatment_module(URL);
    end
  end
  if *Internet availability != Null* **then**
    Request to service/data = True;
  else
    Request_treatment_module(URL);
  end
until *Access to service/data or Request treatment module is called*;

4.2. Mobile Network Scenario

The real network scenario used for the performance evaluation study of MobiCoop proposal may be seen in Figure 5. The figure illustrates part of the first floor of the Department of Informatics from the University of Beira Interior, Portugal. It goals to emulate a corporative environment where collaborators are either mobile, moving around the floor, or static, working on their workbenches. In this use-case scenario, only the user/node identified has *Resp* has Internet connectivity. For evaluation purposes, it is assumed the users/nodes are positioned according to the presented scenario where all the users within rooms are static and on corridors are mobile. It was also included the presence of three un-cooperative nodes.

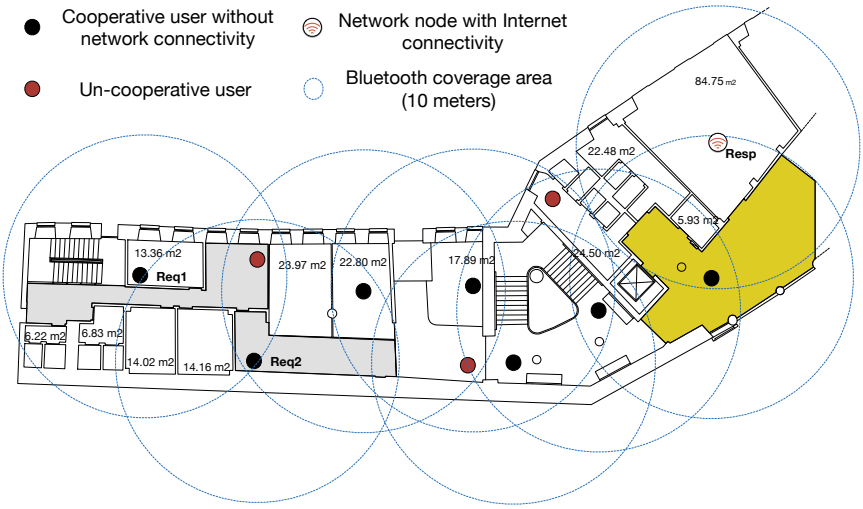


Fig. 5. Illustration of the network scenario used for the performance evaluation of MobiCoop.

For a given scenario, two nodes (identified in the Figure 5 as *Req1* and *Req2*) request two different app services. *Req1* user that is static in his office room wants to send an e-Mail and *Req2* user, that has mobility, wants to send an instant message, however, both do not have Internet connectivity. *Req1* user application starts searching for neighbor users using a Bluetooth connection until it finds a cooperative user. Through cooperation, and repeating the process, network nodes will forward the e-Mail request until a node with Internet connectivity is found (identified in the figure as *Resp*). *Resp* will then communicate with the CWS that verifies the reputation value of *Req1*, and allows or denies access to the requested service. *Req2* repeats the same processes as *Req1*. However, in this case, the *Resp* node, after the reputation verification, will allow access to the application Web service and then send the requested authentication to *Req1* also through cooperation. This response will be forwarded through the network nodes, and cooperative behaviors will also be observed. The main goal is to analyze the service requests delivery probability and the service average delay. The service requests delivery probability is used to observe whether, and the number of times, a node request is delivered. The service average delay focuses on the average time between the request from the application service and its delivery. Furthermore, the number of un-cooperative nodes will change and the results will be compared to the ones presented in [Silva et al. 2013b].

4.3. Performance Evaluation Analysis

This section focuses on the performance analysis of the proposed cooperative approach and its impact on the overall network performance. The study was performed through the above-described scenario and mobile apps. The case study scenario included eleven (11) users with both applications.

Non-cooperative cases were controlled and measured to a maximum of 6 (3 mobile users and 3 static users) to guarantee the minimum service performance. The most important analysis refers to the use-case where MobiCoop is not used and any user with no Internet connectivity were unable to use the respective mobile appli-

cation. Through cooperation, all the devices can indeed use the application services. Un-cooperative nodes affect directly the service delivery probability, service average delay, and the overall network performance. The performance metrics considered in this study are the service delivery probability (in percentage) and the service average delay (in seconds). The service delay is measured as the time between the request for the application service and its delivery. It was considered a worst-case scenario of 6 un-cooperative nodes. Moreover, and considering that this performance evaluation would be conducted assuming, most of the time, extreme and worst-case scenarios, the ACT was also modified to 90 seconds.

Figure 6 presents the service delivery probability and the service average delay as function of the number of un-cooperative mobile users/nodes. Both *Req1* and *Req2* requested the respective services thirty (30) times in the following eight (8) different scenarios: *i*) 2 static un-cooperative nodes and 1 mobile un-cooperative node; *ii*) 3 static un-cooperative nodes and 1 mobile un-cooperative node; *iii*) 1 static un-cooperative node and 2 mobile un-cooperative nodes; *iv*) 1 static un-cooperative node and 3 mobile un-cooperative nodes; *v*) 2 static un-cooperative nodes and 2 mobile un-cooperative nodes; *vi*) 3 static un-cooperative nodes and 2 mobile un-cooperative nodes; *vii*) 2 static un-cooperative nodes and 3 mobile un-cooperative nodes; and *viii*) 3 static un-cooperative nodes and 3 mobile un-cooperative nodes.

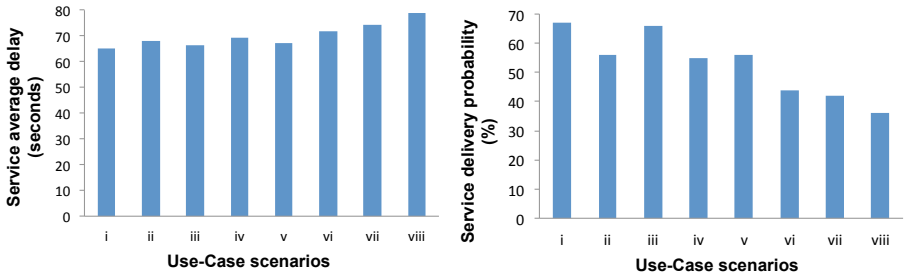


Fig. 6. Service delivery probability and service average delay as function of the increase number of uncooperative mobile users/nodes.

It was observed that when the number of un-cooperative nodes increase, both service delivery probability and service average delay decrease, as expected. However, the variation of static and mobile users present different values for the same number of un-cooperative nodes. In comparison with increasing only the static un-cooperative nodes, the presence of more mobile un-cooperative nodes shown that both metrics present a greater degraded performance. In the worst-case scenario, the service average delay was about 78.8 seconds and the service delivery probability was about 36%. Mobile devices constrains, such as, loss of Bluetooth connection, distance variation, and different devices hardware specifications also affected both performance metrics.

An analytic model was used to deeply study and analyze the service average delay. Equations 2 and 3 calculate the maximum service delay and the service average delay, respectively. The equations results will present comparisons results that will aid to access the above performance evaluation results.

$$\text{Maximum service delay} = (\alpha + \sigma + \varphi) \times T_c + (\alpha + \sigma) \times T_{uc} \tag{2}$$

$$\text{Service Average delay } = (\alpha + \sigma + \beta) \times T_c + (\alpha + \sigma) \times T_{uc} \quad (3)$$

where,

— α = Average connection establishment time = 3.4 seconds
— σ = Average node control message transfer time = 0.45 seconds
— φ = Average request for service+Cooperation List transfer time = 0.38 seconds
— β = Average service response delivery time = 0.29 seconds
— T_c = Total of cooperative nodes
— T_{uc} = Total of uncooperative nodes (variable)

The maximum service delay obtained by (2) was about 69,63 seconds, slightly below that one obtained by real experiments. This difference is due to the mobility aspect that is not considered in (2) that only considers static positioning. Therefore, it proves that selfish behaviors from nodes with constant mobility have a different and more negative effect in the network overall performance. A comparison between the service average delay results from the real experiments and the results obtained by (3) are depicted in Figure 7. As may be seen, the observed results follows the same expected behavior. Results obtained by (3) that only considers static positions presents equal service delay for cases with the same number of un-cooperative nodes. However, in the real experiments, cases with the same number of un-cooperative nodes but variating its type, presented different delays due to their mobility.

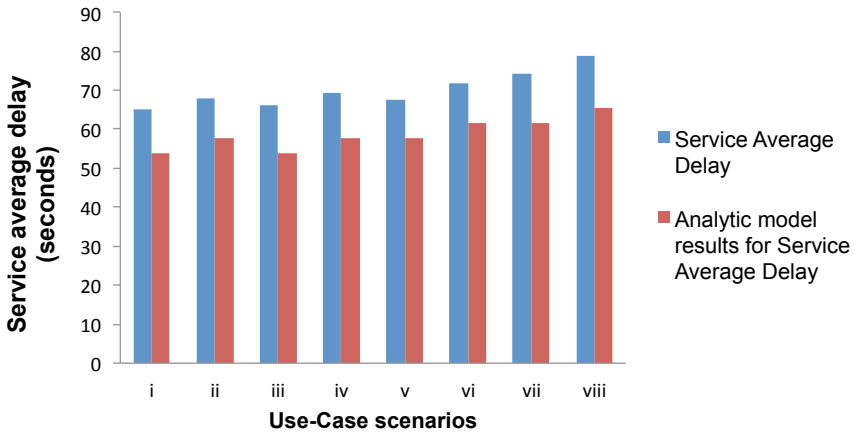


Fig. 7. Performance comparison of the service average delay as function of the number of un-cooperative nodes considering results obtained by real experiments and by the equation (3).

For comparison with the results obtained in [Silva et al. 2013b], a more complex network scenario was considered. The main goal of this comparison was to observe and compare the effect of non-cooperative mobile users with the results obtained in a earlier scenario where non-cooperative users were static or with minor random mobility. Table II presents the results of the use-case scenarios considered to study the performance of the service average delay with the increase of non-cooperative nodes. The number of users and non-cooperative users are the same. However, for each number of

un-cooperative users, it was considered all the possible combinations from minimum to the maximum of mobile users. The results highlighted by "Without user mobility" are obtained in the early above-mentioned work [Silva et al. 2013b]. The same network scenario was also considered for the performance evaluation of the service delivery probability and the results are presented in Table III.

Table II. Performance evaluation results for service average delay considering the total of non-cooperative users and the number of users with mobility.

		Without user mobility	With user mobility/ Number of mobile users				
	Users	0	1	2	3	4	5
Total of non-cooperative users	3	63,2	65,3	66,2			
	4	66,7	67,4	68	69,3		
	5	70,1	70,9	71,8	72,9	74,22	
	6	74,3	74,9	75,4	76,9	77,6	78,8

Table III. Performance evaluation results for service delivery probability considering the total of non-cooperative users and the number of users with mobility.

		Without user mobility	With user mobility/ Number of mobile users				
	Users	0	1	2	3	4	5
Total of non-cooperative users	3	69	67	66			
	4	57	56	56	53		
	5	45	45	44	43	39	
	6	38	38	37	36	32	27

Figure 8 presents the obtained comparison results of the service average delay performance. As expected, results shown that with the increase of non-cooperative mobile nodes the service average delay degraded. Moreover, performance results of the service delivery probability also presents the same behavior, as shown in Figure 9. Compared with the case scenario of static users the probability of a service being delivered to its destination dramatically decreases with a high number of non-cooperative mobile users.

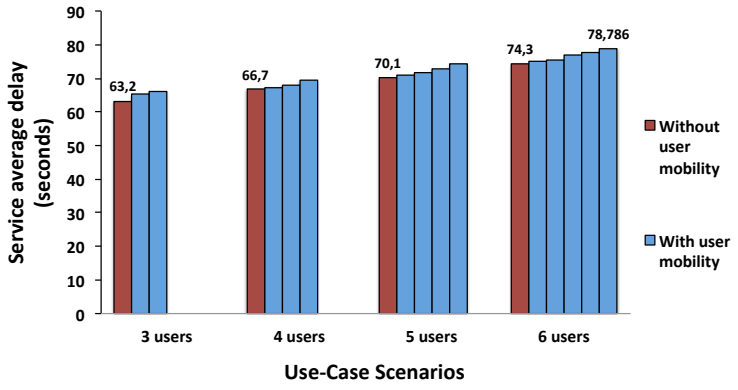


Fig. 8. Performance comparison of the service average delay as function of the increase number of non-cooperative mobile nodes.

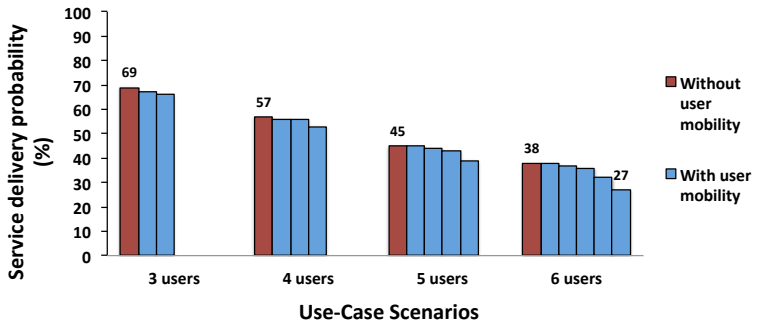


Fig. 9. Performance comparison of the service delivery probability as function of the increase number of non-cooperative mobile nodes.

Compared to the results presented in [Silva et al. 2013b], all the performed test-case scenarios shown slight but worst results. However, this is due to the introduction and variation of node types (static and mobile) and to the average 2% of time that the inclusion of DE4MHA increases in each communication. The network scenario was also bigger and for performance analysis purposes, it considered the communication between the two most distant users/nodes. However, these comparison results are promising, proving the feasibility of the obtained results from the early experiments that clearly follows the same behaviors.

5. CONCLUSION AND FUTURE WORK

This paper proposed a generalized cooperation mechanism for mobile applications called, MobiCoop. This proposal is a reputation-based scheme where a Web service manages all the network cooperation, along with the access control to service/data requests. It considers three main modules: a request treatment module, a cooperation module (that includes neighbors and reputation lists, among other components), and a Web service cooperative module. It aimed to provide an increased network infrastructure and Internet connectivity independent to any mobile application with service-oriented architectures and it was fully accomplished.

The proposed solution was evaluated, demonstrated, and validated through a prototype experimented in a real scenario using two mobile applications, one for instant messages that uses a Web service and another for the popular e-Mail service. The service delivery probability and the service average delay performance metrics were considered. It was shown that the proposed approach provides network connectivity independency to the users mobile apps when Internet connection is unavailable. It was evaluated the influence of the number of un-cooperative nodes on the network performance considering two type of nodes, static and mobile. The results confirm that when the number of un-cooperative nodes increases, both considered performance metrics increases, as expected, confirming also the direct impact of the non-cooperative nodes on the performance of the network. Furthermore, through comparison results of real experiments with an analytic model, it was concluded that un-cooperative nodes with mobility have a more negative impact on the network performance. Through the performance evaluation study and the analysis of its results, it was possible to conclude that MobiCoop improved significantly the overall network performance and the quality of service (QoS) for a given mobile application.

Future work should consider novel network scenarios where the focus should be on energy optimization. All the neighbor nodes know their device battery status through the exchange of the Node Control Message (NCM). Therefore, every time that a cluster of nodes is formed, only the node with better battery state has access to the network. This node relays information with the other nodes helping them to save energy.

REFERENCES

L. Al-Kanj and Z. Dawy. 2010. Optimized energy efficient content distribution over wireless networks with mobile-to-mobile cooperation. In *Telecommunications (ICT), 2010 IEEE 17th International Conference on*. 471–475. DOI:http://dx.doi.org/10.1109/ICTEL.2010.5478815

S. Althunibat, G. Kibalya, and F. Granelli. 2012. Energy-efficient Network Discovery mechanism by exploiting cooperation among terminals. In *Communications and Vehicular Technology in the Benelux (SCVT), 2012 IEEE 19th Symposium on*. 1–5. DOI:http://dx.doi.org/10.1109/SCVT.2012.6399398

Sorav Bansal and Mary Baker. 2003. Observation-based Cooperation Enforcement in Ad Hoc Networks. *CoRR* cs.NI/0307012 (2003). http://dblp.uni-trier.de/db/journals/corr/corr0307.html\#cs-NI-0307012

Sonja Buchegger and Jean-Yves Le Boudec. 2002. Performance Analysis of the CONFIDANT Protocol. In *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking &Amp; Computing (MobiHoc '02)*. ACM, New York, NY, USA, 226–236. DOI:http://dx.doi.org/10.1145/513800.513828

Levente Buttyán and Jean-Pierre Hubaux. 2001. *Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks*. Technical Report.

L. Buttyán and J-P. Hubaux. 2003. Stimulating Cooperation in Self-Organizing Mobile Ad hoc Networks. *Mobile Networks and Applications* 8 (2003), 579–592.

V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss. 2007. Delay-Tolerant Networking Architecture. RFC 4838 (Informational). (April 2007). http://www.ietf.org/rfc/rfc4838.txt

Dimitris E. Charilas and Athanasios D. Panagopoulos. 2010. A Survey on Game Theory Applications in Wireless Networks. *Comput. Netw.* 54, 18 (Dec. 2010), 3421–3430. DOI:http://dx.doi.org/10.1016/j.comnet.2010.06.020

Kang Chen and Haiying Shen. 2013. Multicent: A multifunctional incentive scheme adaptive to diverse performance objectives for DTN routing. In *Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2013 10th Annual IEEE Communications Society Conference on*. 532–540. DOI:http://dx.doi.org/10.1109/SAHCN.2013.6645025

S. Corson and J. Macker. 1999. Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. (1999).

M. Felegyhazi and J-P. Hubaux. 2007. *Game theory in wiress networks: A tutorial*. Technical Report. EPFL.

M. H. Lofti Froushani, B.H. Khalaj, and S. Vakilinia. 2011. A Novel Approach to Incentive-Based Cooperation in Wireless Ad Hoc Networks. In *18th International Conference on Telecommunications (ICT)*. 78–83.

Inc. Gartner. 2013. Gartner Says Mobile App Stores Will See Annual Downloads Reach 102 Billion in 2013. (Setember 2013). http://www.gartner.com/newsroom/id/2592315

Google. Google Maps API. (????). https://developers.google.com/maps/

László Gyarmati and Tuan Anh Trinh. 2011. Cooperative strategies of wireless access technologies: A game-theoretic analysis. *Pervasive and Mobile Computing* 7, 5 (2011), 545–568. http://dblp.uni-trier.de/db/journals/percom/percom7.html\#GyarmatiT11

Qi He, Dapeng Wu, and Pradeep Khosla. 2004. SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks. In *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE*, Vol. 2. 825–830 Vol.2. DOI:http://dx.doi.org/10.1109/WCNC.2004.1311293

O.R. Helgason, F. Legendre, V. Lenders, M. May, and G. Karlsson. 2010. Performance of opportunistic content distribution under different levels of cooperation. In *Wireless Conference (EW), 2010 European*. 903–910. DOI:http://dx.doi.org/10.1109/EW.2010.5483523

Mohammad Asharful Hoque, Matti Siekkinen, Jukka K. Nurminen, Sasu Tarkoma, and Mika Aalto. 2014a. Saving Energy in Mobile Devices for On-Demand Multimedia Streaming – A Cross-Layer Approach. *ACM Trans. Multimedia Comput. Commun. Appl.* 10, 3, Article 25 (April 2014), 23 pages. DOI:http://dx.doi.org/10.1145/2556942

Mohammad Asharful Hoque, Matti Siekkinen, Jukka K. Nurminen, Sasu Tarkoma, and Mika Aalto. 2014b. Saving Energy in Mobile Devices for On-Demand Multimedia Streaming – A Cross-Layer Approach. *ACM Trans. Multimedia Comput. Commun. Appl.* 10, 3, Article 25 (April 2014), 23 pages. DOI:http://dx.doi.org/10.1145/2556942

Jiangyi Hu and Mike Burmester. 2006. LARS: A Locally Aware Reputation System for Mobile Ad Hoc Networks. In *Proceedings of the 44th Annual Southeast Regional Conference (ACM-SE 44)*. ACM, New York, NY, USA, 119–123. DOI:http://dx.doi.org/10.1145/1185448.1185475

Jiangyi Hu and Mike Burmester. 2009. Cooperation in Mobile Ad Hoc Networks. In *Guide to Wireless Ad Hoc Networks*, Sudip Misra, Isaac Woungang, and Subhas Chandra Misra (Eds.). Springer London, 43–57. DOI:http://dx.doi.org/10.1007/978-1-84800-328-6_3

Juan José Jaramillo and R. Srikant. 2007. DARWIN: Distributed and Adaptive Reputation Mechanism for Wireless Ad-hoc Networks. In *Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking (MobiCom '07)*. ACM, New York, NY, USA, 87–98. DOI:http://dx.doi.org/10.1145/1287853.1287865

Wu Jianping, Li Hewu, Sun Wenqi, Wu Qian, Jiang Zhuo, and Zhao Wei. 2013. Technology trends and architecture research for future mobile Internet. *IEEE China Communications* 10, 6 (June 2013), 14–27.

J. Jonsson and B. Kaliski. 2003. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. (2003).

Ma Kai, Guan Xinping, and Zhao Bin. 2010. Symmetrical cooperative strategies in wireless networks: A cooperative game approach. In *Control Conference (CCC), 2010 29th Chinese*. 4175–4179.

U.A. Khan, S. Kar, and J.M.F. Moura. 2009. Distributed Sensor Localization in Random Environments Using Minimal Number of Anchor Nodes. *Signal Processing, IEEE Transactions on* 57, 5 (May 2009), 2000–2016. DOI:http://dx.doi.org/10.1109/TSP.2009.2014812

Thanasis Korakis, Zhifeng Tao, Shashi Raj Singh, Pei Liu, and Shivendra S. Panwar. 2009. Implementation of a Cooperative MAC Protocol: Performance and Challenges in a Real Environment. *EURASIP J. Wireless Comm. and Networking* 2009 (2009). http://dblp.uni-trier.de/db/journals/ejwcn/ejwcn2009.html\#KorakisTSLP09

Gerhard Kramer, Ivana Marić, and Roy D. Yates. 2006. Cooperative Communications. *Found. Trends Netw.* 1, 3 (Aug. 2006), 271–425. DOI:http://dx.doi.org/10.1561/1300000004

G. Kramer, I. Maric, and R. D. Yates. June 2007. *Cooperative communications (Foundations and Trends in Networking)*. Now Publishers Inc.

Lifeng Lai, Ke Liu, and H. El-Gamal. 2006. The three-node wireless network: achievable rates and Cooperation strategies. *Information Theory, IEEE Transactions on* 52, 3 (March 2006), 805–828. DOI:http://dx.doi.org/10.1109/TIT.2005.864421

Lei Lei, Zhangdui Zhong, Kan Zheng, Jiadi Chen, and Hanlin Meng. 2013. Challenges on wireless heterogeneous networks for mobile cloud computing. *Wireless Communications, IEEE* 20, 3 (June 2013), 34–44. DOI:http://dx.doi.org/10.1109/MWC.2013.6549281

Yun Li, Xiaofen Zhu, and Weiliang Zhao. 2011. Cooperation mode selection for maximizing throughput in wireless networks. In *Wireless and Optical Communications Networks (WOCN), 2011 Eighth International Conference on*. 1–5. DOI:http://dx.doi.org/10.1109/WOCN.2011.5872935

Cong Liu, Jie Wu, Xin Guan, and Li Chen. 2011. Cooperative File Sharing in Hybrid Delay Tolerant Networks. In *Proceedings of the 2011 31st International Conference on Distributed Computing Systems Workshops (ICDCSW '11)*. IEEE Computer Society, Washington, DC, USA, 339–344. DOI:http://dx.doi.org/10.1109/ICDCSW.2011.68

Pei Liu, Zhifeng Tao, Sathya Narayanan, Thanasis Korakis, and Shivendra S. Panwar. 2007. CoopMAC: A Cooperative MAC for Wireless LANs. *IEEE Journal on Selected Areas in Communications* 25, 2 (2007), 340–354. http://dblp.uni-trier.de/db/journals/jsac/jsac25.html\#LiuTNKP07

Yuting Luo and R. Deters. 2009. Using cooperation to improve the experience of mobile Web Services consumers. In *Services Computing Conference, 2009. APSCC 2009. IEEE Asia-Pacific*. 213–218. DOI:http://dx.doi.org/10.1109/APSCC.2009.5394122

N. Magaia, P. Rogerio Pereira, and M.P. Correia. 2013. Selfish and malicious behavior in Delay-Tolerant Networks. In *Future Network and Mobile Summit (FutureNetworkSummit), 2013*. 1–10.

Pietro Michiardi and Refik Molva. 2002. Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. In *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security*. Kluwer, B.V., Deventer, The Netherlands, The Netherlands, 107–121. http://dl.acm.org/citation.cfm?id=647802.737297

T. Mshvidobadze. 2012. Evolution mobile wireless communication and LTE networks. In *Application of Information and Communication Technologies (AICT), 2012 6th International Conference on*. 1–7.

Patrick Murphy, Ashutosh Sabharwal, and Behnaam Aazhang. 2009. On Building a Cooperative Communication System: Testbed Implementation and First Results. *EURASIP J. Wireless Comm. and Networking* 2009 (2009). http://dblp.uni-trier.de/db/journals/ejwcn/ejwcn2009.html\#MurphySA09

N. Patwari, J.N. Ash, S. Kyperountas, A.O. Hero, R.L. Moses, and N.S. Correal. 2005. Locating the nodes: cooperative localization in wireless sensor networks. *Signal Processing Magazine, IEEE* 22, 4 (July 2005), 54–69. DOI:http://dx.doi.org/10.1109/MSP.2005.1458287

J.M. Pozo, O. Trullols, J.M. Barcelo, and J.G. Vidal. 2008. A Cooperative ARQ for Delay-Tolerant Vehicular Networks. In *Distributed Computing Systems Workshops, 2008. ICDCS '08. 28th International Conference on*. 192–197. DOI:http://dx.doi.org/10.1109/ICDCS.Workshops.2008.58

K. Raeburn. 2005. Advanced Encryption Standard (AES) Encryption for Kerberos 5. RFC 3962 (Proposed Standard). (February 2005). http://www.ietf.org/rfc/rfc3962.txt

D. Raychaudhuri and Narayan B. Mandayam. 2012. Frontiers of Wireless and Mobile Communications. *Proc. IEEE* 100, 4 (April 2012), 824–840. DOI:http://dx.doi.org/10.1109/JPROC.2011.2182095

R. Rivest. 1992. The MD5 Message-Digest Algorithm. (1992).

Lawrence A. Rowe. 2013. Looking Forward 10 Years to Multimedia Successes. *ACM Trans. Multimedia Comput. Commun. Appl.* 9, 1s, Article 37 (Oct. 2013), 7 pages. DOI:http://dx.doi.org/10.1145/2490825

C. Sammarco, F.H.P. Fitzek, G.P. Perrucci, A. Iera, and A. Molinaro. 2008. Localization Information Retrieval Exploiting Cooperation Among Mobile Devices. In *Communications Workshops, 2008. ICC Workshops '08. IEEE International Conference on*. 149–153. DOI:http://dx.doi.org/10.1109/ICCW.2008.33

Haiying Shen and Ze Li. 2012. Game-Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Networks. *IEEE Transactions on Mobile Computing* 11, 8 (2012), 1287–1303. DOI:http://dx.doi.org/10.1109/TMC.2011.151

Yuan Shen, Henk Wymeersch, and Moe Z. Win. 2010. Fundamental Limits of Wideband Localization - Part II: Cooperative Networks. *CoRR* abs/1006.0890 (2010). http://dblp.uni-trier.de/db/journals/corr/corr1006.html\#abs-1006-0890

U. Shevade, Han Hee Song, Lili Qiu, and Yin Zhang. 2008. Incentive-aware routing in DTNs. In *Network Protocols, 2008. ICNP 2008. IEEE International Conference on*. 238–247. DOI:http://dx.doi.org/10.1109/ICNP.2008.4697042

Bruno M.C. Silva, Joel J.P.C. Rodrigues, Ivo M.C. Lopes, Tiago M.F. Machado, and Liang Zhou. 2013b. A Novel Cooperation Strategy for Mobile Health Applications. *Selected Areas in Communications, IEEE Journal on* 31, 9 (September 2013), 28–36. DOI:http://dx.doi.org/10.1109/JSAC.2013.SUP.0513003

M. Bruno Silva, JPC Joel Rodrigues, Fábio Canelo, C. Ivo Lopes, and Liang Zhou. 2013a. A Data Encryption Solution for Mobile Health Apps in Cooperation Environments. *J Med Internet Res* 15, 4 (25 Apr 2013), e66. http://www.jmir.org/2013/4/e66/

Vasco N. G. J. Soares and Joel J. P. C. Rodrigues. 2011. *Cooperative Networking*. Wiley, Chapter Cooperation in DTN-Based Network Architectures, 101–115.

Shuhuan Wen, Baozhu Hu, Ahmad B. Rad, Xinbin Li, Huibin Lu, and Jianhua Zhang. 2012. Robust Nash Dynamic Game Strategy for User Cooperation Energy Efficiency in Wireless Cellular Networks. *Mathematical Problems in Engineering* 2012 (2012).

M.Z. Win, A. Conti, S. Mazuelas, Yuan Shen, W.M. Gifford, D. Dardari, and M. Chiani. 2011. Network localization and navigation via cooperation. *Communications Magazine, IEEE* 49, 5 (May 2011), 56–62. DOI:http://dx.doi.org/10.1109/MCOM.2011.5762798

H. Wymeersch, J. Lien, and M.Z. Win. 2009. Cooperative Localization in Wireless Networks. *Proc. IEEE* 97, 2 (Feb 2009), 427–450. DOI:http://dx.doi.org/10.1109/JPROC.2008.2008853

Lei Yin, Hui mei Lu, Yuan-Da Cao, and Jian min Gao. 2010. Cooperation in delay tolerant networks. In *Signal Processing Systems (ICSPS), 2010 2nd International Conference on*, Vol. 1. V1–202–V1–205. DOI:http://dx.doi.org/10.1109/ICSPS.2010.5555572

Jong-Woon Yoo and Kyu Ho Park. 2011. A Cooperative Clustering Protocol for Energy Saving of Mobile Devices with WLAN and Bluetooth Interfaces. *IEEE Transactions on Mobile Computing* 10, 4 (April 2011), 491–504. DOI:http://dx.doi.org/10.1109/TMC.2010.161

Per Zetterberg, Christos Mavrokefalidis, Aris S. Lalos, and Emmanouil Matigakis. 2009. Experimental Investigation of Cooperative Schemes on a Real-Time DSP-Based Testbed. *EURASIP J. Wireless Comm. and Networking* 2009 (2009). http://dblp.uni-trier.de/db/journals/ejwcn/ejwcn2009.html\#ZetterbergMLM09

S. Zhong, J. Chen, and Y.R. Yang. 2003. Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks. In *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, Vol. 3. 1987–1997 vol.3. DOI:http://dx.doi.org/10.1109/INFCOM.2003.1209220

Chapter 8

Conclusion and Future Work

This chapter presents the main conclusions that result from the research work described in this thesis. Furthermore, it discusses several research topics related to the work developed along the doctoral programme that can be addressed in further research works.

8.1 Final Conclusions

This thesis proposes and evaluates a novel incentive based cooperation strategy for m-Health services and applications. To achieve this objective the research work was split in four main partial objectives. These parts can be summarized as follows: the first was dedicated to the study of the research topic and analyses of the state of the art in order to identify the main open issues; the second part was dedicated to the construction and performance evaluation of a novel cooperation strategy for m-Health services and applications; the next describes a cryptography solution for m-Health applications under cooperative environments; and the final part was devoted to the proposal and performance evaluation of a generalized and interoperable incentive-based cooperative application framework for mobile applications.

The first part of this research work was included in chapters 2 and 3 of this document. At this stage a detailed research of the main thesis topic was performed in order to prepare a comprehensive review of the state of the art. Then, the focus of this research work was defined and delimited and its main objectives were described. Chapter 2 presents a detailed survey of the state of the art on the evolution of e-Health and m-Health technologies. Through this study it was possible to identify the main open issues and constraints in m-Health applications and supporting network architectures. This study also identified that cooperation schemes was a viable solution to the identified problem. Chapter 3 presents a detailed review on existing cooperation strategies and mechanisms on e-Health, wireless networks, ad-hoc networks, and delay-tolerant networks. Through this study it was possible to identify and gather important contributions from cooperative schemes in similar scenarios to m-Health network architectures. After analysing and identifying the main limitations of the existing solutions, some open issues were identified.

The second part of this work, presented in detail at chapter 4, includes the proposal and performance evaluation of a novel cooperation strategy for m-Health services and applications. This incentive-based cooperation approach presents a reputation-based strategy where a Web service manages the fair access control and the cooperation among nodes along with their reputation. The evaluation of this proposal was performed through a real network scenario involving 19 users with a real m-Health application that requires constant network connectivity, called SapoFit [8]. The evaluation metrics used for this evaluation were the service average delay, that consists in the average time that a response takes to return to the original requester node, and the average delivery probability, that considers the probability of a requester node to receive

its requested service/data. The number of un-cooperative nodes was variable, considering the worst case scenario with 9 un-cooperative nodes. Evaluation results were very positives, the first and perhaps the most important conclusion is that without the cooperation strategy, devices with no Internet connectivity were unable to access the application Web services and, therefore, cannot use the m-Health application. In the worst case scenario the maximum service delay observed was about 83.7 seconds with an average delivery probability of 19%. Taking in consideration middle case scenarios with 4 or 5 un-cooperative nodes the service average delay was about 60 to 70 seconds with an average delivery probability of 60%. Furthermore, all these results also variate negatively due to mobile devices constrains, such as loss of Bluetooth connection between nodes, distance variation, and different devices hardware specifications.

The third part of this work, is described in detail in chapters 5 and 6 and concerns a proposal of a cryptography solution for m-Health application under cooperative environments, called, DE4MHA (Data Encryption Solution for M-Health Applications). Chapter 5 describes the proposal that considers a hybrid encryption solution that uses both synchronous and asynchronous encryption algorithms and was especially designed and deployed for the cooperative strategy for m-Health services and applications. This proposal guaranties the confidentiality, integrity, and authenticity of sensitive health data/information during cooperative processes. Chapter 6 presents the performance evaluation of DE4MHA and a field survey of the proposed cryptography proposal, with real users. This evaluation study was performed involving 35 real users with SapoFit application under a cooperative environment. Evaluation results shown that DE4MHA does not deteriorate the overall performance of the proposed cooperation strategy for m-Health applications. Hence, it can conclude that with DE4MHA incorporation, the average time added with encryption/decryption tasks is about 0,003557 seconds, corresponding to an increase of 2% of the overall service delivery time. The online survey concludes that users were generally satisfied with the application performance and that are more confidant in using m-Health applications knowing that their data/information is protected.

The fourth and last part of this thesis, is presented in chapter 7, that describes in detail the proposal and performance evaluation of a generalized and interoperable incentive-based cooperative application framework for mobile applications, called, MobiCoop. This proposal was based on the incentive based approach for m-Health applications and it aims to offer an application framework to developers easily incorporate the cooperative strategy in their applications. MobiCoop was incorporated in two mobile applications: an instant text message application and a mail send/receiving application. The same metrics were considered for the performance evaluation in a real scenario involving 11 users. However, in order to emulate a more realistic scenario, two different type of users were considered: users with mobility and static users. The worst case scenario was assumed with 6 un-cooperative nodes (3 mobile users and 3 static users). Results were very positives. The worst case scenario presented a service average delay of 78.8 seconds and a service delivery probability about 36%.

The main objective of this thesis was accomplished, as well the defined partial objectives.The objective of providing an increased network infrastructure and Internet connectivity independency to m-Health applications with service-oriented architectures was fully accomplished. Due to the sensitive health information a cryptography solution called DE4MHA was also proposed and evaluated with success. Finally, a generalized and interoperable reputation-based cooperative application framework for mobile applications, called, MobiCoop, was successfully

proposed and evaluated.

8.2 Future Work

To conclude this thesis, the next paragraphs present some future research directions that can be followed and which result from this research work.

For future work, a more profound study on the effect of the proposed cooperation strategy on un-cooperative nodes is considered. In this work, un-cooperative nodes are punished with negative reputation rating and are deprived of access to the respective services. However, how can this nodes can regain reputation and access privileges? And, in what way the neighbors reputation can mitigate selfish behaviors promoting cooperation?

Another further insight is the node mobility effect on the network performance. The performance evaluation of MobiCoop, presented in chapter 7, considered both static and mobile users. From the evaluation results, it was clear that un-cooperative nodes with mobility have a greater negative impact than static users. For future work, mobility should be taken in consideration to the reputation rating for uncooperative nodes. Furthermore, ubiquitous mechanisms and procedures should be created for assessing if a node is static or mobile.

Future work also should consider a novel network scenarios where the focus should be on energy optimization. All the neighbor nodes know their device battery status through the exchange of the Node Control Message (NCM). Therefore, every time that a cluster of nodes is formed, only the node with better battery state has access to the network. This node relays information with the other nodes helping them to save energy.