Redes Sem Fios IEEE 802.11: Instalação, Configuração e Segurança

Tiago Lages[1], Humberto Santos[1] e Fernando J. Velez[1,2]

[1] *DEM, Universidade da Beira Interior, Covilhã, Portugal*
[2] *Instituto de Telecomunicações, IST, Lisboa, Portugal*
tlages@netvisao.pt, humberto@ubi.pt, fjv@ubi.pt

Resumo: Esta comunicação descreve a forma como foi implementada a rede sem fios do Departamento de Engenharia Electromecânica no âmbito do projecto SAMURAI. Abordam-se os principais aspectos relacionados com a sua implementação, configuração e segurança, nomeadamente a encriptação WEP, aspectos de autenticação, o protocolo 802.1x e o protocolo EAP. Discute-se a sua evolução e a inclusão sucessiva de mecanismos de encriptação de pacotes e de autenticação de clientes. Finalmente, parte-se de um levantamento de medidas de potência do sinal, para a discussão do impacto da interferência na reutilização de recursos.

© *Tiago Lages 2003*

Palavras Chave: Redes sem fios, Samurai, 802.11, 802.1x, Radius.

1. INTRODUÇÃO

Nos últimos anos tem-se dado uma enorme vulgarização da utilização da Internet como forma privilegiada de comunicação, ferramenta de trabalho e lazer. Os métodos e aplicações para a centralização de informação e das ferramentas de trabalho têm vindo a evoluir de dia para dia e a necessidade de tornar os sistemas informáticos mais portáveis tem acompanhado essa evolução.
Em paralelo com a vulgarização da Internet e das redes locais na sociedade em geral, a comunidade cientifica e a industria informática empenham-se em criar novos sistemas que permitam gerir e tirar proveito de todas estas tecnologias. Neste contexto, têm sido desenvolvidos num processo que tenta acompanhar a evolução das redes locais, aplicações com vista a uma maior portabilidade e flexibilidade dessas redes.
As redes locais sem fios constituem uma alternativa às redes convencionais com fios, fornecendo as mesmas funcionalidades, mas de forma flexível, de fácil configuração e com boa conectividade, em áreas densamente urbanizadas ou de *campus*.
As novas tecnologias inerentes a toda esta flexibilidade das redes sem fios evoluem a olhos vistos, verificando-se uma maior implantação no mercado de massas de dia para dia, com o aparecimento de novos terminais móveis e com a possibilidade de tornar móveis e mais versáteis todos os equipamentos que conhecemos do dia a dia.
Este trabalho teve como objectivo a criação de uma rede sem fios experimental no polo 8 da Universidade da Beira Interior, com vista a desenvolver uma implementação idêntica no Centro Hospitalar da Cova da Beira no âmbito do projecto SAMURAI (Serviços e Aplicações Multimédia em Ambiente Hospitalar, Universitário e Urbano). O projecto SAMURAI é uma parceria entre a Faculdade de Ciências da Saúde (FCS), o Departamento de Engenharia

Electromecânica (DEM), ambos da Universidade da Beira Interior (UBI), a PT Inovação (PTIN) e o Centro Hospitalar da Cova da Beira (CHCB). O projecto tem duas vertentes principais, a vertente hospitalar e a vertente universitária. A vertente universitária consiste basicamente na construção de uma plataforma de *e-learnig* enquanto que a vertente hospitalar consiste na implementação de um sistema que permita realizar tele-trabalho e aceder a dados clínicos através de terminais móveis utilizando a rede sem fios.
Uma das principais características desta rede é a restrição do seu uso por parte de utilizadores não autorizados. Numa fase em que os protocolos padrão destas redes estão em constante evolução, elas tornam-se vulneráveis a ataques vindos do exterior. Há vários aspectos a ter em conta quando se configura e instala uma rede com estas características, desde a cobertura à segurança, passando pelo controlo das interferências na utilização de recursos. A rede sem fios tem que estar configurada de forma a permitir o acesso não só a computadores pessoais e computadores portáteis, mas também a novos terminais que aparecem agora no mercado, como é o caso dos *tablet pc* e *pocket pc*.
A estrutura da comunicação é a seguinte. Na Secção 2, apresentam-se aspectos da segurança em redes IEEE 802.11. Na secção 3, estão descritas as etapas da implementação da rede sem fios do DEM, apresentando-se detalhes da sua configuração em cada fase, enquanto que a Secção 4 aborda o enquadramento de rede sem fios no contexto da rede do DEM, as medidas de sinal que se efectuaram e as perspectivas de evolução futura. Por fim, na Secção 5, são apresentadas as conclusões.

2. SEGURANÇA EM REDES IEEE 802.11

A segurança é uma das principais questões que se coloca em relação às redes sem fios [1]. Não há dúvida que um administrador de uma rede deste tipo tem que estar muito bem informado e actualizado sobre a evolução dos mecanismos de segurança, pois muitos dos existentes são simples adaptações de métodos e protocolos desenhados para redes com fios. Neste trabalho, concentrámo-nos em explorar os aspectos da encriptação WEP (*Wired Equivalent Privacy*), autenticação, protocolo 802.1x e protocolo EAP (*Extensible Authentication Protocol*).

2.1 Encriptação WEP

As comunicações rádio sempre tiveram o problema de interferências durante a comunicação, sendo este um meio vulnerável, pois aparelhos a operar na mesma frequência podem facilmente comprometer a confidencialidade da informação. São necessários portanto, mecanismos de encriptação dos dados. A norma 802.11 utiliza um mecanismo de encriptação denominado WEP. O objectivo do WEP é tornar as comunicações numa WLAN (*Wireless Local Area Network*) segura tal como as LANs (*Local Area Network*) usuais, possibilitando a autenticação e a confidencialidade. O WEP usa o mecanismo de chaves partilhadas com cifra simétrica chamado RC4. A chave que o cliente da rede sem fios usa tem que ser a mesma que é utilizada pelo AP (*Access Point*) utilizado na encriptação da comunicação.

2.2 Autenticação

Quando um cliente detecta o sinal emitido por um AP, necessita de se autenticar, caso a rede esteja munida dos requisitos mínimos de segurança.
Após esta detecção, o cliente e o AP trocam informações acerca do método de autenticação. Se o tipo de autenticação for aberto, de facto, não existe mesmo nenhum tipo de autenticação.
No entanto, o AP e o cliente podem no mínimo partilhar uma chave secreta comum. Se a chave partilhada pelo cliente for igual à chave do AP, então o cliente está apto a entrar na rede.

2.3 Protocolo 802.1x

Este protocolo é utilizado para permitir a autenticação de clientes na rede sem fios. Nem todo o hardware é compatível com este protocolo. Por isso, no projecto SAMURAI, houve uma preocupação de adquirir software de acordo com a compatibilidade desta norma. Para além

disso, a autenticação com este protocolo necessita a configuração de muitos outros aspectos, por exemplo, a configuração de um servidor RADIUS (*Remote Authentication Dial In User Service)*. O IEEE 802.1x é uma norma IEEE que foi desenvolvida tendo em conta o protocolo EAP.
Antes de se estabelecer a ligação existe um período de autenticação que implica o uso de *username* e *password*. O EAP disponibiliza vários métodos de autenticação que podem ser usados com o 802.1x, ou seja, o IEEE 802.1x é simplesmente uma norma que permite transportar pacotes EAP sobre uma rede com ou sem fios, tendo três intervenientes no processo de autenticação, Figura 1: (i) o cliente móvel (cliente da rede sem fios), (ii) o autenticador (neste caso o AP) e (iii) o Servidor RADIUS.

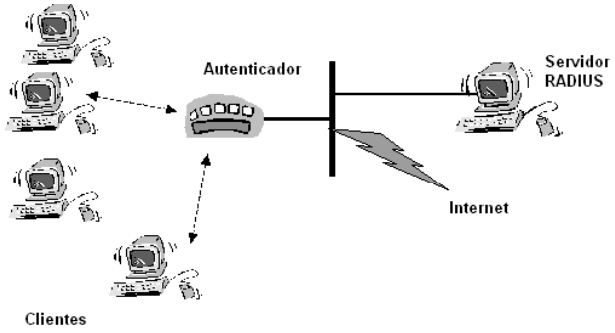

Figura 1 – Intervenientes do IEEE 802.1x

2.4 Protocolo EAP
No ambiente de redes sem fios, este protocolo está associado ao protocolo 802.1x. Para usar o protocolo 802.1x é necessário escolher qual o mecanismo EAP de autenticação que vamos utilizar. Apesar de existirem vários métodos de autenticação EAP, somente três são usados com mais frequência: o MD5 (*Message Digest 5*), o TLS (*Transport Layer Security*) e o TTLS (*Tunneled Transport Layer Security*). Estes dois últimos exigem uma autenticação mútua entre os dois agentes, o cliente móvel e o autenticador, enquanto que o MD5 só necessita de autenticação do cliente móvel.

3. ETAPAS DA IMPLEMENTAÇÃO DA REDE

A rede sem fios implementada foi configurada de forma a funcionar na sub-rede já existente no DEM.

3.1 Sem qualquer mecanismo de autenticação
A primeira configuração da rede resumiu-se ao ponto de acesso AP-500 ligado directamente à *Ethernet* existente e configurado para receber um IP dinamicamente, através do servidor de DHCP (*Domain Host Control Protocol*) que funciona na máquina *ftpdem.ubi.pt*, Figura 2.

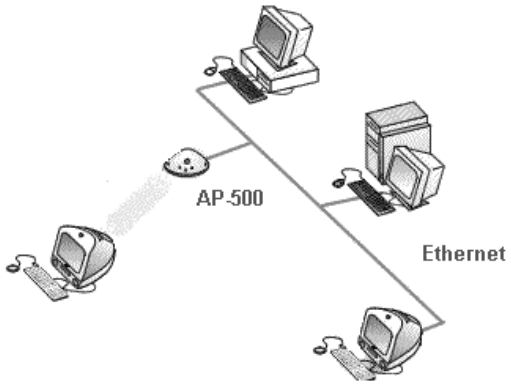

Figura 2 – WLAN inicial

O problema desta rede consiste na inexistência de encriptação para os pacotes que circulam entre o AP e o cliente logo, qualquer cliente que detecte o sinal emitido pelo AP-500 podia-se ligar à rede sem fios sem limitações, e neste caso estar ligado à rede da UBI.

3.2 Com encriptação dos pacotes

A rede foi posteriormente protegida com a utilização de chaves WEP. Nesta fase, o funcionamento da rede permitia que a comunicação entre o AP e os clientes fosse encriptada. Para isso, os intervenientes têm que conhecer a chave que servirá de cifra na encriptação dos pacotes. Essa chave, configurada no ponto de acesso, tem de ser introduzida no cliente e será igual para todos os clientes da rede sem fios. Assim, a rede já se pode considerar mais segura pois um potencial cliente só se liga à rede conhecendo a chave. No entanto como a chave é do conhecimento de todos os utilizadores, facilmente se dará a conhecer a utilizadores indevidos. O facto de se utilizar sempre a mesma chave também torna a rede vulnerável, pois facilmente, com algum tempo e com algum software já disponível, se poderá descobrir a chave.

3.3 Com mecanismo de encriptação dos pacotes e mecanismo de autenticação clientes

Trocou-se o AP-500 pelo AP-2000, ambos da marca Orinoco. Este ponto de acesso é mais robusto, mais potente e tem muito mais opções de configuração e monitorização do que o AP-500. Nesta ultima fase, configuraram-se os parâmetros do ponto de acesso para a utilização do protocolo 802.1x. O AP-2000 possibilita a configuração de quatro chaves de 128 bits. Com este ponto de acesso e com estas quatro chaves, é possível assegurar a rotação contínua destas chaves num determinado intervalo de tempo, o que reduz a probabilidade de a chave ser descoberta, sendo ela configurada para ser distribuída automaticamente aos clientes. Na configuração do AP-2000 é indicado o endereço IP da máquina onde se encontra o serviço Radius e o porto onde este se encontra à escuta. Cada cliente desta rede sem fios tem de possuir um certificado digital emitido pelo servidor Radius e possuir um *username* e *password*, para poder entrar na rede.

4. REDE SEM FIOS DO DEPARTAMENTO DE ENGENHARIA ELECTROMECÂNICA

A rede sem fios do DEM é apoiada pela *Ethernet* já existente, nomeadamente o servidor de DHCP, que é passou a ser também utilizado pela rede sem fios, tendo sido necessário configurar um servidor RADIUS. A configuração dos APs utilizados na rede sem fios do DEM é realizada através de sessões de telnet ou através de um interface Web. Sempre que foi necessário fazer um *update* de *firmware* aos pontos de acesso ou carregar uma nova configuração foi utilizado um servidor de TFTP (*Trivial File Transfer Protocol*).

Depois, para cada cliente da rede sem fios do DEM, será necessário configurar elementos, o que envolve vários passos [2]. Após o cliente estar configurado, os passos seguintes são efectuados no controlador do domínio wireless.ubi.pt. Os procedimentos são os seguintes:

- Nas ferramentas de administração, escolher *Active Directory Users and Computers*.
- Na lista de utilizadores selecciona-se: *adicionar um novo utilizador*.
- Especificar dados do utilizador como o *username* e a *password* e no menu *Dial-In* seleccionar a opção *Allow access*.
- Se necessário especifica-se as horas e dias da semana quando é permitida a ligação de uma dado utilizador.

Os APs desta rede estão configurados de forma a que os clientes se possam re-autenticare de 10 em 10 minutos. A vantagem que isto traz em termos de segurança é a seguinte: a chave WEP usada numa comunicação muda em cada 10 minutos, dificultando assim possíveis tentativas de "cracar" as chaves e furar a segurança da rede.

O nível de segurança da rede sem fios do DEM é muito bom. As principais razões para este nível de segurança deve-se ao facto desta usar chaves WEP de 128 bits e de ter capacidade de autenticar clientes da rede sem fios. As chaves WEP de 128 bits são mais difíceis de violar.

Houve aqui preocupação em abdicar de um pouco de velocidade em prol da segurança. A característica de re-autenticar os clientes de 10 em 10 minutos fortalece o nível de segurança da rede pois a principal vantagem que trás é a mudança da chave WEP sempre que o cliente é re-autenticado.
No final desta implementação, onde um AP faz a cobertura da zona das salas práticas do DEM, foi feita a ampliação da rede de forma a permitir *roaming*, Figura 3. Para isso, foi usado mais um AP, nas mesmas condições do já existente, e que permite fazer a cobertura do corredor de gabinetes no piso 4 do DEM.

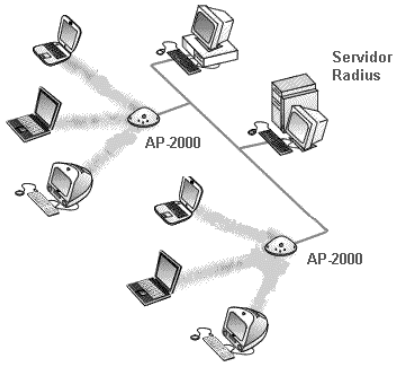

Figura 3 – WLAN do DEM

Foi efectuado um levantamento da cobertura da rede, com medições feitas de metro a metro, com o objectivo de registar a potência do sinal nos corredores e dentro de alguns gabinetes, Figura 4. No próximo passo pretende-se abranger alguns laboratórios, biblioteca, sala de reuniões e sala de conferências.

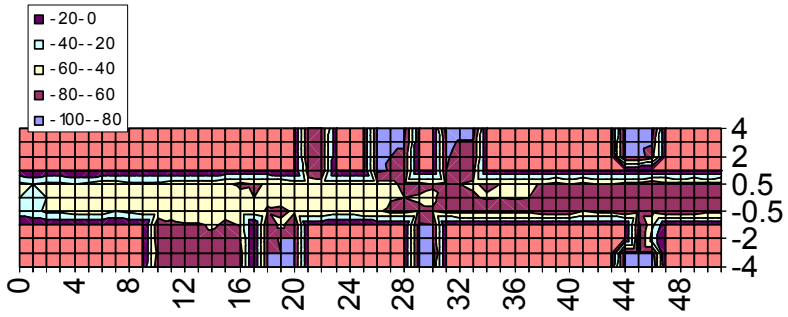

Figura 4 – Levantamento da potência do sinal (em dBm) em função da distância no DEM

5. CONCLUSÕES

As redes IEEE 802.11 são uma tecnologia que começa agora a expandir-se pelas, universidades, empresas e outras organizações portuguesas. Nesta comunicação, para além de aspectos da segurança em redes IEEE 802.11, estão descritas as etapas da implementação da rede sem fios do DEM, apresentando-se detalhes da sua configuração em cada fase, o seu enquadramento no contexto da rede do DEM e as medidas de sinal que se efectuaram.
Nas redes sem fios, o mecanismo de encriptação WEP tem de evoluir num futuro próximo pois prejudica o desempenho da rede em termos de velocidade quando se usam chaves de 128 bits. Quanto à utilização de chaves de 64 bits, pode-se afirmar que as rede sem fios fica vulnerável. Os mecanismos de autenticação com base no protocolo 802.1x tornam a rede protegida de utilizadores indesejados e são, portanto, um dos aspectos a ter em conta. No entanto, a

implementação de um mecanismo de autenticação não é simples de se concretizar e necessita de ter um servidor de suporte para a toda a rede sem fios.
O trabalho de implementação foi descrito e os detalhes de impementação foram apresentados. Este tipo de redes, são uma solução promissora para a instalação de redes locais em edifícios de escritórios, univerisdades, laboratórios, ou mesmo hospitais. Por exemplo, no contexto do SAMURAI, pensa-se que o projecto poderá a vir dar contribuições importantes no planeamento da rede no Centro Hospitalar da Cova da Beira. Um dos locais poderá ser o Hospital do Fundão, um edifício que já tem alguns anos. Poderá instalar-se uma rede com fios, nos corredores principais, garantindo-se, a partir dessa espinha dorsal, o acesso à rede nos consultórios, gabinetes, enfermarias, etc, através da interface sem fios, com APs criteriosamente colocados, de forma a fazer uma cobertura completa. Algum cuidado tem que ser posto nos aspectos de contabilização da interferência. Embora numa fase incial, quando o problema maior é a cobertura, a tendência seja adicionar cada vez mais APs, numa fase posterior, com o aumento do número de utilizadores, o problema de aumento de capacidade começará a pôr-se, sendo necessário que a proliferação de APs não seja anárquica, mas obedeça a critérios de minimização da interferência.

REFERÊNCIAS

[1] Potter, Bruce & Fleck, Bob, *802.11 Security*, O'Reilly, Sebastopol, CA, 2003.
[2] Lages, Tiago, *Estágio Curricular de Matemática/Informática*, UBI, Julho 2003.