1
Introdução

A comunicação de dados por redes sem fio (*Wireless Local Area Network* - WLAN - Padrão IEEE 802.11b) experimenta uma rápida expansão tecnológica, proporcionando novas soluções para serem implementadas em ambientes empresariais, governamentais e residenciais.

Vários fatores contribuíram para que as WLAN se tornassem uma promessa de evolução das redes fixas cabeadas (LAN – *Local Area Network*), não substituindo-as, mas agregando funcionalidades antes não alcançadas.

Estas novas funcionalidades estão, principalmente, relacionadas à mobilidade do terminal. Trazem também vantagens como, por exemplo: menor tempo de instalação; significativa redução nos custos com infra-estrutura; implantação de redes temporárias; maior robustez (áreas sujeitas à intempéries e a desastres); implantação em locais de difícil cabeamento (prédios históricos); e implantação de redes de computadores em locais onde não há viabilidade técnico-financeira para construção de redes cabeadas.

No entanto, possui as desvantagens e dificuldades inerentes a uma comunicação rádio: interferências por equipamentos de terceiros e por equipamentos operando na mesma faixa de freqüência; efeitos de multipercursos causados pelos fenômenos de reflexão, difração e espalhamento; perdas decorrentes da distância da estação móvel ao *access point*; largura de banda variável e difícil de se prever *a priori*; alta taxa de erro; elevado atraso e variação no atraso; baixa qualidade de serviço (QoS); restrições no uso de freqüências (regulamentação governamental); e processamento limitado devido ao consumo de energia e interoperabilidade de sistemas (soluções proprietárias).

1.1
Motivação

Enquanto o uso das WLAN cresce em ritmo acelerado, inúmeros problemas relacionados à tecnologia de segurança, definida no IEEE 802.11b, têm sido abordados em publicações técnicas, apontando as deficiências e as vulnerabilidades, através dos quais indivíduos não autorizados podem ter acesso às informações disponibilizadas pela rede de maneira relativamente fácil e rápida.

O Padrão IEEE 802.11b possui mecanismos básicos para aumentar a segurança da rede, incluídos na própria especificação, que devem ser implementados pelo Administrador de Rede assim que o equipamento é ativado. Estes mecanismos, apesar de fracos, possibilitam o primeiro nível de segurança e não devem ser desconsiderados.

O Padrão IEEE 802.11b possui um procedimento de segurança denominado WEP (*Wired Equivalent Privacy)* que, utilizando uma chave secreta compartilhada com as partes envolvidas na comunicação, tem a intenção de cumprir as seguintes metas de segurança:

a) Autenticação (Controle de Acesso): deve garantir que apenas pessoas autorizadas tenham acesso à rede;

b) Criptografia (Confidencialidade): deve evitar que elementos estranhos tomem conhecimento do conteúdo das mensagens transmitidas através da rede;

c) Integridade dos Dados: deve garantir que o conteúdo da mensagem não seja modificado. Ou seja, deve garantir que os dados indevidos não sejam inseridos e removidos durante a transmissão.

Em todas as três metas, a segurança da rede se sustenta na dificuldade em se obter a chave secreta.

O Padrão IEEE 802.11b não especifica como deve ser realizada a distribuição das chaves secretas. A distribuição é feita manualmente pelo Administrador da Rede. Dependendo da dimensão da rede e do número de usuários, fica bastante complexa a atualização da chave periodicamente, sendo possível, para usuários mal–intencionados, utilizar as falhas de criptografia do WEP para realizar ataques de força bruta, descobrir a chave de criptografia e acessar dados potencialmente confidenciais.

A solução objetiva conjugar a operação dos mecanismos internos do Padrão IEEE 802.11b com uma autenticação externa, utilizando o Padrão IEEE 802.1x. Nesta situação, o *access point* (AP) passa a ser um repassador de pacotes de autenticação, já que toda a base de dados é controlada por um elemento autenticador externo à rede sem fio, normalmente um servidor RADIUS (*Romote Authentication Dial-In User* Service), possibilitando:

a) Autenticação mútua do cliente e do servidor RADIUS;

b) O controle de acesso para permitir o acesso à rede para clientes autorizados e negá–lo a clientes não autorizados;

c) A criptografia de alta segurança do tráfego da rede sem fio;

d) Gerenciamento das chaves de criptografia, com a geração e distribuição de forma confiável e segura.

A criptografia segura dos dados no canal sem fio passa a ser realizada pelo WEP a partir da chave de sessão gerada na autenticação. Portanto, a estratégia básica para reduzir as ameaças à chave de criptografia é garantir que as chaves de sessão sejam atualizadas periodicamente, e o tempo para uma nova autenticação seja inferior ao tempo necessário para capturar o tráfego e executar as operações de força bruta.

O Padrão IEEE 802.1x define diferentes mecanismos de transporte seguro das credenciais dos usuários até o servidor de autenticação. O 802.1x utiliza o protocolo EAP *(Extensible Authentication Protocol*) para efetuar a autenticação através de métodos com base em senhas, certificados de chaves públicas (PKI – *Public Key Infrastructure), Smart Card, Token Cards*, etc. Os mecanismos de autenticação mais comuns oferecidos pelas camadas superiores são o EAP-TLS, EAP-TTLS, PEAP e LEAP.

O mecanismo EAP–TLS usa o protocolo TLS (*Transport Layer Security)* para autenticar mutuamente a estação e o servidor RADIUS, usando métodos de criptografia de alta segurança e gerando uma chave secreta a cada vez que a estação se associar ao AP. O EAP-TLS é um dos métodos mais seguros, porém sua potencialidade tem um alto custo no que se refere à necessidade da empresa/instituição que implementá-lo possuir certificado emitido por Autoridade Certificadora para o cliente e para o servidor.

O mecanismo PEAP *(Protected Extensible Authentication Protocol),* desenvolvido pela *Microsoft, Cisco Systems* e *RSA Security*, oferece autenticação

baseada em senha e exige que o servidor de autenticação possua um certificado digital, porém não exige certificado no cliente. O método mais comum transportado pelo PEAP é o MS-CHAPv2, dentro de um canal protegido pelo protocolo TLS. A autenticação por senha é uma boa solução para as pequenas/médias empresas que atualmente não têm uma infra–estrutura de certificado e não precisam de certificados para outras finalidades.

O mecanismo EAP-TTLS (*Tunnuled Transport Layer Security)*, similar ao PEAP, permite a utilização de diversos tipos de métodos de autenticação, tais como: EAP-MD5, PAP, CHAP, MS-CHAP e MS-CHAPv2. Pelo fato do EAP-TTLS não ser suportado pelo Windows, há necessidade de instalação de um Cliente de Autenticação (por exemplo: *SECURE W2 Client, Meetinghouse AEGIS Client ou Funk Odyssey).*

O LEAP (*Lightweight Extensible Authentication Protocol)*, com autenticação baseada em senha, foi desenvolvido pela *Cisco Systems* e foi um dos primeiros mecanismos de autenticação disponível para redes sem fio.

1.2
Objetivo

A adoção de um mecanismo de segurança gera uma sobrecarga de pacotes, devido à inserção de tráfego extra para autenticação dos usuários e criptografia das mensagens, podendo ocasionar comprometimento na *performanc*e da rede. Quanto mais forte o procedimento de segurança, maior o custo de desempenho. Ou seja, quanto maior o processamento computacional do mecanismo de segurança adotado, maior o impacto no tráfego de dados.

Esta preocupação é discutida em algumas publicações acadêmicas. Os resultados apresentados mostram que esta sobrecarga é considerável, dependente do mecanismo adotado e deve ser levada em conta na decisão de qual modelo a ser implementado, tendo em vista que a mesma pode degradar o desempenho da rede.

Porém, os resultados os quais, em sua essência, mostram que a implementação de um modelo mais eficiente de segurança para as redes IEEE 802.11b pode inviabilizar a sua operação, precisam ser complementados e atualizados.

O objetivo deste trabalho é avaliar qual a efetiva degradação no desempenho (*performance*) das redes IEEE 802.11b, devido à implementação de mecanismos de segurança, sejam eles intrínsecos ao Padrão ou combinados com o Padrão IEEE 802.1x, utilizando os protocolos de aplicação FTP (*File Transfer Protocol*) e HTTP (*Hipertext Transfer Protocol*).

Para análise do desempenho será realizada a simulação de uma WLAN com um cliente e um *access point* e, com os resultados obtidos, avaliar:

a) Como os diferentes mecanismos de segurança influenciam o desempenho da rede;

b) Como varia o desempenho nos diferentes tipos de tráfego;

c) O impacto da autenticação de um usuário em cada mecanismo utilizando Padrão IEEE 802.1x.

Para complementar o trabalho, será realizada também uma simulação com:

a) 02 usuários, em duas situações distintas: ambos configurados para transmitir a 11Mbps, e com um configurado a 11Mbps e outro a 1Mbps. Esta segunda situação representa com mais fidelidade o uso práticos das WLAN, pois as redes IEEE 802.11b têm sua aplicação mais difundida em ambientes fechados (*indoor*). Por esse motivo, o comportamento do canal rádio pode ser fortemente influenciado por interferências de equipamentos de terceiros, equipamentos operando na mesma faixa de freqüência, perdas de penetração em paredes e pisos, e efeitos de multipercursos causados pelos fenômenos de reflexão, difração e espalhamento;

b) 03 usuários configurados para transmitir à 11Mbps e sem mecanismo de segurança implementado;

c) 04 usuários configurados para transmitir à 11Mbps e sem mecanismo de segurança implementado.

1.3
Composição da Dissertação

O capítulo 2 descreve o Padrão IEEE 802.11b, em especial as características envolvidas nas camadas física e de enlace.

O capítulo 3 explora os aspectos referentes à segurança do Padrão IEEE 802.11b, e as fragilidades e vulnerabilidades do WEP. Neste mesmo capítulo é apresentado o Padrão IEEE 802.1x e o princípio de funcionamento dos mecanismos de autenticação externa.

O capítulo 4 descreve a metodologia e o ambiente experimental utilizado na simulação.

O capítulo 5 contém a avaliação e análise dos resultados obtidos.

Por fim, o capítulo 6 apresenta as conclusões e sugestões para trabalhos futuros.

O Apêndice A contém as planilhas com os valores obtidos nos experimentos.