Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Marcio Maia de Castro

SEGURANÇA EM REDES IEEE 802.16:
Uma Visão Geral

Rio de Janeiro

2008

Marcio Maia de Castro

SEGURANÇA EM REDES IEEE 802.16:
Uma Visão Geral

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Profª. Luci Pirmez, D.Sc., COPPE/UFRJ, Brasil

Rio de Janeiro

2008

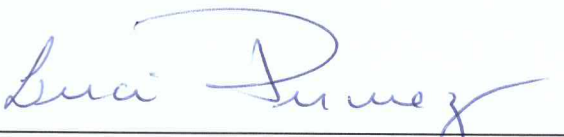
Marcio Maia de Castro

SEGURANÇA EM REDES IEEE 802.16:

Uma Visão Geral

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em outubro de 2008.



Profª. Luci Pirmez, D.Sc., COPPE/UFRJ, Brasil

A meu pai, que me deixou como herança a força e a disposição para buscar meus objetivos.

AGRADECIMENTOS

Gostaria de agradecer à minha esposa, Mônica, por “segurar a barra” de cuidar de meus filhos sozinha enquanto eu escrevia esta monografia.

RESUMO

CASTRO, Marcio Maia de. **SEGURANÇA EM REDES IEEE 802.16: Uma Visão Geral**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2008.

No intuito de promover a ampla adoção de tecnologias de redes sem fio, além de reduzir custos e garantir a interoperabilidade, diversas organizações como o Institute of Electrical and Electronics Engineers (IEEE), a Internet Engineering Task Force (IETF), a Wireless Ethernet Compatibility Alliance (WECA) e a International Telecommunication Union (ITU) integram vários esforços de padronização.

O padrão do Institute Electrical and Electronics Engineers (IEEE) 802.16, também conhecido como Worldwide Interoperability for Microwave Access (WIMAX), que define a interface aérea e os métodos de acesso ao meio para Redes Metropolitanas Sem Fio, está sendo visto, dentre as tecnologias que integrarão a comunicação sem fio nos ambientes de computação ubíquos, como a mais promissora para possibilitar o acesso de banda larga de próxima geração.

Este trabalho irá apresentar um estudo sobre os diversos padrões de rede sem fio, incluindo as redes sem fio em malha, abordando questões de segurança da informação e apresentando trabalhos relacionados que visam incrementar a segurança nessas redes.

ABSTRACT

CASTRO, Marcio Maia de. **SEGURANÇA EM REDES IEEE 802.16: Uma Visão Geral**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2008.

In order to promote broad adoption of technologies for wireless networks, in addition to reducing costs and ensuring interoperability, diverse organizations as the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), the Wireless Ethernet Compatibility Alliance (WECA) and the International Telecommunication Union (ITU) integrate various efforts to standardize.

The Institute of Electrical and Electronics Engineers (IEEE) standard 802.16, also known as Worldwide Interoperability for Microwave Access (WIMAX), which defines the air interface and media access methods to Metropolitan Wireless Networks, is being seen, among the technologies which would incorporate the wireless communication in ubiquitous computing environments, as the most promising to access broadband for next generation.

This work will present a study about different wireless network standards, including wireless mesh networks and addressing issues of information security and presenting related works that aim to enhance security in these networks.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

AK	Authentication Key
BS	Base Station
CBC	Cipher Block Chaining
DES	Data Encryption Standard
DNS	Domain Name System
DoS	Denial of Service
EAP	Extensible Authentication Protocol
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HIDS	Host Intrusion Detection System
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU	International Telecommunication Union
MAC	Media Access Control
MitM	Man-in-the-Middle
NIDS	Network Intrusion Detection System
NGN	Next Generation Networks
OSS	Operator Shared Secret
P2P	Peer-to-Peer
PDA	Personal Digital Assistant
PKM	Privacy Key Management
PMP	Point-Multi-Point
POS	Personal Operating Space
QoS	Quality of Service
SLA	Service Level Agreement
SS	Suscriber Station
TEK	Traffic Encryption Key
UMTS	Universal Mobile Telecommunication System
WECA	Wireless Ethernet Compability Alliance
WIDS	Wireless Intrusion Detection System
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network

SUMÁRIO

1 **INTRODUÇÃO**

A introdução deste trabalho foi baseada no projeto para segurança em redes de computadores, denominado Prometheus, de autoria da professora Luci Pirmez, no qual propõe um serviço de segurança adaptativo.

O avanço tecnológico das redes sem fio, a recente proliferação de dispositivos portáteis (celulares, laptops, PDAs, etc.) aliados ao aumento de popularidade da computação móvel, levaram ao surgimento de aplicações e ambientes de computação ubíquos [Weiser, 1991]. A computação ubíqua é um paradigma de interação usuário-computador em que a tecnologia é integrada de forma transparente a ambientes físicos para auxiliar pessoas na realização de suas tarefas diárias de forma contínua e onipresente [Weiser, 1991]. Em tais ambientes vislumbra-se a integração das diversas tecnologias de redes sem fio tais como WLAN, Bluetooth, GSM, GPRS, UMTS, WIMAX, entre outras.

Dentre as tecnologias que integrarão a comunicação sem fio nos ambientes de computação ubíquos, o padrão IEEE 802.16 (WIMAX) está sendo visto como a mais promissora para possibilitar o acesso de banda larga de próxima geração. Além disso, o WIMAX é uma tecnologia adequada para ser usada como infra-estrutura de aplicações consideradas críticas, como as militares, e aquelas aplicações que em situações de catástrofes atendem os serviços relacionados ao centro nervoso de uma cidade (por exemplo, defesa civil, saúde e sistema financeiro) [Makarevitch B, 2006].

O padrão IEEE 802.16 ou WIMAX define a interface aérea e o protocolo MAC para redes metropolitanas sem fio, com o intuito de satisfazer as necessidades dos usuários que, cada vez mais, usam serviços multimídia (voz, dados e imagem) de alta qualidade, associados a um sistema de acesso com elevada disponibilidade.

Este padrão promete expandir o mercado de acesso à banda larga, através de uma redução significativa de investimentos de infra-estrutura necessários, de uma imediata facilitação da distribuição do acesso, e de um conseqüente barateamento do serviço para os usuários finais. Com a suplantação das restrições de expansão inerentes às tecnologias DSL e TV a cabo, pode-se vislumbrar o real aparecimento de uma alternativa capaz de promover a difusão do acesso Internet a comunidades distantes. Em outras palavras, o WIMAX está provocando mudanças profundas no mundo das telecomunicações. Além da concorrência com as operadoras fixas, outrora responsáveis pelo fornecimento de banda larga, e com as redes das empresas celulares, as quais provêem redes de terceira geração desenhadas e construídas a um altíssimo custo justamente para transmitir dados e oferecer acesso à internet, a tecnologia WIMAX também está causando uma ruptura importante nos modelos de negócio dessas operadoras de telefonia. Tais operadoras passam a não apenas prover conectividade para os usuários e empresas, mas também a disponibilizar novos serviços para os mesmos. Através do WIMAX, as empresas do futuro se tornam verdadeiramente colaborativas. Uma empresa é colaborativa quando a informação é compartilhada regularmente com os clientes (móveis ou não), e na qual os funcionários móveis ou remotos podem acessar a empresa e outros dados de missão crítica. Garantir segurança para as redes sem fio é essencial para que essas empresas alcancem os objetivos estratégicos do negócio.

Mediante esse fato, foi incorporada uma camada de segurança denominada Privacy Sublayer no próprio padrão do IEEE 802.16. No estabelecimento da troca de mensagens entre as estações pertencentes a uma rede aderente a tal padrão, esta camada provê os mecanismos de autenticação e criptografia das mesmas em nível de enlace. Apesar das melhorias introduzidas na mais nova versão desse padrão, o

802.16e (WIMAX móvel) [IEEE 802.16e, 2005], as redes metropolitanas, em especial as do tipo malha (mesh), não podem prescindir do emprego de sistemas de seguranças adicionais, pois algumas vulnerabilidades ainda persistem [Marks, 2005; Mandim, 2005]. Nessas redes (mesh), da forma similar ao que ocorre em ambientes P2P, não existe nenhuma estação central responsável pela autenticação das estações subscritoras. Portanto, as redes com topologia em malha precisam ter um sistema eficiente para auxiliar as estações subscritoras a localizar parceiros confiáveis, isto é, estações vizinhas que estão na sua área de cobertura e trocar informações de maneira segura no nível da aplicação. Uma possível solução para aumentar a confiabilidade nessas redes seria a utilização de modelos baseados em Sistemas de Reputação [LAGES, A., 2007] [Resnick, P., 2000; Song, S., 2005; Kamvar, S., 2003; Despotovic, Z. 2005].

Adicionalmente, os problemas de segurança passam a ter dimensões maiores quando são tratados concomitantemente com a mobilidade. A Mobilidade é um dos pilares fundamentais da computação ubíqua e, portanto, está presente no padrão [IEEE 802.16e, 2005]. A mobilidade, ao ser atendida, não deve comprometer a segurança e as necessidades de QoS exigidas pelos usuários e aplicações. No entanto, QoS, mobilidade e segurança devem ser agrupados e tratados de uma forma única, pois possuem uma relação de dependência mútua.

Nos ambientes de computação ubíquas, a integração de forma transparente das tecnologias de redes sem fio caracteriza as Redes de Próxima Geração (NGN - Next Generation Networks). Redes de Próxima Geração referem-se à nova infra-estrutura de suporte a serviços/aplicações convergentes (ou seja, dados, vídeo e voz). Em outras palavras, com a introdução das Redes de Próxima Geração, em vez de manter diversas redes sobrepostas, cada uma oferecendo um único serviço (voz,

dados ou telefonia móvel), a operadora de serviços de cada rede poderá ofertar múltiplos serviços em uma mesma infra-estrutura de comunicação, e de uma forma mais eficiente, quanto à utilização da banda, por exemplo.

Assim, as redes NGN tornam possível aos usuários móveis acessarem suas aplicações a partir das melhores redes sob os pontos de vista do usuário, da aplicação e da rede a qualquer momento e de qualquer lugar. Essas aplicações devem permanecer disponíveis para seus respectivos usuários móveis por longos períodos de tempo, mesmo quando estes se deslocam de uma rede para outra, ou seja, de um ambiente para outro.

2 **REFERENCIAL TEÓRICO**

2.1 SEGURANÇA EM SISTEMAS COMPUTACIONAIS

De uma maneira geral segurança é a condição de estar protegido ou livre de qualquer perigo ou perda. Na área de sistemas computacionais um computador é dito seguro se este atende a requisitos básicos relacionados aos recursos que o compõem: confidencialidade, integridade, disponibilidade, autenticidade e não repúdio [CERT, 2006].

A confidencialidade é a propriedade que limita o acesso à informação tão somente às entidades devidamente autorizadas pelo proprietário da informação.

A integridade é a propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (criação, manutenção e destruição). A integridade garante também que o sistema tem um desempenho correto.

A disponibilidade é propriedade que garante que a informação esteja sempre disponível para o uso legítimo por todos os autorizados sempre que necessário.

A autenticidade é a propriedade que certifica que um sistema se comporta como esperada por usuários autorizados.

Como garantia contra a negação de execução de alguma tarefa, a característica de não repúdio deve ser implementada de modo a permitir auditorias de acesso, sejam autorizados ou não, a uma informação ou sistema.

2.1.1 **Tipos de Ataques**

Ataque, no âmbito da computação, é uma tentativa de enganar, intencional, as medidas de segurança adotadas nos computadores, ou sistemas computacionais de alguma forma [CROTHERS, 2002]. Em outras palavras é qualquer ação que

comprometa a segurança da informação. Os ataques se classificam basicamente em quatro tipos: interrupção, interceptação, modificação e fabricação.

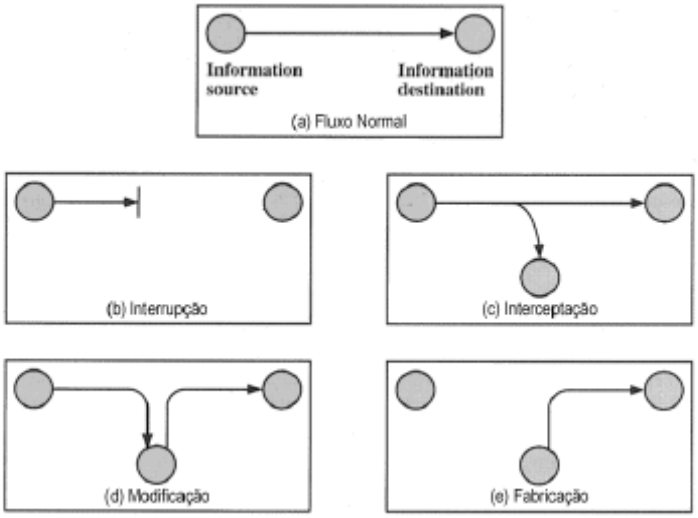


Figura 1 – Tipos de Ataques

2.1.1.1 Interrupção

Caracteriza-se por uma interrupção no fluxo normal da informação, desativando um ou mais serviços oferecidos. Os ataques desse tipo afetam diretamente a disponibilidade.

2.1.1.2 Interceptação

Neste tipo de ataque o objetivo é capturar tudo que está sendo transmitido sem que a origem ou o destino percebam. Neste tipo de ataque a confidencialidade das informações é a afetada.

2.1.1.3 Modificação

Ataques desse tipo alteram as informações que estão sendo transmitidas, ou seja, ataca-se a integridade das informações.

2.1.1.4 Fabricação

Ocorre quando um usuário ou sistema computacional não autorizado tem acesso ao sistema, utilizando uma identidade autorizada, introduz ou transmite informações falsificadas, atacando assim a autenticidade das informações.

2.1.2 **Técnicas Utilizadas em Ataques**

Existem diversas técnicas utilizadas para se obter um ataque bem sucedido contra um sistema. Essas técnicas normalmente tentam esconder a verdadeira identidade do atacante, assim como a ação executada pelo mesmo, fazendo com que, muitas vezes a vítima nem saiba que sofreu ou está sofrendo um ataque.

Veremos algumas dessas técnicas a seguir.

2.1.2.1 Spoofing

No contexto de redes de computadores, spoofing é uma técnica de subversão de sistemas que consiste em mascarar (spoof) quadros, pacotes ou informações de rede substituindo endereços verdadeiros por endereços falsificados. Em outras palavras, o atacante utiliza esta técnica para se passar por alguém que não é, falsificando seu endereço, obtendo assim acesso a informações que não deveria ter.

Dentre os principais métodos de spoofing destacam-se o MAC spoofing, o IP spoofing e o DNS spoofing.

2.1.2.2 MAC Spoofing

Nesse método o endereço físico da placa de rede é falsificado. É bastante simples falsificar este endereço, existem diversas ferramentas que ajudam a forjar este endereço, como por exemplo o SMAC (http://www.klcconsulting.net/smac/) que altera o MAC address em sistemas Windows.

É importante ressaltar que cada quadro transmitido em uma rede tem um endereço de origem contido, mas não existe nenhuma garantia de que a máquina que envia o quadro é realmente a que o coloca na rede. Dessa forma é possível realizar ataques de spoofing dos quadros da máquina de origem. [Roger, 2005]

2.1.2.3 IP Spoofing

Devido as características do protocolo IP, o reencaminhamento de pacotes é feito com base na premissa que o pacote tem que chegar ao endereço destino. Não existe verificação do endereço do remetente, e quando este é roteado, o pacote não tem qualquer ligação com outro pacote do mesmo remetente. Assim torna-se muito simples falsificar o endereço de origem. [Roger, 2005]

2.1.2.4 DNS Spoofing

O Domain Name System (DNS) é um protocolo da camada de aplicação usado para mapear endereços de domínios inteligíveis para as pessoas em endereços que o computador entenda (endereços IP). Para realizar tal tarefa, um cliente DNS envia uma solicitação de tradução a um servidor de DNS.

O objetivo do método de ataque de spoofing de DNS é substituir um servidor legítimo de DNS por um falso, que irá enviar resposta maliciosas as requisições dos clientes de DNS. [Roger, 2005]

2.1.2.5 Man-In-The-Middle

Um ataque do tipo man-in-the-middle (MitM) é um ataque no qual o atacante se insere no meio da comunicação entre as partes interessadas, fazendo parte deste canal de comunicação, tornando-se assim não só capaz de ler, como de inserir e alterar as mensagens trocadas entre as partes, sem que estas sequer tenham conhecimentos que sua comunicação está comprometida. [Valeri, 2002]

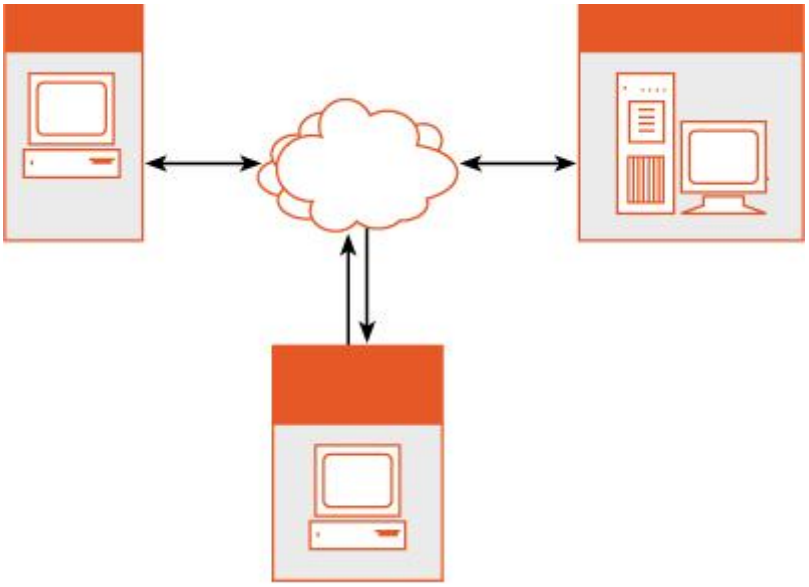


Figura 2 – Ataque Man-InThe-Middle

A presença do atacante é transparente para as vítimas e, desta forma, as estações pensam que estão se comunicando normalmente. O MitM pode ser usado contra diversos protocolos vulneráveis a esse tipo de ataque. Para cada protocolo existe uma técnica específica para a sua utilização (MitM-SSHv1, MitM-Ipsec, MitM-HTTPS, etc.).

2.2 REDES SEM FIO

As redes sem fio formam atualmente uma grande vertente tecnológica, justificada pela busca de praticidade e acessibilidade aos meios de comunicação. As tecnologias de redes sem fio incluem desde redes de dados e de voz globais, que permitem que os usuários estabeleçam conexões sem fio por longas distâncias, até tecnologias de freqüência de rádio e luz infravermelha que são otimizadas para conexões sem fio de curta distância.

A rápida proliferação dos dispositivos de computação móveis conduziu a uma mudança revolucionária na computação nos últimos tempos. Entre os dispositivos utilizados com freqüência nas redes sem fio estão computadores portáteis, computadores de mesa, computadores de bolso, assistentes digitais pessoais

(PDAs), telefones celulares, computadores com canetas e pagers. As tecnologias sem fio atendem a vários fins práticos. Por exemplo, os usuários de celulares podem usar seus aparelhos para acessar emails. Os viajantes com computadores portáteis podem se conectar à Internet através de estações de base instaladas em aeroportos, estações ferroviárias e outros locais públicos. Em casa, os usuários podem conectar dispositivos em seus computadores de mesa para sincronizar dados e transferir arquivos.

2.2.1 **Padrões de Redes Sem Fio**

No intuito de promover a ampla adoção de tecnologias de redes sem fio, além de reduzir custos e garantir a interoperabilidade, diversas organizações como o Institute of Electrical and Electronics Engineers (IEEE), a Internet Engineering Task Force (IETF), a Wireless Ethernet Compatibility Alliance (WECA) e a International Telecommunication Union (ITU) integram vários esforços de padronização.

Dentre os padrões podemos destacar os que dizem respeito a distancia através dos quais os dados podem ser transmitidos.

2.2.1.1 Redes Pessoais Sem Fio (WPAN)

As tecnologias WPAN [IEEE 802.15, 2005] permitem que os usuários estabeleçam comunicações ad hoc sem fio para dispositivos (como PDAs, telefones celulares ou laptops) que são utilizados em um espaço operacional pessoal (POS). Um POS é o espaço que cerca uma pessoa, até a distância de 10 metros. No momento, as duas principais tecnologias WPAN são a Bluetooth e a luz infravermelha.

Figura 3 – Wireless Personal Area Network

Para padronizar o desenvolvimento de tecnologias WPAN, o IEEE estabeleceu o grupo de trabalho 802.15 para WPANs.

2.2.1.2 Redes Locais Sem Fio (WLAN)

As tecnologias WLAN [IEEE 802.11, 2005] permitem que os usuários estabeleçam conexões sem fio em uma área local (por exemplo, em um prédio corporativo ou de um campus, ou em um espaço público, como um aeroporto). As WLANs podem ser usadas em escritórios temporários ou em outros espaços em que a instalação extensiva de cabos teria um custo muito elevado, ou para complementar uma LAN existente de modo que os usuários possam trabalhar em diferentes locais em um prédio, em diferentes horários. As WLANs podem funcionar de duas maneiras distintas. Em WLANs de infra-estrutura, estações sem fio (dispositivos com placas de rede de rádio ou modems externos) se conectam a pontos de acesso sem fio que funcionam como pontes entre as estações e o backbone de rede existente. Em WLANs ponto a ponto (ad hoc), vários usuários em uma área limitada, como uma sala de conferências, podem formar uma rede temporária sem usar pontos de acesso, se não precisarem de acesso a recursos de rede.

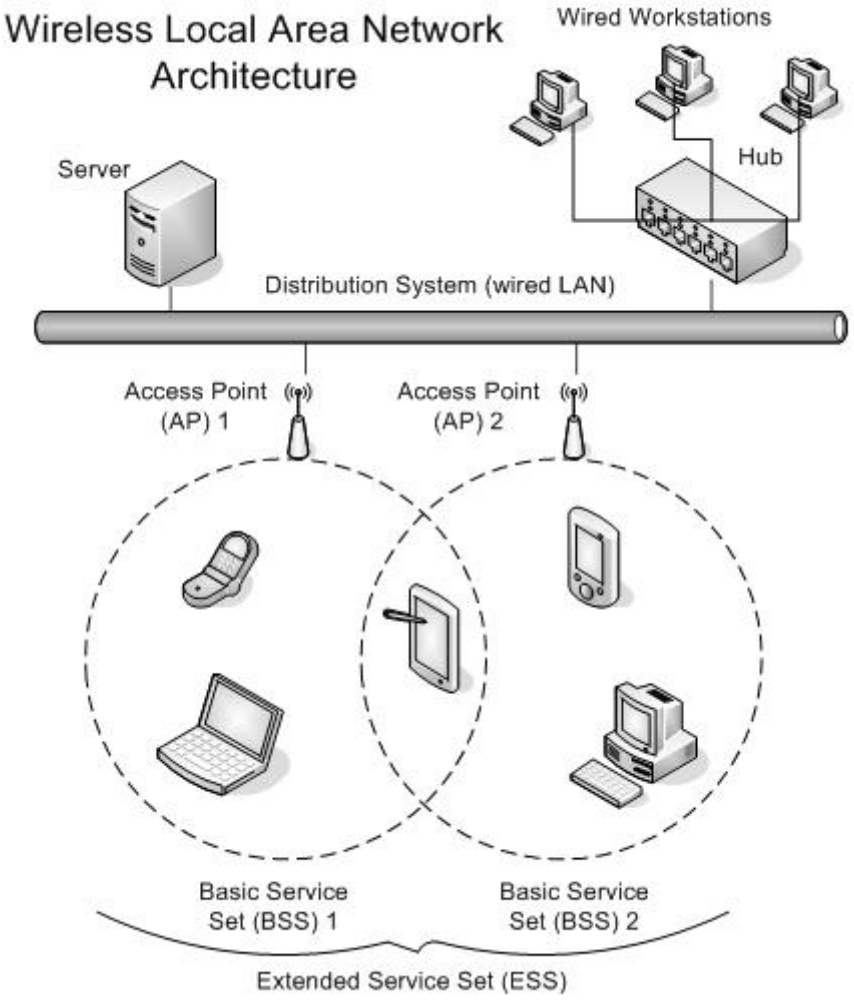


Figura 4 – Wireless Local Area Network

2.2.1.3 Redes Metropolitanas Sem Fio (WMAN)

As tecnologias WMAN [IEEE 802.16, 2005] permitem que os usuários estabeleçam conexões sem fio entre vários locais em uma área metropolitana (por exemplo, entre vários prédios de escritórios em uma cidade ou em um campus universitário), sem o custo elevado proveniente da instalação de cabos de cobre ou fibra e da concessão de linhas. Além disso, as WMANs podem funcionar como backups das redes que utilizam cabos, caso as principais linhas dedicadas dessas redes não estejam disponíveis.

Há uma demanda crescente por redes de acesso sem fio de banda larga que forneçam aos usuários acesso de alta velocidade à Internet.

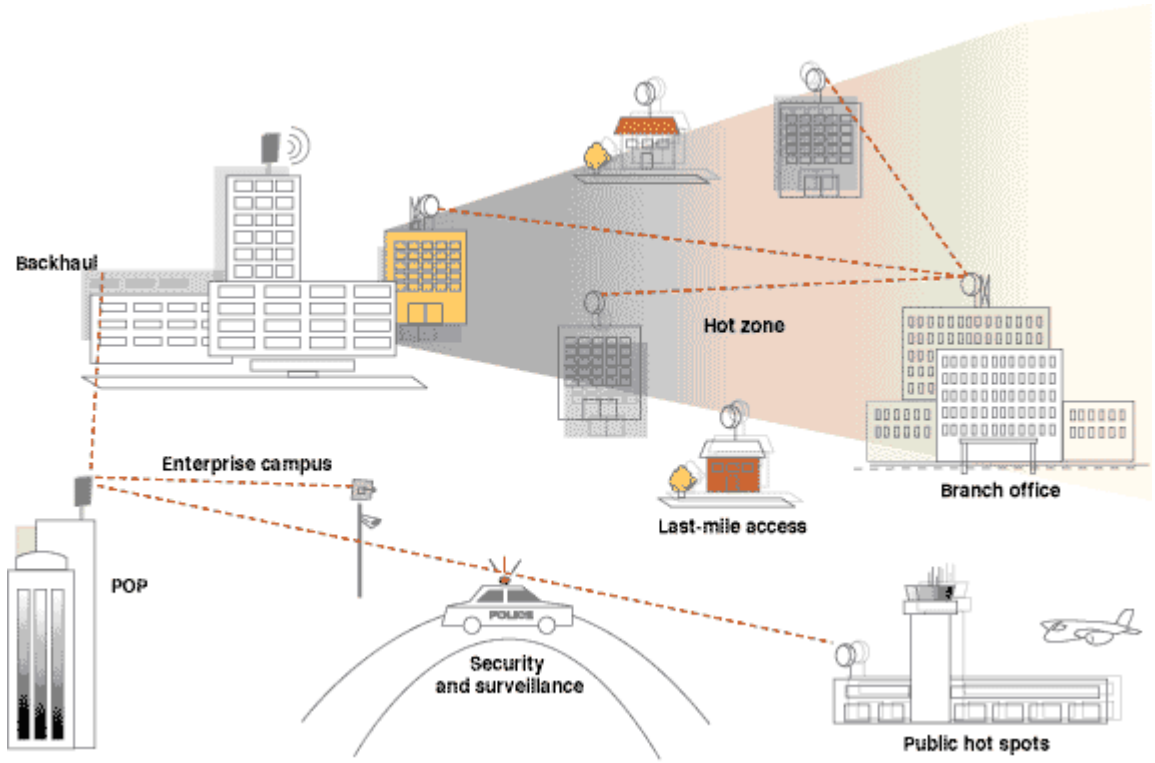


Figura 5 – Wireless Metropolitan Area Network

2.2.2 **Redes em Malha**

Quanto a redes sem fio do tipo mesh, o padrão IEEE 802.16 está sendo visto como uma tecnologia promissora para construir aplicações usando como infra-estrutura uma rede mesh, especialmente quando se tratam de aplicações consideradas críticas como as militares. Entretanto, um dos maiores obstáculos para essas aplicações é justamente as vulnerabilidades inerentes ao meio que são exploradas nas redes sem fio. Tais vulnerabilidades se tornam ainda maiores e mais complexas quando se adota como infra-estrutura de comunicação uma rede do tipo mesh (se comparada com uma topologia PMP).

Mediante desse fato, foi incorporado uma camada de segurança no próprio padrão do IEEE 802.16, no intuito de prover controle de acesso e confidencialidade do enlace de dados. Apesar das melhorias introduzidas na mais nova versão desse padrão, o padrão 802.16e, as redes metropolitanas, em especial as do tipo mesh, não podem prescindir do emprego de sistemas de seguranças adicionais, pois algumas vulnerabilidades ainda persistem.

As vulnerabilidades mais críticas que o padrão 802.16e está sujeito são: (i) a falta de mecanismos para garantir a integridade e não-repúdio no processo de autorização [Yun Zhou, 2006; Sen Xu (a), 2006]; (ii) a possibilidade de ataque do tipo DoS que visam reduzir a disponibilidade da rede uma vez que o processo de autenticação é iniciado pelos clientes móveis [Yun Zhou, 2006; Sen Xu (a) , 2006]; (iii) espaço de chaves utilizadas na geração das chaves AKs (Authentication Key) e TEKs (Traffic Encryption Key), é insuficiente para protegê-la contra ataques; (iv) a criptografia dos dados usada é DES em modo CBC, não sendo suficiente para prover a confidencialidade dos dados na comunicação entre SS e BS [Sen Xu (a) , 2006;]; (v) como a mobilidade é suportada no padrão 802.16e novos ataques podem ser explorados no processo de handover [Sen Xu (a) , 2006; Fuqiang Liu , 2006] uma vez que a fase de autenticação PKM é omitida, possibilitando que uma BS clone possa criar uma resposta para forjar a identidade de uma BS e se passar por ela; e (vi) utilização de métodos EAP inseguros na autenticação dos usuários.

Quanto ao padrão 802.16e mesh móvel, a vulnerabilidade mais crítica é a falta de autenticação mútua, já que mesmo o protocolo PKMv2 tendo sido incorporado ao padrão 802.16e ele só suporta operação em modo PMP [Suthida W., 2006]. Desta forma torna-se necessário o emprego do protocolo PKMv1 que não provê autenticação mútua e está sujeito a ataques conhecidos como Man-in-the-

Middle, replay attacks e Security Level Rollback [Yun Zhou, 2006; Sen Xu (a), 2006; Sen Xu (b), 2006; Fuqiang Liu, 2006]. Outra vulnerabilidade encontrada no 802.16e mesh é o fato do padrão não mencionar como distribuir a chave OSS (Operator Shared Secret) [Yun Zhou, 2006], chave esta que é única e compartilhada por todos os nós no estabelecimento de enlace entre um nó e seu vizinho e pode ser capturada e explorada por um atacante.

2.3 SISTEMAS DE DETECÇÃO DE INTRUSOS

Sistemas de Detecção de Intrusos são sistemas que ficam monitorando, em tempo real, um determinado ambiente para determinar se as ações executadas neste ambiente caracterizam um uso legítimo ou um ataque. [DEBAR, 1999]

Os IDS, além de muito úteis no monitoramento das atividades de uma rede, servem para analisar informações de auditoria de um sistema de forma automatizada, com maior precisão e rapidez.

Podemos classificar os IDS de acordo com vários conceitos. Dentre os mais utilizados estão o Método de Detecção e a Origem dos Dados.

Com relação aos Métodos de Detecção, estes descrevem as características da ferramenta com relação à forma de monitoramento, de acordo com a maneira de identificação do ataque, que pode ser por anomalia ou por padrão de ataque. No caso da identificação por anomalia, a ferramenta coleta informações iniciais do ambiente e determina um padrão de normalidade para este ambiente. Qualquer ação executada no ambiente diferente do padrão estabelecido é classificada com uma invasão ou possível ataque. Já na utilização de padrões de ataques pela ferramenta de IDS, esta utiliza uma base de informações com padrões de ataques (assinaturas de ataques), comparando cada atividade realizada no ambiente com esses padrões para determinar se esta atividade é ou não uma invasão.

Com relação a Origem dos Dados para classificação de IDS, estes dizem respeito a localização das informações que serão analisadas pela ferramenta. Estas informações podem estar, entre outros, nos nós que compões uma rede, ou nos dados que trafegam nesta rede, definindo assim a classificação como: HIDS (Host Intrusion Detection System), NIDS (Network Intrusion Detection System), e ainda WIDS (Wireless Intrusion Detection System).

3 **TRABALHOS RELACIONADOS**

In [Makarevitch, B, 2006] é apresentada uma arquitetura resistente a ataques do tipo jamming para aplicações militares em uma rede WIMAX do tipo mesh. Nessa proposta são usadas múltiplas estações bases, pontos de acessos para redes fixa, de forma a garantir a sobrevivência de uma rede (survivability) ambos em caso de destruição de BS ou em caso de ataques de jamming. Quando os nós são afetados por ataques de jamming, esses mesmos nós podem rerotear seus dados para outra estação base. A arquitetura de múltiplas BS requer um escalonamento distribuído já que não há nenhum ponto central nessa proposta que pode processar um escalonamento centralizado. Vários algoritmos de escalonamento distribuído foram avaliados, inclusive o que foi proposto nesse trabalho, em presença ou não de ataques de jamming.

Além disso, algumas técnicas previstas nesse padrão, baseadas em robustez criptográfica, são de difícil emprego em face da baixa capacidade computacional [HERNANDES, M., 2005] de alguns tipos de dispositivos móveis. Para aumentar a segurança são empregados sistemas como o IDSs (Sistema de Detecção de Intrusos) , sendo este o foco do presente trabalho.

Quanto a sistemas de reputação, essa frente está relacionada com os modelos baseados em Sistemas de Reputação [Resnick, P., 2000] que são bastante utilizados em redes Peer-to-Peer (P2P) e se baseiam em interações prévias ocorridas entre os peers. Na maior parte dos Sistemas de Reputação existentes na literatura [Song, S., 2005; Kamvar, S., 2003;, Despotovic, Z., 2005], o valor de reputação é atribuído ao próprio peer, e é usado para nortear suas interações com os outros peers.

Um exemplo de Sistema de Reputação é apresentado em [Singh, A , 2003] e utiliza uma arquitetura distribuída para armazenar valores sobre a reputação dos peers, com a característica de manter anônimos os peers responsáveis pelo armazenamento, dessa forma, impedindo ataques como a formação de conluios. Entretanto, para garantir o anonimato dos peers é utilizado um nó especial chamado bootstrap para a escolha dos peers que armazenarão a reputação de um novo peer que entra na rede. Quando um peer deseja conhecer a reputação de outro é utilizado o processo de inundação na rede, apresentando como desvantagem um grande consumo de banda.

Em [Kamvar, S., 2003] é apresentado o algoritmo EigenTrust que calcula a reputação de um peer utilizando o histórico de transações realizadas por ele. Para minimizar o tempo de busca dos valores de reputação dos peers é utilizado o protocolo Chord [Stoicay, I., 2003]. De posse das reputações é realizada uma média ponderada dos valores para o cálculo final da reputação.

O trabalho descrito em [Song, S., 2005] é o que apresenta maior semelhança com a proposta de [Lages, 2006(b)]. Em [Song, S., 2005] é proposto um algoritmo que utiliza Lógica Nebulosa para o cálculo da reputação global de um peer. Entretanto, tal trabalho não adota a abordagem orientada a serviços, sendo os valores de reputações atribuídos aos peers isoladamente. Além disso, no artigo não é tratado a possibilidade de um peer ter acesso a um serviço, mesmo tendo ele uma baixa reputação.

Em ambos os trabalhos [Song, S., 2005; Kamvar, S., 2003] não é tratada a possibilidade de formação de conluios dentro da rede P2P. Como estes trabalhos utilizam um algoritmo global de reputação, um grupo de peers pode ser formado com o intuito de aumentar ou diminuir o grau de reputação de um ou vários peers. Para

evitar que este problema afete as reputações armazenadas nos peers pertencentes à rede, no trabalho [Lages, 2006(b)] dois filtros serão utilizados no momento em que o peer recebe um valor de reputação para armazenar em sua tabela. A reputação de um peer será atualizada somente se o valor de reputação passar pelos dois filtros com sucesso.

Com o intuito de avaliar o problema da formação de conluios em redes P2P, em [Despotovic, Z., 2005] são comparados dois métodos para o cálculo da reputação: (i) utilização de todos os valores de reputação de um determinado peer, distribuídos em diversos peers, e (ii) utilização de métodos estatísticos em somente uma fração dos valores de reputação distribuídos pelos peers. O primeiro método retorna um valor de reputação mais preciso, entretanto ocasiona um grande número de mensagens geradas e também uma maior sobrecarga de processamento da reputação. A utilização do segundo método reduz o número de buscas necessárias para o cálculo da reputação, permitindo uma maior escalabilidade e o desenvolvimento de aplicações mais eficientes, mas gera perda de precisão no cálculo da reputação, por usar somente uma fração da rede de relacionamento. O trabalho de [Lages, 2006(b)] difere deste último pela adoção de um método mais simples de cálculo da reputação, através da utilização de Lógica Nebulosa, e pelo cálculo da reputação atribuído ao peer-serviço, e não ao peer isoladamente.

Em [Lages, 2006(a), Lages, 2006(b)] foi apresentada uma proposta para sistemas de reputação, que adota tal abordagem orientada a serviços. Os trabalhos descrevem a concepção inicial dessa nossa abordagem orientada a serviços para Sistemas de Reputação e um filtro para evitar ataques do tipo conluio. Adotou-se como cenário de aplicação do sistema proposto uma Rede Metropolitana Sem Fio.

Em [PIRMEZ, P, 2007, LAGES, A., 2007] foi apresentado o Sistema de Avaliação de SLAs (SAS), para o aumento da confiança no uso de transações de comércio eletrônico baseadas em Serviços Web. No SAS, valores objetivos de avaliação da QoS fornecida por um provedor de serviços são calculados e armazenados em uma entidade monitora de SLAs e são usados em conjunto com valores subjetivos fornecidos pelos clientes e validados pelo sistema. Ambos os valores são comparados de forma a: (i) detectar e tratar as discrepâncias entre valores subjetivos e objetivos; (ii) e estabelecer grupos de preferências em termos dos requisitos de QoS contemplados em um SLA que um cliente julgue mais importante ao avaliar um serviço; e (iii) calcular um valor de reputação final para o provedor.

Em [Vianna, N., 2006] foi apresentado uma extensão para arquiteturas de IDS em redes sem fio metropolitanas, que incorpora, através de uma máquina de inferência nebulosa, processos de detecção baseados em assinaturas de transmissão de rádio e uma análise cinemática da mobilidade dos dispositivos. A utilização destas abordagens possibilitou o aumento da taxa de detecção de invasores, incrementando assim os níveis dee segurança das redes sem fio metropolitanas.

A analise de resultados indica que a arquitetura proposta limita a área de abrangência do atacante, determinando que este esteja o mais próximo possível de seu alvo, para minimizar os ricos de ser detectado. Em se tratando de uma rede metropolitana, que chega a quilômetros, retira toda possibilidade do atacante melhor se posicionar.

4 **CONCLUSÃO**

Este trabalho apresentou um estudo sobre os diversos padrões de redes sem fio, as redes pessoais sem fio (WPAN), as redes locais sem fio (WLAN), e redes metropolitanas sem fio (WMAN).

Foi feito um estudo, também, sobre as redes sem fio em malha (Mesh), principalmente as metropolitanas, ressaltando sua extrema importância para situações de emergência, e para operações militares, onde não existe a possibilidade de se implantar uma infra-estrutura cabeada para suportar.

Também foram estudados neste trabalho questões referentes a segurança da informação, mostrando alguns tipos de ataques e suas técnicas.

Foram apresentados alguns trabalhos relacionados nas áreas de rede sem fio e sistemas que visam incrementar a segurança nessas redes, como os sistemas de reputação em redes P2P e os Sistemas de Detecção de Intrusos.

4.1 TRABALHOS FUTUROS

Como trabalho futuro fica a proposta de uma arquitetura para Sistemas de Detecção de Intrusos para redes sem fio que utilizam topologia em malha, e com seus nós sendo nós móveis, tentando assim aprimorar os trabalhos já realizados nesta área.

REFERÊNCIAS

[STALLINGS, 2002] STALLINGS, W., Network Security Essentials. 2002: Ed. Prentice Hall.

[CROTHERS, 2002] CROTHERS, T., Implementing Intrusion Detection Systems: A Hands-On Guide for Securing the Network. 2002: Ed. Wiley.

[Berners-Lee, 2001] Berners-Lee, T., Hendler, J. and Lassila, O., The Semantic Web. Scientific American, 284(5):35{43, 2001.

[Fuqiang Liu , 2006] Fuqiang Liu e Lei Lu, “Security Issues in Privacy and Key Management Protocols of IEEE 802.16”, ACM SE’06, March 10-12, 2006, Melbourne, Florida, USA, 2006.

[IEEE 802.16e, 2005] Institute of Electrical and Electronics Engineers, IEEE Draft 802.16e – Air Interface for Fixed and Mobile Broadband Wireless Access Systems. 2005.

[LAGES, A., 2007] Lages, A., DELICATO, Flávia Coimbra PIRES, Paulo Figueiredo ; PIRMEZ, Luci.(2007) SATYA: A Reputation-based Approach for Service Discovery and Selection in Service Oriented Architectures.. In: 9th ACM International Workshop on Web Information and Data Management, Proce, 2007, Lisboa. Proceedings of 9th ACM International Workshop on Web Information and Data Management, 2007.

[Makarevitch, B , 2006] Makarevitch, B.,”Jamming Resistant Architecture for WiMAX Mesh Network” Military Communications Conference, 2006. MILCOM 2006, 23-25 Oct. 2006.

[Mandim, 2005] MANDIN, J.e.a., IEEE 802.16e Security Review. Disponível em http://www.drizzle.com/~aboba/EAP/802.16eNotes.pdf. Acessado em fevereiro de 2005.

[CERT, 2006] CERT.Br, Cartilha de Segurança para Internet versão 3.1. Disponível em http://cartilha.cert.br/. Acessado em novembro de 2007.

[Roger, 2005] Roger, D., SecForum, Técnicas de Ataque em Redes Wireless, 2005.

[Valeri, 2002] VALERI, Marco, ORNAGHI, Alberto, “Man-in-the-middle” , Technical White Paper, Italian Black Hats Association. Setembro 2002.

[Marks, 2005] MARKS, R.B., Security review of IEEE 802.16e D8. Disponível em http://www.drizzle.com/~aboba/EAP/review.txt]. Acessado em fevereiro de 2005.

[Sen Xu (a), 2006] Sen Xu, Manton Matthews, Chin-Tser Huang, “ A WPKI-based Security Mechanism for IEEE 802.16e” , IEEE Communications Society, Wuhan University, China, 2006.

[Sen Xu (b), 2006] Sen Xu, Chin-Tser Huang, “Attacks on PKM Protocols of IEEE 802.16 and Its Later Versions”, Computer Science and Engineering Department University of South Carolina Columbia SC 29208, USA, 2006.

[Suthida W. , 2006] Suthida Wattanachai , “Security Architecture of the IEEE 802.16 Standard for Mesh Networks”, thesis of the Department of Computer and Systems Sciences, Stockholm University / Royal Institute of Technology, 2006.

[Weiser, 1991] Weiser, M.: The Computer for the Twenty-First Century. Scientific American, pp. 94-10, September, 1991.

[Yun Zhou, 2006] Yun Zhou , Yuguang Fang, “Security of IEEE 802.16 in Mesh Mode”, IEEE Communications Society, 2006.

[DEBAR, 1999] DEBAR, H., Marc Dacier e Andreas Wespi. Towards a taxonomy of intrusion-detection systems. Computer Networks, 1999(31): p. 805-822.

[Vianna, 2006] VIANNA, Nilson Rocha, Reinaldo de B. Correia, Luci Pirmez, EWIDS: Uma Extensão para Arquiteturas de Sistemas de Detecção de Intrusos para Redes Sem Fio Metropolitanas, Simpósio Brasileiro de Redes de Computadores (SBRC), Curitiba, 2006.

[IEEE 802.16, 2005] Padrão, Institute of Electrical and Electronics Engineers, IEEE Standard 802.16 – Air Interface for Fixed Broadband Wireless Access Systems. 2001.

[IEEE 802.11, 2005] Padrão, Institute of Electrical and Electronics Engineers, IEEE 802.11 - Wireless Local Area Networks. 1999.

[IEEE 802.15, 2005] Padrão, Institute of Electrical and Electronics Engineers, IEEE 802.15 – Wireless Personal Area Networks. 2002.