Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Marcos Floresta Dias Filho

REDES 802.16:

Considerações sobre a segurança no modo mesh

Rio de Janeiro

2007

Marcos Floresta Dias Filho

REDES 802.16:

Considerações sobre a segurança no modo mesh

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.

Orientadora:

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

Rio de Janeiro

2007

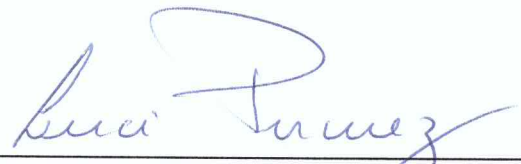
Marcos Floresta Dias Filho

REDES 802.16:

Considerações sobre a segurança no modo mesh

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 dezembro de 2007.



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

AGRADECIMENTOS

Gostaria de agradecer à Professora Luci Pirmez, profissional de grande capacidade e principal responsável por meu sucesso na realização deste trabalho e na conquista da primeira colocação no curso MOT-CN. Não fosse pelo susto que ela me deu com o dificílimo primeiro trabalho em grupo que propôs logo nas primeiras aulas do curso, minha dedicação aos estudos não teria sido tão grande. À professora Luci também agradeço o convite para realização do Mestrado sob sua orientação, sonho que sempre tive e ainda hei de realizar. Meus agradecimentos também ao professor Moacyr, pela maestria na coordenação do curso e pela amizade e especial atenção a mim dedicada desde o início de minha jornada no MOT-CN. Finalmente, agradeço a paciência de todos os meus colegas de sala de aula que, com grande paciência em responder minhas perguntas mais absurdas, ajudaram a transformar esse marinheiro em um respeitável profissional da área de redes.

RESUMO

DIAS FILHO, Marcos Floresta. **REDES 802.16: uma análise da segurança em modo mesh**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2007.

O padrão IEEE 802.16 começa a ser empregado em larga escala em todo o mundo. Dentre seus modos de operação, o modo mesh aparece como um dos mais promissores em termos de custo e rapidez de implementação. No entanto, por tratar-se de uma tecnologia sem fio e, consequentemente, sem fronteiras físicas, o padrão IEEE 802.16 está sujeito a muito mais vulnerabilidades que uma rede cabeada. Este trabalho explica o funcionamento do modo mesh das redes 802.16 e sua subcamada de segurança e descreve os possíveis ataques a que este modo de operação pode estar sujeito.

ABSTRACT

DIAS FILHO, Marcos Floresta. **REDES 802.16: uma análise da segurança em modo mesh**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2007.

The standard IEEE 802.16 is now starting to be deployed in large scale all over the world. Within its operational modes, the mesh shows up as one of the most promising in terms of deployment costs and deployment speed. However, as it is a wireless technology, and, consequently, does not have physical boundaries, the standard IEEE 802.16 faces much more vulnerabilities than a wired network does. This paper explains how the mesh mode and the security sublayer of 802.16 networks work and describes the possible attacks on this operational mode.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AES	Advanced Encryption Standard
ARQ	Automatic Repeat Request
ANATEL	Agência Nacional de Telecomunicações
AAA	Authentication, Authorization and Accounting
AK	Authorization Key
BS	Base Station
BRAN	Broadband Radio Access Network
BWA	Broadband Wireless Access
CMAC	Cipher-based Message Authentication Code
CPS	Common Part Sublayer
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
DSL	Digital Subscriber Line
DHCP	Dynamic Host Configuration Protocol
EP	Encapsulation Protocol
ETSI	European Telecommunication Standard Institute
EAP	Extensible Authentication Protocol
HMAC	Hashed Message Authentication Code
HIPERMAN	High Performance Radio Metropolitan Area Network
IEEE	Institute of Electric and Electronics Engineer
IP	Internet Protocol
LSB	Less Significant Bit
LOS	Line-of-Sight
MAC-SS	Mac Security Sublayer
MIB	Management Information Base
MSK	Master Session Key
MAC	Medium Access Control
MSB	Most Significant Bit
NLE	Neighbor Link Establishment
NCS	Network Control Subframe
NLOS	Non-Line-of-Sight
OSS	Operator Shared Secret
OFDM	Orthogonal Frequency Division Multiplexing
PMK	Pairwise Master Key
PHY	Physical Layer
PKM	Pont-Multiponto
PMP	Pont-Multiponto
PDU	Protocol Data Unit
RFC	Request for Comments
RSA	Rivest, Shamir e Adleman
SCS	Schedule Control Subframe
SHA	Secure Hash Algorithm
SA	Security Association
SAID	Security Association Identifier
SSCS	Service Specific Convergence Sublayer

SS	Subscriber Station
TTA	Telecommunications Technology Association
TDM	Time Division Multiplexing
TEK	Traffic Encryption Key
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
WIBRO	Wireless Broadband
WMAN	Wireless Metropolitan Area Network
WIMAX	Worldwide Interoperability for Microwave Access

SUMÁRIO

1 **INTRODUÇÃO**

Nesta seção serão apresentados os fatores que motivaram a escrita desta monografia e os objetivos que se pretendem alcançar com ela. Além disso, a metodologia de pesquisa empregada será brevemente descrita e a relevância do tema será mostrada por meio de um pequeno resumo dos panoramas mundial e nacional do emprego da tecnologia 802.16.

1.1 MOTIVAÇÃO

O uso da Internet para oferecer serviços multimídia em tempo real e a custos vantajosos tem crescido rapidamente. Com isso, a demanda de acesso em banda larga na chamada última milha (*last mile*) por parte de usuários domésticos e de pequenos e médios empresários tem sido cada vez maior. Nesse cenário, as operadoras de telefonia e de televisão a cabo são praticamente as únicas fornecedoras desse acesso em banda larga. Isso ocorre por serem essas operadoras as detentoras do parque de cabeamento atualmente instalado. Desse modo, tecnologias como linha digital do assinante (*digital subscriber line* - DSL) e modem a cabo (*cable modem*) são as únicas opções disponíveis. Somente o emprego de novas tecnologias pode vir a quebrar o monopólio do fornecimento de acesso em banda larga na última milha.

As tecnologias de acesso sem fio em banda larga (*broadband wireless access* - BWA) surgem como uma opção para atender a necessidade crescente de largura de banda. Essas tecnologias trazem como grande vantagem a eliminação do uso de cabos e a redução dos custos de infra-estrutura decorrentes dessa eliminação. Permite-se, assim, que outras empresas além das empresas de telecomunicações e de televisão a cabo venham a fornecer o acesso em banda larga na última milha. Uma das tecnologias de acesso sem fio em banda larga é o padrão IEEE 802.16, aberto e de domínio público.

O padrão IEEE 802.16 teve sua primeira versão publicada em 2001. Essa versão não incluía a especificação de redes mesh. A publicação do padrão IEEE 802.16a (2003) veio definir os fluxos de sinalização e os formatos de mensagem que permitem a formação de uma rede mesh. O padrão IEEE 802.16 – 2004, que

engobla os padrões anteriores, mantém e amplia a especificação das redes mesh. A preocupação com a especificação de um modo de operação mesh para o padrão IEEE 802.16 decorre do fato que, em algumas situações, o modo mesh pode ser empregado com vantagens em relação ao modo ponto-multiponto (*point-to-multipoint* - PMP). Bruno [2005] enumera diversas áreas onde as redes mesh podem ser aplicadas de maneira vantajosa. Dentre essas áreas, destacam-se os sistemas de transporte público inteligentes, a segurança pública e o acesso público à Internet. Segundo Wei [2005], quando uma rede 802.16 é usada para prover acesso à Internet, as vantagens do uso do modo mesh são: aumento da área de cobertura da estação base, menor custo de ativação e maior rapidez na montagem e reconfiguração da rede.

Assim, em um futuro muito próximo, ver-se-á um grande número de pessoas utilizando a tecnologia IEEE 802.16 para fazer transações *on-line* que dependerão fortemente de um bom esquema de segurança. O uso de bancos por computador, a aplicação em ações por meio de *homebroker* virtual e as compras em sites especializados, por exemplo, constituem um grande desafio para a segurança do padrão IEEE 802.16, especialmente no modo de operação mesh.

1.2 OBJETIVOS

O objetivo desta monografia é apresentar os conceitos básicos de funcionamento, os mecanismos de segurança e as vulnerabilidades do modo de operação mesh das redes IEEE 802.16. Neste trabalho, busca-se responder a seguinte questão: Quais são os principais ataques a que podem ser submetidas as redes 802.16 mesh?

As principais contribuições dessa monografia são: (i) o referencial teórico sobre o funcionamento das redes 802.16 mesh; (ii) a descrição dos mecanismos de segurança e das vulnerabilidades conhecidas das redes 802.16 mesh.

Por versar sobre um tema ainda muito recente, a respeito do qual muito pouco foi escrito, o presente trabalho pretende ser bastante útil ao oferecer material para reflexão e amadurecimento da tecnologia 802.16.

1.3 METODOLOGIA DE PESQUISA

Esta monografia expõe o pensamento de diversos autores sobre os mecanismos de segurança e as vulnerabilidades das redes 802.16 mesh. Assim, segundo Eco [1996 *apud* NUNES, 2000], esta monografia classifica-se como uma Monografia de Compilação.

O trabalho foi iniciado com um levantamento bibliográfico das obras que abordam o funcionamento das redes 802.16 do tipo mesh, incluindo os padrões IEEE 802.16 – 2004 e IEEE 802.16e. A partir desse levantamento, foi possível confeccionar o referencial teórico. Em seguida, foi feita uma ampla pesquisa nas revistas e periódicos do IEEE de modo a reunir os artigos mais recentes disponíveis sobre o tema versado. Esses artigos foram resumidos e as contribuições de seus autores condensadas a fim de apresentar o panorama mais atualizado possível sobre as vulnerabilidades conhecidas das redes 802.16 mesh.

1.4 RELEVÂNCIA

De acordo com o Jornal Folha de São Paulo, a operadora de celular norte-americana Sprint Nextel está planejando lançar redes WiMax (leia-se IEEE 802.16) em várias cidades dos Estados Unidos em 2008. O lançamento comercial do serviço será em Washington (abril de 2008), mas Baltimore, Boston e Nova York também terão redes instaladas pela operadora; levando o WiMax a 100 milhões de norte-americanos até o final de 2008. Para isso, a Sprint Nextel pretende investir cerca de 5 bilhões de dólares em WiMax até 2010. A operadora prevê que a venda do serviço gere entre 2 e 2,5 bilhões de dólares em receitas ao longo dos próximos 3 anos. Percebe-se, claramente, que a tecnologia IEEE 802.16 deixou de ser apenas assunto de pesquisa acadêmica com possíveis possibilidades de ganhos comerciais futuros e passou a ter relevância também no mundo dos negócios.

O panorama brasileiro é um pouco mais complicado, mas igualmente promissor. Como o IEEE 802.16 opera em faixas de freqüência licenciadas é necessário que as empresas interessadas em fornecer o serviço adquiram o direito de fazê-lo em um leilão da ANATEL. O primeiro leilão de licenças para as freqüências de 3,5 GHz e 10,5 GHz foi realizado em fevereiro de 2003 e não despertou muito interesse devido

ao pouco amadurecimento da tecnologia IEEE 802.16 até aquela data. Mesmo assim, de acordo com a revista PC World as seguintes empresas adquiriram licenças para as freqüências em tela: Telmex, Neovia, Brasil Telecom, WKVE e Grupo Editorial Sinos. Até agora, a Neovia foi a única empresa a anunciar investimento em WiMax. Ela atende 35 mil usuários com 5 mil pontos de presença em 52 municípios paulistas.

Desde meados de 2006, a ANATEL tenta realizar um novo leilão de freqüências, a fim de permitir a entrada de novas empresas no mercado. Contudo, ações judiciais das concessionárias de telefonia têm impedido que o leilão aconteça. O interesse das operadoras de telefonia em obstar o leilão e, com isso, impedir a entrada de concorrentes no mercado, é mais um exemplo da importância da tecnologia IEEE 802.16 para o mercado nacional.

Conforme mencionado, o Brasil ainda não é um exemplo a ser seguido no setor comercial. No entanto, destaca-se em outro aspecto relevante do uso tecnologia IEEE 802.16: a inclusão digital. O projeto realizado pela Intel em Parintins, cidade localizada numa ilha no rio Amazonas, é modelo para o mundo no que se refere a inclusão digital. Desde setembro de 2006, os 114 mil moradores dessa comunidade isolada e carente já possuem acesso sem fio e em banda larga à Internet em um centro de saúde, duas escolas públicas e um centro comunitário. Isso permite, inclusive, o uso de telemedicina, colocando os profissionais de saúde de Parintins em contato com os médicos da Universidade da Amazônia, em Manaus. Logo, vê-se que o WiMax é uma solução vantajosa para o desenvolvimento de projetos de inclusão digital, pois sua implementação é mais rápida e tem custo menor em comparação a outras tecnologias. De acordo com Cherry [2003] “uma área de serviço de 200 quilômetros quadrados custa a um provedor DSL mais de 11 milhões de dólares. A mesma área pode ser servida com tecnologia sem fio por cerca de 450 mil dólares.”.

1.5 ORGANIZAÇÃO DO TRABALHO

Esta monografia está organizada em 5 capítulos. O capítulo 1, apresenta a motivação para o uso das redes IEEE 802.16, os objetivos desta monografia, a relevância do tema abordado e a metodologia de pesquisa empregada. O capítulo 2 descreve o processo de padronização do acesso sem fio em banda larga (BWA) e

cita os padrões publicados por alguns órgãos de padronização. O capítulo 3 explica o funcionamento básico do modo de operação mesh do padrão IEEE 802.16 com ênfase no processo de entrada na rede. O capítulo 4 descreve os aspectos fundamentais da subcamada de segurança do padrão IEEE 802.16. O capítulo 5 apresenta as deficiências de segurança das redes 802.16 mesh conhecidas. Em cada sessão desse capítulo, são descritas as vulnerabilidades encontradas nos artigos estudados e as soluções e trabalhos futuros propostos pelos autores dos artigos.

2 **O ACESSO SEM FIO EM BANDA LARGA**

Vários foram os padrões desenvolvidos para proporcionar o acesso sem fio em banda larga (BWA). Nesta seção, os principais padrões mundiais de BWA serão abordados. No entanto, será dada ênfase ao padrão IEEE 802.16, por ser o mais abrangente. Dele, serão mostradas a regulamentação no Brasil e evolução tecnológica.

2.1 OS PADRÕES DE ACESSO SEM FIO EM BANDA LARGA

A primeira organização a iniciar os estudos para padronização do acesso sem fio em banda larga (BWA) foi o Instituto Europeu de Normas de Telecomunicações (ETSI - *European Telecommunications Standard Institute*), em 1997, com o grupo de estudo denominado Redes de Acesso via Rádio em Banda Larga (BRAN - *Broadband Radio Access Networks*). Em 1999, o IEEE criou o grupo de estudo IEEE 802.16 com a mesma finalidade. Ainda em 1999, as duas instituições (IEEE e ETSI) estabeleceram um acordo de cooperação com o intuito de compatibilizar seus padrões. Em 2004, a Associação de Tecnologia de Telecomunicações (TTA - *Telecommunications Technology Association*) iniciou seu grupo de estudo para padronização do BWA em seu país de atuação, a Coréia.

O padrão mais importante publicado pelo ETSI-BRAN foi chamado de Rede de Área Metropolitana de Alta Performance via Rádio (HiperMAN - *High Performance Radio Metropolitan Area Network*) e pode ser considerado um subconjunto do padrão IEEE 802.16a – 2003, baseado em OFDM. O trabalho mais significativo da TTA denomina-se Banda Larga sem Fio (WiBro - *Wireless Brodband*) e também pode ser considerado um subconjunto de padrões do IEEE (IEEE 802.16.2004 e IEEE 802.16e). Logo, pode-se observar que o padrão IEEE 802.16 engloba os padrões ETSI - HiperMAN e TTA – WiBro. Por isso, esta monografia vai se concentrar no padrão IEEE 802.16.

WiMax é um termo criado pelo mercado, comumente considerado sinônimo de IEEE 802.16. O termo WiMax refere-se a um padrão de referência adotado para certificar equipamentos considerados conformes com o padrão IEEE 802.16. O *WiMax Forum*, entidade sem fins lucrativos responsável pela certificação, seleciona um conjunto de características técnicas previstas pelo padrão IEEE 802.16 e confere

o título de certificação aos equipamentos que, submetidos a testes específicos, comprovam atender a todo esse conjunto de características. Desse modo, o *WiMax Forum* busca garantir a interoperabilidade entre os dispositivos IEEE 802.16 produzidos pelos diversos fabricantes existentes. Neste trabalho, os termos WiMax e IEEE 802.16 serão usados indistintamente.

2.2 REGULAMENTAÇÃO NO BRASIL

No Brasil, o órgão responsável por regular e fiscalizar as telecomunicações é a Agência Nacional de Telecomunicações (ANATEL). Assim, o uso de quaisquer freqüências do espectro rádio deve ser aprovado por essa autarquia federal. Para o fornecimento de acesso sem fio em banda larga no Brasil, foram alocadas 4 faixas de freqüência. O quadro 1 apresenta as faixas de freqüência regulamentadas pela ANATEL.

Quadro 1 – Freqüências disponíveis para BWA no Brasil

Faixa (GHz)	Regulamentação	Freqüências (MHz)	Comentário
2,6	Resolução 429	2500-2530 2570-2620 2620-2650	-
3,5	Resolução 416	3400-3600	-
5	Resolução 365	5150-5350 5470-5725	Não precisa de licença
10,5	Resolução 307	10150-10300 10500-10650	-

2.3 A EVOLUÇÃO DO PADRÃO IEEE 802.16

A primeira versão, 802.16 - 2001, especificou uma rede ponto-multiponto (PMP), que operava necessariamente com visada direta (line-of-sight - LOS) e empregava multiplexação por OFDM no espectro de 10 a 66 GHz. Chegava a uma taxa teórica máxima de 134 Mbps e permitia apenas nós fixos.

Por causa dos já conhecidos benefícios dos usos de redes mesh, o padrão 802.16a - 2003 introduziu os principais procedimentos para a operação nesse modo. Além disso, as redes passavam a poder operar sem visada direta (non-line-of-sight -

NLOS) em freqüências de 2 a 11 GHz. A taxa máxima teórica chegava aos 75 Mbps e a distância máxima a 50 Km. Ainda não era prevista a operação de terminais móveis no padrão.

Em 2004, a versão 802.16d foi publicada, contendo alguns avanços na camada MAC. Essa versão engloba e substitui todas as anteriores, inclusive a 802.16c. Essa última foi publicada em 2002 e estabelecia os perfis de uso para as freqüências de 10 a 66 GHz.

Em dezembro de 2005, a última versão, IEEE 802.16e, foi aprovada. Essa versão introduziu a tão esperada mobilidade de terminais e aperfeiçoou o modo de operação mesh. A taxa máxima teórica pode chegar a 15 Mbps por cada canal de 5 MHz de largura de banda. O quadro 2 resume a evolução do padrão 802.16.

Quadro 2 – Evolução histórica do padrão 802.16

Versão	Ano	Descrição
802.16	2001	MAC e PHY para acesso fixo sem fio em banda larga para freqüências de 10-66 GHz
802.16a	2003	Acréscimo de nova PHY para freqüências de 2-11 GHz. Inclui a operação em modo mesh
802.16c	2002	Perfis de sistema para operação na faixa de freqüências de 10-66 GHz
802.16d	2004	Engloba versões 802.16 e 802.16a. Aperfeiçoamento da camada MAC. Padrão referência.
802.16e	2005	Correções de segurança e acréscimo de suporte a mobilidade
802.16f	2005	Management Information Base (MIB) para 802.16
802.16g	2007	Gerenciamento da rede e de serviços
802.16h	Em andamento	Coexistência de padrões em freqüências não licenciadas
802.16i	Em andamento	MIB para terminais móveis
802.16j	Em andamento	Especificações Multihop e aperfeiçoamentos na camada MAC e no uso de OFDM
802.16k	2007	Adaptação de pontes transparentes (*transparent bridging*) ao padrão 802.16

2.4 CONSIDERAÇÕES FINAIS DO CAPÍTULO

Neste capítulo foram descritos, de forma resumida, os principais padrões de acesso sem fio em banda larga e a regulamentação brasileira de freqüências para uso com esses padrões. Em seguida, foi abordada a evolução histórica do padrão mais significativo de acesso sem fio em banda larga, o IEEE 802.16. O capítulo 3 apresenta uma visão geral do modo mesh de operação desse padrão.

3 **O MODO MESH NO PADRÃO IEEE 802.16**

O padrão IEEE 802.16 define dois tipos de topologias ou modos: ponto-multiponto (PMP) e mesh.

No modo PMP, todo o tráfego entre estações assinantes (*subscriber station* – SS) necessariamente é coordenado pela estação base (*base station* – BS). Essa arquitetura é bastante similar a das redes de telefonia celular.

No modo mesh, cada SS pode se comunicar diretamente com as SS vizinhas sem qualquer coordenação com a BS. Por isso, não existe a necessidade da existência de um enlace (*link*) físico direto entre SS e BS. Essa é a principal diferença entre os modos PMP e mesh. A conexão lógica entre uma SS e a BS pode ser feita através de uma SS vizinha.

Em uma rede IEEE 802.16 mesh, por definição, o nó que tem conexão direta para interligar serviços para fora da rede mesh (conexão com o *backhaul*) é uma estação base. Qualquer outro nó da rede é uma SS. Os nós com os quais uma estação possui conexão direta são chamados vizinhos (*neighbors*). O conjunto de todos os vizinhos de um nó é chamado de vizinhança (*neighborhood*) desse nó. A vizinhança estendida (*extended neighborhood*) inclui, adicionalmente, os nós vizinhos à vizinhança. Ou seja, os nós pertencentes à vizinhança estendida de uma estação estão a 2 saltos (*hops*) dessa estação. Por isso, a vizinhança estendida também é chamada de vizinhança a dois saltos (*two- hop neighborhood*). A figura 1 ilustra os modos de operação PMP e mesh.

O modo mesh é considerado opcional pelo padrão IEEE 802.16. Isso significa que um equipamento que opera no modo ponto-multiponto não precisa, necessariamente, implementar os padrões de operação do modo mesh. Contudo, o padrão exige que um equipamento que opere em modo mesh suporte o padrão de operação ponto-multiponto.

A topologia mesh ainda não faz parte dos perfis de certificação *WiMax*. Mesmo assim, alguns fabricantes planejam incluir a funcionalidade mesh em seus produtos antes mesmo que o *WiMax Forum* estabeleça os requisitos necessários à certificação.

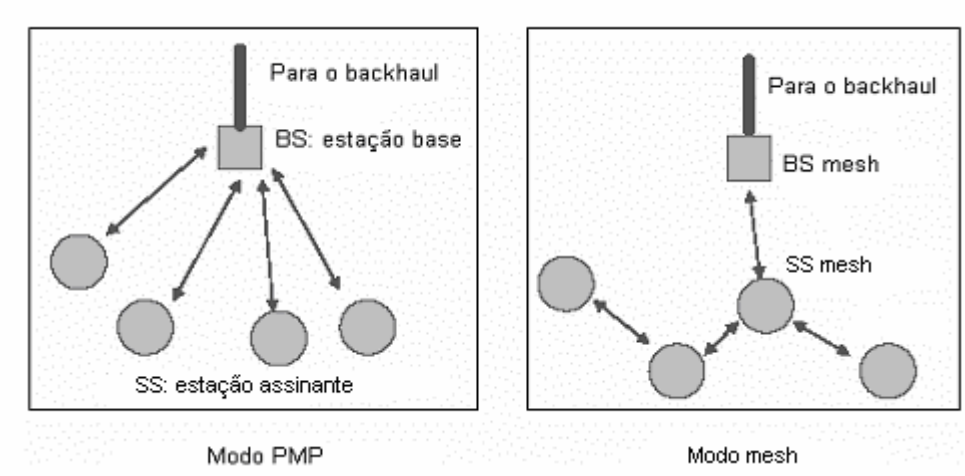


Figura 1 – Modos de operação das redes 802.16

3.1 VISÃO GERAL DA CAMADA FÍSICA

O padrão IEEE 802.16 define três especificações diferentes para a camada física do modo ponto-multiponto. A especificação mais eficiente em situações NLOS e menos exigente no que tange a sincronização, é a WMAN-OFDM. Por isso, essa especificação foi a adotada pelo *WiMax Forum* para certificação de dispositivos que operam no modo ponto-multiponto.

A WMAN-OFDM também é definida pelo padrão IEEE 802.16 para uso no modo mesh. Essa especificação prevê o uso de multiplexação por divisão no tempo (*time division multiplexing* - TDM). Nesse tipo de multiplexação, o tempo é dividido em *slots* de igual duração e, em cada *slot*, um bloco de bytes é transmitido. Para implementar o TDM, é utilizada uma técnica de modulação conhecida como OFDM (*orthogonal frequency division multiplexing*), com 256 subportadoras (freqüências moduladas). Na modulação OFDM, os blocos de bits são agrupados em símbolos de igual duração e cada símbolo é modulado em uma das 256 subportadoras. Foge ao escopo deste trabalho uma descrição pormenorizada da camada física do padrão IEEE 802.16.

3.2 VISÃO GERAL DA CAMADA MAC

A camada MAC é composta de três subcamadas: subcamada SSCS (*service specific convergence sublayer*), subcamada CPS (*common part sublayer*) e subcamada de segurança (*security sublayer*).

A subcamada SSCS faz a interface com as camadas superiores e a função de mapeamento dos diversos tráfegos possíveis para a camada MAC.

A subcamada CPS é responsável pelas principais funções da camada MAC, incluindo: controle de acesso, tratamento de colisões, agendamento do tráfego de controle e de dados e requisição e alocação de largura de banda. Todas as comunicações ocorrem no contexto de um enlace que é estabelecido entre dois nós. Cada nó tem um endereço MAC de 48 bits. Esse endereço é usado no processo de entrada na rede. Após ser autorizado a operar na rede, o nó recebe um identificador de nó (*node ID*) de 16 bits. Esse identificador é a base de identificação do nó durante as operações. Para endereçar os nós na vizinhança, identificadores de enlace (*link ID*) de 8 bits são usados. Cada nó atribui um identificador para cada enlace que estabelece com seus vizinhos. Os *link ID* são comunicados durante o processo de estabelecimento do enlace.

A subcamada de segurança visa garantir o estabelecimento seguro de conexões, a autenticação do acesso à rede e a troca de chaves para criptografia.

3.3 QUADRO 802.16 MESH

O quadro (*frame*) mesh é sempre composto por dois subquadros (*subframes*): subquadro de controle e subquadro de dados, descritos a seguir.

O subquadro de controle pode ser de dois tipos: NCS (*network control* subframe) e SCS (*schedule control subframe*).

O subquadro de controle do tipo NCS transporta dois tipos de mensagem: “MSH-NENT” (*mesh network* entry) e “MSH-NCFG” (*mesh network configuration*). A mensagem “MSH-NENT” ocorre sempre na primeira oportunidade de transmissão e é utilizada pelos novos nós durante o processo de entrada na rede. A “MSH-NCFG” ocorre nas oportunidades de transmissão restantes e contém as informações de configuração da rede. Essas informações são transmitidas em broadcast por todos

os nós ativos na rede. Em suma, o subquadro de controle do tipo NCS é destinado primariamente a novos nós que desejem adquirir sincronismo e entrar na rede.

O subquadro de controle do tipo SCS transporta, basicamente, três tipos de mensagem: “MSH-DSCH” (*mesh distributed schedule*), “MSH-CSCH” (*mesh centralized schedule*) e “MSH-CSCF” (*mesh centralized schedule configuration*). Tais mensagens transportam as informações necessárias para que os algoritmos de agendamento possam garantir a transmissão de dados livre de colisão. A figura 2 mostra a composição dos quadros (*frames*) mesh com o subquadro de controle do tipo NCS (a) e com o subquadro de controle do tipo SCS (b).

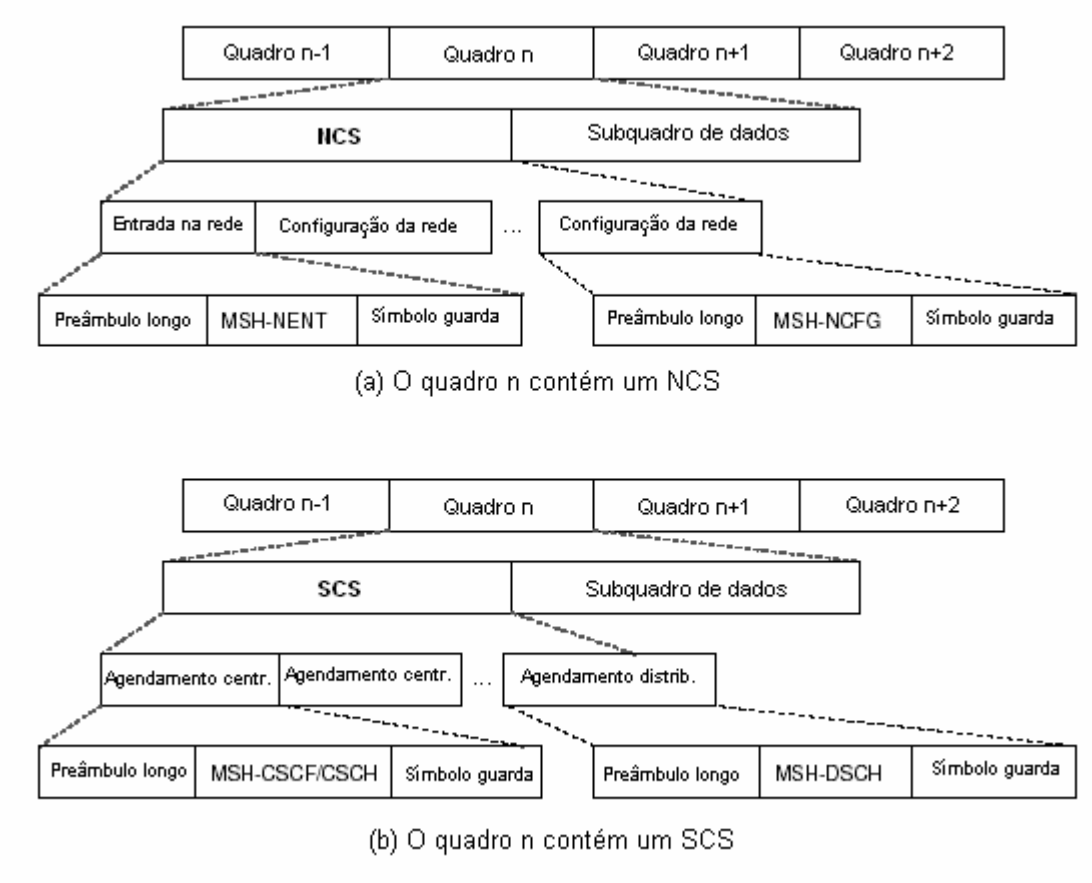


Figura 2 – Quadros 802.16 mesh

O subquadro de dados inicia-se sempre com um preâmbulo longo, composto de 2 símbolos OFDM, para sincronização das estações. Ao preâmbulo seguem-se imediatamente as unidades de dados do protocolo MAC (*MAC protocol data unit* – MAC PDU). Cada unidade de dados do protocolo MAC (PDU MAC) contém um cabeçalho de 6 bytes, um subcabeçalho mesh de 2 bytes (que contém o *node ID*), um *payload* variável (de 0 a 2.039 bytes) e um CRC (*cyclic redundancy check*)

opcional de 4 bytes. Consequentemente, o tamanho de um MAC PDU 802.16 mesh varia de 8 a 2051 bytes. O formato genérico de um MAC PDU é mostrado na figura 3.

MSB LSB

Cabeçalho MAC Genérico	Payload (opcional)	CRC (opcional)

Figura 3 – MAC PDU 802.16

3.4 SINCRONIZAÇÃO E ENTRADA NA REDE NO MODO MESH

O processo completo de entrada na rede, isto é, até o estágio no qual um nó passa ter suas transmissões agendadas, pode ser dividido em nove fases: (i) varredura (*scan*) e sincronização inicial; (ii) obtenção dos parâmetros da rede; (iii) abertura do canal de patrocínio (*sponsor channel*); (iv) negociação das capacidades básicas; (v) autorização; (vi) registro; (vii) estabelecimento de conectividade IP; (viii) acerto de horário; e (ix) transferência de parâmetros operacionais. Na figura 4, é apresentada uma visão geral consolidada das fases supracitadas, que são descritas a seguir.

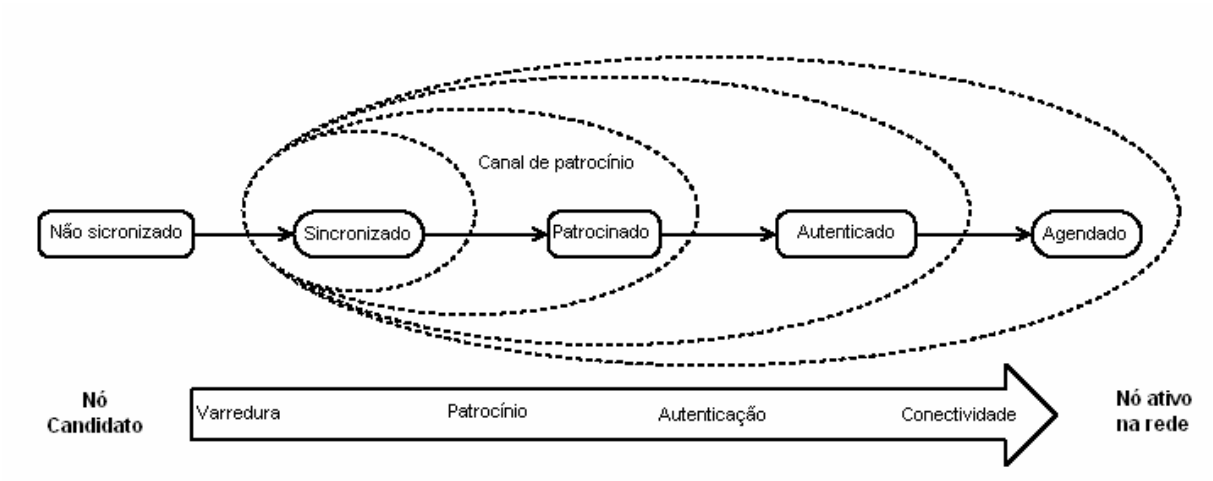


Figura 4 – Visão geral do processo de entrada na rede

3.4.1 **Varredura e Sincronização Inicial**

Na inicialização ou em caso de eventual perda de sinal, o novo nó varre continuamente todos os possíveis canais da faixa de freqüência de operação, até que uma rede mesh válida seja encontrada. Após estar sintonizado no canal de operação correto, o novo nó passa a receber as mensagens do tipo “MSH-NCFG:Networkdescriptor”, que são transmitidas periodicamente pelos nós ativos em uma rede mesh. Essas mensagens contêm, no campo *timestamp*, os parâmetros necessários para que o novo nó proceda sua sincronização inicial. A sincronização obtida nessa fase é uma sincronização grosseira, que vai ser aprimorada em uma fase posterior do processo. Uma vez que a camada física está sincronizada, a camada MAC pode obter os parâmetros da rede.

3.4.2 **Obtenção dos Parâmetros da Rede**

O processo de sincronização continua até que o novo nó receba duas mensagens “MSH-NCFG:Networkdescriptor” de um mesmo nó ativo na rede. Enquanto isso não ocorre, o novo nó utiliza as informações contidas no parâmetro “MSH-Nbr_Physical_IE” das mensagens “MSH-NCFG:Networkdescriptor” que recebe para montar e armazenar uma lista de vizinhos. Encerrada a sincronização, o novo nó utiliza essa lista de vizinhos para selecionar um candidato a nó patrocinador (*candidate sponsoring node*) e com ele se sincroniza desconsiderando o atraso de propagação. Após ter selecionado seu nó patrocinador candidato, o novo nó passa a ser denominado nó candidato (*candidate node*).

3.4.3 **Abertura do Canal de Patrocínio**

Para prosseguir no processo de entrada na rede, o novo nó deve ser capaz de transmitir dados na rede. Para isso, faz-se necessário que algum nó ativo reserve temporariamente *slots* de tempo para a transmissão das mensagens necessárias ao restante do processo de inicialização do novo nó. Esses *slots* são reservados pelo nó patrocinador que os utiliza para retransmitir aos destinatários as mensagens originadas no novo nó. Essa reserva de *slots* de tempo forma um canal de

comunicação entre o novo nó e o nó patrocinador. Esse canal é denominado canal de patrocínio (*sponsor channel*).

A abertura do canal de patrocínio é realizada por meio da troca de três mensagens. O nó candidato inicia o processo por meio da transmissão da mensagem “MSH-NENT:NetEntryRequest”. Ao receber essa mensagem, o nó patrocinador candidato avalia a solicitação e decide como vai respondê-la: se com a mensagem “MSH-NCFG:NetEntryOpen”, aceitando a solicitação; ou com a mensagem “MSH-NCFG:NetEntryReject”, recusando a solicitação. A abertura do canal de patrocínio é finalizada pelo nó candidato com o envio da mensagem de confirmação “MSH-NENT:NetEntryAck” ao nó patrocinador candidato.

Ao receber uma mensagem “MSH-NCFG:NetEntryOpen”, o nó candidato faz uma sincronização mais apurada de seu tempo de transmissão. Isso é feito a partir das informações contidas no parâmetro *estimated propagation delay* da mensagem “MSH-NCFG:NetEntryOpen”. Esse parâmetro informa o atraso de propagação estimado pelo nó patrocinador candidato e permite ao nó candidato aplicar um fator de correção ao sincronismo conseguido na fase de obtenção dos parâmetros da rede. Encerrada essa fase, o nó patrocinador candidato passa, então, a ser denominado nó patrocinador. As etapas seguintes do processo de inicialização são conduzidas utilizando o agendamento de *slots* realizado nesta fase.

3.4.4 **Negociação de Capacidades Básicas**

A negociação de capacidades básicas é efetuada em todas as ocasiões em que um nó estabelece um enlace lógico com outro nó da rede mesh. Esse processo é realizado através da troca de duas mensagens. O nó que solicitou o estabelecimento do enlace lógico informa a seu vizinho suas capacidades básicas através da transmissão da mensagem “SBC-REQ” (*SS basic capability request*). O nó vizinho responde com a mensagem “SBC-RSP” (*SS basic capability response*), na qual informa as capacidades básicas comuns entre os nós. Por capacidades básicas entende-se: Suporte a ARQ (*automatic repeat request*), número máximo de fluxos simultâneos suportados, suporte ao CRC na camada MAC, número máximo de transações PKM (*privacy key management*), entre outras informações. No caso específico do processo de entrada na rede, o nó candidato é o responsável por

iniciar o processo. Nesta fase, o uso dos enlaces ainda não é possível, visto que o nó candidato ainda não está autenticado na rede.

3.4.5 **Autorização**

Nesta etapa são feitas as verificações de segurança necessárias à autorização do uso da rede. O nó candidato procede a autorização através do nó patrocinador, o qual faz o tunelamento sobre UDP/IP das mensagens necessárias do nó candidato para o nó de autenticação (*authentication node*). O processo de autorização faz uso do protocolo PKM (*privacy key management*).

3.4.6 **Registro**

Registro é o processo no qual um nó recebe seu identificador de nó (*node ID*). Ao receber a mensagem “REG-REQ”, o nó patrocinador faz o tunelamento sobre UDP/IP ao nó de registro (*registration node*) que responde com a mensagem “REG-RSP”. Ao receber o “REG-RSP” tunelado do nó de registro, o nó patrocinador encaminha a mensagem ao nó candidato.

3.4.7 **Estabelecimento de Conectividade IP**

Nesta fase o nó candidato adquire seu endereço IP por meio do protocolo DHCP. Como já mencionado o canal de patrocínio é usado no processo.

3.4.8 **Acerto de Horário**

Realizado de acordo com a RFC 868 (*time protocol*) com as mensagens carregadas sobre UDP/IP no canal de patrocínio.

3.4.9 **Transferência de Parâmetros Operacionais**

Após a obtenção do endereço IP via DHCP, o nó candidato deve fazer o download de um arquivo de configuração, utilizando o protocolo TFTP. Terminado o download, o processo de inicialização é finalizado com a transmissão por parte do

novo nó mesh da mensagem “MSH-NENT:NetEntryClose”. Essa última é confirmada pela mensagem “MSH-NCFG:NetEntryAck” do nó patrocinador. A figura 5 ilustra o processo de entrada na rede mesh.

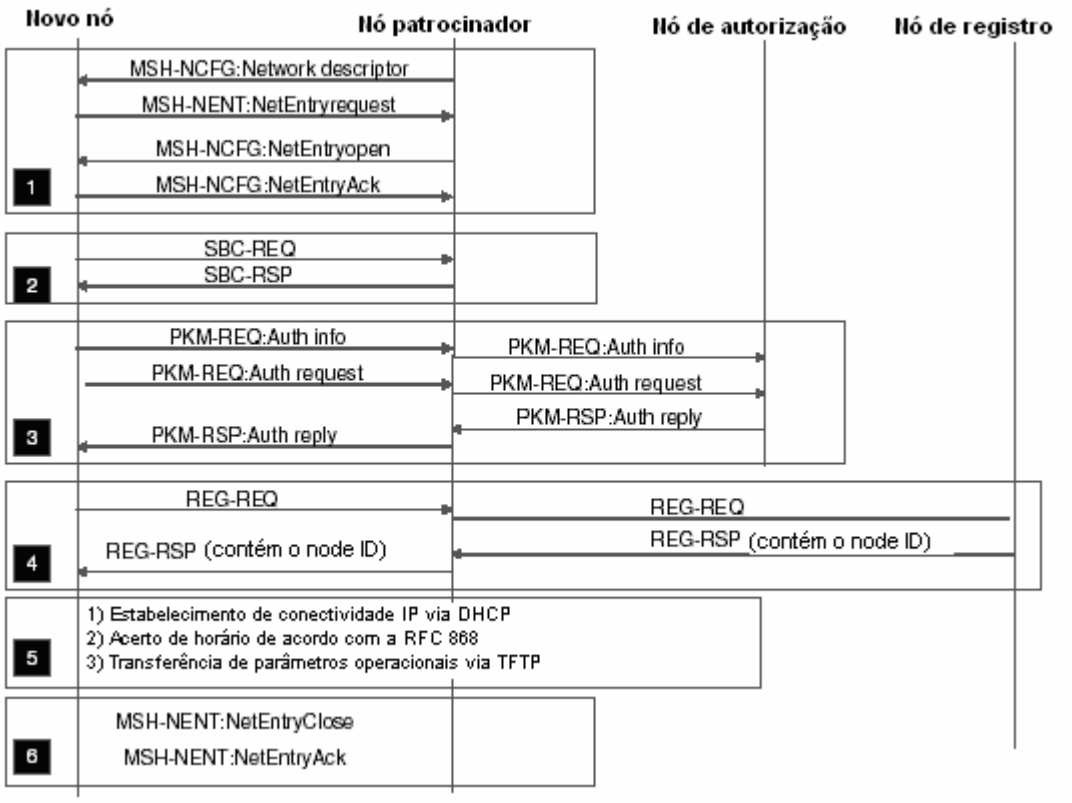


Figura 5 – Troca de mensagens durante o processo de entrada na rede

3.5 CONSIDERAÇÕES FINAIS DO CAPÍTULO

Neste capítulo foi descrito, resumidamente, o funcionamento do modo mesh de operação das redes 802.16. Foi dada ênfase no processo de entrada na rede, por ser ele o mais importante para compreensão das vulnerabilidades de segurança existentes no padrão. O capítulo 4 apresenta uma visão geral da subcamada de segurança 802.16 e seus componentes.

4 **A SUBCAMADA DE SEGURANÇA NO PADRÃO 802.16**

Para compreender as vulnerabilidades existentes no modo de operação mesh do padrão 802.16, é preciso entender o funcionamento de sua subcamada de segurança, descrito nesta seção.

4.1 PRINCIPAIS COMPONENTES DA SUBCAMADA DE SEGURANÇA

A subcamada de segurança possui dois componentes principais: um protocolo de encapsulamento e um protocolo de gerenciamento de chaves.

O protocolo de encapsulamento garante a segurança dos pacotes que atravessam a rede por meio do uso de autenticação e criptografia no *payload* dos PDU MAC.

O protocolo de gerenciamento de chaves é o responsável por prover a distribuição segura das chaves criptográficas a serem utilizadas na rede. No IEEE 802.16, o protocolo de gerenciamento de chaves é chamado PKM (*Privacy Key Management*). O PKM também é o protocolo utilizado para condicionar o acesso à rede, o que faz dele o protocolo de autenticação do padrão.

4.2 ALGORITMOS DE CRIPTOGRAFIA DO IEEE 802.16 MESH

Para cada função específica, o padrão 802.16 estabelece os algoritmos criptográficos a serem empregados. O quadro 3 resume os algoritmos de encriptação previstos e seus respectivos usos.

Quadro 3 - Algoritmos de criptografia do IEEE 802.16 em modo mesh

Uso	Algoritmo de Criptografia Utilizado
Encriptação do OSS	RSA
Encriptação de TEK	RSA, 3-DES, AES
Encriptação do Tráfego de Dados	DES, AES
Autenticação de Mensagens	HMAC

4.3 SUÍTES CRIPTOGRÁFICAS E ASSOCIAÇÕES DE SEGURANÇA

O padrão define uma associação de segurança (*security association* – SA) como o conjunto de informações de segurança que dois nós devem compartilhar a fim de tornar possível o estabelecimento de comunicações seguras entre eles. Uma suíte criptográfica (*cryptografic suite*) é o conjunto de métodos empregados em uma associação de segurança para permitir encriptação de dados, autenticação de dados e troca de chaves de encriptação de dados (*traffic encryption key* – TEK). Cada SA possui um identificador de associação de segurança (*security association identifier* - SAID) de 16 bits que a identifica univocamente.

4.4 O PROTOCOLO PKM

Conforme mencionado, o PKM é o protocolo de gerenciamento de chaves utilizado pela subcamada de segurança do padrão IEEE 802.16. Ele emprega um modelo baseado na arquitetura cliente-servidor. Ou seja, no PKM o nó de autorização faz o papel do servidor e controla a distribuição de chaves aos demais nós, que são os clientes.

O padrão IEEE 802.16e criou uma nova versão para o protocolo PKM. Assim, desde sua publicação, o PKM passou a ter duas versões. A versão 1 (PKMv1) é a mesma especificada no padrão IEEE 802.16 – 2004. A versão 2 (PKMv2), que difere da primeira principalmente no que tange ao processo de autorização, é especificada por completo no padrão IEEE 802.16e.

4.4.1 **Principais Chaves Criptográficas Usadas pelo PKM no Modo Mesh**

O protocolo PKM utiliza diversas chaves criptográficas para garantir a segurança do processo de autorização na rede. O quadro 4 apresenta um resumo dessas chaves, indicando em qual versão do protocolo elas são utilizadas.

Quadro 4 - Chaves criptográficas utilizadas pelo PKM no modo mesh

Abreviatura	Nome	Versão do PKM	Observação
PMK	Pairwise Master Key	2	Obtida da Autenticação EAP
PAK	Primary Authorisation Key	2	Obtida da Autenticação RSA
TEK	Traffic Encryption Key	1 e 2	Usada para encriptação de dados
OSS	Operator Shared Secret	1 e 2	Chave comum entre os nós. No caso do PKMv2 é obtida da: PMK ou PAK
HMAC_KEY_S	HMAC Key in the Mesh mode	1	Usada para autenticar mensagens

4.4.2 **Mensagens MAC Utilizadas pelo PKM**

O protocolo PKM utiliza dois tipos de mensagem MAC: “PKM-REQ” (*PKM request*) e “PKM-RSP” (*PKM response*). A primeira sempre é enviada de um nó ativo da rede para o nó de autorização. A segunda é enviada sempre no sentido contrário, ou seja, de um nó de autorização para um nó da rede.

4.5 O PROCESSO DE AUTORIZAÇÃO EM UMA REDE 802.16 MESH

O processo de autorização possui duas etapas consecutivas: a autenticação e o estabelecimento de uma chave criptográfica comum. Na autenticação, as identidades do nó de autorização e do nó candidato são verificadas e tidas como autênticas. Nessa etapa, o que se quer assegurar é que o nó A esteja realmente falando com o nó B e não com o invasor Z. No processo de estabelecimento de uma chave criptográfica comum, o nó de autorização envia ao nó candidato, devidamente criptografada, uma chave criptográfica de uso comum a todos os nós da rede mesh, sem a qual nenhum nó consegue fazer uso da rede. Essa chave é denominada OSS (*operator shared secret*) e tem um período de validade determinado, devendo ser renovada periodicamente por todos os nós da rede mesh. O método de renovação

do OSS é o mesmo método utilizado para renovação da AK (*authorization key* – chave criptográfica usada com a mesma finalidade do OSS no modo ponto-multiponto). Assim, antes de o OSS expirar, o nó mesh deve iniciar um processo de reautorização. Esse processo vai variar conforme a versão do protocolo PKM utilizada e o respectivo método de autenticação empregado.

Os procedimentos relativos à autorização no PKM são bastante semelhantes para as topologias mesh e ponto-multiponto. No entanto, devido às peculiaridades da topologia mesh, o padrão admite que o nó de autorização seja qualquer nó ativo na rede, desde que este nó exerça as funções de autorização preconizadas para as estações base que operam no modo ponto-multiponto. Desse modo, a centralização do processo de autorização é mantida em um mesmo nó. Assim, pode-se considerar a autorização mesh é como sendo uma versão em múltiplos saltos (*multihop*) da autorização no modo ponto-multiponto.

4.5.1 **Autorização na Versão 1 do Protocolo PKM**

Na versão 1 do protocolo PKM (PKMv1), o processo de autorização é efetuado por meio da troca de três mensagens entre o nó candidato e o nó de autorização. Esse processo é iniciado pelo nó candidato, que envia a mensagem “PKM-REQ:AuthorizationInfo”. Essa mensagem contém o certificado X.509 de seu fabricante e é apenas informativa, podendo ser ignorada pelo nó de autorização. Em seguida, o nó candidato envia a mensagem “PKM-REQ:AuthorizationRequest” contendo seu certificado X.509 (assinado digitalmente por seu fabricante) e as suítes de criptografia por ele suportadas. Nesse certificado está incluída a chave criptográfica pública do nó candidato. Ao receber o certificado, o nó de autorização verifica a assinatura do fabricante do nó candidato e o autentica. Em seguida, o nó de autorização envia a mensagem “PKM-RSP:AuthorizationReply” que contém a chave criptográfica OSS, cifrada na a chave pública do nó candidato.

No PKMv1, o nó candidato não autentica o nó de autorização. Esse tipo de autenticação é chamado de autenticação de mão única (*one-way authentication*). O processo de autorização do PKMv1 é mostrado na figura 6.

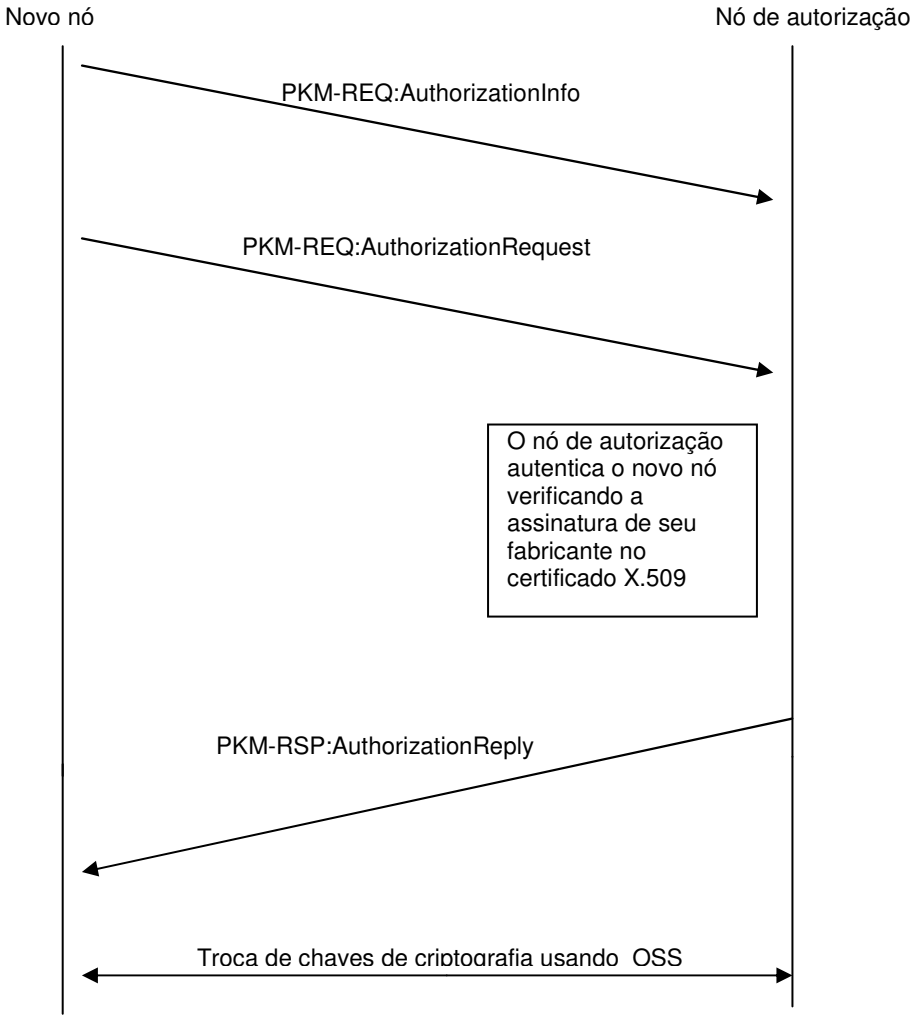


Figura 6 – O processo de autorização no PKMv1

4.5.2 **Autorização na Versão 2 do Protocolo PKM**

Na versão 2 do protocolo PKM, ao contrário do que ocorre na versão 1, o nó candidato também autentica o nó de autorização. Esse tipo de autenticação é chamado de autenticação mútua (*two-way authentication*). Dois mecanismos de autenticação são suportados pelo PKMv2: RSA e EAP.

A autenticação por RSA é baseada no uso de certificados X.509. A troca de mensagens nesse caso, é quase idêntica à do PKMv1. Entretanto, a fim de permitir a autenticação mútua, na mensagem PKM-RSP:AuthorizationResponse, o nó de

autenticação inclui seu certificado X.509 a ser verificado pelo nó candidato, conforme mostra a figura 7. Tanto no PKMv1, quanto no PKMv2, o padrão impõe o uso da versão 3 dos certificados X.509.

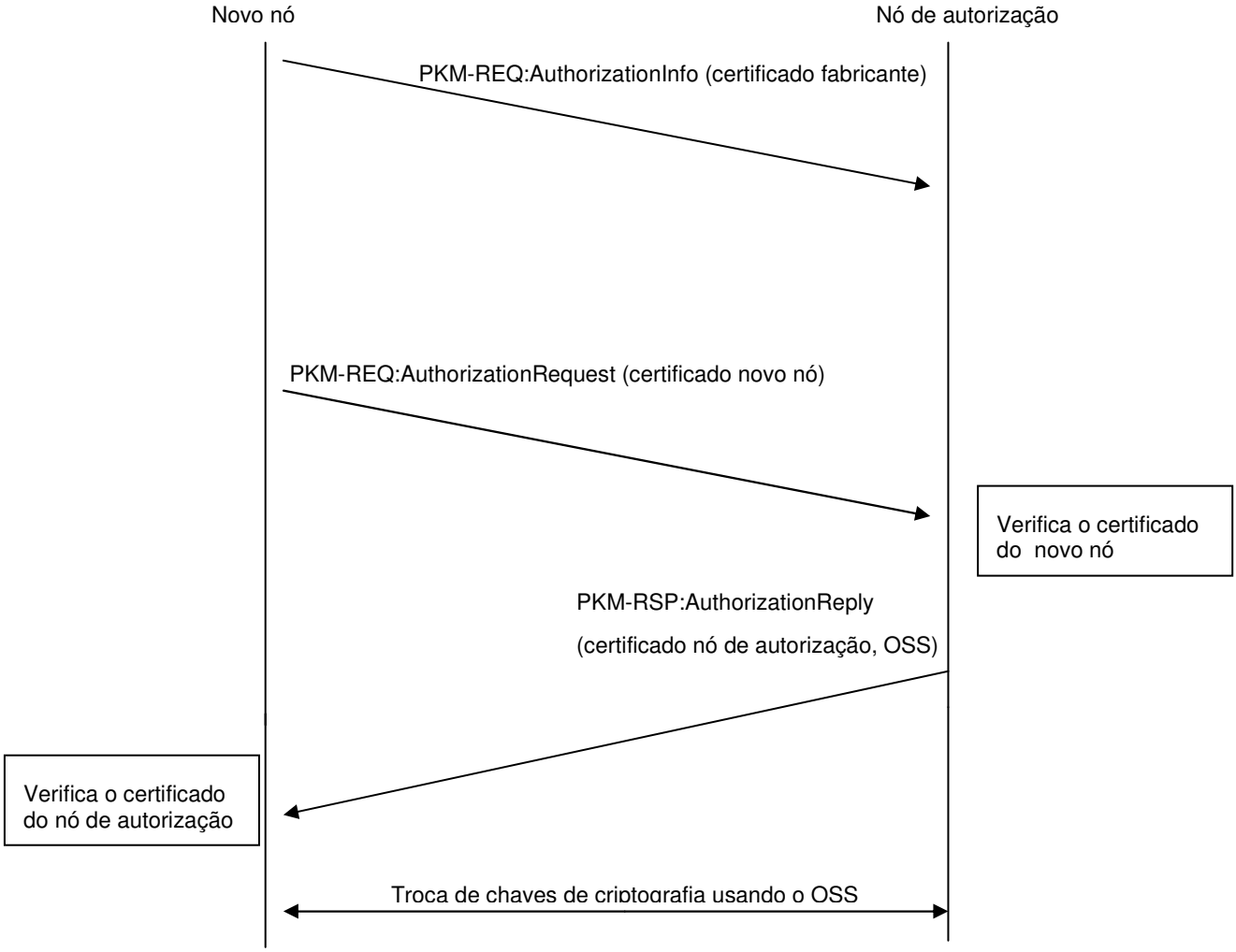


Figura 7 – O processo de autorização no PKMv2 usando RSA

A implementação e o modo de operação do protocolo EAP estão fora do escopo do padrão IEEE 802.16. O protocolo prevê a existência de um servidor de autenticação com o qual o autenticador EAP troca mensagens com o objetivo de autenticar o suplicante EAP. Nas redes 802.16 mesh, o nó de autorização faz o papel de autenticador EAP e o novo nó a ser autenticado faz o papel de suplicante EAP. O resultado obtido através da troca de mensagens EAP que é utilizado pela versão 2 do protocolo PKM é a chave criptográfica MSK (*master session key*). Essa chave é de conhecimento do nó de autorização e do nó candidato ao final da

execução do protocolo EAP. Do truncamento da MSK, o nó de autorização e o nó candidato obtêm a chave criptográfica PMK (*pairwise master key*). Da PMK é gerado o OSS. A figura 8 ilustra o processo de autorização no PKMv2 usando EAP.

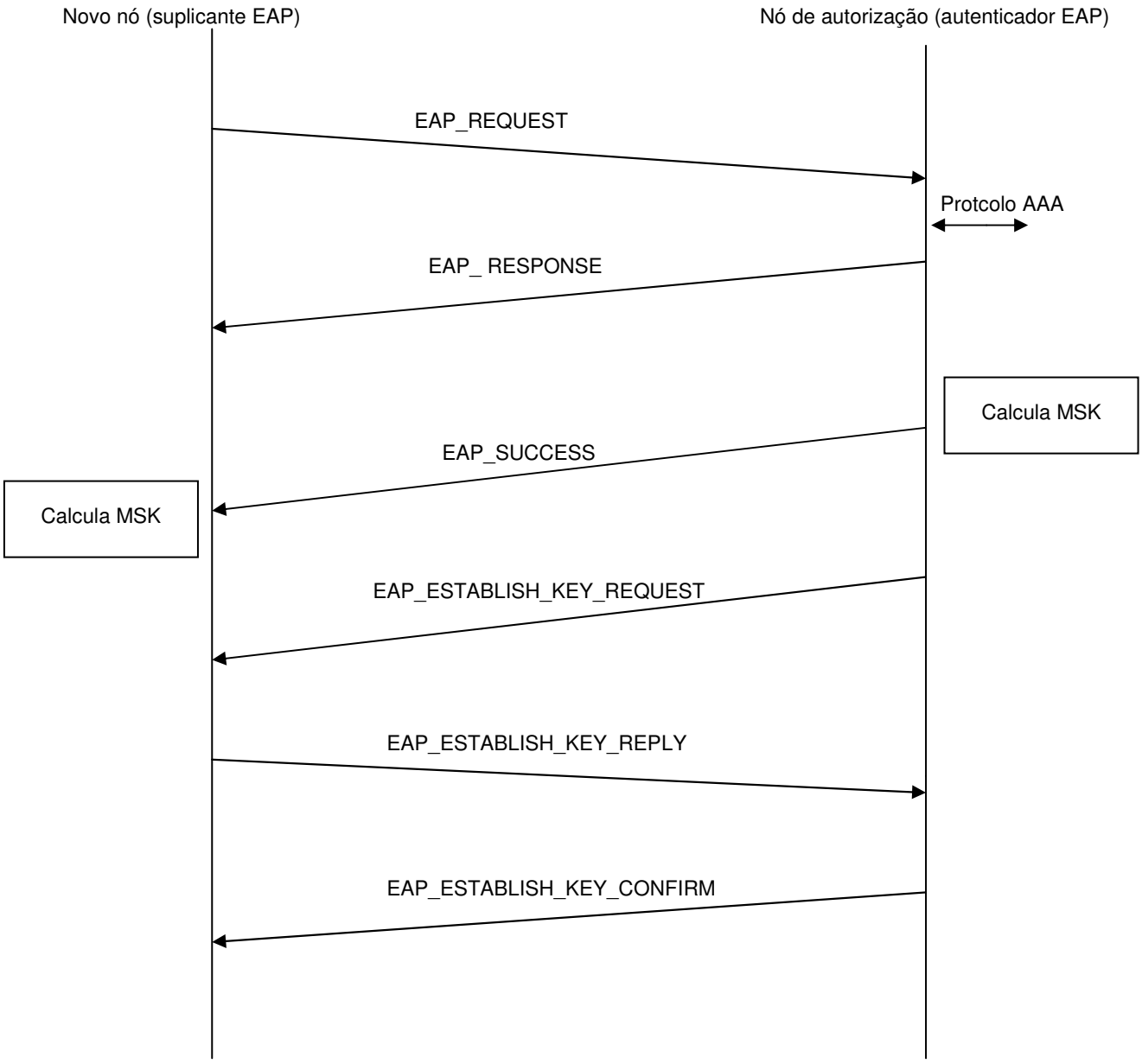


Figura 8 – O processo de autorização no PKMv2 usando EAP

O padrão também não define o método EAP a ser usado. Entretanto, exige que o método selecionado cumpra as exigências dos critérios obrigatórios (*mandatory criteria*) listados na seção 2.2 da RFC 4017. Segundo Nuaymi, apenas o algoritmo EAP-TLS cumpre essas exigências.

4.6 AUTENTICAÇÃO DE MENSAGENS MAC COM O HMAC

O padrão 802.16 prevê o uso do HMAC (*hased message authentication code*) para controle de integridade de mensagens MAC. Para cada mensagem MAC autenticada, é calculado um *hash* HMAC que é enviado juntamente com a mensagem. O cálculo do mesmo *hash* por parte do destinatário permite a verificação da integridade da mensagem. O algoritmo utilizado é o SHA-1 (*secure hash algorithm*).

Para a versão 2 do protocolo PKM, o padrão IEEE 802.16e acrescenta a possibilidade de se usar o CMAC (*cipher-based message authentication code*) em substituição ao HMAC. O algoritmo utilizado é o CMAC-AES 2005. No entanto, o padrão não define que chave criptográfica deve ser usada para geração dos *hash* CMAC no caso de operação no modo mesh.

4.7 ESTABELECIMENTO DE ENLACES COM VIZINHOS

Após entrar na rede mesh, o novo nó pode estabelecer enlaces (*links*) com outros nós vizinhos que não o seu nó patrocinador. Essa fase denomina-se estabelecimento de enlaces com vizinhos (*neighbor link establishment* – NLE) e ocorre de acordo com os passos a seguir. Na descrição dos passos, a seguinte nomenclatura é empregada: o nó A representa o novo nó e o nó B representa um nó ativo na rede com o qual o nó A deseja estabelecer um enlace.

a) O nó A envia ao nó B um desafio contendo: C/HMAC { OSS, nº do quadro, *node ID* B, *node ID* A}, onde nº do quadro é o número do último quadro no qual o nó B enviou uma mensagem “MSH-NCFG”;

b) O nó B, ao receber o desafio, verifica o número do quadro e envia uma resposta ao desafio contendo: C/HMAC { OSS, nº do quadro, *node ID* A, *node ID* B}, onde o nº do quadro, nesse caso, é o número do quadro no qual o nó A enviou o desafio; e

c) Ao receber a resposta o nó A verifica o número do quadro e o enlace é estabelecido.

4.8 TROCA DE CHAVES DE ENCRIPTAÇÃO DE DADOS

A próxima fase após o estabelecimento de um enlace com um vizinho é a troca das chaves de encriptação de dados (TEKs) a serem usadas nesse enlace. Para cada enlace deve ser gerada uma TEK. Como o próprio nome diz, as TEKs são usadas para criptografar o tráfego na rede. No entanto, no padrão IEEE 802.16 a criptografia é aplicada somente nos *payload* dos PDU MAC. O primeiro cabeçalho MAC, conhecido como cabeçalho MAC genérico, nunca é criptografado. Além disso, todas as mensagens MAC de gerenciamento são enviadas em claro de modo a facilitar a operação da camada MAC.

Cada nó é responsável por manter e renovar periodicamente as TEKs entre ele mesmo e todos os vizinhos com os quais ele iniciou uma troca de TEKs. Para iniciar uma troca de TEKs, um nó envia a seu vizinho a mensagem PKM-REQ:KeyRequest. O vizinho responde com a mensagem PKM-RSP:KeyReply contendo a TEK criptografada com a chave pública do nó que iniciou a troca, encerrando o processo. A encriptação das TEKs em modo mesh é feita com as chaves públicas dos nós envolvidos para garantir a privacidade da comunicação com diferentes nós. Caso fosse utilizado o OSS para cifrar as TEKs, um nó qualquer da rede poderia interceptar todas as comunicações entre todos os outros nós que estivessem dentro de seu alcance rádio, já que, ao contrário das AK do modo ponto-multiponto, o OSS é comum a todos os nós ativos em uma rede mesh.

4.9 CONSIDERAÇÕES FINAIS DO CAPÍTULO

Neste capítulo foram apresentados os conceitos básicos relativos à subcamada de segurança do padrão 802.16, com ênfase no modo mesh de operação. Esse conhecimento é necessário ao entendimento dos resumos dos trabalhos de pesquisa mais recentes sobre a segurança das redes 802.16 mesh, apresentados no capítulo 5.

5 CONSIDERAÇÕES SOBRE SEGURANÇA NAS REDES 802.16 MESH

Neste capítulo serão apresentadas as pesquisas mais recentes a sobre a segurança das redes 802.16 mesh. Cada sessão é baseada em um estudo publicado e descreve as opiniões e conclusões de seus autores a respeito das vulnerabilidades encontradas e suas possíveis soluções.

5.1 SEGURANÇA 802.16 MESH SEGUNDO ZHOU E FANG

Zhou e Fang fazem uma análise da segurança do padrão IEEE 802.16 no modo mesh. Em seu trabalho, são apontadas diversas vulnerabilidades existentes no padrão para esse modo de operação. Os autores também fazem uma análise das melhorias e dos problemas de segurança introduzidos pelo padrão IEEE 802.16e e propõem algumas soluções para melhorar a segurança das redes 802.16 mesh. Não são propostos trabalhos futuros. Esta seção apresenta um resumo do trabalho de Zhou e Fang.

5.1.1 **Ameaças à Segurança do IEEE 802.16 no Modo Mesh**

Zhou e Fang classificam as vulnerabilidades do modo mesh em 5 grupos: ataques à topologia, ameaças ao processo de autorização, ameaças ao processo de estabelecimento de enlaces com vizinhos, ameaças à troca de chaves de encriptação de dados e ameaças ao tráfego de dados.

5.1.1.1 Ataques à Topologia

As mensagens “MSH-NCFG:NetworkDescriptor” não são criptografadas ou autenticadas. Essas mensagens transportam a lista de vizinhos divulgada periodicamente pelos nós ativos na rede. Assim, informando ter um número de saltos menor até o nó de autorização, um atacante aumenta suas chances de tornar um nó patrocinador. Como nó patrocinador, ele pode monitorar, modificar ou personificar (fazer *spoofing*) as mensagens de autorização trocadas entre novos nós e o nó de autorização.

A ausência de criptografia e autenticação nas mensagens “MSH-NCFG:NetworkDescriptor” da origem a outra vulnerabilidade. A inserção de informações falsas na lista de vizinhos pode levar um novo nó a ter uma visão incorreta sobre a topologia da rede, gerando problemas aos protocolos de roteamento.

Caso existam dois atacantes na rede, outro tipo de ataque topológico pode ocorrer. Os atacantes podem estabelecer um túnel de mensagens “MSH-NCFG:NetworkDescriptor” entre eles, levando nós distantes na rede a acreditarem que são vizinhos. Outra vez, uma visão topológica distorcida da rede pode prejudicar o desempenho dos protocolos de roteamento.

5.1.1.2 Ameaças ao Processo de Autorização

As mensagens “PKM-REQ” e “PKM-RSP” também não são autenticadas. Três tipos de ataque podem se aproveitar desse fato.

A mensagem “PKM-REQ:AuthorizationRequest” divulga as capacidades criptográficas do novo nó durante o processo de autorização. Assim, um atacante interno fazendo o papel de um nó patrocinador pode modificar essa mensagem e divulgar algoritmos criptográficos mais fracos do que os realmente suportados pelo novo nó. Isso faz com que o nó de autorização seja forçado a escolher dentre esses algoritmos criptográficos fracos, reduzindo a segurança na rede.

A mensagem “PKM-RSP:AuthorizationReply” informa ao novo nó as associações de segurança (SA) que ele está autorizado acessar. Um atacante pode modificar essa mensagem e remover todas as SA autorizadas, negando serviço ao novo nó.

A mensagem “PKM-RSP:AuthorizationReply” também transporta a chave criptográfica OSS. Um atacante pode modificá-lo fazendo com que o novo nó não consiga juntar-se à rede. Além disso, o atacante pode reduzir o tempo de vida do OSS. Assim, o nó atacado tem que efetuar o processo de reautorização mais freqüentemente, levando a um maior consumo de energia.

5.1.1.3 Ameaças ao Estabelecimento de Enlaces com Vizinhos

A segurança do processo de estabelecimento de enlaces com vizinhos é totalmente dependente da confidencialidade da chave criptográfica OSS. Um atacante que tome conhecimento do OSS pode vir a se juntar à rede e obter serviços de seus vizinhos.

5.1.1.4 Ameaças à Troca de Chaves de Encriptação de Dados

Para proteger a troca de chaves de encriptação de dados (TEKs), *hashes* HMAC são anexados às mensagens "PKM-REQ:KeyRequest" e "PKM-RSP:KeyReply". No entanto, os *hashes* HMAC são calculados com o OSS. Em caso de vazamento do OSS, isso pode levar à adulteração dessas mensagens.

5.1.1.5 Ameaças ao Tráfego de Dados

Um dos algoritmos de criptografia de dados permitidos pelo padrão, o DES-CBC, não garante a integridade desses dados, apenas sua confidencialidade. Consequentemente, o uso do DES-CBC pode permitir o *spoofing* e a adulteração de mensagens MAC.

5.1.2 **A segurança do Padrão 802.16e em Modo Mesh**

A publicação do padrão IEEE 802.16e, conforme já citado, trouxe melhorias à segurança do modo mesh. Em seu trabalho, Zhou e Fang descrevem as melhorias obtidas e as ameças que ainda permanecem.

5.1.2.1 Melhorias Obtidas

O padrão IEEE 802.16e preconiza a inclusão de números aleatórios nas mensagens de autenticação por RSA, a fim de evitar os ataques de reprodução (*replay*), nos quais uma mensagem é gravada e reproduzida posteriormente. Além disso, a partir da publicação do 802.16e, os métodos de autenticação por RSA e por

EAP passaram a suportar autenticação mútua, reduzindo vulnerabilidades. O padrão 802.16e também incluiu o uso dos algoritmos de criptografia AES-CTR e AES-CBC para encriptação dos *payload* dos PDU MAC, reforçando a segurança.

5.1.2.2 Ameaças em Potencial

A mensagem “MSH-NCFG:NetworkDescriptor” permanece sendo uma ameaça potencial, podendo ser modificada por atacantes. Todas as mensagens MAC de gerenciamento continuam sem criptografia, podendo ser interceptadas.

5.1.3 **Soluções Propostas para os Problemas Encontrados**

5.1.3.1 Autenticação entre Vizinhos

Os autores propõem a utilização de certificados digitais para autenticação entre vizinhos. Para isso, durante o processo de autorização, o nó receberia um certificado digital emitido pelo nó de autorização, chamado de certificado mesh. Os certificados mesh seriam incluídos nas mensagens de estabelecimento de enlace com vizinhos. Nesse novo processo, um nó B qualquer, ao receber o pedido de um nó A para o estabelecimento de um enlace, verificaria junto ao nó de autorização, o certificado mesh do nó A. Garantida a autenticidade do certificado, B extrairia a assinatura de A e a utilizaria para verificar a autenticidade das mensagens trocadas. Os certificados mesh também seriam usados para garantir a segurança da troca de chaves de encriptação de dados. O estabelecimento de enlaces com vizinhos proposto é mais seguro que o original porque se baseia no uso de certificados mesh individuais, ao invés de utilizar o OSS que é único em toda a rede.

5.1.3.2 Problemas com Criptografia

Geralmente a criptografia baseada no uso de chaves públicas RSA consome mais recursos computacionais do que a criptografia simétrica. Por isso, os autores propõe o uso da criptografia de curva elíptica (*Elliptic Curve Cryptography* – ECC), a qual, com chaves menores, consegue alcançar o mesmo nível de segurança que o RSA.

5.2 SEGURANÇA 802.16 MESH SEGUNDO MACCARI, PAOLI E FANTACCI

Maccari, Paoli e Fantacci analisam a segurança do padrão IEEE 802.16 como um todo. No que tange à operação no modo mesh, propõem dois cenários a partir dos quais apontam falhas do padrão para esse modo de operação. Os autores também analisam separadamente as melhorias e as falhas do padrão 802.16e. Não são propostas soluções nem trabalhos futuros. Esta seção apresenta um resumo do trabalho de Maccari, Paoli e Fantacci.

5.2.1 **Cenários Propostos e Falhas de Segurança Encontradas**

Os autores apresentam dois cenários para representar as possíveis aplicações das redes 802.16 mesh.

No primeiro cenário a rede mesh é formada por nós fixos, sem mobilidade. Nesse caso, o principal uso dessa rede é a distribuição de serviços. Cada nó mesh tem duas interfaces, a primeira fazendo o papel de ponto de acesso na rede local e a segunda conectada à rede de distribuição. Nesse cenário, os nós estão sob controle de um mesmo administrador e certamente existe uma relação de confiança entre eles. Assim, uma vez que um nó se autentica na rede, não são esperados ataques provenientes desse nó.

No segundo cenário, a mobilidade é introduzida. Com isso, é esperada a criação de uma rede de cooperação *ad-hoc* composta por equipamentos portáteis como *smartphones* e *laptops* numa área limitada, mas com possibilidades de crescimento. Nesse cenário, cada nó é administrado por uma entidade diferente. Consequentemente, não há uma relação prévia de confiança entre eles. Mesmo que um nó se autentique na rede, ele ainda pode ser fonte de ataques. É com base no segundo cenário que devem ser feitas as análises de segurança.

No padrão IEEE 802.16 não existe nenhuma chave criptográfica para uso exclusivo de um nó com a estação base. Existe apenas uma chave criptográfica comum, (o OSS) compartilhada por todos os nós da rede. Isso pode ter as seguintes conseqüências: (i) a chave única pode vazar para nós não autorizados, permitindo que eles entrem na rede. Como essa chave é compartilhada por todos os nós, fica muito difícil descobrir o nó responsável pelo comprometimento da chave; (ii) Na

renovação do OSS (processo de reautorização) cada nó solicita um novo antes do vencimento do OSS em uso. Deste modo, diferentes OSS podem estar em uso simultaneamente na rede, o que pode levar o estabelecimento do enlace com um vizinho a falhar, caso os nós envolvidos estejam utilizando OSS diferentes. Como o OSS é compartilhado por todos os nós, um atacante pode ainda responder no lugar do nó de autenticação e autorizar nós que não possuam as credenciais corretas. Além disso, qualquer nó da rede mesh pode impedir uma autorização de ser realizada, enviando um OSS incorreto, o que vai inutilizar o processo de troca das TEKs.

O processo de troca de chaves de encriptação de dados (TEKs) também apresenta problemas. Não há como fazer diferença entre processos diferentes de troca de TEKs. Assim, um atacante que conheça o OSS pode repetir o processo de troca de TEKs quantas vezes quiser, desde que use um identificador de nó diferente. Desse modo, a vítima pensaria ter estabelecido enlaces com mais de um nó, mas na verdade teria vários enlaces estabelecidos com o atacante. Esse tipo de falha pode ser usada para realizar um ataque do tipo *man in the middle*, pois praticamente garante que todo o tráfego proveniente da vítima passe pelo atacante. Além disso, não existe nenhuma correlação entre o processo de estabelecimento de enlace com um vizinho e o processo de troca de chaves de encriptação de dados com esse mesmo vizinho. Isso porque o nó que solicitou uma TEK não tem como ligar o identificador de nó (*node ID*) obtido durante o estabelecimento do enlace com a chave pública utilizada para cifrar a TEK. Assim, um atacante interno pode responder a uma solicitação de TEK feita a outro nó, bastando para isso usar o *node ID* desse outro nó.

5.2.2 **A segurança do Padrão 802.16e em Modo Mesh**

O padrão IEEE 802.16e introduz modificações que elevam a segurança das redes mesh. No entanto, não há qualquer recomendação para que os novos métodos sejam usados preferencialmente em relação aos preconizados nas versões anteriores do padrão. Os procedimentos antigos e mais inseguros são descritos como equivalentes aos novos.

Embora o protocolo EAP seja reconhecidamente seguro, sua segurança depende de que o enlace entre o autenticador (nó de autorização) e o servidor de

autenticação seja protegido por algum tipo de protocolo AAA (*authentication, authorization, accounting*) como o protocolo RADIUS. No entanto, o padrão 802.16e não prevê o uso desse tipo de protocolo no tunelamento UDP/IP utilizado no processo de autorização. O uso do RADIUS garantiria inclusive que o nó patrocinador estivesse autenticado na rede. Sem a modificação do processo de estabelecimento de enlaces com vizinhos, o uso do protocolo EAP pode ser inútil. O padrão também não deixa claro como o mesmo OSS vai ser gerado em todos os nós.

5.3 CONCLUSÃO

Esta monografia apresentou um resumo das pesquisas mais recentes a respeito da segurança do modo mesh das redes do padrão 802.16. Foram descritos, também, de forma resumida, os principais aspectos de funcionamento do padrão a fim de fornecer o embasamento necessário ao entedimento dos trabalhos apresentados. Pode-se perceber que ainda existem diversas vulnerabilidades no modo de operação mesh, mesmo após a publicação do padrão 802.16e. Assim, as redes 802.16 mesh ainda se constinuem num campo de pesquisa aberto, onde ainda há muito trabalho a ser feito.

REFERÊNCIAS BIBLIOGRÁFICAS

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **Air Interface for Fixed Broadband Wireless Access Systems (IEEE Std 802.16 – 2004)**. 2004.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **Air Interface for Fixed and Mobile Broadband Wireless Access Systems - Amendment 2 and Corrigendum 1 (IEEE Std 802.16e – 2005)**. 2005.

NUAYMI, Loutfi. **WiMAX-Technology for Broadband Wireless Access**. 1. ed. West Sussex: Wiley & Sons, 2007.

ZHANG, Yan; LUO, Jijun; HU, Honglin (cords.). **Wireless Mesh Networking: Architecures, Protocols and Standards**. 1. ed. New York: Auerbach, 2007.

WALKE, Bernard H.; MANGOLD, Stefan; BERLEMANN, Lars. **IEEE 802 Wireless Systems: Protocols, Multi-Hop Mesh/Relaying, Performance and Spectrum Coexistance**. 1. ed. West Sussex: Wiley & Sons, 2006.

YUKSEL, ENDER. **Analysis of the PKMv2 Protocol in IEEE 802.16e-2005 Using Static Analysis**. Kogens Lyngby: Technical University of Denmark, 2007.

DJUKIC, Petar; VALAEE, Shahrokh. **802.16 Mesh Networks**. Toronto: Department of Electrical and Computer Engineering of the University of Toronto, 2006.

HAMID, Zara; KHAN, Shoab A. **An Augmented Security Protocol for WirelessMAN Mesh Networks**. Bangkok: International Symposium on Communications and Information Technologies ISCIT06, p. 861 a 865, 2006.

SCHWINGENSCHLOGL, Christian et al. **Performance Analysis of the Real-time Capabilities of Coordinated Centralized Scheduling in 802.16 Mesh Mode**. Melbourne: Vehicular Technology Conference IEEE VTC2006-Spring, vol. 3, p. 1241 a 1245, 2006.

CAO, Min et al. **Analysis of IEEE 802.16 Mesh Mode Scheduler Performance**. New York: IEEE Transactions on Wireless Communications, vol. 6, issue 4, p. 1455 a 1464, 2007.

ZHOU, Yun; FANG, Yuguang A. **Security of IEEE 802.16 in Mesh Mode**. Washington: Military Communications Conference MILCOM2006, p. 1 a 6, 2006.

LEE, Joo-Chul et al. **Considerations of Neighbor Discovery Protocol over IEEE 802.16 Networks**. Phoenix Park: The 8th International Conference on Advanced Communication Technology ICACT 2006, vol. 2, p. 951 a 955, 2006.

YANG, Fan et al. **An Improved Security Scheme in WMAN based on IEEE Standard 802.16**. Beijing: International Conference on Wireless

Communications, Networking and Mobile Computing WCNMC2005, vol. 2, p. 1191 a 1194, 2005.

WEI, Hung-Yu et al. **Interference-Aware IEEE 802.16 WiMax Mesh Networks**. Stockholm: IEEE 61st Vehicular Technology Conference VTC 2005-Spring, vol. 5, p. 3102 a 3106, 2005.

HAN, Bo et al. **Performance Evaluation of Scheduling in IEEE 802.16 Based Wireless Mesh Networks**. Vancouver: IEEE International Conference on Mobile Adhoc and Sensor Systems MASS2006, p. 789 a 794, 2006.

LEBRUN, Yann et al. **Feasibility Study of the Mesh Extension for the IEEE 802.16e Communication System**. Liege: Symposium on Communications and Vehicular Technology CVT2006, p. 93 a 96, 2006.

LIU, Fuqiang; LU, Lei. **A WPKI-based Security Mechanism for IEEE 802.16e**. Wuhan: International Conference on Wireless Communications, Networking and Mobile Computing WiCOM2006, p. 1 a 4, 2006.

BURBANK, Jack L.; KASCH, William T.. **IEEE 802.16 Broadband Wireless Technology and Its Application to the Military Problem Space**. Atlantic City: Military Communications Conference MILCOM2005, vol. 3, p. 1905 a 1911, 2005.

ADIBI, Sasan et al. **Authentication, Authorization and Acounting (AAA) Schemes in WiMAX**. East Lansing: IEEE International Conference on Electro/Information Technology EIT2006, p. 210 a 215, 2006.

MACCARI, Leonardo; PAOLI, Matteo; FANTACCI, Romano. **Security Analysis of IEEE 802.16**. Atlantic City: IEEE International Conference on Communications ICC apos07, p. 1160 a 1165, 2007.

BRUNO, Raffaele; CONTI, Marco; GREGORI, Enrico. **Mesh Networks: Commodity Multihop Ad Hoc Networks**. s.l.: IEEE Communications Magazine, vol. 43, issue 3, p. 123 a 131, 2005.

FRIEDRICHS, Bernd. **BRAN Summary**. Disponível em: http://portal.etsi.org/bran/Summary.asp. Acesso em 18 out. 2007.

IEEE STANDARDS. Disponível em: http://standards.ieee.org/cgi-bin/status. Acesso em 18 out. 2007.

WIMAX FORUM CERTIFIED PRODUCT REGISTRY. Disponível em: http://www.wimaxforum.org/kshowcase/view. Acesso em 21 out. 2007.

NOVA YORK ganhará rede sem fio WiMax. **Folha de São Paulo**. São Paulo, 5-9-2007, p F6.

MARQUES, Marineide. **Indefinição quanto ao leilão de 3,5 GHz provoca desmobilização de empresas**. Disponível em: http://

www.telecomonline.com.br/v01/noticias/indefinicao-quanto-ao-leilao-de-3-5-ghz-provoca-desmobilizacao-de-empresas. Acesso em 01 out. 2007.

SANTOS, Ceila. **WiMax e os leilões de licença de uso**. Disponível em: http://pcworld.uol.com.br/reportagens/2007/08/03/idgnoticia.2007-08-03.3078838401/. Acesso em 01 out. 2007.

SPRINT NEXTEL CITES WIMAX NETWORK PROGRESS FOR 2007. Disponível em: http://www2.sprint.com/mr/news_dtl.do?id=15000. Acesso em 01 out. 2007.

NUNES, Luiz Antonio Rizzatto. **Manual da Monografia: como se faz uma monografia, uma dissertação, uma tese**. 2. ed. São Paulo: Saraiva, 2000.