Ataques aos protocolos PKMv1 e PKMv2 em redes WiMAX

Gerson Cristiano Fischer[1], **Charles Christian Miers**[1], **Omir Correia Alves Jr.**[1]

[1]Centro de Ciências Tecnológicas (CCT)
Universidade do Estado de Santa Catarina (UDESC) - Joinville, SC - Brasil

gerson@inbox.com, charles@joinville.udesc.br, omalves@brturbo.com.br

Resumo. *Este artigo tem como objetivo fundamental descrever os problemas de segurança relacionados aos protocolos PKMv1 e PKMv2, devido não somente aos poucos estudos como, também, pelo fato de que o protocolo PKM, sendo o responsável por todo o processo de segurança, acaba tornando-se o alvo de vários tipos de ataques. Entretanto, é necessário, primeiramente, apresentar um resumo sobre o funcionamento do protocolo PKMv1 e, também, mencionar as melhorias, em relação ao protocolo vulnerável PKMv1, com o protocolo atualizado PKMv2.*

1. Introdução

O projeto de redes metropolitanas sem fio em alta velocidade teve início em 2001 com o padrão IEEE 802.16, referenciado como WiMAX (*Worldwide Interoperability for Microwave Access*), pelo órgão IEEE (*Institute Electrical of Electronic and Engineers*). No princípio, o padrão atendia apenas a operação LOS (*Line-Of-Sight*) a uma banda de freqüências de 10-66 GHz, tornando-o uma tecnologia muito limitada. Assim, para suportar novas características foi projetada a versão fixa IEEE 802.16d e homologada em 2004. Dentre estas características, além das já mencionadas no padrão original IEEE 802.16, estão o suporte da operação NLOS (*Non-Line-Of-Sight*) e banda de freqüências de 2-11 GHz. Da mesma forma, limitada a uma tecnologia fixa, no ano seguinte, em 2005, foi apresentada a versão móvel, conhecida como IEEE 802.16e.[Goleniewski and Jarrett 2006]

Com o evolução da comunicação sem fio, no segmento de redes, o fator segurança também tornou-se, na mesma proporção, um conceito de suma importância. Diferente das redes guiadas, que possuem uma infra-estrutura física e limitada, as redes sem fio tornam-se menos seguras pelo simples fato da dificuldade que elas tem em controlar os sinais de rádio que propagam-se no espaço livre. Desse modo, necessita-se ter uma atenção especial na segurança de redes sem fio. [Xu and Huang 2006]

Em uma rede WiMAX, ambas as estações base e assinante podem ser alvos de vários tipos de ataques como, por exemplo, ataques de *replay*. Os padrões IEEE 802.16d/e especificam a mesma subcamada de segurança e que se encontra internamente a camada MAC (*Medium Access Control*). O objetivo desta subcamada de segurança é fornecer o controle de acesso e confidencialidade do canal de dados. Além disso, atua um dos principais componentes de segurança, o protocolo de privacidade e gerenciamento de chave (PKM, *Privacy and Key Management*), que fortalece a distribuição segura de chaves de uma estação base para uma estação assinante específica. [Johnston and Walker 2004]

O protocolo PKM utiliza certificados digitais X.509, algoritmo de chave pública RSA (*Rivest Shamir Adleman*) e algoritmos criptográficos, usados para a troca segura

de chaves entre as estações assinante e base, seguindo o modelo cliente/servidor. As operações do protocolo PKM divide-se em dois sistemas de chaves, primeiro a estação base autentica a estação assinante, estabelecendo uma chave compartilhada AK (*Authentication Key*) via criptografia de chave pública. Conseqüentemente, após a estação assinante ter registrado-se na rede WiMAX, inicia o segundo sistema de chave, responsável pela a chave AK, a qual é usada para estabelecer com segurança a troca de chaves TEK (*Transport Encryption Key*). [IEEE 2004] [IEEE 2005]

Entretanto, o primeiro sistema, etapa de autenticação, constam alguns problemas de segurança como, por exemplo, falta de autenticação da estação base, inexistência de identificadores de testes, entre outros [Xu and Huang 2006]. Visando isso, este artigo propõe um estudo dos problemas de segurança que envolve não somente o protocolo PKMv1, versão original, como também a versão atualizada PKMv2.

Este artigo está organizado através da seção 2, que explicará, resumidamente, os protocolos de privacidade e gerenciamento seguro em redes WiMAX, ou seja, os protocolos PKMv1 e PKMv2. Internamente a está seção, será apresentada a sub-seção 2.1, que detalha todos os problemas relacionados ao protocolo PKMv1. Por fim, a sub-seção 2.2, que apresentará as melhorias de segurança do protocolo PKMv2 como também os problemas de segurança.

2. Protocolos de Privacidade e Gerenciamento Seguro em Redes WiMAX

A subcamada de segurança MAC do padrão IEEE 802.16d especifica para privacidade e gerenciamento seguro de chaves o protocolo PKMv1, cuja função principal é comunicar-se através de mensagens de requisição e resposta entre as estações assinantes (clientes) e base (servidor). [Hardjono and Dondeti 2005]

O protocolo PKMv1 é usado pela estação assinante para obter autorização e material criptográfico (Ex: chaves de cifragem/decifragem) através da estação base e suporta, também, reautorizações e atualizações de chaves periodicamente. Entretanto, se durante a negociação de capacidades, a estação assinante especifica que não há suporte ao protocolo de segurança PKMv1, as etapas de autorização e troca segura de chaves serão ignoradas[1]. [IEEE 2005]

Com o suporte a segurança, o protocolo utiliza certificados digitais X.509 e chaves intermediárias, que asseguram na troca de chaves entre uma determinada estação assinante e uma estação base, seguindo o modelo cliente/servidor. Dessa forma, a estação assinante, como cliente, requisita material criptográfico enquanto que a estação base, como servidor, responde às requisições, garantindo, que as estações assinantes individuais receberão, apenas, o material criptográfico para as quais foram autorizadas. O processo para ter acesso a rede e utilizar os recursos disponíveis é realizado através de duas etapas: fase de autenticação e fase de negociação de chaves. [IEEE 2004]

A fase de autenticação está resumida, essencialmente, na aquisição de uma chave simétrica de autenticação AK de 160 *bits*, conhecida somente entre estações assinante e base autorizadas. Esta chave é gerada independentemente do material criptográfico negociado entre as estação assinante e base visto que, somente, será utilizada para derivar

[1]Essa informação é válida também para o protocolo atualizado PKMv2, utilizado em redes móveis IEEE 802.16e. [IEEE 2005]

as chaves subseqüentes. Além da chave, outras informações também são compartilhadas, conforme é ilustrado na Figura 1. [Hardjono and Dondeti 2005]

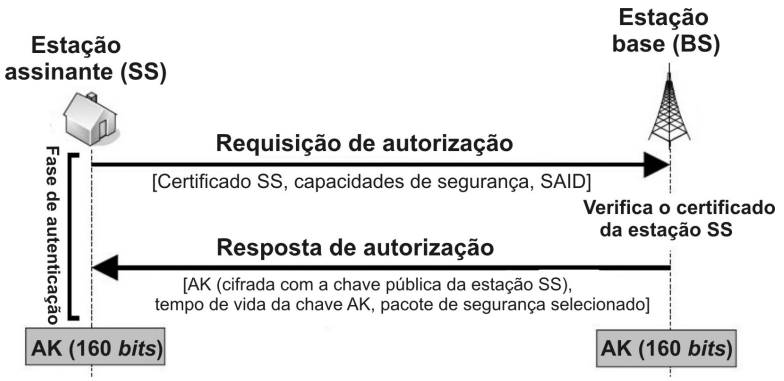

Figura 1. Fase de autenticação pela qual é usada para ter acesso às redes IEEE 802.16d. Adaptado de Hardjono e Dondeti (2005)

A Figura 1 ilustra a etapa inicial de acesso seguro a rede IEEE 802.16d, que inclui na mensagem de requisição (Auth-REQ), o certificado da estação assinante (SS), as capacidades de segurança como, por exemplo, tipos de algoritmos criptográficos suportados e a identificação SAID (*Security Association Identification*), que identifica uma associação segura[2] a qual será utilizada na troca de informações seguras. Entretanto, na mensagem de resposta (Auth-RSP), consta a última etapa da negociação da fase de autenticação, que inclui a chave AK, cifrada pela chave pública da estação assinante (SS), localizado no certificado digital, o tempo de vida da chave AK e o material criptográfico selecionado, baseado nas informações da mensagem Auth-REQ. Uma vez finalizada essa fase, ambas as estações terão uma chave AK e, conseqüentemente, a estação assinante estará autenticada na rede.

Nesta primeira versão do protocolo PKM, apenas a estação base está habilitada a autenticar a estação assinante, isto é, autenticação unilateral. Isso é devido a limitação do próprio protocolo que não suporta autenticação mútua ou bilateral, ou seja, onde ambas as estações assinante e base são autenticadas. [IEEE 2004]

A segunda fase do protocolo PKMv1 estabelece, após a derivação da chave AK, as chaves KEK (*Key Encryption Key*) e HMAC (*Hash Message Authentication Code*). A chave KEK controla com segurança a transmissão da chave TEK à estação assinante, cujo propósito é cifrar e decifrar todo tráfego de dados realizado entre as estações base e assinante. Já a chave HMAC fica responsável juntamente com o seu algoritmo em calcular e verificar a integridade das mensagens de requisição e resposta. O processo ilustrativo dessa fase encontra-se na Figura 2. [Hardjono and Dondeti 2005]

[2] *Security Association* (SA) ou associação segura - É um conjunto de informações de segurança que uma estação base e uma ou várias estações assinantes compartilham como uma forma de suportar uma comunicação segura em uma rede WiMAX. [IEEE 2004]

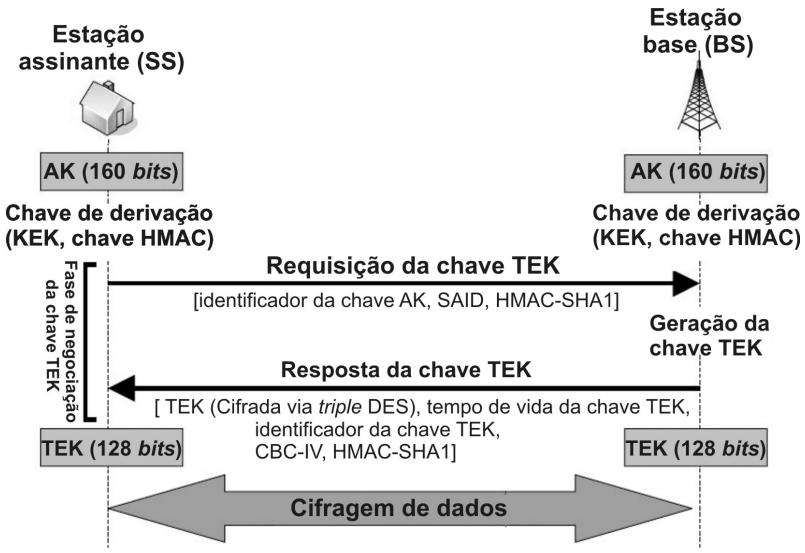

Figura 2. Fase de negociação do material criptográfico utilizado para a transmissão segura das chaves e do tráfego de dados em redes IEEE 802.16d. Adaptado de Hardjono e Dondeti (2005)

Na Figura 2, após finalizada a fase de autenticação, inicia-se a fase de negociação das chaves seguras com envios e recebimentos de mensagens. Nesta fase, para preservar a integridade das mensagens de requisição e resposta, é utilizado o algoritmo de *hash* com chave, identificado por HMAC. Além disso, a estação base, após ter recebida e verificada a integridade da mensagem de requisição, estabelece uma chave TEK com um identificador e um tempo de vida. Entretanto, como se trata de uma chave simétrica, a mesma é então cifrada, neste caso, pelo algoritmo criptográfico *triple* DES através da chave KEK e enviada a estação assinante. Como a estação assinante possui, também, as chaves KEK e HMAC, ela consegue efetuar as operações necessárias para dar início ao processo de cifragem/decifragem de informações.

Além do algoritmo criptográfico *triple* DES que utiliza duas chaves de 64 *bits* no modo EDE *Encryption-Decryption-Encryption*, o protocolo PKMv1 suporta, também, para cifragem/decifragem da chave TEK o algoritmo criptográfico de chave pública RSA com uma chave de 1024 *bits* e o algoritmo AES-ECB (*Advanced Encryption Standard-Electronic CodeBook*) com suporte a chaves de 128 *bits*. [IEEE 2004]

Desse modo, conforme observado, o protocolo PKMv1 estabelece mecanismos de segurança, que integralmente fortalece a privacidade das informações e o gerenciamento seguro de chaves compartilhadas entre as estações base e assinante. Entretanto, traz consigo alguns problemas sérios de segurança que acabam afetando tanto a estação assinante quanto a estação base. Assim, serão apresentados na sub-seção 2.1, principalmente os problemas mais graves como, por exemplo, ausências de autenticação da estação assinante e dos mecanismos de prevenção aos ataques de *replay*

2.1. Problemas de Segurança do Protocolo PKMv1

De acordo com Xu, Matthews e Huang (2006), os maiores problemas de segurança estão relacionados ao ataque de *replay*, que explora as várias vulnerabilidades encontradas no protocolo PKMv1. Os autores acrescentam ainda, “Se as mensagens são transportadas através de um protocolo de autenticação que não emprega identificadores de teste (Ex:

challenge/response), então um atacante pode, facilmente, capturá-las autenticada de uma sessão legítima de autenticação e reusá-las novamente (*replay*) no sistema, sem ser detectado". [XU at el. 2006, pag.2]

Sendo assim, como não há mecanismos de teste nas mensagens de requisição e resposta de autorização SA (fase de autenticação), o protocolo PKMv1, utilizado em redes IEEE 802.16d e opcional em redes IEEE 802.16e, torna-se vulnerável a ataques de *replay*, visto que não há como distingüir uma instância de autorização SA de outra. Além disso, a instância de autorização SA não inclui a identidade (certificado digital) da estação base, então não tem como diferenciar uma estação base autozizada de uma estação base não-autorizada (falsa). Desse modo, as redes IEEE 802.16d/e, que suportam o protocolo PKMv1, podem sofrer ataques de *spoofing* (personificação) e *man-in-the-middle* (homem-no-meio), resultando em conseqüências indesejadas na comunicação legítima de uma rede WiMAX, já que o gerenciamento de todo o tráfego da rede será realizado e manipulado por um atacante, com gerações de chaves falsas, autenticações falsas e, sobretudo, tendo o controle pleno das informações de todas as estações assinantes/bases pertencentes ao domínio daquela estação base falsa. [Xu and Huang 2006]

Além desses ataques, o ataque de negação de serviço (DoS, *Denial of Service*) também pode ser aplicado em redes IEEE 802.16d/e, pois o protocolo PKMv1 está aberto a esse tipo de ataque através de envios simultâneos de mensagens de autenticação rejeitada, parte do processo de autenticação. Por exemplo, no envio de uma mensagem de requisição de autenticação à estação base, o atacante pode capturá-la e enviar diversas mensagens de resposta de autenticação rejeitada, pois não há esquema de verificação de integridade e autenticidade da mensagem. Desso modo, a estação assinante, a cada mensagem de autenticação recebida, precisa aguardar um instante de tempo (característica das redes IEEE 802.16d/e) até voltar a fazer requisições novamente [Xu et al. 2006].

O protocolo PKMv1 suporta, para reautenticação, instantes de tempo de 10, 60 e 600 segundos, sendo que o padrão é 60 segundos [IEEE 2004]. Portanto, a cada mensagem de autenticação rejeitada, a estação assinante terá que aguardar um instante de tempo de 60 segundos até voltar a enviar, novamente, uma nova mensagem de requisição de autenticação. Essa indesejada operação ocorre devido a inexistência de algum meio que identifique a mensagem de resposta como autêntica, que pode ser facilmente solucionado via assinatura digital [Johnston and Walker 2004]. Entretanto, para que seja resolvida essa questão, a estação base precisa, necessariamente, do suporte ao certificado digital composto por um par de chaves pública e privada. [IEEE 2005]

O problema mais sério no protocolo de gerenciamento de chaves (parte do protocolo PKMv1) está no uso do espaço de seqüência de chave TEK. O protocolo identifica cada chave TEK com uma seqüência de números de dois *bits*, reiniciando a seqüência de números de três para zero a cada quatro chaves TEK. Portanto, o protocolo usa essa seqüência de números para distingüir mensagens de ataques de *replay*. Entretanto, se ocorrer com sucesso o ataque de *replay* e se não houver mecanismo que detecte esse tipo de ataque, chaves TEK poderão ser reusadas, expondo quanto a chave TEK quanto as informações compartilhadas entre as estações assinante e base [Barbeau 2005]. O recomendado é expandir o espaço de identificação da chave de 2 *bits* para pelos menos 12 *bits* de modo que não ocorra repetições de identificadores de chave.

2.2. Protocolo PKMv2

Segundo Barbeau (2005), a porção do protocolo PKMv2, que refere-se a autenticação e estabecimento de chaves, teve algumas melhorias com novas propriedades e proteção contra vários tipos de ataques ao protocolo vulnerável PKMv1. Entre essas melhorias, está a adição de valores *nonces* (*challenge/response*) e assinatura digital, o que protege contra os ataques de *replay* e *spoofing*, respectivamente. Essas melhorias, serão apresentadas na Figura 3, como processo de segurança de acesso a rede IEEE 802.16e.

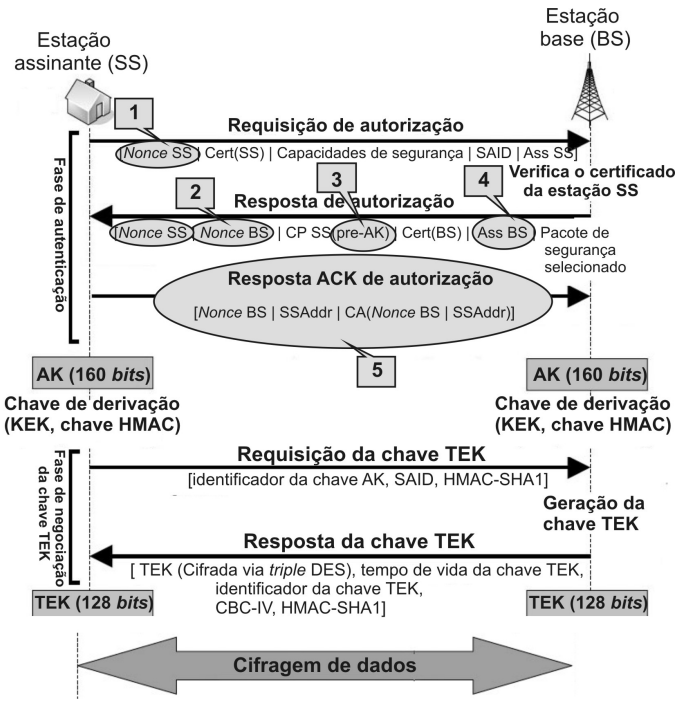

Figura 3. Apresentação de algumas melhorias constatadas no protocolo PKMv2 e utilizadas em redes IEEE 802.16e. Adaptado de Hardjono e Dondeti (2005)

Na Figura 3, ilustra uma comunicação com algumas informações adicionais de segurança, comparado ao protocolo PKMv1, realizada entre as estações assinante e base através do protocolo PKMv2. Entre essas, estão os valores *nonce* SS (1) e *nonce* BS (2) ou *challenge/response*, gerados pelas estações assinante (SS) e base (BS), respectivamente. Além dessa informação, a estação BS, ainda, gera uma chave pre-AK (3), utilizada como uma pré-autenticação, e assina a mensagem de resposta de autorização (4), como uma forma de autenticidade das informações. Por fim, a estação SS responde com uma mensagem ACK de autorização (5), que contém o valor *nonce* BS, gerado pela estação base, o endereço MAC da estação SS (SSAddr) e o valor de verificação da autenticidade da mensagem $CA(nonceBS|SSAddr)$.

Apesar do suporte a autenticação mútua, inserções de valores *challenge/response* nas mensagens de requisição e resposta de autorização SA e de assinatura digital de ambas as estações base e assinante, ainda existe vulnerabilidade no protocolo PKMv2. Segundo Xu e Huang (2006), o atacante pode personificar uma estação assinante legítima (SS) e manipulá-la junto com uma estação base (BS), como meio de ter acesso a rede IEEE 802.16e. Entretanto para isso acontecer, o ataque precisa efetuar alguns passos, conforme é ilustrado na Figura 4. [Xu et al. 2006]

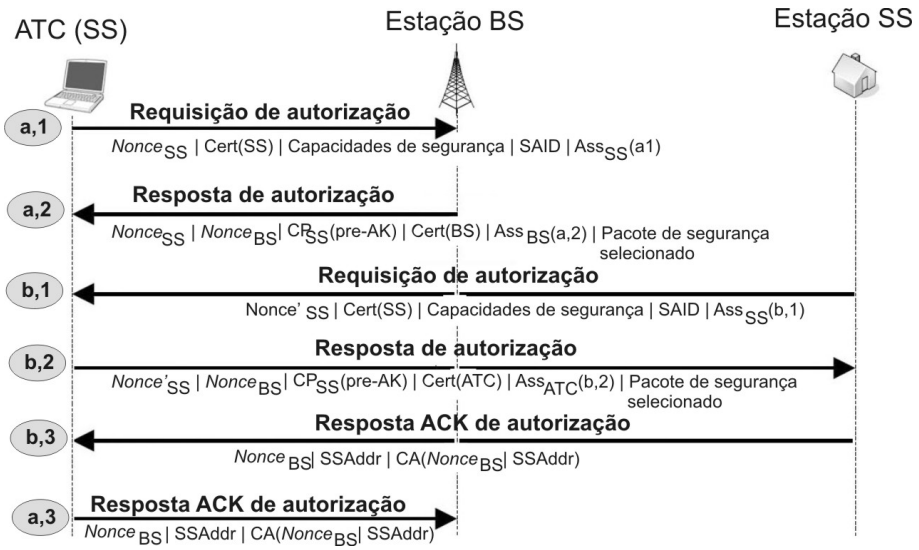

Figura 4. Processo de ataque para ter acesso às redes IEEE 802.16e. Adaptado de Xu e Huang (2006)

Na Figura 4, "a,1" significa mensagem 1 em uma instância do protocolo que executa "a", ATC(SS) representa um atacante personificando a estação SS, $Cert_{(X)}$, o certificado digital de X, $Ass_{(X)}$, a assinatura digital de X, SSID, a identificação do certificado digital da estação SS, $Nonce_{(X)}$, o valor aleatório de X, $CP_{(X)}$, a chave pública de X, SSAddr, o endereço MAC da estação SS e BSAddr, o endereço MAC da estação base. Então, para executar "a", o atacante personifica a estação SS e reusa (*replay*) a mensagem 1 para a estação BS, que é uma cópia de uma mensagem já enviada pela estação SS legítima. No momento que o atacante recebe a mensagem 2 da estação base, é necessário responder com a mensagem 3 para que a autenticação seja efetuada com sucesso. Dessa forma, o atacante pode usar a estação SS, como uma estação intermediária, para responder esse valor *nonce*. Nesse caso, o atacante pode forçar a estação SS executar uma outra instância, chamada de "b" e responder a estação SS com o mesmo valor *nonce* que recebeu da estação BS. Após, a estação SS receber essas informações, a mensagem será autenticada através do valor *nonce* da estação BS e do endereço MAC (SSAddr), enviada ao atacante, que pode, então, encaminhar à estação BS e terminar a instância "a".

Diante desses dois protocolos, PKMv1 e PKMv2, apesar da existência de vulnerabilidades, as redes IEEE 802.16d/e precisam estabelecer meios de autenticação e de cifragem/decifragem das informações, como uma forma de prevenir contra as atividades maliciosas. Sem o acesso a esses protocolos, a rede torna-se aberta para qualquer usuário mal intencionado, o que não é interessante. Portanto, é melhor ter o suporte a um mecanismo de segurança, mesmo sabendo que não é totalmente seguro, do que não ter nenhum mecanismo de proteção.

3. Considerações Finais

Conforme o estudo realizado neste artigo, constatou-se que o protocolo PKMv1 possui diversas vulnerabilidades de nível alto de segurança, ou seja, podem resultar em conseqüências sérias na segurança de uma rede WiMAX como, por exemplo, controle total sobre um conjunto de estações assinantes/bases com a introdução de uma estação base

falsa, pela falta de autenticação da estação base. Além disso, não somente o ataque de personificação (*spoofing*) pode ser aplicado como, também, ataques de negação de serviço e *replay*. Sem nenhum mecanismo de teste, o protocolo fica aberto a ataques de *replay*, fator de extrema gravidade, pois poderá dar acesso não-autorizado a um atacante no sistema, resultando nos acessos aos recursos de forma indevida.

Com o suporte ao certificado digital, acabam minimizando os problemas, visto que há como identificar como autêntica uma estação assinante ou até mesmo uma estação base via protocolo PKMv2. Outra solução, através do certificado digital, é a adição da assinatura digital tanto nas mensagens de requisição quanto nas mensagens de resposta de autorização SA. Dessa forma, previne-se a integridade e a autenticidade da mensagem utilizada no processo. A recomendação para a cifragem da chave TEK é utilizar o algoritmo criptográfico AES, pois o espaço de chaves é maior tornando-o mais resistente a ataques de força bruta comparado ao ao tamanho do espaço de chaves do algoritmo DES.

Já para o protocolo PKMv2, consta menos vulnerabilidades devido as adicões de valores *nonces*, assinatura digital e suporte a autenticação mútua, já que é de suma importância para a prevenção de ataques de personificação. Além disso, é um protocolo recente comparado ao protocolo PKMv1, o que acaba resultando em poucos estudos de segurança. Apesar de haver ainda vulnerabilidades no protocolo PKMv2, o nível de ataque diminui e, conseqüentemente, torna-o mais seguro para atender as redes IEEE 802.16e.

Referências

Barbeau, M. (2005). Wimax/802.16 threat analysis. *1st ACM Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet)*, pages 8–15.

Goleniewski, L. and Jarrett, K. W. (2006). *Telecommunications Essentials: The Complete Global Source*. Addison Wesley, Boston, 2 edition.

Hardjono, T. and Dondeti, L. R. (2005). *Security in Wireless LANs and MANs*. Artech House, Boston.

IEEE (2004). *IEEE Standard for Local and Metropolitan Area Networks, part 16: Air Interface For Fixed Broadband Wireless Access Systems (802.16-2004)*. IEEE Press, New York.

IEEE (2005). *IEEE Standard for Local and Metropolitan Area Networks, part 16: Air Interface For Fixed and Mobile Broadband Wireless Access Systems (802.16-2004)*. IEEE Press, New York.

Johnston, D. and Walker, J. (2004). Overview of ieee 802.16 security. *Security & Privacy Magazine*, 2:40–48.

Xu, S. and Huang, C.-T. (2006). Attacks on pkm protocols of ieee 802.16 and its later versions. Disponível em `http://www.cse.sc.edu/~huangct/PID266938.pdf` [Acesso em 29 julho 2007].

Xu, S., Matthews, M., and Huang, C.-T. (2006). Security issues in privacy and key management protocols of ieee 802.16. *Proceedings of the 44th ACM Southest - ACMSE*.