PROPOSTA PARA MELHORIA DOS MECANISMOS DE SEGURANÇA DE REDES LOCAIS SEM FIO

Gilson Marques da Silva
Curso de Bacharelado em Sistemas de Informação
UNIMINAS
38411-113 – Uberlândia – MG – Brasil
gilson@uniminas.br

João Nunes de Souza
Faculdade de Computação
Universidade Federal de Uberlândia
38400-902 – Uberlândia – MG – Brasil
nunes@ufu.br

RESUMO

Este artigo apresenta uma proposta para melhoria dos mecanismos de segurança implementados em redes locais sem fio. São identificadas as fragilidades associadas aos mecanismos atuais, implementados nos padrões IEEE 802.11 e 802.1X. Também são propostas melhorias que possibilitam a elevação do nível de segurança. É apresentada ainda uma avaliação desta nova proposta.

ABSTRACT

This paper presents a set of proposals to improve the security mechanisms implemented in the wireless local area networks. The fragilities related to the current security mechanisms, implemented in the IEEE 802.11 and 802.1X standards are identified. Also some improvements which possibility rising the security level are proposed. An evaluation of this new propose is still presented.

1 INTRODUÇÃO

As redes locais sem fio têm se tornado, cada vez mais, uma opção para ambientes corporativos; e com isso, os requisitos de segurança são cada vez mais importantes. Acessos indevidos à rede e a leitura ou alteração de dados em trânsito representam uma grande ameaça a estes ambientes.

O padrão IEEE 802.11 (IEEE Std 802.11-1999, 1999), responsável pela definição das redes locais sem fio, agrega alguns mecanismos de segurança, como por exemplo, o protocolo WEP (*Wired Equivalent Privacy*). Além disso, o padrão IEEE 802.1X (IEEE Std 802.1X-2001, 2001) também agrega mecanismos de segurança, não somente às redes locais sem fio, mas a todo o conjunto IEEE 802. No entanto, estes mecanismos e também os mecanismos agregados pelos fabricantes não são considerados eficazes face aos atuais requisitos de segurança. Certamente, por estes e por outros motivos, o IEEE está trabalhando na evolução deste padrão através do grupo 802.11i que deve ser publicado ao final de 2003.

Este artigo apresenta uma proposta para melhoria dos mecanismos de segurança das redes locais sem fio. É considerada também uma avaliação da proposta em um ambiente corporativo.

Uma das premissas utilizadas nesta proposta é a compatibilidade com o padrão IEEE 802.11. Os mecanismos propostos podem ser implementados sem desrespeitar o padrão. Além disso, a proposta é compatível com o *hardware* atualmente utilizado na maioria dos ambientes, o que proporciona menos investimento e mais benefício.

Outro artigo que trata deste assunto, escrito pelos mesmos autores aborda a mesma questão, porém de maneira menos detalhada e em estágio mais inicial (Silva e Souza, 2003) .

A seção 2 apresenta uma visão geral do padrão IEEE 802.11. A seção 3 apresenta os mecanismos de segurança do IEEE 802.11 e suas fragilidades. A seção 4 considera a segurança agregada pelos fabricantes de equipamentos para redes locais sem fio e suas fragilidades. A seção 5 apresenta os mecanismos de segurança inseridos pelo padrão 802.1X e também apresenta suas fragilidades. As fragilidades de administração são apresentadas na seção 6. Em seqüência a seção 7 apresenta uma proposta para melhorar o nível de segurança de redes locais sem fio, observando todas as fragilidades identificadas nas seções anteriores. Na seção 8 os aspectos que levam a redução das fraquezas do protocolo WEP são apresentados. A seção 9 apresenta a proposta de um processo de revogação de chaves. Na seção 10 o formato dos quadros de rede e suas mensagens são definidos. Finalmente a avaliação da proposta é trabalhada na seção 11.

2 UMA VISÃO GERAL DO PADRÃO IEEE 802.11

O IEEE 802.11 é um padrão para as redes locais sem fio em todos seus aspectos, incluindo mecanismos de controle de acesso, confidencialidade e integridade.

O padrão define três fases pelas quais qualquer cliente deve passar com sucesso, antes de obter acesso à rede sem fio. A figura 1 ilustra estas 3 fases. Ela apresenta um esquema da conexão à rede local sem fio, incluindo as fases de sondagem, autenticação e associação. Cada seta para a direita representa a transmissão dos dados nela nomeados do cliente para o ponto de acesso, e cada seta para a esquerda representa uma transmissão dos dados nela nomeados do ponto de acesso para o cliente. No caso do exemplo ilustrado na figura 1, o padrão IEEE

802.11 é utilizado com o algoritmo SKA (*Shared Key Authentication*) e dois mecanismos adicionais: o SSID (*Service Set Identifier*) e a filtragem de endereços MAC (*Medium Access Control*). Estes mecanismos são detalhados nas seções 3 e 4.

As fases de conexão são:

Fase de sondagem – O cliente envia requisições de acesso pelo ar. Em seguida, todos os pontos de acesso que estiverem na área de cobertura respondem com informações que podem ser utilizadas nas fases de autenticação e associação. A fase de sondagem é indicada na figura 1 pelas três primeiras linhas.

Fase de autenticação – Existem dois tipos de autenticação definidos no padrão; *Open Systems Authentication* (OSA) e *Shared Key Authentication* (SKA). A configuração do ponto de acesso e a indicação do cliente definem qual esquema é utilizado. Estes dois protocolos são detalhados na seção 3. A fase de autenticação é indicada na figura 1 pelas linhas de ordem quatro a onze.

Fase de associação – O cliente, já autenticado e de posse das informações recebidas na fase de sondagem, envia uma requisição de associação para o ponto de acesso escolhido. O ponto de acesso retorna uma resposta contendo o identificador da associação que pode ser utilizado para pedidos de reassociação ou desassociação. Esta fase é indicada na figura 1 pelas duas últimas linhas.

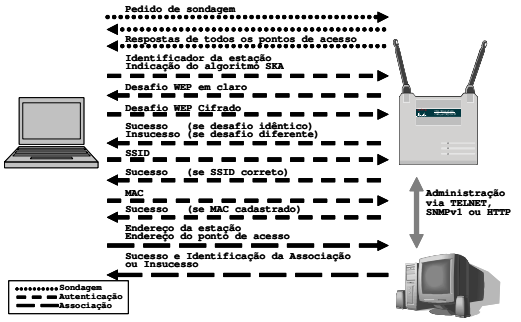

Fig. 1 - Conexão a rede local sem fio, padrão 802.11.

O padrão IEEE 802.11 utiliza o protocolo WEP para garantir a confidencialidade dos dados no ar. A integridade é garantida pelo uso de um algoritmo redundante do tipo CRC32 (*Cyclic Redundancy Check*), denominado ICV (*Integrity Check Value*), conforme mostrado em (Peres e Weber, 2003).

O protocolo WEP, por sua vez, é baseado no protocolo *stream cipher* RC4. Ele é considerado vulnerável, pois apresenta falhas na programação de chaves, no algoritmo KSA (*Key Scheduling Algorithm*) (Fluhrer, Mantin, e Shamir), que trata a questão de reuso de *key-stream*. Estudos sobre as fraquezas do protocolo WEP são apresentados em (Arbaugh, Wan e Shankar, 2001) e (Roshan, 2002).

3 MECANISMOS DE SEGURANÇA DO PADRÃO IEEE 802.11 E SUAS FRAGILIDADES

O padrão IEEE 802.11 considera o controle de acesso à rede, a confidencialidade e integridade dos dados. Ele propõe um modelo de acesso baseado nas três fases apresentadas na seção 2. Como os mecanismos de segurança estão implementados na fase de autenticação, este artigo analisa esta fase em mais detalhes. O padrão permite dois tipos de autenticação:

OSA (*Open System Authentication*) – Neste protocolo toda negociação é feita em texto claro e nenhuma condição é imposta, ou seja, todos clientes que solicitam a autenticação são autenticados. Basicamente é uma autenticação nula e pode ser utilizada em redes de acesso público.

SKA (*Shared Key Authentication*) – Neste tipo de autenticação, o ponto de acesso, normalmente denominado por AP (*Access Point*), envia um desafio em texto claro para o cliente. O cliente deve cifrar o desafio com o protocolo WEP, utilizando uma chave de sessão pré-compartilhada, e depois deve enviá-lo novamente ao ponto de acesso. O ponto de acesso verifica se a resposta ao seu desafio está correta. Estes passos estão ilustrados nas quatro primeiras linhas da fase de autenticação da figura 1.

Uma deficiência neste processo de autenticação é que apenas o cliente é autenticado, não existe a autenticação do ponto de acesso perante o cliente.

O padrão IEEE 802.11 utiliza o atributo SSID (*Service Set Identifier*) como um identificador para a rede. Ele é transmitido periodicamente por *broadcast*, em texto claro. Isto permite que qualquer cliente o capture, através da escuta em modo simples na rede sem fio, e o use quando necessário. Assim sendo, o SSID não é considerado um mecanismo eficaz de segurança quando implementado desta forma.

Neste contexto existe a possibilidade de mapeamento da rede. Tal mapeamento possibilita que os *war drivers* (Etter, 2002) tenham sucesso ao identificar e conseguir informações sobre redes sem fio. Isto pode ser feito, por exemplo, dirigindo-se um automóvel pela rua equipado com um receptor e algum software instalado em um *notebook*.

Como na fase de sondagem os pontos de acesso respondem a qualquer solicitação de informação, a tarefa de mapear a rede fica simples e direta, pois qualquer cliente pode obter informações a partir da solicitação direta aos pontos de acesso. Além disso, como o SSID é enviado em texto claro e por *broadcast* sua leitura também torna-se direta.

São apresentadas a seguir algumas conclusões sobre a efetividade dos mecanismos de segurança identificados neste artigo.

No algoritmo OSA não existe qualquer tipo de controle de acesso. Logo, considerar as fragilidades deste esquema não faz sentido. Neste cenário a rede é considerada como pública, pois oferece acesso a qualquer cliente que esteja em sua área de cobertura.

Por outro lado, quando o algoritmo SKA é utilizado, existe uma validação por desafio/resposta utilizando o protocolo WEP. Neste caso, o desafio é enviado em texto claro e pode ser capturado por qualquer cliente que esteja coletando os pacotes na rede de forma promíscua. A resposta ao desafio, embora cifrada, também pode ser capturada. Logo, de posse do texto em claro e do texto cifrado, através de operações de ou-exclusivo, tem-se acesso ao *key-stream*. Este é o primeiro passo para a leitura de dados confidenciais e para a quebra da chave WEP, conforme descrito em (Roshan, 2002).

Outro problema, como já mencionado, é a falta de autenticação do ponto de acesso. É totalmente viável que o invasor insira um ponto de acesso para que este se passe por um dos pontos de acesso legítimos da rede. Neste caso, o único objetivo deste falso ponto de acesso é capturar credenciais de acesso e outras informações que deveriam ser confidenciais.

Este esquema de comunicação não impede ataques criptográficos do tipo homem-do-meio (*man-in-the-middle*) (Stallings, 1998). Um intruso pode capturar as credenciais de um cliente e se passar por ele. Da mesma forma o intruso pode se passar por um ponto de acesso.

Várias ferramentas de auditoria e ataques existem. A grande maioria delas têm distribuição *freeware*, e estão disponíveis na Internet juntamente com receitas de como proceder em ataques a estes ambientes. Muitas destas ferramentas são descritas em (Peikari e Fogie, 2003).

4 MECANISMOS DE SEGURANÇA AGREGADOS PELOS FABRICANTES E SUAS FRAGILIDADES

Os principais fabricantes de equipamentos para redes locais sem fio, face às necessidades de segurança do mercado, estão antecipando-se aos padrões e agregando novos mecanismos de segurança aos seus equipamentos. Entretanto nem sempre tais mecanismos são eficazes (Arbaugh, Wan e Shankar, 2001).

O primeiro mecanismo é denominado "rede fechada" onde não se transmite o SSID por *broadcast.* O SSID é utilizado como uma senha simples, necessária no processo de autenticação. Neste caso, o cliente é solicitado a informar o SSID correto como uma das etapas do processo de autenticação.

Quando um cliente legítimo percorre o processo de autenticação, de acordo com a figura 1, ele envia o SSID em texto claro, o que possibilita sua captura e posterior utilização. Desta maneira o SSID não agrega muito ao nível de segurança do sistema.

Outro mecanismo considerado é a filtragem de endereços MAC. Como mais uma etapa no processo de autenticação, o endereço MAC do cliente é verificado contra uma base de endereços MAC autorizados. Esta base pode ser armazenada em cada ponto de acesso ou de forma centralizada, em um servidor RADIUS (*Remote Authentication Dial-In User Service*).

Embora pareça, a filtragem MAC não é a solução para os problemas de acesso indevido às redes locais sem fio. Como os endereços MAC podem ser falsificados e alterados com facilidade, um invasor pode capturar um endereço MAC cadastrado através da captura de pacotes na rede. Em seguida ele pode alterar o endereço MAC de sua interface de rede para o endereço MAC capturado, obtendo assim acesso à rede.

5 MECANISMOS DE SEGURANÇA DO PADRÃO IEEE 802.1X E SUAS FRAGILIDADES

O padrão IEEE 802.1X prevê o controle de acesso por porta para toda a família IEEE 802 e também pode ser utilizado para as redes locais sem fio. Porém existe uma grande diferença entre as redes locais sem fio e as demais redes cabeadas da família 802. Nas redes cabeadas a ligação entre o cliente e sua porta de acesso é definida por um cabo fisicamente conectado às duas partes e no caso das redes locais sem fio, esta ligação é o ar. Assim sendo, o padrão falha justamente em não se preocupar com os aspectos de segurança nesta parte da conexão, sendo possível a captura, adulteração e repetição de pacotes de validação. Em (Mishra e Arbaugh, 2002) é feita uma análise dos aspectos de segurança do 802.1X onde são exibidas algumas possibilidades de ataques contra o padrão.

O padrão IEEE 802.1X considera um autenticador no processo de autenticação. O ponto de acesso pode tornar-se um repassador de pacotes de autenticação já que toda a base é armazenada no autenticador. O autenticador pode ser definido no próprio ponto de acesso ou em servidores especializados, como por exemplo, servidores RADIUS. As atuais soluções de mercado não têm optado pela implementação desta funcionalidade nos equipamentos, mas sim em servidores, na maioria dos casos servidores RADIUS.

A validação de usuário e senha através do protocolo RADIUS pode ser realizada de várias maneiras, como mostrado em (ORiNOCO, 2003). Neste caso, quando utilizada sem mecanismos adicionais de cifragem, as credenciais do usuário trafegam entre o cliente e o ponto de acesso em texto claro, pois o protocolo RADIUS é implementado

entre o ponto de acesso e o autenticador. Neste trecho, as credenciais estão protegidas pela chave do próprio protocolo RADIUS.

Quando as credenciais trafegam em claro pela rede elas podem ser facilmente capturadas no ar e oportunamente utilizadas. No entanto, mesmo quando recursos adicionais protegem estas credenciais, ainda existem problemas. Isto ocorre porque ainda é possível capturar tais credenciais e mesmo sem poder interpretá-las, o invasor pode utilizá-las oportunamente, de modo a fornecer acesso ao sistema, caracterizando um ataque por repetição ou do tipo homem-do-meio.

O padrão 802.1X pode ser utilizado para a distribuição automática de chaves de sessão, que são utilizadas entre o cliente e o ponto de acesso. Esta funcionalidade elimina os riscos associados ao uso de chave pré-compartilhada e diminui os perigos advindos das fragilidades do protocolo WEP. Entretanto, para ser eficaz, o mecanismo de troca de chave de sessão deve estar associado a processos de reautenticação, com geração e distribuição de novas chaves de forma periódica. Infelizmente na maioria das implementações comerciais esta funcionalidade não é implementada desta forma.

Neste contexto se o invasor consegue credenciais válidas para autenticação, ele pode receber uma chave de sessão sem maiores dificuldades. E ainda, se o processo não estiver protegido por outros algoritmos, como o MD5 (*Message Digest* 5) (Ferguson e Schneier, 2003), a chave de sessão pode ser capturada quando estiver em trânsito entre o ponto de acesso e o cliente.

6 ADMINISTRAÇÃO E GERÊNCIA DOS PONTOS DE ACESSO E SUAS FRAGILIDADES

O padrão IEEE 802.11 é omisso quanto à forma de administração dos pontos de acesso. Neste caso, cada fabricante determina um tipo de acesso e interface em seu equipamento para que este possa ser administrado e gerenciado.

A maioria dos equipamentos disponíveis no mercado é administrada remotamente via rede. Tais equipamentos podem ser configurados para permitir sua administração via interfaces sem fio ou por aquelas conectadas à rede cabeada, quando existentes. Uma deficiência de tais esquemas é que freqüentemente são utilizados protocolos sem funcionalidades de confidencialidade. Exemplos incluem o TELNET, SNMPv1 (*Simple Network Management Protocol version 1*) e HTTP (*Hypertext Transfer Protocol*). Nenhum destes protocolos provê cifragem dos dados. Logo, propiciam a um invasor a possibilidade de captura do tráfego de administração. A partir deste tráfego, é possível a extração de chaves definidas, credenciais para administração e gerência dos equipamentos, além de outros detalhes da rede.

Protocolos que oferecem a cifragem dos dados transmitidos devem ser adotados para as comunicações de administração e gerência. Exemplos destes protocolos são o SSH (*Secure Shell*), SNMPv3 (*Simple Network Management Protocol version 3*) e HTTPS (*HyperText Transfer Protocol Secure*).

7 PROPOSTA DE MELHORIA DO NÍVEL DE SEGURANÇA DAS REDES LOCAIS SEM FIO

Esta seção apresenta uma proposta para melhorar os mecanismos de segurança das redes locais sem fio. Esta proposta pode ser considerada uma extensão do padrão IEEE 802.11, já que é compatível com as premissas e protocolos atualmente utilizados. Logo, sua implementação pode ser adotada sem a necessidade de expansão do *hardware* dos atuais equipamentos. Além disso, não é necessário o desenvolvimento ou agregação de novas funcionalidades, como por exemplo, novos algoritmos criptográficos, funções *hash* e outras.

A figura 2 apresenta um esquema de conexão à rede local sem fio, incluindo a fase de sondagem, autenticação e associação de acordo com a proposta. Sua interpretação é análoga a da figura 1 e é analisada nas seções seguintes.

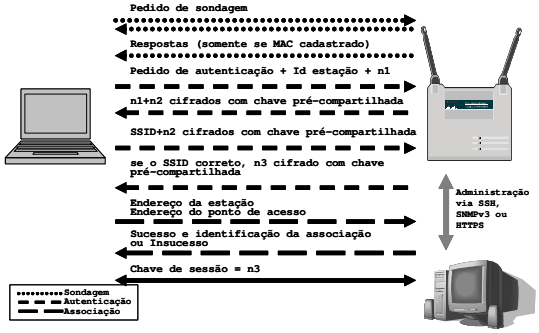

Fig. 2 - Conexão a rede local sem fio, segundo a proposta.

7.1 Fase de Sondagem

Esta seção apresenta mecanismos que dificultam o mapeamento da rede na fase de sondagem. Estes mecanismos se fundamentam na filtragem MAC.

Na proposta apresentada, o mapeamento da rede, por um intruso, é dificultado considerando a verificação do endereço MAC durante a fase de sondagem. Nesta fase o endereço MAC do cliente é verificado contra uma base de endereços MAC cadastrados. Caso o endereço MAC do cliente não esteja armazenado na base, o ponto de acesso fica mudo e não transmite resposta alguma. Assim a descoberta de uma rede sem fios é dificultada. Atualmente, os produtos que disponibilizam algum tipo de filtragem MAC consideram a filtragem em

fases subseqüentes a de sondagem. Logo, mesmo tendo o acesso à rede negado, o invasor tem a chance de capturar dados sobre a rede.

Mesmo considerando os pontos citados, é possível que a filtragem MAC não seja adotada. Em redes grandes e dinâmicas o custo de administração da base de endereços MAC deve ser observado.

O problema da captura e falsificação de um endereço MAC cadastrado continua existindo. No entanto, esta medida evita que *war drivers* e usuários comuns usem o software de suas interfaces de rede sem fio para mapear a rede. Entretanto, isto não confere a rede, segurança diante de usuários mais experientes e determinados a mapeá-la. Logo, este não é um mecanismo eficaz contra a falsificação ou clonagem de endereços MAC. Este mecanismo apenas dificulta o mapeamento da rede.

7.2 Fase de Autenticação

A proposta apresentada neste artigo também previne a captura do SSID na fase de autenticação. No esquema convencional o SSID trafega em claro quando enviado do cliente para o ponto de acesso. Isto permite que seja facilmente capturado e posteriormente utilizado.

No esquema desta proposta o SSID é transmitido concatenado a um número pseudo-aleatório e de forma cifrada pelo algoritmo WEP. Assim, a leitura do SSID fica impossibilitada devido à criptografia e mesmo se o pacote for capturado para posterior utilização, o ataque não terá sucesso devido ao número pseudo-aleatório que está concatenado ao SSID.

A partir do pacote cifrado, não é viável a separação das duas partes sem o uso da chave adequada. A correlação entre o desafio e a resposta não pode ser feita já que em cada um destes pacotes existe um número pseudo-aleatório diferente, concatenado aos valores do desafio e da resposta. Este processo é ilustrado nas quatro primeiras linhas da fase de autenticação da figura 2.

Outro mecanismo proposto é a redução da quantidade de tráfego protegido pela chave pré-compartilhada. Considera-se o uso de uma chave pré-compartilhada que é utilizada somente no processo de autenticação. Observa-se que no padrão IEEE 802.11 a chave pré-compartilhada é utilizada no processo de autenticação e também para prover a confidencialidade dos dados no ar.

Nesta proposta a chave pré-compartilhada somente é utilizada para autenticar o cliente, autenticar o ponto de acesso e distribuir novas chaves de sessão. Logo, uma quantidade bem menor de tráfego é cifrada com esta chave. Desta forma, os ataques citados em (Roshan, 2002) contra o protocolo WEP tornam-se inviáveis devido à quantidade pequena de dados que trafegam sob a proteção da chave pré-compartilhada.

O processo de autenticação tem dois propósitos: autenticar o cliente perante o ponto de acesso e autenticar o ponto de acesso perante o cliente. Da mesma maneira que não se deseja que clientes quaisquer tenham acesso à rede, também se deseja que nenhum ponto de acesso clandestino possa fazer parte dela.

No primeiro passo o pedido de autenticação é enviado do cliente para o ponto de acesso. O identificador da estação é concatenado ao pedido, juntamente com um primeiro número pseudo-aleatório (n1) gerado pela estação. Todas estas informações são transmitidas em claro. O número gerado funciona como o desafio que deve ser cifrado pelo ponto de acesso e devolvido ao cliente para verificação.

No entanto para que n1 não possa ser correlacionado com a resposta do desafio, o ponto de acesso gera um novo número pseudo-aleatório(n2). Este número funciona como o desafio para o cliente. Logo, n1 e n2 são concatenados e cifrados com a chave pré-compartilhada. Em seguida este conjunto é enviado do ponto de acesso para o cliente.

O cliente ao receber o conjunto, deve decifrá-lo e verificar se o desafio (n1) que emitiu está correto. Em seguida o cliente responde ao desafio lançado pelo ponto de acesso. Cifrando e enviando n2 de volta. No entanto o pacote é aproveitado para o envio do SSID. Este valor também é validado pelo ponto de acesso. O conjunto, n2+SSID, é cifrado pela chave pré-compartilhada e enviado do cliente para o ponto de acesso. Ao receber o conjunto, o ponto de acesso verifica o desafio que lançou ao cliente (n2) e verifica também o SSID. Se tanto n2 quanto o SSID estiverem corretos o ponto de acesso envia uma resposta positiva ao cliente. Nesta resposta segue um terceiro número pseudo-aleatório (n3), gerado pelo ponto de acesso. Este número é utilizado como chave de sessão para garantir a confidencialidade dos dados. Esta chave é utilizada até que seja revogada ou até que haja um processo de reautenticação.

O primeiro número pseudo-aleatório (n1), gerado pelo cliente, é utilizado no processo de autenticação do ponto de acesso. Isto evita que um cliente legítimo possa se conectar a um ponto de acesso inserido maliciosamente, com o propósito de capturar as credenciais de acesso.

O segundo número pseudo-aleatório (n2), gerado pelo ponto de acesso, é utilizado no processo de autenticação do cliente. Isto permite que seja verificado se o cliente conhece a chave pré-compartilhada e se tem a habilidade de utilizá-la de forma correta.

Estas autenticações ocorrem em esquema de desafio/resposta. No entanto, os dados não trafegam isoladamente e nem em claro. Assim, evita-se que o *key-stream* possa ser derivado do desafio e da resposta. Os dois campos somente podem ser

correlacionados se não tiverem outras informações agrupadas.

A filtragem MAC, definida na fase de sondagem, é considerada como uma pré-autenticação. Logo passos adicionais são eliminados na fase de autenticação.

7.3 Processo de Reautenticação

O processo de reautenticação é muito similar ao processo de autenticação. No entanto, o processo de reautenticação é iniciado pelo ponto de acesso que é responsável por controlar os períodos de reautenticação. Primeiramente o cliente é autenticado e em seguida o ponto de acesso, ao contrário do processo de autenticação. O processo de reautenticação é exibido na figura 3.

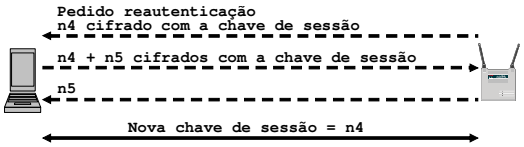

Fig. 3 - Processo de Reautenticação.

Outra grande diferença está na chave utilizada para a troca das informações. Enquanto o processo de autenticação utiliza a chave pré-compartilhada, o processo de reautenticação utiliza a chave de sessão até então utilizada. Esta chave ainda é segura, desde que não tenha sido revogada.

O ponto de acesso, ao requisitar a reautenticação, envia um número pseudo-aleatório n4, cifrado pela atual chave de sessão. Este número deve ser decifrado pelo cliente que o concatena a um segundo número gerado. As duas informações são concatenadas, cifradas pela chave de sessão e depois enviadas ao ponto de acesso. O ponto de acesso verifica que o cliente conseguiu responder o desafio lançado, e recebe um novo desafio (n5) que deve ser decifrado e devolvido para o cliente. Neste caso, não há a necessidade de que este número seja cifrado, já que não pode ser correlacionado ao pacote anterior e não precisa ser mantido confidencial.

7.4 Processo de Desautenticação

O processo de desautenticação é iniciado pelo cliente. O objetivo é encerrar sua participação na rede. Esta notificação é muito importante para evitar que outros clientes tentem se passar pelo cliente que deixa a rede. Isto seria um ataque do tipo seqüestro de sessão. Este processo é mostrado na figura 4.

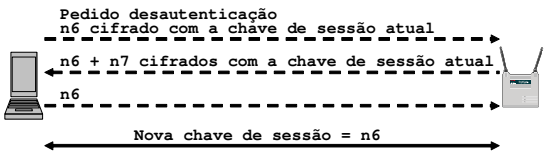

Fig. 4 - Processo de Desautenticação.

Um número pseudo-aleatório (n6) é gerado pelo cliente cifrado pela chave de sessão em uso e enviado junto com a identificação do pedido de desautenticação ao ponto de acesso. Este é o desafio que autentica o ponto de acesso perante o cliente. O ponto de acesso ao receber o número concatena este a um outro número (n7) gerado pelo ponto de acesso que é utilizado para autenticar o cliente. Este conjunto de informações é cifrado com a chave de sessão e enviado novamente ao cliente. O cliente verifica o desafio lançado ao ponto de acesso (n6). Para finalizar o processo, o cliente deve responder ao desafio lançado pelo ponto de acesso (n7), devolvendo em texto claro a resposta ao desafio. Conforme indicando anteriormente não é necessário que esta última resposta seja protegida quanto a confidencialidade.

8 REDUÇÃO DOS EFEITOS DAS FRAQUEZAS DO PROTOCOLO WEP

Esta seção apresenta mecanismos que reduzem os efeitos das fraquezas do protocolo WEP. Isto é conseguido através da distribuição e uso de chaves de sessão de forma periódica e dinâmica.

Um processo de distribuição dinâmica de chaves de sessão é adicionado ao final da fase de autenticação. O processo consiste na transmissão de mais um número pseudo-aleatório gerado pelo ponto de acesso. Este número passa a ser utilizado como chave de sessão. Esta chave de sessão garante a confidencialidade dos dados trafegados na rede.

Uma nova chave de sessão é gerada e distribuída a cada processo de reautenticação, que ocorre periodicamente. Neste caso os dados estão protegidos, pois mesmo se a chave WEP for quebrada, a chave revelada não estará mais em uso.

O processo de quebra da chave WEP somente é viável após a coleta de uma certa quantidade de tráfego. Assim, o período de reautenticação deve ser menor que o período necessário para a coleta desta quantidade de tráfego. Este tempo depende da quantidade de tráfego sendo transmitido na rede e da velocidade de transmissão dos equipamentos. O período para a reautenticação deve ser definido de acordo com a carga da rede, quanto maior a carga menor o tempo de reautenticação. Alguns parâmetros de carga são considerados em (Mahan, 2001). Além disso, a seção 11.2 apresenta os cálculos dos períodos de reautenticação utilizados na avaliação desta proposta.

Este processo de geração e distribuição da chave de sessão é apresentado na última linha da fase de autenticação da figura 2 e também na figura 3.

9 REVOGAÇÃO DE CHAVES DE SESSÃO

Esta seção apresenta mecanismos que possibilitam a revogação de chaves de sessão em uso. Estas chaves são revogadas quando são consideradas comprometidas ou inseguras.

O administrador, ao considerar uma chave comprometida, pode revogá-la. Para isso, o administrador deve iniciar o processo através do ponto de acesso. Este processo é muito similar às últimas etapas da fase de autenticação, já que tanto o ponto de acesso quanto a estação são novamente autenticados. A autenticação é realizada com base na chave pré-compartilhada e não na chave de sessão comprometida.

Assim que a estação e o ponto de acesso estão autenticados, o número que foi gerado pelo ponto de acesso passa a ser utilizado como a nova chave de sessão.

O processo de revogação de chaves é apresentado na figura 5. Ele segue o mesmo modelo que o processo de reautenticação. No entanto, como a chave de sessão em uso foi considerada insegura, esta não deve ter qualquer participação no processo. O uso da chave considerada insegura pode comprometer a segurança, permitindo ao atacante o acesso à nova chave de sessão.

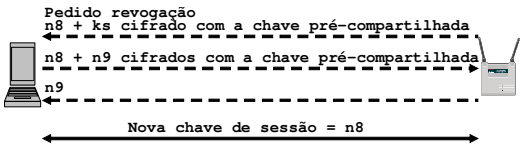

Fig. 5 - Processo de Revogação de Chaves.

O ponto de acesso é responsável pelo início do processo. No primeiro passo o ponto de acesso envia um número pseudo-aleatório (n8) concatenado a atual chave de sessão. Este conjunto é cifrado com a chave pré-compartilhada que ainda é mantida em segurança. O número enviado (n8) é o desafio ao cliente no processo de validação. O cliente ao receber os dados e decifrá-los, consegue, separar e identificar a chave a ser revogada e responder o desafio lançado. Como resposta ao desafio e também já lançando o desafio ao ponto de acesso, o cliente concatena o número recebido a um novo número pseudo-aleatório (n9). O conjunto é cifrado com a chave pré-compartilhada e enviado ao ponto de acesso. O ponto de acesso ao decifrar o conjunto, pode verificar o desafio que antes lançou ao cliente e deve ainda responder ao seu desafio. Pelos mesmos motivos citados anteriormente, observa-se que esta resposta não precisa ser cifrada. A nova chave de sessão é o primeiro número enviado do ponto de acesso ao cliente.

10 FORMATO DOS QUADROS DE REDE

Esta seção apresenta o formato do pacote MAC utilizado no padrão IEEE 802.11 adaptado à proposta deste artigo. Os pacotes e mensagens de cada processo também são apresentados de forma que possam ser transportados em um pacote MAC definido pelo padrão.

O esquema do pacote MAC é apresentado na figura 6. O tamanho deste quadro pode variar entre 34 e 2346 bytes. Esta variação ocorre justamente pelos dados que o quadro pode transportar. O cabeçalho MAC utiliza 30 bytes e um campo FCS (*Frame Check Sequence*) ocupa 4 bytes. O campo de dados, chamados de *frame body* pode ocupar até 2312 bytes.

Frame Control	Duration ID	Address 1	Address2	Address3	Sequence Control	Address4	Frame Body	FCS
2	2	6	6	6	2	6	0-2312	4

Fig. 6 – Formato do Quadro MAC.

Cada uma das mensagens existentes em cada um dos processos, são transportadas por um quadro nesta estrutura. Na seqüência, a estrutura dos processos de autenticação, reautenticação, revogação e desautenticação são apresentados de modo a se encaixarem no *frame body* de um quadro.

Dentro do campo de dados do pacote MAC, existe mais um nível de estruturação, onde existem três campos de tamanho fixo e um último de tamanho variável. O esquema deste sub-quadro é apresentado na figura 7.

Alg. Number	Seq. Number	Status Code	Text
2	2	2	7-14

Fig. 7 – Formato do *Frame Body*.

O campo *Algorithm Number* indica o tipo de processo que está sendo transportado. O campo *Sequence Number* indica a seqüência daquela mensagem dentro do processo. O campo *Status Code* indica um estado associado ao processo. Os possíveis valores deste campo podem ser consultados em (IEEE Std 802.11-1999, 1999). O campo *Text* transporta os dados propriamente ditos.

A seguinte relação pode ser utilizada para o campo *Algorithm Number*:

0 ➔ Autenticação padrão OSA
1 ➔ Autenticação padrão SKA
2 ➔ Reautenticação
3 ➔ Revogação
4 ➔ Desautenticação

Os possíveis valores para os campos *Sequence Number* e *Text* são detalhados em separado para cada processo, nas tabelas 1, 2, 3 e 4. Vale notar que o tamanho do campo *Text* é apresentado em bits e o tamanho total do pacote é apresentado em bytes.

Nas tabelas a seguir, E_{ks} indica um processo de cifragem (*Encryption*) com a chave secreta ks (chave de sessão) e E_{kc} indica um processo de cifragem com a chave secreta kc (chave pré-compartilhada). O número 34 no campo Total é o tamanho total do cabeçalho mais FCS do pacote MAC. O número 6 é o total do cabeçalho do *frame-body*. O número 7 ou 14 é o tamanho do campo *Text*.

Tabela 1 – Processo de Autenticação.

Seq. Number	Text	Tam. bits	Total Bytes
1	n1	128	34+6+07=**47**
2	E_{kc}(n1+n2)	256	34+6+14=**54**
3	E_{kc}(SSID+n2)	160	34+6+12=**52**
4	E_{kc}(n3)	128	34+6+07=**47**

Tabela 2 – Processo de Reautenticação.

Seq. Number	Text	Tam. bits	Total Bytes
1	E_{ks}(n1)	128	34+6+07=**47**
2	E_{ks}(n1+n2)	256	34+6+14=**54**
3	n2	128	34+6+07=**47**

Tabela 3 – Processo de Desautenticação.

Seq. Number	Text	Tam. bits	Total Bytes
1	E_{ks}(n1)	128	34+6+07=**47**
2	E_{ks}(n1+n2)	256	34+6+14=**54**
3	n2	128	34+6+07=**47**

Tabela 4 – Processo de Revogação de Chaves.

Seq. Number	Text	Tam. bits	Total Bytes
1	E_{kc}(n1+ks)	128	34+6+07=**47**
2	E_{kc}(n1+n2)	256	34+6+14=**54**
3	n2	128	34+6+7=**47**

11 AVALIAÇÃO DA PROPOSTA

Esta seção apresenta uma avaliação desta proposta. O objetivo é avaliar o desempenho da rede face aos controles adicionados. Além do incremento de tráfego, o cálculo do período de reautenticação é feito com base na carga, número e tamanho de pacotes.

11.1 Overhead de Banda Inserido

Esta proposta tem um incremento de banda quando comparada com a estrutura do padrão IEEE 802.11. Em especial, pelo fato do padrão não contemplar as mensagens de reautenticação. A tabela 5 apresenta o incremento em bytes de cada um dos processos. No caso dos processos de autenticação e desautenticação o incremento também é exibido em porcentagem. Os processos de reautenticação e revogação não podem ser considerados na comparação pois eles não são implementados no padrão IEEE 802.11.

Tabela 5 - Tamanho de Processos no Padrão e na Proposta.

Fase	IEEE 802.11 bytes	Proposta bytes	Incremento bytes
Autenticação	174	200	26 ➔ 15%
Reautenticação	0	148	148
Revogação	0	155	155
Desautenticação	42	148	106➔ 52%

Observa-se que as informações da tabela 5 não permitem determinar o incremento gerado na rede de forma real. Para determinar o incremento de tráfego na rede foi realizado um estudo do perfil dos usuários de uma rede local sem fio. O objetivo do estudo foi a identificação do número médio de processos de autenticação e desautenticação. Com base nestas informações, tornou-se possível uma análise mais aproximada da realidade do tráfego determinado pelas modificações definidas pela proposta apresentada neste artigo.

A tabela 6 apresenta o resumo do levantamento realizado. A tabela foi gerada com base nos *logs* do ponto de acesso, coletado por 5 dias úteis, entre 7 horas da manhã e 7 horas da noite. A rede analisada contém apenas um ponto de acesso, operando a 11Mbits/s, de acordo com o padrão IEEE 802.11 e com o máximo de 7 usuários.

Tabela 6 – Perfil de Autenticação e Desautenticação.

Usuário	Seg.	Ter.	Qua.	Qui.	Sex.	Média
1	3	2	4	0	3	**2.4**
2	2	2	2	2	2	**2**
3	5	3	2	2	4	**3.2**
4	1	1	0	2	1	**1**
5	6	7	5	6	6	**6**
6	3	2	2	1	3	**2.2**
7	0	0	5	4	4	**2.6**
Média	**2.85**	**2.42**	**2.85**	**2.42**	**3.28**	**2.77**

Com os dados da tabela 6 e com o tamanho dos processos, é calculada a quantidade de tráfego utilizada para implementar os mecanismos de segurança.

Tráfego no padrão IEEE 802.11:

2.8 autenticações * 7 usuários * 174 bytes = 3.4Mbytes
2.8 desautenticações * 7 usuários * 42 bytes = 0.8Mbytes

Com base nestes cálculos, em um dia, cerca de 4.2Mbytes são transmitidos nesta rede com o objetivo de implementar os controles de segurança. O número 174 é o tamanho total de um processo de autenticação e 42 é o tamanho total de um processo de desautenticação no padrão IEEE 802.11.

Tráfego na proposta apresentada:

2.8 autenticações * 7 usuários * 200 bytes = 3.9Mbytes
2.8 desautenticações * 7 usuários * 148 bytes = 2.9Mbytes
24 reautenticações * 7 usuários * 148 bytes = 24.8Mbytes

Com base nestes cálculos, em um dia, cerca de 32Mbytes são transmitidos nesta rede com o objetivo de implementar os controles de segurança.

De acordo com as tabelas anteriores o número 200 é o tamanho total de um processo de autenticação e 148 é o tamanho total de um processo de desautenticação ou reautenticação. O número de reautenticações, 24, foi definido de modo a ocorrer uma reautenticação a cada meia hora. Este valor é definido e calculado como apresentado na última seção deste artigo, mas deve ainda levar outros fatores em consideração.

Com base nas informações das tabelas 5 e 6, conclui-se que o incremento em termos de banda inserida na rede por esta proposta é em média de 661%.

Porém, o que parece ser inviável, um aumento de 661%, pode ser muito satisfatório. Comparando a quantidade de tráfego utilizada pelos processos acima com a quantidade total de tráfego transmitida na rede obtêm-se percentuais pequenos. No caso do padrão IEEE 802.11 apenas 0.007% do total do tráfego transmitido na rede é referente aos processos de autenticação e desautenticação. No caso da proposta apenas 0.05% do tráfego total transmitido é referente aos processos de autenticação, reautenticação e desautenticação. Estes cálculos baseiam-se na capacidade de transmissão da rede e nos dados calculados anteriormente e é apresentado em seguida. O *overhead* ocasionado pela cifragem dos dados transmitidos não foi levado em conta, pois existe tanto no padrão quanto na proposta, sem alterações.

A capacidade da rede é de 11Mbits/s ou 1.375Mbytes/s o que equivale a 4.95Gbytes/h. A capacidade multiplicada por 12 horas dá um total de 59.4Gbytes por dia. Considerando um dia formado por 12 horas úteis, como considerado no levantamento de dados na rede local sem fio.

Como no caso do padrão 4.2Mbytes são utilizados diariamente pelos controles de segurança e no caso da proposta 32Mbytes são utilizados diariamente, tem-se que 0.007% e 0.05% do tráfego são utilizados pelos controles de segurança no padrão e na proposta respectivamente.

11.2 Período de Reautenticação e Quebra da Chave

Esta seção apresenta considerações sobre o período necessário para quebra da chave WEP e a relação com o período de reautenticação.

O período de reautenticação deve ser cuidadosamente observado. É devido a reautenticação e a distribuição de nova chave de sessão de forma periódica que as fragilidades do protocolo WEP são minimizadas.

Com base no tráfego da rede, calcula-se o tempo necessário para que um possível invasor possa coletar a quantidade necessária de tráfego que lhe permita revelar as informações transmitidas. Logo, o período de reautenticação deve ser inferior a este tempo.

Uma das fragilidades do WEP está no reuso de valores para o vetor de inicialização (IV). A análise a seguir considera como base o cálculo do número de pacotes que leva à repetição destes valores. Como o IV tem 3 bytes, ou seja 24 bits, existem 2^{24} possibilidades para o mesmo. Logo, em média, a cada 2^{24} pacotes o valor do IV é repetido.

Considerando que os pacotes MAC variam entre 34 e 2346 bytes, e que cada pacote utiliza um e apenas um IV, têm-se dois cálculos:

Pior caso, pacotes com tamanho mínimo:
2^{24} pacotes * 34 bytes = 570Mbytes = 4.5Gbits
Logo, neste caso após 4.5Gbits transmitidos o primeiro IV utilizado é considerado novamente.

Melhor caso, pacotes com tamanho máximo:
2^{24} pacotes * 2346 bytes = 40Gbytes = 320Gbits
De forma alánoga, nesse caso, após 320Gbits transmitidos o primeiro IV utilizado é considerado novamente.

Como um ponto de acesso pode transmitir 11Mbits/s. O que equivale a 39.6Gbits/hora, tem-se que 570Mbytes gastariam cerca de 7 minutos para serem transmitidos e 320Gbits cerca de 8 horas. Logo, nestes casos, os períodos de reautenticação devem ser menores que os referidos tempos.

Mesmo baseado nestes cálculos o valor do período de reautenticação deve levar outras variáveis em consideração, como por exemplo, o valor das informações que estão a trafegar pela rede.

12 TRABALHOS FUTUROS E CONCLUSÃO

Este artigo apresenta uma proposta de melhoria do nível de segurança de redes locais sem fio. Trabalhos futuros podem considerar a implementação desta proposta em redes reais, para análises mais efetivas.

Uma dos princípios seguidos ao elaborar esta nova proposta é a sua adequação ao padrão IEEE 802.11. Isto leva a vantagem da possibilidade de adoção da proposta em diversas redes que utilizam este padrão. Face a relação custo/benefício.

Entretanto, novas propostas com protocolos que garantem a segurança de redes sem fio podem ser consideradas. Podem ser considerados também outros mecanismos de autenticação diferentes daqueles considerados neste artigo. Além de novos mecanismos de autenticação, podem também serem considerados protocolos criptográficos modernos que tratam do gerenciamento das senhas dos usuários.

Outro importante ponto é a questão da facilidade de falsificação e uso de endereços MAC que não é resolvida nesta proposta e pode ser tratada como trabalho futuro.

Mesmo estando ainda em estado de evolução, a presente proposta eleva o nível de segurança das atuais redes locais sem fio melhorando a proteção de seus componentes e usuários.

REFERÊNCIAS BIBLIOGRÁFICAS

IEEE Std 802.11-1999. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Março de 1999.

IEEE Std 802.1X-2001. Port-Based Network Access Control. Junho de 2001.

Silva, G. e Souza, J. Uma análise dos mecanismos de segurança de redes locais sem fios e uma proposta de melhoria. In: III WORKSHOP EM SEGURANÇA DE SISTEMAS COMPUTACIONAIS. Maio de 2003.

Fluhrer, S., Mantin, I. e Shamir, A., Weaknesses in the Key Scheduling Algorithm of RC4, www.crypto.com/papers/others/rc4_ksaproc.ps.

Peres, A. e Weber, R. Considerações sobre Segurança em Redes Sem Fio. In: III WORKSHOP EM SEGURANÇA DE SISTEMAS COMPUTACIONAIS. Maio de 2003.

Arbaugh, W., Wan, Y. e Shankar, N., Your 802.11 Wireless Network has No Clothes, http://www.cs.umd.edu/%7Ewaa/wireless.pdf, Março de 2001.

Roshan, P., 802.11 Wireless LAN Security White Paper, http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00800b469f.shtml, 2002.

Etter, A., A Guide to Wardriving and Detecting Wardrivers,http://www.sans.org/rr/papers/68/174.pdf, Setembro de 2002.

Stallings, W., Cryptography and Network Security, Prentice Hall, 1998.

Peikari, C. e Fogie, S., Wireless Maximum Security. SAMS Publishing, 2003.

Mishra, A. e Arbaugh, W., An Initial Security Analysis of the IEEE 802.1X Standard, http://www.cs.umd.edu/~waa/1x.pdf, Fevereiro de 2002.

Orinoco, ORiNOCO security paper v2.2, http://www.orinocowireless.com/learn/library/whitepapers/wireless_security.pdf, 2003.

Ferguson, N. e Schneier, B., Practical Cryptography, Wiley Publishing, 2003.

Mahan, R., Security in Wireless Network, http://www.sans.org/rr/wireless/wireless_net3.php, Novembro de 2001.