Estudo e Melhoria dos Mecanismos de Segurança em Redes Locais Sem Fio

Gilson Marques Silva – gilsonm@ctbctelecom.net.br e João Nunes de Souza – nunes@ufu.br
Faculdade de Computação – Universidade Federal de Uberlândia
Uberlândia – MG – Brasil

***Abstract*-- This paper presents the fragilities related to the current security mechanisms implemented in the wireless local area networks. A set of proposals to improve these security mechanisms and some improvements are proposed and they can permit rising the security level. An evaluation of this new proposed is still presented.**

***Index Terms*-- Communication system security, Computer network security, Cryptography, Security, Wireless LAN.**

I. 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 [1], 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 [2] 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 em breve.

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.

A seção II apresenta uma visão geral dos padrões IEEE 802.11 e 802.1X. A seção III apresenta uma proposta de melhoria do nível de segurnaça das redes locais sem fio. Na seção IV é apresentado o detalhamento dos processos que compõe a proposta apresentada na seção anterior. Finalmente na seção V o resultado de uma avaliação desta proposta é apresentado.

II. UMA VISÃO GERAL DOS PADRÕES IEEE 802.11 E 802.1X

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. Já 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.

O padrão 802.11 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.

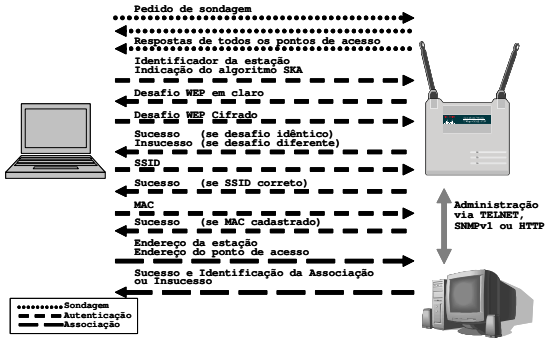

Fig. 1. Fases de acesso a rede sem fio de acordo com o padrão IEEE 802.11.

No caso do exemplo ilustrado na fig. 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. Estes mecanismos são melhorias implementadas por fabricantes e são detalhados mais adiante.

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 fig. 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 fig. 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 fig. 1 pelas duas últimas linhas.

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 [3].

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*), que trata a questão de reuso de *key-stream*. Estudos sobre as fraquezas do protocolo WEP são apresentados em [4] e [5].

Quanto ao padrão 802.1X, sua contirubição às redes locais sem fio está relacionada a autenticação dos clientes através de uma base centralizada, seja no próprio ponto de acesso, seja em um servidor centralizado como por exemplo um servidor RADIUS.

Existem algumas opções de proteção das mensagens de autenticação de uma validação no padão 802.1X. Logo no caso mais simples as credenciais trafegam em claro pela rede e podem ser facilmente capturadas no ar e oportunamente utilizadas. Mas 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.

III. 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. Certamente atualização do *firmware* dos equipamentos será necessária para a correta implementação desta proposta.

A fig. 2 apresenta um esquema de conexão à rede local sem fio, incluindo a fase de sondagem, autenticação e associação de acordo com a proposta. A figura representa as etapas da nova proposta. Sua interpretação é análoga a da fig. 1.

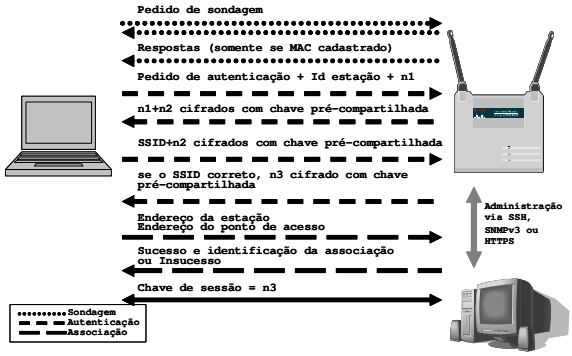

Fig. 2. Fases de acesso a rede sem fio de acordo com a proposta.

As alterações propostas elevam o nível de segurança das redes locais sem fio, sob os seguintes aspectos:

A. Proteção ao Mapeamento da Rede

Esta seção apresenta mecanismos que dificultam o mapeamento da rede. Estes mecanismos se fundamentam na filtragem MAC e no uso de um número pseudo-aleatório.

Na proposta apresentada, o mapeamento da rede, por um intruso, é dificultado considerando a verificação do endereço MAC durante a fase de sondagem. Nesta sondagem 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. Atualmente, os produtos que disponibilizam algum tipo de filtragem MAC consideram a filtragem em fases subsequentes 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 fatos acima 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 *wardrivers* e usuários comuns usem o software de seus cartões 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.

Esta proposta também previne a captura do SSID. No esquema convencional o SSID trafega em claro. Isto permite que o SSID seja facilmente capturado.

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 a criptografia. 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 correta. 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 fig. 2.

B. Autenticação mais Eficaz e Robusta

Esta seção apresenta mecanismos que tornam o processo de autenticação mais eficaz, através do uso de chave pré compartilhada, números pseudo-aleatórios e chaves de sessão.

Estes mecanismos prevêem o uso de uma chave pré compartilhada que é utilizada somente no processo de autenticação. Diferente do padrão IEEE 802.11 que utiliza a chave pré compartilhada no processo de autenticação e também para prover a confidencialidade dos dados no ar.

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 cifrado com esta chave. Desta forma os ataques citados em [5] contra o protocolo WEP tornam-se inviáveis devido a quantidade pequena de dados que trafegam sob a proteção da chave pré compartilhada.

De acordo com a fig. 2, 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 em claro, pois 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.

Passos adicionais são eliminados na fase de autenticação. E a filtragem MAC, definida na fase de sondagem, é considerada como uma pré autenticação.

C. Redução dos Efeitos das Fraquezas do 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 um terceiro número pseudo-aleatório (n3) 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. Quanto mais tráfego, menor o tempo para a quebra. O período para a reautenticação deve ser definido de acordo com a carga da rede, quanto mais carga menor o tempo de reautenticação. Alguns parâmetros de carga são considerados em [6]. Além disso a seção V deste artigo 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 fig. 2. Primeiro o ponto de acesso transmite ao cliente um novo número pseudo-aleatório. Este número é protegido pela chave pré compartilhada, e será utilizado como a nova chave de sessão.

D. 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 o cliente são novamente autenticados. A autenticação é realizada com base na chave pré compartilhada e não na chave de sessão comprometida.

Assim que o cliente 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.

E. Melhores Práticas de Administração dos Pontos de Acesso

Esta seção apresenta as melhores práticas que tornam o processo de administração e gerência dos pontos de acesso mais seguro. O uso de protocolos com recursos que garantem a confidencialidade dos dados é a base para esta proteção. Estas práticas já são adotadas por alguns fabricantes.

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*).

Protegido por estes protocolos o tráfego de administração e gerência dos pontos de acesso não pode ser utilizado para a obtenção de chaves e credenciais de acesso.

IV. Detalhamento dos processos da proposta

Esta seção apresenta os detalhes de cada um dos processos considerados nesta proposta. É apresentado também a estrutura dos pacotes, tipos e tamanhos de seus campos.

A. Processo de Autenticação

O processo de autenticação é a etapa mais importante para conferir o controle de acesso à rede. A filtragem MAC como descrita na seção anterior pode ser definida como uma pré autenticação. O seu posicionamento na fase de sondagem e não na fase de autenticação melhora a proteção ao mapeamento, pois nenhuma resposta é emitida aos possíveis invasores.

O processo de autenticação tem dois propósitos: autenticar o cliente perante o ponto de acesso e autenticar o ponto de acesso perante o cliente. Ambos propósitos são importantes. 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 da rede.

Basicamente o processo de autenticação consiste em duas validações por desafio/resposta utilizando o protocolo WEP. O padrão 802.11, também usa o protocolo WEP. No entanto somente provê uma destas validações, com o objetivo de autenticar o cliente. Além do mais, existe uma grande diferença entre as validações desta proposta e a do padrão. No padrão é possível correlacionar o desafio em claro e a resposta cifrada obtendo-se o *key stream* utilizado. Já nesta proposta isso não é possível, já que os campos de desafio e resposta não podem ser correlacionados. O fato deles serem concatenados a números pseudo-aleatórios e depois criptografados impede esta correlação. Este números são verificados no processo de validação e variam a cada mensagem trocada.

A fig. 3 mostra a fase de autenticação. A partir dela evidencia-se as duas validações por desafio/resposta e as propriedades explicadas.

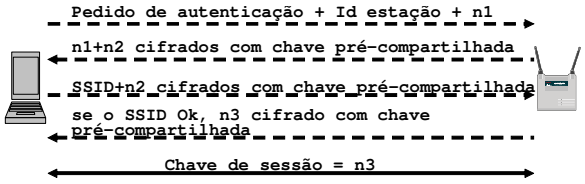

Fig. 3. Processo de autenticação.

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 deverá 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. 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 que emitiu está correto (n1). 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 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.

Vale notar que o SSID não trafega em claro pela rede. E nem de forma isolada. Assim, mesmo se capturado não pode ser posteriormente utilizado.

B. 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 fig. 4.

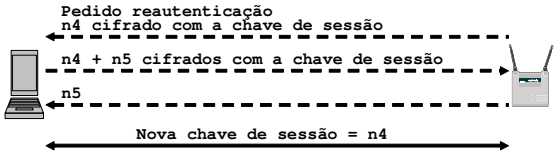

Fig. 4. Processo de reautenticação.

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 n1, 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 enviados ao ponto de acesso. O ponto de acesso verifica que o cliente conseguiu responder o desafio lançado. E recebe um novo desafio (n2) 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, que embora cifrado contém dois números. E também pelo fato de que não precisa ser mantido confidencial. Haja

vista que o primeiro número é utilizado como a nova chave de sessão e não o segundo.

C. Processo de Revogação de Chaves

O processo de revogação de chaves é apresentado na fig. 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 insegura pode comprometer a segurança, ermitindo ao atacante o acesso a nova chave de sessão.

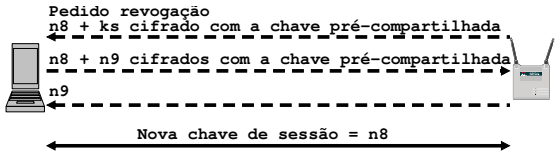

Fig. 5. Processo de revogação de chaves.

O ponto de acesso é responsável pelo início do processo. No primeiro passo o ponto de acesso envia um número pseudo-aleatório concatenado a atual chave de sessão. Este conjunto é cifrado com a chave pré compartilhada que ainda é mantida em segurança. O número enviado (n1) 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 (n2). 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 na seção anterior 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.

D. 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 fig. 6.

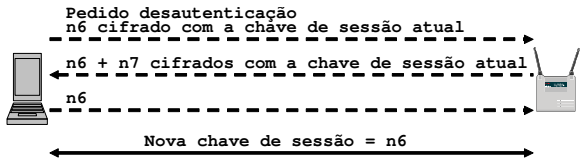

Fig. 6. Fase de desautenticação.

Um número pseudo-aleatório (n1) 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 (n2) gerado pelo ponto de acesso que é utilizado para autenticar o cliente. Este conjunto de informações é cifrado com a chave de sessão e enviada novamente ao cliente. O cliente pode verificar o desafio lançado ao ponto de acesso. Para finalizar o processo o cliente deve responder ao desafio lançado pelo ponto de acesso, devolvendo em texto claro a resposta ao desafio. Pelos mesmos motivos apresentados na seção 8.3 não é necessário que esta última resposta seja protegida quanto a confidencialidade.

E. Esquema e Tamanho dos Quadros de Rede

Esta seção apresenta o esquema do pacote MAC utilizado no padrão IEEE 802.11. Os pacotes e mensagens de cada processo também são apresentadas de forma a se encaixarem no pacote MAC do padrão.

O esquema do pacote MAC é apresentado na fig. 7. 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*) que ocupa 4 bytes. O campo de dados, chamado 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. 7. 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 fig. 8.

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

Fig. 8. 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 [1]. 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. Além disso o tamanho do campo *Text* é apresentados em bits e o tamanho total do pacote é apresentado em bytes.

TABELA 1
MENSAGENS DO 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
MENSAGENS DO 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
MENSAGENS DO PROCESSO DE REVOGAÇÃO

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**

TABELA 4
MENSAGENS DO 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**

Note que E_k, indica um processo de cifragem (Encryption) com a chave secreta k. 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*. Os números 7, 12, 14 são o tamanho do campo *Text*.

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*), que trata a questão de reuso de *key-stream*. Estudos sobre as fraquezas do protocolo WEP são apresentados em [4] e [5].

V. AVALIAÇÃO E IMPLICAÇÕES DA PROPOSTA

Esta seção apresenta uma avaliação desta proposta. O objetivo é avaliar os incrementos inseridos na rede devido aos controles adicionados. Além do incremento de tráfego o cálculo do período de reautenticação é calculado com base na carga, número e tamanho de pacotes.

A. Overhead de Banda Inserido

Esta proposta tem um incremento significativo 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 comparados pelo fato de que não são implementados no padrão IEEE 802.11.

TABELA 5
COMPARATIVOS DE PACOTES: PADRÃO E 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%

Em princípio as informações da tabela 5 não nos permite um definição do incremento gerado na rede de forma real. Para contornar este ponto foi realizado um estudo do perfil de usuários de uma rede local sem fio. O objetivo do estudo é identificar o número médio de processos de autenticação e desautenticação. Com base nestas informações, torna-se possível uma análise mais aproximada da realidade do tráfego inserido pela proposta.

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 PROCESSOS 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

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 nos cálculos anteriores, 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.

Na presente proposta:
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 nos cálculos anteriores, 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 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.

Com base nas informações das tabelas 5 e 6, conclui-se que o incremento em termos de banda inserida na rede pela presente 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 obtém-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 detalhado em seguida.

A capacidade da rede é de 11Mbits/s ou 1.375Mbytes/s o que equivale a 4.95Mbytes/h. A capacidade multiplicada por 12 horas dá um total de 59.4Mbytes 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.

B. 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.

Como a grande fragilidade do WEP está no reuso de valores para o vetor de inicialização (IV) a base do cálculo é o 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 a cada 2^{24} pacotes o valor do IV é repetido.

Considerando que os pacotes MAC variam entre 34 e 2346 bytes, pode-se produzir dois cálculos:

Pior caso, pacotes com tamanho mínimo:
2^{24} pacotes * 34 bytes = 570Mbytes que equivale a 4.5Gbits
Melhor caso, pacotes com tamanho máximo:
2^{24} pacotes * 2346 bytes = 40Gbytes que equivale a 320Gbits

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

No entanto dois fatores podem deixar esta medida mais real: a adoção do tamanho de pacotes médios na rede, e a utilização do paradoxo do aniversário. O paradoxo do aniversário diz que: "Se você tem 23 pessoas em uma sala a chance de duas delas terem o mesmo aniversário pode exceder 50%", conforme [7] e [8].

Utilizando o paradoxo do aniversário e pacotes de tamanho médio, o cálculo anterior pode ser rescrito:
2^{23} pacotes * 1200 bytes = 10Gbytes que equivale a 80Gbits

Note que 2^{23} equivale a 50% do número total de pacotes (paradoxo do aniversário) que podem ser gerados sem a repetição do IV. O número 1200 é um valor mediano que procura representar melhor o tamanho dos pacotes de rede. Com a mesma taxa de transmissão do AP, cerca de 2 horas serão gastas para transmissão deste tráfego. Isto propõe um período de reautenticação menor que 2 horas.

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. Note que embora um período menor que 2 horas seja suficiente para garantir a segurança da chave, foram adotados apenas 30 minutos nos cálculos da seção 8.5. Isso se deve pelo valor da informação analisada em cada caso.

VI. REFERÊNCIAS

[1] IEEE Std 802.11-1999. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Mar. 1999.

[2] IEEE Std 802.1X-2001. Port-Based Network Access Control, Jun. 2001.

[3] A. Peres e R. Weber, "Considerações sobre Segurança em Redes Sem Fio", apresentado no III WORKSHOP EM SEGURANÇA DE SISTEMAS COMPUTACIONAIS. Natal, Brasil, 2003.

[4] W. Arbaugh, Y. Wan e N. Shankar. (2001, Mar.). Your 802.11 Wireless Network has No Clothes. Disponível em http://www.cs.umd.edu/%7Ewaa/wireless.pdf.

[5] P. Roshan. (2002). 802.11 Wireless LAN Security White Paper. Disponível em http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00800b469f.shtml.

[6] R. Mahan. (2003). Security in Wireless Network. Disponível em http://www.sans.org/rr/wireless/wireless_net3.php.

[7] N. Ferguson e B. Schneier, Practical Cryptography, Indiana: Wiley Publishing, 2003,

[8] W. Stallings, Cryptography and Network Security, New Jersey: Prentice Hall, 1998, pp. 33, 34, 80, 88.

VII. BIOGRAFIA

Gilson Marques da Silva nasceu em Matutina no estado de Minas Gerais no Brasil, em 14 de junho de 1975. Ele graduou-se na Universidade Federal de Uberlândia, como bacharel em Ciência da Computação no primeiro semestre de 1998. No início de 2000 concluiu o curso de pós graduação *latu-sensu* em Telecomunicações e no segundo semestre de 2001 terminou o curso de pós graduação *latu-sensu* em Redes de Computadores. Sua experiência profissional inclui atividades como analista de rede na diretoria de processamento de dados da Universidade Federal de Uberlândia além de ter sido professor no nível de graduação na mesma universidade.

Atualmente além das atividades dicentes como mestrando na área de segurança em redes sem fio ele exerce atividade profissional relacionada à segurança da informação em grande empresa de telecomunicações além de ser professor no nível de graduação para o curso de Sistemas de Informação na UNIMINAS.

João Nunes de Souza graduou-se em Engenharia Elétrica e em Matemática pela Universidade Federal de Minas Gerais (UFMG). Concluiu o Mestrado em Matemática também pela UFMG. Doutorou-se em Engenharia Elétrica pela Universidade de Campinas (UNICAMP) em 1989, na área de Inteligência Artificial. Foi um dos fundadores do programa de pós graduação em Ciência da Computação da Universidade Federal de Uberlândia (UFU), onde atua como professor titular e pesquisador da Faculdade de Computação. Suas áreas de interesse são: Bancos de Dados com foco em Recuperação de Informação e Segurança, Criptografia com foco em manipulação de dados cifrados e gerenciamento de senhas.