Um Mecanismo de Proteção de Quadros de Controle para Redes IEEE 802.11

Marcos A. C. Corrêa Júnior, Paulo André da S. Gonçalves

Centro de Informática (CIn)
Universidade Federal de Pernambuco (UFPE)
50.740-560 – Recife – PE – Brasil

{maccj, pasg}@cin.ufpe.br

Abstract. *Only control frames of all the frame types defined by IEEE 802.11 stardard are not yet protected by any kind of security mechanism. This makes it easier for malicious entities to exploit them in order to carry out deny-of-service attacks on the network. Techniques to forge or tamper control frames as well as techniques to reinject them into the network are typically used under such attacks. This paper proposes a mechanism for protecting IEEE 802.11 control frames against such attacks. The proposed mechanism protects all the control frames by using sequence numbers and Message Authentication Codes. Compared to similar studies that aim to protect all the control frames, the proposed mechanism has reduced overhead and provides increased security.*

Resumo. *De todos os quadros definidos pelo padrão IEEE 802.11, apenas os quadros de controle ainda não possuem qualquer tipo de mecanismo de segurança. Isso permite que entidades maliciosas, mesmo não pertencentes à rede, se utilizem de técnicas de forjamento, manipulação e reinjeção desses quadros a fim de gerar algum tipo de negação de serviço na rede. Este artigo propõe um mecanismo de segurança para os quadros de controle do IEEE 802.11. O mecanismo proposto se vale do uso de números de sequência e da geração de Códigos de Autenticação de Mensagem a fim de evitar que estações maliciosas, não pertencentes à rede, tenham sucesso ao forjar, manipular ou reinjetar quadros de controle que levariam à negação de serviços. Além de proteger todos os quadros de controle indistintamente, o mecanismo proposto possui um maior grau de segurança e introduz, nesses quadros, um overhead significativamente menor em comparação aos trabalhos relacionados que também se propõem a proteger todos os quadros de controle.*

1. Introdução

As redes locais sem fio que seguem o padrão IEEE 802.11 [IEEE Standard 802.11 2007] vêm sendo amplamente adotadas em residências, empresas e locais públicos como *shoppings*, aeroportos e restaurantes. Os mecanismos de segurança que atuam na camada enlace dessas redes têm evoluído frequentemente devido à descoberta recorrente de vulnerabilidades [Tews 2007]. Em geral, essas vulnerabilidades são exploradas através do uso malicioso dos diferentes tipos de quadros que trafegam na rede. O padrão IEEE 802.11 define três tipos de quadros: quadros de dados, quadros de gerenciamento e quadros de controle. Os quadros de dados são utilizados para transportar dados e algumas

informações de controle em seu cabeçalho. Os quadros de gerenciamento são usados, entre outras coisas, para sinalizar a presença de uma rede sem fio, iniciar e encerrar a associação de estações com o Ponto de Acesso ou AP (*Access Point*). Os quadros de controle, por sua vez, são usados principalmente para a reserva do canal de comunicação e para a confirmação do recebimento de alguns tipos de quadros.

Em relação à proteção dos quadros de dados, os seguintes protocolos de segurança foram definidos ao longo dos anos: o WEP (*Wired Equivalent Privacy*) [IEEE Standard 802.11 1999], o WPA (*Wi-Fi Protected Access*) [Wi-Fi Alliance 2003] e o WPA2 [IEEE Standard 802.11i 2004]. Dentre os protocolos citados, o WEP é considerado ultrapassado dada a sua longa lista de vulnerabilidades [Tews 2007]. Já a proteção aos quadros de gerenciamento é especificada na emenda IEEE 802.11w [IEEE Standard 802.11w 2009], a qual complementa as especificações do WPA e do WPA2. Essa ementa foi ratificada somente uma década após o surgimento do padrão IEEE 802.11, o que permitiu uma ampla janela de tempo para o desenvolvimento de vários ataques efetivos aos quadros de gerenciamento. Exemplos incluem o pedido falsificado de desassociação de clientes legítimos da rede e a captura de informações sensíveis sendo transportadas nesses quadros (*e.g.* dados sobre recursos de rádio, identificadores baseados em localização e dados para execução de *handoffs* rápidos) [IEEE Standard 802.11k 2008] [IEEE Standard 802.11r 2008] [IEEE Standard 802.11v 2011].

A emenda IEEE 802.11w associada ao WPA2 resolve grande parte das vulnerabilidades conhecidas nas redes IEEE 802.11. Contudo, ainda não existe um padrão IEEE que se proponha a proteger os quadros de controle dessas redes contra qualquer tipo de ataque. Também não há qualquer grupo de trabalho IEEE desenvolvendo emendas para a segurança desses quadros. A ausência de mecanismos de segurança nos quadros de controle permite a qualquer estação maliciosa, pertencente ou não à rede, efetuar diversos ataques de negação de serviço ou DoS (*Denial-of-Service*). Exemplos incluem o bloqueio do uso do canal de comunicação por um período de tempo pré-determinado, a confirmação falsa de recebimento de informações que não foram efetivamente recebidas e a solicitação falsificada de transmissão de informações armazenadas no AP que seriam destinadas a estações que não estariam prontas para recebê-las, causando, na prática, o descarte dessas informações.

Por causa do impacto dos vários ataques aos quadros de controle, diversas pesquisas vêm sendo realizadas com o intuito de prover mecanismos efetivos para a segurança desses quadros [Myneni and Huang 2010], [Khan and Hasan 2008]. Este artigo propõe um mecanismo de segurança para a proteção dos quadros de controle de redes IEEE 802.11. O mecanismo proposto se vale do uso de números de sequência e da geração de Códigos de Autenticação de Mensagem ou MACs (*Message Authentication Codes*) a fim de evitar que estações maliciosas, não pertencentes à rede, tenham sucesso ao forjar, manipular ou reinjetar quadros de controle que levariam à negação de serviços. Além de proteger todos os quadros de controle indistintamente, o mecanismo proposto possui um maior grau de segurança e introduz, nesses quadros, um *overhead* significativamente menor em comparação aos trabalhos relacionados que também se propõem a proteger todos os quadros de controle.

O restante deste artigo está organizado da seguinte forma: a Seção 2 apresenta os quadros de controle do IEEE 802.11 e os ataques existentes contra eles. A Seção 3

apresenta os trabalhos relacionados e como o trabalho proposto se diferencia de cada um deles. A Seção 4 apresenta o mecanismo proposto neste artigo para a proteção dos quadros de controle IEEE 802.11. A Seção 5 apresenta um estudo do *overhead* introduzido pelo mecanismo proposto no tráfego total de uma rede sem fio. Finalmente, a Seção 6 apresenta as conclusões deste trabalho.

2. Quadros de Controle do IEEE 802.11

Esta seção apresenta as funcionalidades dos 8 tipos de quadros de controle definidos pelo padrão IEEE 802.11 [IEEE Standard 802.11 2007]. Os diversos ataques contra tais quadros também são apresentados. É importante ressaltar que o foco deste artigo está nos ataques de origem externa, ou seja, naqueles executados por entidades maliciosas não pertencentes à rede sem fio.

2.1. RTS (*Request To Send*) e CTS (*Clear to Send*)

O mecanismo RTS/CTS é utilizado em redes IEEE 802.11 para a redução de colisões no meio de comunicação. Um nó que deseja transmitir dados inicia um *handshake* com o destinatário, enviando um quadro RTS. Ao receber o RTS, o destinatário responde com um quadro CTS. Qualquer outro nó da rede, ao escutar o RTS ou o CTS enviados, deve postergar suas transmissões por um determinado período de tempo. Tal período engloba o tempo necessário para a subsequente transmissão dos dados e recepção da confirmação de seu recebimento. Assim sendo, o mecanismo RTS/CTS permite a reserva do canal de comunicação para a troca de dados. Tipicamente, o uso do mecanismo RTS/CTS só ocorre quando o tamanho do quadro com os dados excede um limiar pré-definido que pode variar de 0 a 2347 *bytes*.

O RTS possui 20 *bytes* de comprimento, sendo dividido em 5 campos: FC (*Frame Control*), *Duração*, *Endereço 1*, *Endereço 2* e FCS (*Frame Check Sequence*). O campo FC possui 2 *bytes*. Ele permite identificar o tipo de quadro e provê algumas informações de controle. O campo *Duração* possui 2 *bytes* e informa o tempo de reserva do canal. Seu valor máximo é de 32.767 μs [IEEE Standard 802.11 2007]. Os campos *Endereço 1* e *2* possuem 6 *bytes* cada e representam, respectivamente, o endereço do receptor e do transmissor. O campo FCS possui 4 *bytes* e é preenchido com um CRC-32 para a detecção de erros. O quadro CTS possui 4 dos 5 campos do quadro RTS. O campo ausente no CTS é o campo *Endereço 2*, tornando o comprimento do quadro igual a 14 *bytes*.

Existem dois ataques conhecidos contra o mecanismo RTS/CTS [Myneni and Huang 2010]: o ataque de *replay* e o ataque de injeção de RTS e CTS falsificados. No primeiro ataque, uma estação maliciosa escuta o canal para capturar quadros RTS ou CTS e reinjetá-los na rede. No segundo ataque, uma estação maliciosa cria quadros RTS ou CTS com um ou mais campos forjados e os envia à rede. Este último ataque pode ser potencializado se a estação maliciosa preencher o campo *Duração* desses quadros com o valor máximo permitido.

Ambos os ataques são efetivos porque o IEEE 802.11 não provê qualquer mecanismo de autenticação de quadros de controle, nem de identificação de quadros de controle previamente transmitidos. Assim, as estações que escutam os quadros RTS e CTS usados nesses ataques executam as ações previstas pelo protocolo, bloqueando temporariamente suas transmissões e, portanto, sofrendo uma negação de serviço.

2.2. ACK (*Acknowledgement*)

Os quadros ACK são usados para confirmar o recebimento de alguns tipos de quadros. O ACK possui o mesmo formato e tamanho do CTS. Os ataques conhecidos aos quadros ACK são os seguintes: injeção de ACK falsificado e ataque de *replay*. Em [Chen and Muthukkumarasamy 2006], é mostrado como forjar ACKs para a manipulação do tempo de reserva do canal de comunicação. Os autores demostram que os quadros ACK podem ser utilizados de forma tão efetiva quanto os quadros RTS/CTS para a negação de serviços. Em [Rachedi and Benslimane 2009], é apresentado um ataque denominado *False Packet Validation*. Nesse ataque, a entidade maliciosa força a ocorrência de uma colisão num receptor-alvo para, em seguida, enviar um ACK falsificado que confirma ao emissor a correta recepção das informações enviadas. Caso a colisão tenha sido efetuada com sucesso, o emissor, ao receber o ACK forjado, concluirá erroneamente que as informações transmitidas foram corretamente recebidas no receptor.

2.3. BAR (*Block Ack Request*) e BA (*Block Ack*)

Os quadros BAR e BA foram introduzidos pela emenda IEEE 802.11e [IEEE Standard 802.11e 2005] e tiveram suas funcionalidades estendidas pela especificação IEEE 802.11n. Esses quadros são usados para permitir a confirmação de um bloco de quadros usando apenas um quadro de confimação. O quadro BAR é usado para se requisitar a confirmação de recepção de um bloco de quadros enquanto o quadro BA serve como resposta. O quadro BA pode ainda ser utilizado para a confirmação de recepção de um bloco de quadros sem a necessidade de uso do quadro BAR.

O quadro BAR possui 24 *bytes* de comprimento e é formado por 7 campos: FC (*Frame Control*), *Duração*, *Endereço 1*, *Endereço 2*, BAR *control*, *Block Ack Starting Sequence Control* e FCS (*Frame Check Sequence*). O campo BAR *control* possui 2 *bytes* e é usado, entre outras coisas, para informar parâmetros de qualidade de serviço. O campo *Block Ack Starting Sequence Control* possui 2 *bytes* e inclui, entre outras informações, o número de sequência do primeiro quadro em um bloco. O campo *Duração* possui 2 *bytes* e informa um tempo maior ou igual ao necessário para a recepção do quadro BA a ser enviado como resposta. Os demais campos possuem o mesmo tamanho e descrição já apresentados para os quadros RTS.

O quadro BA possui 152 *bytes* de comprimento e inclui 8 campos: FC (*Frame Control*), *Duração*, *Endereço 1*, *Endereço 2*, BA *control*, *Block Ack Starting Sequence Control*, *Block Ack Bitmap* e FCS (*Frame Check Sequence*). O campo BA *control* possui 2 *bytes* e armazena informações de controle específicas do quadro. O campo *Block Ack Starting Sequence Control*, também de 2 *bytes*, é usado para informar a qual quadro BAR pertence a resposta. O campo *Block Ack Bitmap* possui 128 *bytes* e informa, através de um mapa de *bits*, quais quadros de um bloco não foram recebidos. O campo *Duração* possui 2 *bytes* e a informação de tempo contida nele depende do quadro ser ou não uma resposta a um quadro BAR. Os demais campos possuem tamanho e descrição similares aos apresentados para o quadro RTS.

O mecanismo de confirmação em bloco de quadros também pode ser explorado através da falsificação de informações em quadros BAR. Um estudo sobre o uso malicioso dos quadros BAR é apresentado em [Cam-Winget et al. 2007]. Os autores mostram que é possível manipular o número de sequência informado nos quadros BAR, causando

o descarte de qualquer quadro com número de sequência menor do que o informado. Um único quadro BAR manipulado pode causar uma negação de serviço na rede por 10 segundos [Koenings et al. 2009].

2.4. PS-Poll (*Power Save Poll*)

Os APs são projetados para dar suporte a toda estação que esteja utilizando gerenciamento de energia em sua interface de comunicação. Nesse caso, a estação desliga e liga sua interface de comunicação periodicamente para economizar energia. O AP deve armazenar os quadros destinados à estação até que a mesma esteja pronta para a recepção de quadros. Ao religar sua interface, a estação procura por *beacons* do AP que informam se existem quadros armazenados para ela. Caso haja, a estação deve enviar um quadro de controle PS-Poll para recuperar os quadros armazenados pelo AP. A estação pode voltar a desligar sua interface após recuperar todos os quadros armazenados ou após ouvir do AP algum *beacon* indicando que não há quadros armazenados para aquela estação.

O quadro PS-Poll possui 20 *bytes* de comprimento e é formado por 5 campos: FC (*Frame Control)*, AID (*Association ID*), Endereço 1, Endereço 2 e FCS (*Frame Check Sequence*. O campo AID representa um identificador de associação da estação e possui 2 *bytes*. Os demais campos possuem tamanho e descrição idênticos aos já apresentados para o RTS.

Em [Qureshi et al. 2007], é mostrado como o quadro PS-Poll pode ser utilizado para que uma estação maliciosa assuma, perante ao AP, a identidade de uma estação legítima para a qual o AP possua quadros armazenados. Ao receber o quadro falso, o AP enviará os quadros armazenados que seriam destinados à estação legítima. Assim sendo, o ataque causa o "descarte" de informações pertencentes a outra estação, efetivando uma negação de serviço. Mais uma vez, o ataque só é possível por causa da falta de autenticação dos quadros PS-Poll.

2.5. CF-End (*Contention Free End*) e CF-End+CF-Ack (*CF-End+Contention Free Ack*)

A PCF (*Point Coordination Function*) é uma forma opcional de acesso ao meio definido no IEEE 802.11 e utilizada para a oferta, por parte do AP, de períodos livres de contenção às estações. Por ser um método opcional, poucos dispositivos o implementam. Quando um período livre de contenção termina, o AP transmite um quadro CF-End para liberar as estações das regras de operação do modo PCF e informá-las do início do serviço baseado em contenção sob o método DCF (*Distributed Coordination Function*). O quadro CF-End+CF-Ack combina duas funções, sendo utilizado pelo AP quando o mesmo precisa informar o término de um período livre de contenção e confirmar, ao mesmo tempo, quadros anteriormente recebidos.

Ambos os quadros possuem 20 *bytes* de comprimento divididos em 5 campos: FC (*Frame Control*), *Duração*, *Endereço 1*, *Endereço 2* e FCS (*Frame Check Sequence*). Em particular a esses quadros, o campo *Endereço 1* deve conter o endereço de *broadcast* da rede e o campo *Duração* deve conter o valor zero. O significado dos demais campos e seus tamanhos são idênticos aos já descritos para o RTS.

Em [Malekzadeh et al. 2010], é mostrado experimentalmente que a manipulação do campo *Duração* dos quadros CF-End e CF-End+CF-Ack permite lançar ataques que

tornam a rede indisponível, bloqueando a comunicação de dispositivos legítimos. Os efeitos são idênticos aos obtidos com ataques similares a outros tipos de quadros de controle.

3. Trabalhos Relacionados

Em [Bellardo and Savage 2003], são apresentadas propostas para se minimizar os efeitos de ataques ao mecanismo RTS/CTS. Uma das propostas consiste na limitação do valor máximo informado no campo *Duração* dos quadros de controle. Outra proposta consiste na observação da sequência de transmissões a partir de um RTS. A ausência de dados transmitidos após o RTS é considerada uma indicação de que a rede está sendo atacada. Nesse caso, as estações voltariam imediatamente a concorrer pelo uso do canal. Em [Ray and Starobinski 2007], a mesma ideia de observação da sequência de transmissões a partir de um RTS é utilizada para se propor técnicas não-criptográficas de mitigação de ataques ao mecanismo RTS/CTS, mas no contexto de redes sem fio *multihop*. Em [Qureshi et al. 2007], é apresentada uma proposta para se proteger apenas os quadros PS-Poll contra ataques de falsificação e *replay*. A medida proposta se concentra no uso de artifícios criptográficos exclusivamente sobre o campo *Association ID*.

A primeira proposta de proteção criptográfica de todos os quadros de controle do IEEE 802.11 é apresentada em [Khan and Hasan 2008]. Nessa proposta, o campo FCS dos quadros de controle deixa de ser preenchido com um CRC-32 para conter um código de autenticação de 16 *bits* seguido de um CRC-16. Isso objetiva a manutenção do tamanho original dos quadros de controle. O código de autenticação é gerado por uma versão modificada de uma PRF (*Pseudo Random Function*) do WPA2 para produzir uma saída de 16 bits. Contudo, o uso de apenas 16 *bits* para o código de autenticação torna a proteção provida pelo mecanismo fraca [Whiting et al. 2003]. As PRFs usadas em especificações do IEEE 802.11, por exemplo, têm saída de pelo menos 128 *bits*, podendo alcançar 512 *bits* em caso de necessidade de aumento do nível de segurança. A proposta apresentada por [Khan and Hasan 2008] também não traz mecanismos contra ataques de *replay*.

Outra proposta que visa proteger de forma criptográfica todos os quadros de controle é apresentada em [Myneni and Huang 2010]. Para identificar ataques de *replay* e poder torná-los sem efeito, os autores se valem do uso de um número de sequência de 32 *bits* em todos os quadros de controle. O *framework* IAPP (*Inter-Access Point Protocol*) ou IEEE 802.11F é utilizado para a distribuição e gerenciamento da chave criptográfica a ser utilizada. O IEEE 802.11F era uma extensão opcional do IEEE 802.11 para o provimento de serviços de comunicação entre APs compondo um ESS (*Extended Service Set*). O protocolo permite a troca de contextos de segurança entre APs durante períodos de *handoff* das estações. Em 2006, o IEEE retirou a extensão 802.11F do padrão 802.11.

Ainda em relação ao trabalho apresentado em [Myneni and Huang 2010], o mesmo também se propõe a proteger os quadros de controle por meio de um código de autenticação de mensagem (MAC). O MAC possui 160 *bits* e é gerado através do HMAC-SHA1. Como o MAC pode ser usado para verificação de integridade, o campo FCS dos quadros de controle é eliminado. O uso do MAC de 160 *bits* dificulta a falsificação dos quadros de controle em relação à proposta em [Khan and Hasan 2008], porém introduz neles um *overhead* significativo. Além disso, há estudos que mostram fraquezas do HMAC-SHA1 [Kim et al. 2006], [Rechberger and Rijmen 2008]. Em particular à SHA-

1, a mesma apresenta diversas vulnerabilidades importantes [Cannière and Rechberger 2006], [Manuel 2008]. Um dos ataques mais rápidos contra a versão completa da SHA-1 possui complexidade de tempo $O(2^{63})$ ao passo que a complexidade de tempo de um ataque de força bruta é $O(2^{80})$ [Bellovin and Rescorla 2005].

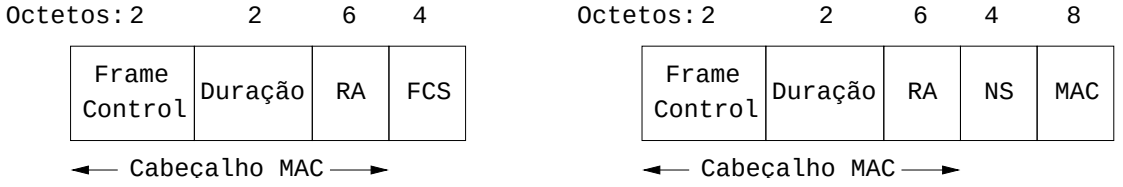
Dentre os trabalhos relacionados, apenas [Myneni and Huang 2010] e [Khan and Hasan 2008] se propõem a proteger todos os quadros de controle, sendo que o primeiro apresenta uma proposta mais segura e completa, embora incorra em um *overhead* significativo. Neste artigo, é proposto um mecanismo de proteção de quadros de controle contra ataques que levariam à negação de serviços. O objetivo principal é, em comparação à proposta em [Myneni and Huang 2010], prover um maior grau de segurança com um menor *overhead*, fazendo uso dos mecanismos de segurança mais recentes presentes no IEEE 802.11. Além disso, a proposta faz uso de chave criptográfica já empregada no protocolo de segurança WPA2, evitando a necessidade de se usar o IEEE 802.11F dado que o mesmo foi removido do padrão IEEE 802.11.

4. O Mecanismo de Proteção Proposto

O mecanismo aqui proposto também se vale do uso de números de sequência e da geração de códigos de autenticação de mensagens para proteger os quadros de controle. Contudo, a geração desses códigos emprega partes do protocolo CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) já utilizado pelo WPA2. O CCMP usa o modo de operação do AES *(Advanced Encryption Standard)* conhecido por CCM, o qual combina o CTR (*Counter Mode*) com o CBC-MAC (*Cipher Block Chaining Message Authentication Code*). O CTR é utilizado para prover confidência enquanto o CBC-MAC é utilizado para prover autenticação e integridade. A seguir, a proposta é detalhada.

4.1. Novos Quadros de Controle

O mecanismo proposto neste artigo introduz 8 novos tipos de quadros de controle no padrão IEEE 802.11. Esses quadros de controle são versões seguras dos quadros de controle originais. O padrão IEEE 802.11 utiliza 4 *bits* para a identificação de tipos de quadros de controle. Como já existem 8 tipos de quadros de controle definidos, a especificação consegue acomodar os novos quadros definidos pelo mecanismo proposto. A versão segura dos quadros de controle se diferencia dos quadros de controle originais apenas por não possuir o campo FCS e, em seu lugar, haver o campo NS (Número de Sequência) de 4 *bytes* seguido do campo MAC (*Message Authentication Code*) de 8 *bytes*. A Figura 1 apresenta, como exemplo, o ACK atual do padrão IEEE 802.11 e sua versão a ser utilizada no mecanismo de segurança proposto.



(a) ACK no padrão IEEE 802.11. (b) Versão segura do ACK no mecanismo proposto.

Figura 1. Formato dos quadros de controle ACK.

O campo MAC permitirá, ao nó receptor, verificar a autenticidade e a integridade do quadro de controle recebido. Como o campo MAC permitirá a detecção de mudanças no quadro de controle, não há necessidade de se manter o campo FCS original para a detecção de erros. O campo NS carregará a informação do número de sequência do quadro. Assim, cada nó da rede deve manter um contador de 32 *bits*, o qual deverá ser incrementado de 1 unidade a cada novo quadro de controle. O campo NS deverá ser preenchido com o valor atual desse contador e nunca poderá ser repetido durante a utilização da mesma chave de segurança utilizada no cálculo do MAC.

4.2. Cálculo do Valor do Campo MAC

O CBC-MAC [Whiting et al. 2003] considera uma mensagem B, a ser autenticada, dividida em uma sequência de blocos $B_0, B_1, B_2 \ldots B_n$, onde $n+1$ é o número total de blocos da mensagem. O CBC-MAC também define $E()$ como sendo a função de criptografia por blocos a ser utilizada, K como sendo a chave criptográfica e T como sendo o código de autenticação. O cálculo de T é feito de acordo com o Algoritmo 4.1. Inicialmente, B_0 é criptografado e o resultado é armazenado em X_1. Em seguida, é realizada um XOR entre X_1 e o próximo bloco B_1. O resultado é armazenado em X_2. O processo se repete para cada bloco seguinte até a obtenção de $X_{(n+1)}$, sendo este último o código de autenticação e o qual pode ser truncado para os M primeiros *bytes* se necessário.

Algoritmo 4.1: T (K, B, n, M)

$X_1 \leftarrow E(K, B_0)$
para $i = 1$ **até** n **faça**
    $X_{(i+1)} \leftarrow E(K, X_i \oplus B_i)$
$T \leftarrow M\ primeiros\ bytes\ de\ X_{(n+1)}$

Em particular, a mensagem a ser autenticada precisa ter o primeiro bloco B_0 formatado como mostra a Tabela 1. Nessa tabela, $l(m)$ é o número de *bytes* da mensagem m, onde $0 \leq l(m) \leq 2^{(8L)}$. O *Nonce* é um valor único que nunca deverá ser repetido com o uso de uma mesma chave criptográfica. As *Flags* ocupam 1 *byte* e também possuem formatação pré-definida conforme descrição a seguir: o primeiro *bit* de ordem mais alta é reservado para uso futuro e deve ser sempre zero. O segundo *bit* de ordem mais alta, *Adata*, indica a utilização da técnica de autenticação de dados adicionais ou AAD quando igual a 1. Caso a técnica não seja utilizada, *Adata* deve ser zero. Os 3 *bits* seguintes codificam M contendo o valor $(M-2)/2$. Assim, M só pode assumir valores pares de 0 a 16. Os 3 *bits* de ordem mais baixa codificam L contendo o valor $L-1$. Valores válidos para L estão no intervalo de 2 a 8.

Byte Nº	0	$1 \ldots (15-L)$	$(16-L) \ldots 15$
Conteúdo	*Flags*	*Nonce*	$l(m)$

Tabela 1. Composição do Bloco B_0.

O CBC-MAC foi projetado para uso com algoritmos de cifra por blocos de 128 *bits*, sendo o tamanho da chave dependente do algoritmo de cifra por bloco utilizado. Os

blocos com menos de 128 *bits* devem ser completados com zeros. No caso do CCMP definido pelo WPA2, é utilizado o AES com operações com chaves e blocos de 128 *bits*. Assim sendo, toda a operação para o cálculo do código de autenticação com o mecanismo proposto segue esse mesmo princípio. O cômputo do valor do campo MAC é feito através do uso da implementação do CBC-MAC no CCMP. A Figura 2 ilustra esse processo. O bloco inicial a ser criptografado possui 128 *bits* e é representado pelo IV (*Initialization Vector*). Sua formação é explicada como segue:

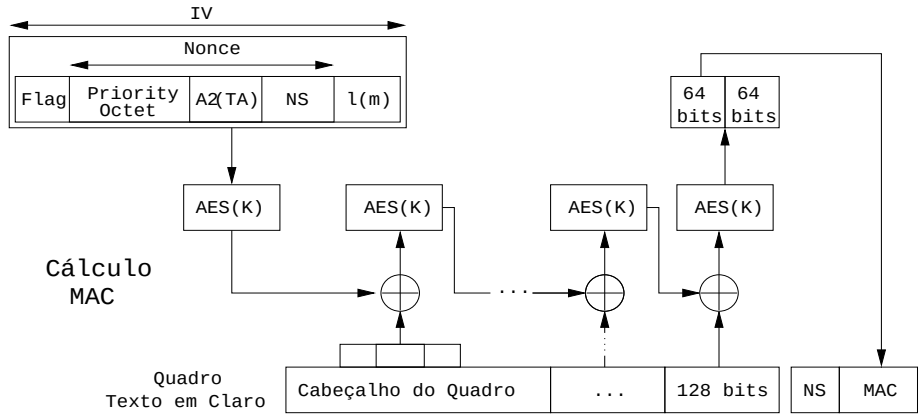


Figura 2. Geração do valor do campo MAC.

- *Flag* - possui 1 *byte*. Contém as informações previstas para o campo *Flags* definido em [Whiting et al. 2003] e possui valor igual a $(00011011)_b$. Ou seja, não é utilizada a técnica AAD, $M = 8$ e $L = 4$;
- *Nonce* - possui 11 *bytes* e é formado pela concatenação do *Priority Octet* (1 *byte*) com os 48 *bits* do endereço do transmissor ou A2(TA) e o número de sequência NS de 32 *bits* do quadro de controle. Esse tipo de construção respeita a formação de *nonces* usada pelo CCM no WPA2 e é usada aqui para fins de compatibilidade. O CCM no WPA2 especifica que o campo *Priority Octet* deve ser preenchido com zeros quando não houver o campo de controle de QoS (*Quality of Service*) no cabeçalho do quadro como é o caso dos quadros de controle. A forma de construção do *nonce* permite que os nós da rede usem sempre *nonces* distintos entre eles.
- $l(m)$ - possui 4 *bytes* e segue a definição em [Whiting et al. 2003] para informar o tamanho da mensagem a ser autenticada.

O processo de construção do MAC segue o algoritmo 4.1 tendo o IV como bloco inicial B_0. Os próximos blocos são obtidos dividindo-se o quadro de controle em pedaços de 128 *bits* mas com a exclusão dos campos NS e MAC. No caso do ACK e do CTS, haverá apenas 80 *bits* de informação que devem ser concatenados com 48 *bits* iguais a zero para compor o próximo e último bloco B_1. No caso dos quadros RTS, CF-End e CF-End+Cf-Ack, o próximo e último bloco B_1 já conterá exatos 128 *bits*. O quadro BAR gerará mais dois blocos (B_1 e B_2), sendo que o último deverá ser completado com 96 *bits* iguais a zero. O quadro BA gerará mais dez blocos ($B_1 \ldots B_{10}$), sendo que o último também deverá ser completado com 96 *bits* iguais a zero.

Para que um nó da rede possa construir o MAC e permitir a qualquer outro verificar a autenticidade e a integridade do quadro, é necessário que uma chave K em comum

seja empregada. A chave criptográfica comum utilizada no WPA2 é a GEK (*Group encryption Key*) que faz parte da chave hieráquica GTK (*Group Temporal Key*). A GEK é a chave usada para a criptografia de tráfego destinado a múltiplos nós da rede. A GTK é distribuída durante o processo de *4-Way Handshake* e renovada periodicamente usando o protocolo GKH (*Group Key Handshake*). Adicionalmente aos critérios de renovação da GTK definidos pelo WPA2, o uso do mecanismo proposto requer a renovação dessa chave para evitar que um nó utilize um mesmo número de sequência com uma mesma GTK. Assim, o nó que esgotar seus números de sequência deve solicitar a renovação da GTK da rede através do uso do protocolo GKH (*Group Key Handshake*).

Ao receber um quadro de controle do mecanismo proposto, o nó da rede sem fio deve recalcular o MAC e comparar o valor obtido com aquele informado no campo MAC. Para isso, ela precisará da chave K e do IV. A chave K é conhecida por todas as estações da rede. O IV possui duas partes: uma parte com valor fixo e pré-definido (*Flag*, *Priority Octet* e $l(m)$), o qual é conhecido pelas estações e uma parte com valor variável composta pelo NS e pelo endereço do transmissor. O NS que é transportado em claro pelo quadro. O endereço do transmissor está presente em todos os quadros de controle, exceto nos quadros CTS e ACK. Para os quadros CTS e ACK, o padrão IEEE 802.11 prevê que o receptor obtenha o endereço do transmissor a partir dos respectivos RTS ou dos respectivos quadros sendo confirmados de acordo com o caso. Ao recalcular o MAC, caso o valor obtido seja diferente daquele informado no campo MAC, a mensagem foi alterada e deve ser desconsiderada. Caso o valor do MAC recalculado seja igual ao informado no campo MAC do quadro recebido, o nó deve verificar se não é um quadro repetido usando como base o número de sequência esperado. Caso o quadro não seja uma repetição, o nó receptor deverá considerar a mensagem e a origem da mesma autenticadas.

4.3. Segurança

A segurança do mecanismo proposto está intimamente ligada à segurança do WPA2. Em redes IEEE 802.11 protegidas pelo WPA2, é possível encontrar a chave GTK através de um ataque de dicionário quando a rede usa o método de autenticação pessoal em conjunto com uma *passphrase*. Contudo, esse ataque só é praticável se a *passphrase* possuir menos de 20 caracteres [Fogie 2005]. Essa vulnerabilidade é considerada do usuário/administrador e não do protocolo de segurança. Em [Rogaway 2011], é apresentado um estudo que mostra que o CCM apresenta propriedades de segurança suficientemente adequadas. O estudo também mostra que as principais críticas ao CCM estão ligadas à sua eficiência de execução. Em relação à segurança do AES, o ataque mais rápido de recuperação de chave contra sua versão completa de 128 *bits* possui complexidade de tempo $O(2^{126,1})$ enquanto a complexidade de tempo de um ataque de força bruta é $O(2^{128})$ [Bogdanov et al. 2011].

4.4. Resumo Comparativo

A Tabela 2 apresenta um resumo da proteção oferecida pelo mecanismo proposto e pelos trabalhos relacionados para cada tipo de quadro de controle. A existência de proteção contra forja e manipulação do quadro é indicada por X. A existência de proteção contra ataques de *replay* é indicada por 0.

	RTS	CTS	ACK	BA	BAR	PS-Poll	CF-End	CF-End + CF-Ack
[Bellardo and Savage 2003]	X	X	X					
[Qureshi et al. 2007]						X		
[Ray and Starobinski 2007]	X							
[Khan and Hasan 2008]	X	X	X	X	X	X	X	X
[Rachedi and Benslimane 2009]	X	X	X					
[Myneni and Huang 2010]	$X/0$	$X/0$	$X/0$	$X/0$	$X/0$	$X/0$	$X/0$	$X/0$
Proposta neste artigo	$X/0$	$X/0$	$X/0$	$X/0$	$X/0$	$X/0$	$X/0$	$X/0$

Tabela 2. Comparativo da proteção oferecida pelas diversas propostas.

5. Estudo de Caso

Esta seção estuda o impacto do mecanismo proposto neste artigo e em [Myneni and Huang 2010] no tráfego global de uma rede sem fio. Para esse estudo, foram capturados quadros ao longo de 1 hora na rede sem fio do Centro de Informática da UFPE, gerando um arquivo *trace* com aproximadamente 1.500.000 quadros. Todos os quadros capturados eram provenientes de um único AP escolhido ou direcionados a ele.

A Figura 3(a) apresenta a quantidade capturada dos 3 tipos de quadros. Note que há uma predominância dos quadros de controle. A Figura 3(b) detalha os tipos de quadros de controle capturados. Em particular, observa-se que foram capturados quadros de controle de todos os tipos, exceto o quadro CF-End+CF-Ack.

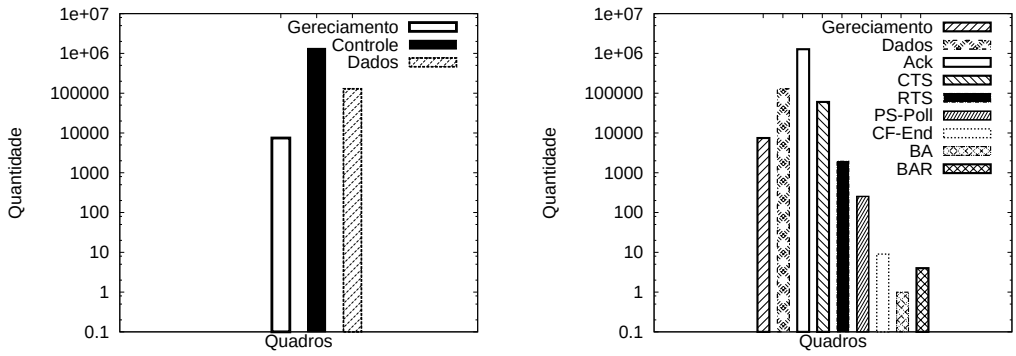
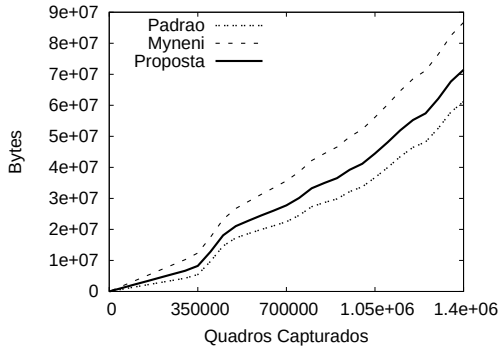


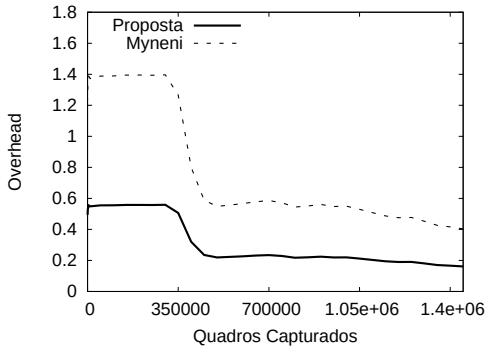
Figura 3. Distribuição da frequência dos quadros.

A partir do *trace* obtido, foram acrescentados aos quadros de controle o *overhead* do mecanismo proposto e da proposta em [Myneni and Huang 2010] para fins de comparação. A ideia é simular o mesmo tráfego de quadros sob esses dois mecanismos de segurança. A Figura 4(a) apresenta o número cumulativo de *bytes* transferidos em função da quantidade de quadros. Note que o mecanismo proposto possui um menor *overhead* cumulativo do que a proposta em [Myneni and Huang 2010].

A Figura 4(b) apresenta o *overhead* normalizado do tráfego considerando as duas propostas avaliadas. Note que até aproximadamente os 300.000 primeiros quadros capturados, o mecanismo proposto têm um impacto de próximo de 57% enquanto a proposta do Myneni tem um impacto de quase 143%. A medida que o volume de quadros aumenta,



(a) Bytes usados para transmitir a mesma informação útil.



(b) Overhead normalizado em relação ao formato padrão dos quadros.

Figura 4. Comparação entre propostas.

observa-se que o impacto do mecanismo proposto tende à 20% enquanto o impacto do mecanismo proposto por Myneni tende à 40%.

6. Conclusões

Este artigo apresentou um mecanismo de proteção de quadros de controle contra ataques de negação de serviço. O mecanismo foi construído de forma a manter a compatibilidade com o padrão IEEE 802.11. O objetivo principal da proposta, em comparação à proposta em [Myneni and Huang 2010], foi o de prover um maior grau de segurança com um menor *overhead*, fazendo uso dos mecanismos de segurança mais recentes presentes no IEEE 802.11. Adicionalmente, a proposta fez uso da chave de grupo já empregada no protocolo de segurança WPA2, evitando a necessidade de se utilizar um mecanismo de gerenciamento e distribuição de chaves abandonado pelo IEEE. Para dar proteção aos quadros de controle contra os ataques estudados, o mecanismo proposto se utilizou de números de sequência e de códigos de autenticação de mensagens obtidos através do emprego do CBC-MAC do CCMP. O *overhead* introduzido com o uso do mecanismo proposto é, por quadro de controle, 2,5 vezes menor do que aquele introduzido pela proposta de Myneni. Um estudo de caso enfatizou que o mecanismo proposto produziu um impacto significativamente menor no tráfego global da rede do que aquele produzido pela proposta de Myneni. Como trabalho futuro, será realizado um estudo da vazão da rede ao se utilizar o mecanismo proposto.

Referências

Bellardo, J. and Savage, S. (2003). 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In *Proc. of the 12th USENIX Security Symposium (SSYM)*, pages 15–28, Washington, DC, USA.

Bellovin, S. and Rescorla, E. (2005). Deploying a New Hash Algorithm. Technical report.

Bogdanov, A., Khovratovich, D., and Rechberger, C. (2011). Biclique Cryptanalysis of the Full AES. In *Proc. of the 17th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*, Seoul, Korea, (To appear).

Cam-Winget, N., Smith, D., and Walker, J. (2007). IEEE 802.11-07/2163r0 - A-MPDU Security Issues. Technical report.

Cannière, C. D. and Rechberger, C. (2006). Finding SHA-1 Characteristics: General Results and Applications. In *Lecture Notes in Computer Science - ADVANCES IN CRYPTOLOGY (ASIACRYPT)*, volume 4284, pages 1–20.

Chen, B. and Muthukkumarasamy, V. (2006). Denial of Service Attacks Against 802.11 DCF Abstract.

Fogie, S. (2005). Cracking Wi-Fi Protected Access (WPA), Part 2. `http://www.fermentas.com/techinfo/nucleicacids/maplambda.htm`.

IEEE Standard 802.11 (1999). IEEE Standards for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

IEEE Standard 802.11 (2007). IEEE Standards for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

IEEE Standard 802.11e (2005). IEEE Standards for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements.

IEEE Standard 802.11i (2004). IEEE Standards for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 6: Medium Access Control (MAC) Security Enhancements Interpretation.

IEEE Standard 802.11k (2008). IEEE Standards for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 1: Radio Resource Measurement of Wireless LANs.

IEEE Standard 802.11r (2008). IEEE Standards for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 2: Fast Basic Service Set (bss).

IEEE Standard 802.11v (2011). IEEE Standards for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 8: IEEE 802.11 Wireless Network Management.

IEEE Standard 802.11w (2009). IEEE Standards for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 4: Protected Management Frames.

Khan, M. and Hasan, A. (2008). Pseudo random number based authentication to counter denial of service attacks on 802.11. In *Proc. of 5th IFIP International Conference on Wireless and Optical Communications Networks (WOCN)*, pages 1–5.

Kim, J., Biryukov, A., Preneel, B., and Hong, S. (2006). On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0, and SHA-1. *Designs, Codes Cryptography*, 4116:242–256.

Koenings, B., Schaub, F., Kargl, F., and Dietzel, S. (2009). Channel Switch and Quiet attack: New DoS Attacks Exploiting the 802.11 Standard. In *Proc. of the 34th IEEE Conference on Local Computer Networks (LCN)*, Zurich, Switzerland.

Malekzadeh, M., Ghani, A. A. A., and Subramaniam, S. (2010). Design of Cyberwar Laboratory Exercises to Implement Common Security Attacks against IEEE 802.11 Wireless Networks. *J. Comp. Sys., Netw., and Comm.*, pages 5:1–5:15.

Manuel, S. (2008). Classification and Generation of Disturbance Vectors for Collision Attacks against SHA-1. Cryptology ePrint Archive, Report 2008/469.

Myneni, S. and Huang, D. (2010). IEEE 802.11 Wireless LAN Control Frame Protection. In *Proc. of the 7th IEEE Conference on Consumer communications and Networking Conference (CCNC)*, pages 844–848, Piscataway, NJ, USA. IEEE Press.

Qureshi, Z. I., Aslam, B., Mohsin, A., and Javed, Y. (2007). A Solution to Spoofed PS-Poll Based Denial of Service Attacks in IEEE 802.11 WLANs. In *Proc. of the 11th WSEAS International Conference on Communications*, pages 7–11, Stevens Point, Wisconsin, USA. World Scientific and Engineering Academy and Society (WSEAS).

Rachedi, A. and Benslimane, A. (2009). Impacts and Solutions of Control Packets Vulnerabilities with IEEE 802.11 MAC. *Wireless Communications and Mobile Computing*, 9(4):469–488.

Ray, S. and Starobinski, D. (2007). On False Blocking in RTS/CTS-Based Multihop Wireless Networks. *IEEE Transactions on Vehicular Technology*, 56(2):849–862.

Rechberger, C. and Rijmen, V. (2008). New Results on NMAC/HMAC when Instantiated with Popular Hash Functions. *Universal Computer Science*, 14(3):347–376.

Rogaway, P. (2011). Evaluation of Some Blockcipher Modes of Operation. Technical report, Cryptography Research and Evaluation Committees (CRYPTREC).

Tews, E. (2007). Attacks on the WEP Protocol. Cryptology ePrint Archive, Report 2007/471.

Whiting, D., Housley, R., and Ferguson, N. (2003). RFC 3610 - Counter with CBC-MAC (CCM).

Wi-Fi Alliance (2003). Wi-Fi Protected Access: Strong, Standards-based, Interoperable Security for Today's Wi-Fi Networks.