Universidade Federal de Pernambuco

Centro de Informática

Pós-graduação em Ciência da Computação

UM MECANISMO DE PROTEÇÃO DE QUADROS DE CONTROLE PARA REDES IEEE 802.11

Marcos Antonio Costa Corrêa Júnior

DISSERTAÇÃO DE MESTRADO

Recife

14 de fevereiro de 2012

Universidade Federal de Pernambuco

Centro de Informática

Marcos Antonio Costa Corrêa Júnior

UM MECANISMO DE PROTEÇÃO DE QUADROS DE CONTROLE PARA REDES IEEE 802.11

Trabalho apresentado ao Programa de Pós-graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre em Ciência da Computação.

Orientador: *Docteur Paulo André da Silva Gonçalves*

Recife

14 de fevereiro de 2012

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus, Pai todo-poderoso, criador de todas as coisas, que me concedeu a graça de existir e que sempre iluminou meu caminho.

À minha família - Mariana, Marquito e Malu - pelo apoio durante esta longa jornada que foi o meu mestrado.

Aos meus pais - Marcos e Maria - que me forneceram subsídios para que eu chegasse até aqui, às minhas irmãs - Diana e Ana Paula - que também enfrentam as dificuldades de um mestrado e me incentivaram.

Agradeço ao grupo de pesquisa liderado pelo meu orientador, pela contribuição, paciência e participação durante as nossas reuniões e apresentações.

Ao meu orientador, Paulo André da Silva Gonçalves, pelas críticas que contribuíram para o aperfeiçoamento do trabalho e ajudaram para que este trabalho atingisse maior grau de maturidade.

Aos demais professores que participaram de minha formação e, com suas disciplinas, contribuíram para a qualidade de minha formação.

Ao Centro de Informática da Universidade Federal de Pernambuco pela infraestrutura e por ser um Centro de Excelência que oferece aos alunos a possibilidade de uma formação de altíssimo nível.

Não sou nada.

Nunca serei nada.

Não posso querer ser nada.

À parte isso, tenho em mim todos os sonhos do mundo.

—ÁLVARO DE CAMPOS HETERÔNIMO DE FERNANDO PESSOA

(Tabacaria, 1928)

RESUMO

As redes sem fio padrão IEEE 802.11 estão presentes nos mais diversos ambientes e continuam a expandir-se devido, principalmente, ao inegável aumento da produtividade para as empresas. Ao mesmo tempo que se expandem, essas redes levam consigo suas vulnerabilidades. As redes sem fio contam com mecanismos para proteção de quadros de dados e também para proteção dos quadros de gerenciamento, apenas os quadros de controle não contam com uma proteção padronizada pelo IEEE. A ausência de proteção possibilita atividades maliciosas que se utilizam de técnicas de manipulação, falsificação e reinjeção de quadros de controle que geram negação de serviço na rede. Esta dissertação propõe um mecanismo de proteção dos quadros de controle do IEEE 802.11, que faz uso de um número de sequência e de um código de autenticação de mensagem a fim de evitar que estações maliciosas, não pertencentes à rede, tenha sucesso ao manipular, falsificar ou reinjetar quadros de controle que levariam a indisponibilidade da rede. O mecanismo proposto destaca-se por proteger todos os quadros de controle indistintamente, possuir um maior grau de segurança e introduz, nesses quadros, um aumento de tamanho significativamente menor em comparação aos trabalhos relacionados que também se propõe a proteger todos os quadros de controle.

Palavras-chave: IEEE 802.11, segurança, quadros de controle, WLAN, redes sem fio, Wi-Fi

ABSTRACT

IEEE 802.11 wireless networks are present in many different environments and continue to expand, mainly due to the undeniable increase in productivity for enterprises. At the same time they expand, these networks lead their vulnerabilities. Wireless networks have mechanisms to protect data frames and also for protection of management frames, only the control frames has not protection mechanisms standardized by IEEE. The absence of protection allows malicious stations use techniques of manipulation, forge and reinjection of control frames that generate denial of service on the network. This dissertation proposes a mechanism for protection of control frames of IEEE 802.11, which uses a sequence number and a message authentication code in order to prevent malicious stations, not belonging to the network, can successfully manipulate, falsify or reinject control frames that would lead to unavailability of the network.The proposed mechanism distinguishes from the others by protecting all control frames, have a higher degree of security and introduces these frameworks, a significantly lower overhead compared to related work that also aims to protect all control frames.

Keywords: IEEE 802.11, security, control frames, WLAN, wireless, Wi-Fi

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

GLOSSÁRIO

AAD *Additional Authentication Data*, ou Dados Adicioais de Autenticação.

ACK *Acknowledgment*.

AES *Advanced Encryption Standard*, ou Padrão de Criptografia Avançada.

AID *Association IDentifier*, ou Identificador de Associação.

AP *Access Point*.

BSSID *Basic Service Set IDentification*.

CCMP *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*, ou Protocolo de Modo Contador com Código de Autenticação de Mensagem por Cifra de Bloco Encadeada.

CRC *Cyclic Redundancy Code*.

CTR *Counter Mode*.

CTS *Clear to Send*.

DoS *Denial-of-Service*, ou negação de serviço.

EAP *Extensible Authentication Protocol*, ou Protocolo de Autenticação Extensível.

EHMAC *Enhanced Hash-based Message Authentication Code*.

FC *Frame Control*.

FCS *Frame Check Sequence*.

FIPS *Federal Information Processing Standard*.

GTK *Group Temporal Key*.

HMAC *Hash-based Message Authentication Code*.

IAPP *Inter-Access Point Protocol*, ou IEEE 802.11F.

IEEE *Institute of Electrical and Electronics Engineers*.

IV *Initialization Vector*, ou Vetor de Inicialização.

MAC *Message Authentication Code*, ou Código de Autenticação da Mensagem.

MPDU *MAC Protocol Data Unit*, ou Unidade de Dados do Protocolo da Camada de Controle de Acesso ao Meio.

NIST *U.S. National Institute of Standards and Technology*.

NS Número de Sequência.

PN *Packet Number*.

PRF *Pseudo Random Function*, ou Funções Pseudoaleatórias.

PS *Power Save (mode)*.

PS-Poll *Power Save Poll*.

PTK *Pairwise Transient Key*.

RA *Receiver Address*, ou *Receiving Station Address*.

RFC *Request for Comments*.

RTS *Request to Send*.

SACK *Secure Acknowledgment*.

SBA *Secure Block Acknowledgment*.

SBAR *Secure Block Acknowledgment Request*.

SCF-End *Secure Contention-Free End*.

SCF-End+CF-Ack *Secure Contention-Free End + Contention-Free ACK*.

SCTS *Secure Clear to Send*.

SHA *Secure Hash Algorithm 1*.

SPS-Poll *Secure Power Save Poll*.

SRTS *Secure Request to Send*.

TA *Transmitter Address*, ou *Transmitting Station Address*.

TK *Temporal Key*.

WEP *Wired Equivalent Privacy*.

WPA *Wi-Fi Protected Access*.

WPA2 *Wi-Fi Protected Access 2*.

CAPÍTULO 1

INTRODUÇÃO

Desde o surgimento do padrão IEEE 802.11 [IEEE Standard 802.11 1999], as redes locais sem fio experimentam um crescimento intenso, já amplamente utilizadas em residências, empresas e espaços públicos de acesso como *shoppings*, aeroportos, bibliotecas e até mesmo restaurantes e bares. Apesar do incremento de usuários, das pesquisas e do aperfeiçoamento da tecnologia, estas redes ainda são vulneráveis a ataques.

1.1 MOTIVAÇÃO

Pouco tempo após surgir a padronização das redes locais sem fio, em 1999, por meio do padrão IEEE 802.11 [IEEE Standard 802.11 1999], o que inibiu a maior adoção destas redes, foi a segurança. Se em uma rede cabeada um indivíduo malicioso deveria, no mínimo, ter acesso a um ponto de rede para conseguir acesso ao fluxo de informações da rede, com as redes sem fio isto não é necessário. O indivíduo malicioso precisa apenas estar dentro da área de cobertura da rede sem fio para que as informações cheguem até ele, e ele possa capturar, modificar ou inserir informações ao fluxo existente. O padrão criado em 1999 trouxe o primeiro mecanismo de proteção para redes sem fio. Rapidamente este mecanismo de proteção começou a ser alvo de questionamentos quanto à sua real capacidade de resistir a ataques e manter o sigilo das informações. A lista de vulnerabilidades deste primeiro mecanismo de segurança, WEP, cresceu bastante criando descrédito na segurança das redes sem fio.

O WEP é considerado ultrapassado devido a esta longa lista de vulnerabilidades e à rapidez com que essas vulnerabilidades podem ser exploradas permitindo um indivíduo malicioso se associar e se autenticar à rede [Fluhrer et al. 2001] [Stubblefield et al.

2001] [Borisov et al. 2001b] [Borisov et al. 2001a] [Tews 2007]. Após o WEP, surgiram dois novos protocolos: o WPA e o WPA2. O WPA introduz um mecanismo de atualização de chaves a cada sessão, melhoramentos no vetor de inicialização (IV) e na verificação de integridade das mensagens, além de implementar também o suporte a 802.1x e ao EAP. WPA representou avanços e melhorias significativos à segurança no que diz respeito à integridade, à autenticação e à privacidade, mesmo ainda utilizando o RC4 como algoritmo criptográfico. O WPA2 veio com a ideia de se tornar o protocolo de segurança de rede sem fio do padrão IEEE 802.11, e não se preocupou com a compatibilidade com os sistemas legados, por isso introduziu um novo algoritmo criptográfico baseado no AES, o CCMP, que é considerado completamente seguro. O WPA2 implementa todos os elementos obrigatórios da emenda IEEE 802.11i posteriormente agregada ao padrão IEEE 802.11 [IEEE Standard 802.11 2007]. O CCMP, utilizado no WPA2, foi projetado para oferecer segurança aos dispositivos, e é mais forte do que o WPA.

Os protocolos e mecanismos já citados no texto, estão voltados para a proteção dos quadros de dados. Em 2009 houve a publicação da emenda IEEE 802.11w [IEEE Standard 802.11w 2009] a qual complementa as especificações do WPA e do WPA2. Essa emenda foi publicada 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 um grupo de trabalho IEEE que desenvolva emendas para a proteção desses quadros. A ausência de mecanismos de proteção aos quadros de controle permite a qualquer estação maliciosa, pertencentes 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 e a confirmação falsa de recebimento de informações que não foram efetivamente recebidas, além da 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.

A falta de proteção aos quadros de controle representa uma lacuna na segurança das redes locais sem fio. Devido a esta lacuna, diversas pesquisas vêm sendo realizadas com a finalidade de prover mecanismos efetivos para a proteção destes quadros [Myneni and Huang 2010] e [Khan and Hasan 2008]. Este trabalho propõe um mecanismo de segurança para a proteção dos quadros de controle de redes IEEE 802.11. Esse novo mecanismo deverá somar-se aos trabalhos anteriores que lograram êxito na proteção dos quadros de dados e nos quadros de gerenciamento, publicados através das emendas IEEE 802.11i e IEEE 802.11w, respectivamente, permitindo com isso, que as redes locais sem fio possuam uma proteção efetiva para os seus três tipos de quadros.

1.2 OBJETIVOS

O objetivo geral desta dissertação é propor um mecanismo que seja capaz de proteger todos os quadros de controle contra ataques que levariam à negação de serviço. O mecanismo deverá realizar a autenticação dos quadros de controle para evitar os efeitos negativos dos quadros forjados à rede, bem como proteger a rede contra o uso destes quadros em ataques de *replay*. Em particular, a proposta deve ser abrangente, proteger indistintamente todos os quadros de controle e ser mais segura que a proposta [Myneni and Huang 2010], a qual também é capaz de proteger os quadros de controle contra diversos ataques, incluindo os ataques de *replay*. Além disso, a proposta deve apresentar um menor impacto negativo na rede devido ao aumento no tamanho dos quadros e utilizar mecanismos de segurança que já estejam presentes em dispositivos compatíveis com o padrão IEEE 802.11.

Para alcançar o objetivo geral, os seguintes objetivos específicos foram definidos:

- Conhecer os quadros de controle do padrão IEEE 802.11;
- Conhecer os ataques aos quadros de controle do padrão IEEE 802.11;
- Estudar as contramedidas aplicadas a ataques direcionados aos quadros de controle;
- Conhecer os mecanismos de segurança presentes nos dispositivos compatíveis com o padrão IEEE 802.11 e o grau de segurança atual destes mecanismos;
- Utilizar os mecanismos de segurança, ainda considerados seguros, compatíveis com o padrão IEEE 802.11 para dar segurança aos quadros de controle;
- Avaliar o reflexo na rede do aumento do tamanho dos quadros e a segurança do mecanismo, comparando-o ao trabalho de Myneni e Huang [Myneni and Huang 2010];
- Apresentar as conclusões quanto à segurança e ao impacto do aumento no tamanho dos quadros devido ao uso do mecanismo proposto.

1.3 ORGANIZAÇÃO

O Capítulo 2 apresenta os quadros de controle do IEEE 802.11 e os ataques existentes contra eles, além de mostrar como é feita a utilização do CCMP com o AES dentro do WPA2. O Capítulo 3 traz uma visão geral dos trabalhos científicos que guardam relação com a segurança dos quadros de controle e realiza uma descrição dos trabalhos previamente desenvolvidos juntamente com uma análise crítica. Os trabalhos são organizados de forma cronológica, permitindo, com isso, entender como os ataques e as propostas de defesa evoluíram. O Capítulo 4 apresenta, detalhadamente, a proposta, fala da formação do vetor de inicialização bem como do uso do CBC-MAC com o AES. O Capítulo 5 avalia a segurança do mecanismo e mostra um estudo do impacto do aumento do tamanho dos quadros no tráfego de uma rede sem fio com o uso do mecanismo proposto e uma simulação de uma rede sem fio com predominância de volume de tráfego de dados. Finalmente, o Capítulo 6 apresenta as conclusões deste trabalho.

CAPÍTULO 2

FUNDAMENTOS

Este capítulo, na Seção 2.1, apresenta os quadros de controle definidos pelo padrão IEEE 802.11 e possíveis ataques contra estes quadros. A Seção 2.2 apresenta como é feita a utilização do CCMP com o AES dentro do WPA2. As informações que serão apresentadas neste capítulo tornarão mais simples a compreensão do mecanismo proposto, o qual será apresentado no Capítulo 4.

2.1 QUADROS DE CONTROLE DO IEEE 802.11

Os quadros de controle são usados para auxiliar no envio dos quadros de dados, para gerenciar o acesso ao meio sem fio e fornecer funções que garantam a confiabilidade na camada de controle de acesso ao meio.

Os quadros de controle são um dos tipos de quadros previstos no padrão IEEE 802.11, juntamente com os quadros de dados e os quadros de gerenciamento. Inicialmente, havia seis quadros de controle conforme a Tabela 2.1 apresentada a seguir (extraída e adaptada do padrão IEEE publicado em 1999).

Os diferentes grupos de trabalho do IEEE propuseram diversos aperfeiçoamentos e criaram novas funcionalidades, com isso, surgiu a necessidade de acrescentar novos quadros de controle. O *Block Ack* e o *Block Ack Request* surgiram com o IEEE 802.11e [IEEE Standard 802.11e 2005], foram posteriormente aperfeiçoados no IEEE 802.11n [IEEE Standard 802.11n 2009] e no decorrer deste trabalho serão também detalhados.

Tabela 2.1 Combinação Válida de Tipos e Subtipos [IEEE Standard 802.11 1999].

Tipo	Descrição Tipo	Subtipo	Descrição Subtipo
01	Controle	1010	*Power Save (PS)-Poll*
01	Controle	1011	*Request to Send (RTS)*
01	Controle	1100	*Clear to Send (CTS)*
01	Controle	1101	*Acknowledgement (ACK)*
01	Controle	1110	*Contention-Free (CF)-End*
01	Controle	1111	*CF-End + CF-Ack*

2.1.1 PS-Poll (Power Save Poll)

Os Pontos de Acesso (APs) são projetados para dar suporte a estações que estejam utilizando gerenciamento de energia em suas interfaces. Nesse caso, a estação desliga e liga sua interface de comunicação periodicamente para economizar energia. Durante o período em que a estação está com sua interface desligada, ela não está transmitindo nem recebendo quadros, este modo mais econômico em termos de consumo energético é o modo *power-save* (PS). Quando uma estação passa para o modo PS, esta deve informar o AP sobre a referida mudança. O AP, por sua vez, sabendo que uma determinada estação está no modo *power-save*, não irá transmitir MSDUs para a referida estação que opera em modo PS, o AP passa então a armazenar os MSDUs destinados àquela estação. Ao religar a interface, a estação procura por *beacons* do AP que informam se existem quadros armazenados para aquela estação. Caso haja quadros armazenados no AP para a estação, ela, que estava operando em modo PS, deve transmitir um pequeno quadro de controle denominado PS-Poll para o ponto de acesso, a fim de recuperar quaisquer quadros armazenados enquanto ela estava no modo *power-save*. O AP deverá responder com o MSDU armazenado correspondente de imediato, ou reconhecer o PS-Poll e responder com o MSDU correspondente depois. 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 mais quadros armazenados para aquela estação.

O quadro PS-Poll, ilustrado na Figura 2.1, possui 20 *bytes* de comprimento e é for-

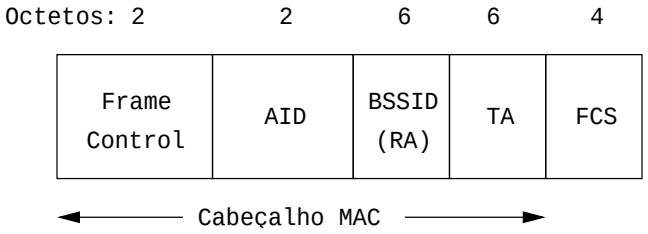


Figura 2.1 PS-Poll no Padrão IEEE 802.11.

mado por 5 campos: FC (*Frame Control)*, AID (*Association ID*), *Endereço 1* (BSSID ou RA), *Endereço 2* (TA) e FCS (*Frame Check Sequence*). O campo FC possui 2 *bytes* e permite identificar o tipo de quadro e provê algumas informações de controle. O campo AID representa um identificador de associação da estação e possui 2 *bytes*. 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 roubo de identidade devido a quadros de controle e gerenciamento não protegidos é uma vulnerabilidade tanto do WEP quanto do 802.11i. As vulnerabilidades são portas abertas para *hackers* lançarem ataques de DoS bem sucedidos. O IEEE 802.11w resolveu, em parte, os problemas de DoS, mas ainda há uma alta taxa de sucesso de ataques à disponibilidade no modo *Power Saving* (PS) devido principalmente a duas coisas:

- dispositivos móveis portáteis operam em modo PS para conservar seus recursos escassos (bateria) e,
- quando os ataques estão sendo executados os usuários legítimos estão inativos e não estão cientes da atividade maliciosa na rede.

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, causando uma negação de serviço bem sucedida, por meio do bloqueio daquela estação vítima de receber os

quadros que o AP armazenou enquanto ela estava "dormindo". O ataque só é possível por causa da falta de autenticação dos quadros PS-Poll.

2.1.2 RTS (Request to Send)

Quadros de controle RTS fazem parte de uma mecanismo usado para obter controle do meio com o intuito de transmitir quadros grandes em redes IEEE 802.11 sem que ocorra colisões, ou que estas colisões sejam significativamente reduzidas, sincronizando o acesso ao canal e evitando a ocorrência de um problema conhecido como Problema do Nó Escondido [Ray and Starobinski 2007]. O mecanismo do qual o RTS faz parte, executa uma rápida inferência de colisão e uma checagem de caminho de transmissão. Neste mecanismo, se não for detectada uma informação de retorno para um quadro RTS na estação que originou o RTS, é provável que naquela rede tenha ocorrido uma colisão. Com o mecanismo, a colisão tem um menor impacto, pois os quadros são menores e esta estação poderá repetir o processo de envio do RTS (depois de observar as outras regras de uso do meio) mais rapidamente do que se um longo quadro de dados tivesse sido transmitido e um quadro de retorno não tivesse sido detectado (provável situação de colisão).

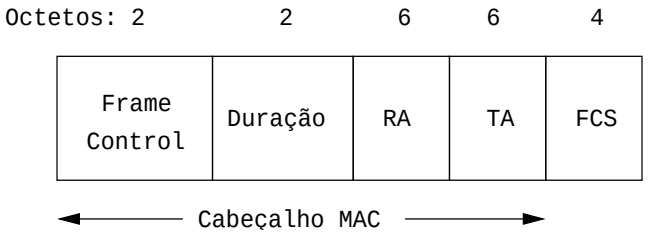


Figura 2.2 RTS no Padrão IEEE 802.11.

O RTS, ilustrado na Figura 2.2, possui 20 *bytes* de comprimento, sendo dividido em 5 campos: FC (*Frame Control*), *Duração*, *Endereço 1* (RA), *Endereço 2* (TA) e FCS (*Frame Check Sequence*). O campo FC possui 2 *bytes* e 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 mecanismo que faz uso de quadros RTS não precisa ser usado em todas as transmissões de quadros, pois este mecanismo adiciona um certo custo e o benefício deste mecanismo nem sempre justifica este custo adicional, especialmente para quadros de dados pequenos. Um atributo pode ser setado na estação, de forma a permitir que as estações sejam configuradas de três diferentes formas: sempre usar o mecanismo (não recomendável por conta do custo adicionado, conforme comentamos), nunca usar o mecanismo, ou só usar em quadros mais longos do que um comprimento especificado.

Todas as estações devem detectar quadros RTS e ainda que a estação seja configurada para não iniciar o mecanismo do qual o RTS faz parte, esta deve ainda atualizar seu tempo de espera com a informação de duração contida no campo *Duração* em um quadro RTS recebido, e deve sempre responder para um RTS endereçado a ela com um quadro de resposta, se permitido pelas regras de acesso ao meio [IEEE Standard 802.11 2007].

Um mecanismo de *carrier sense* (CS) virtual, que irá determinar o tempo de espera, deve ser fornecido pelo controle de acesso ao meio (MAC) e é conhecido como NAV (*Network Allocation Vector*). O NAV mantém uma previsão de tráfego futuro do meio, com base em informações de duração que são anunciadas justamente no campo *Duração* no cabeçalho MAC de praticamente todos os quadros de controle, inclusive do quadro RTS (a exceção fica por conta do quadro *PS-Poll* que não tem campo *Duração*. O mecanismo de ajuste do NAV usando as informações do campo *Duração* é descrito em [IEEE Standard 802.11 2007], o detalhamento foge do nosso escopo.

Um atacante pode fazer uso do quadro de controle RTS para tornar o meio indisponível e com isso realizar um ataque de negação de serviço (DoS), o procedimento usando esse quadro faz uso do NAV para indicar que a rede está ocupada dentro de determinado intervalo de tempo. Para a reserva deste intervalo de tempo, o atacante forja o RTS, através da manipulação de informações desses quadros forjados, o atacante pode inclusive determinar quanto tempo a rede ficará indisponível. O tempo que o ataque de negação de

serviço se estende, está limitado a 32.767 μs [Koenings et al. 2009] [IEEE Standard 802.11 2007] que é o valor máximo do campo *Duração*, conforme descrição feita anteriormente.

O ataque de reserva de NAV acontece de forma que o NAV seja maior que zero para atrasar permanentemente a transmissão legítima. Em [Chen and Muthukkumarasamy 2006] mostrou-se que ataques de DoS usando NAV são independentes de mídia (IEEE 802.11a, b e g), de baixo consumo de energia e que para executar este ataque é necessário injetar repetidamente quadros RTS em uma frequência apropriada, que assegura que o valor do NAV em cada estação é maior do que zero.

O ataque de replay de quadros RTS ocorre quando uma falsa estação pode ouvir o canal e capturar o quadro RTS enviado por uma estação legítima para a AP e retransmite este quadro para a AP em um momento posterior. Quando a AP envia um quadro de resposta àquele RTS o quadro é rejeitado pois o remetente desse RTS não foi a estação legítima e sim a falsa estação. Porém, outra estação vendo o quadro de retorno atualizará o seu NAV. Se o atacante for mais elaborado, minucioso, ele pode mudar a duração para um valor mais alto, fazendo essa outra estação aguardar por um grande período de tempo antes de transmitir, enquanto a estação legítima pode ainda transmitir os pacotes pois ela não atualizou o NAV [Myneni and Huang 2010].

Tanto o ataque de forjar quadros RTS quanto o ataque de replay são efetivos porque o IEEE 802.11 não provê nenhum 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 de retorno do RTS usados nesses ataques executam as ações previstas pelo protocolo, bloqueando temporariamente suas transmissões e, portanto, sofrendo uma negação de serviço.

2.1.3 CTS (Clear to Send)

Os quadros CTS podem ser encontrados como parte do mecanismo RTS/CTS utilizado em redes IEEE 802.11, desta forma, os quadros CTS são transmitidos como quadros de resposta a quadros RTS previamente enviados. No mecanismo RTS/CTS, 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 postegar suas transmissões por um determinado período de tempo, de acordo com o valor que vem determinado no campo *Duração* dos quadros. O período que os outros nós postergam a transmissão, engloba o tempo necessário para a subsequente transmissão dos dados e recepção da confirmação de seu recebimento. 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 2.347 octetos [da Conceição et al. 2006]. Dentro do mecanismo RTS/CTS os quadros de controle CTS jamais seriam gerados sem um RTS que o antecedesse.

A segunda utilização dos quadros de controle CTS se dá em um mecanismo de proteção que aperfeiçoa a co-existência entre os padrões IEEE 802.11g e IEEE 802.11b evitando a interferência do padrão IEEE 802.11g com estações legadas do padrão IEEE 802.11b, esse mecanismo é frequentemente referenciado como *CTS-to-self* [Bai et al. 2009] [IEEE Standard 802.11g 2003], pois o quadro CTS é transmitido por algum dispositivo com o endereço MAC dele mesmo como destino, para com isso realizar a reserva do meio.

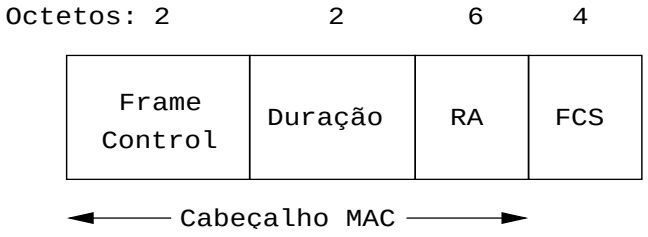


Figura 2.3 CTS no Padrão IEEE 802.11.

O CTS, ilustrado na Figura 2.3, possui 14 *bytes* de comprimento, sendo dividido em 4 campos: FC (*Frame Control*), *Duração*, *Endereço 1* (RA) e FCS (*Frame Check Sequence*). O campo FC possui 2 *bytes* e 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]. O campo *Endereço 1* possui 6 *bytes* e representa o endereço do receptor. O campo FCS possui 4 *bytes* e é preenchido com um CRC-32 para a detecção de erros.

O ataque de injetar falsos *frames* CTS ocorre quando uma falsa estação pode formar quadros CTS falsos e transmiti-los. Esse ataque é muito poderoso, pois tanto as estações

1 e 2 quanto os APs presentes na rede, irão atualizar o tempo do seu contador NAV. Todas as estações e APs presentes no canal que consigam ouvir a transmissão irão retardar o envio de seus dados de acordo com o que estiver indicado pelo quadro CTS.

No ataque de replay CTS, a estação falsa pode ouvir o canal e capturar os quadros CTS enviados por um AP em resposta a qualquer RTS enviado pela estação 1 e pode reenviar este mesmo quadro CTS capturado. A estação 1, assim como no caso anterior do ataque de replay RTS, rejeita o quadro CTS e não atualizará o seu NAV. As outras estações, no entanto, com a recepção do quadro CTS, atualizam o contador do NAV com o valor presente no campo *Duração* do quadro CTS, o que fará com que as outras estações retardem a transmissão até o contador NAV expirar.

2.1.4 ACK (Acknowledgement)

Os quadros ACK são usados para confirmar o recebimento de alguns tipos de quadros, esse processo de confirmação é necessário na camada MAC e faz dos quadros de controle ACK os quadros que trafegam em maior quantidade nas redes sem fio IEEE 802.11.

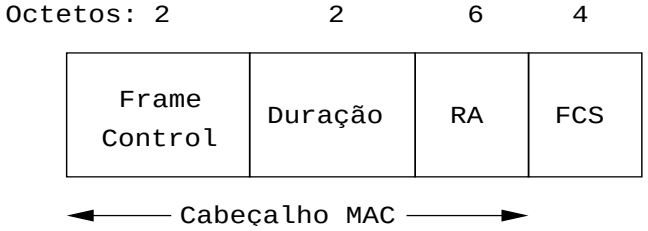


Figura 2.4 ACK no Padrão IEEE 802.11.

O quadro ACK, ilustrado na Figura 2.4, possui o mesmo formato e tamanho dos quadros CTS. Possuem 14 *bytes* de comprimento, sendo dividido em 4 campos: FC (*Frame Control*), *Duração*, *Endereço 1* (RA) e FCS (*Frame Check Sequence*). O campo FC possui 2 *bytes* e 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]. O campo *Endereço 1* possui 6 *bytes* e representa o endereço do receptor. O campo FCS possui 4 *bytes* e é preenchido

com um CRC-32 para a detecção de erros.

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 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 e CTS para a negação de serviço. Em [Rachedi and Benslimane 2009], os autores apresentam o ataque denominado *False packet validation*. Neste 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.

2.1.5 CF-End (Contention Free End)

O IEEE 802.11 [IEEE Standard 802.11 2007] define duas funções de coordenação do canal, DCF (usada na maior parte dos dispositivos) e PCF. 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, este modo de coordenação do canal é usado, portanto, para um acesso ao canal centralizado e livre de disputa. 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*).

Os quadros CF-End, cujo formato está ilustrado na Figura 2.5, possuem 20 *bytes* de comprimento divididos em 5 campos: FC (*Frame Control*), *Duração*, *Endereço 1* (RA), *Endereço 2* (BSSID ou TA) e FCS (*Frame Check Sequence*). Em particular nesses 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.

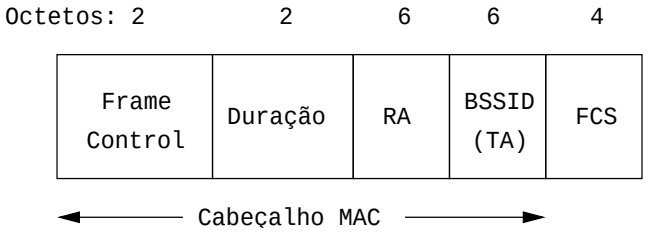


Figura 2.5 *Contention Free End* no Padrão IEEE 802.11.

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

2.1.6 CF-End+CF-Ack (CF-End+Contention Free Ack)

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 anteriores que já foram recebidos.

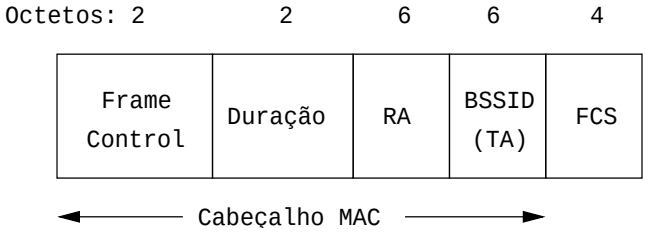


Figura 2.6 *CF-End+Contention Free Ack* no Padrão IEEE 802.11.

O CF-End+CF-Ack, ilustrado na Figura 2.6, também possui 20 *bytes* de comprimento, dividido em 5 campos: FC (*Frame Control*), *Duração*, *Endereço 1* (RA), *Endereço 2* (BSSID ou TA) e FCS (*Frame Check Sequence*). Os campos deste quadro são preenchidos de forma similar ao preenchimento efetuado para os quadros CF-End, descrito anteriormente.

Assim como foi mostrado para os quadros CF-End, o ataque aos quadros CF-End+CF-Ack pode ser executado através da manipulação do campo *Duração* com o intuito de tor-

nar a rede indisponível, bloqueando a comunicação dos dispositivos legítimos. Em [Malekzadeh et al. 2010] mostrou-se que os efeitos são tão nocivos para o funcionamento da rede quanto os ataques similares direcionados a outros tipos de quadros de controle.

2.1.7 Novos Quadros de Controle

Em sistemas legados 802.11 a/b/g um ACK é enviado da estação receptora para a transmissora para confirmar recepção de cada *frame*. Se a estação transmissora não recebe o ACK, retransmite o *frame* até um ACK ser recebido. Isso adiciona robustez, mas degrada eficiência. Com o passar do tempo, surgiram novos aperfeiçoamentos ao padrão original, cresceu a necessidade de adicionar eficiência sem abrir mão da robustez. Foram acrescentados os quadros de controle BlockAck e BlockAckReq [IEEE Standard 802.11e 2005], que permitem um novo esquema de confirmação (*acknowledgement*), esses quadros foram definidos para reduzir o desperdício devido às transmissões frequentes de quadros de controle ACK. Com o acréscimo dos dois novos quadros de controle a Tabela 2.1 passa a ter dois novos subtipos identificados por 1000 e 1001, BlockAckReq e BlockAck respectivamente, como mostrado na Tabela 2.2 presente inicialmente na emenda IEEE 802.11e [IEEE Standard 802.11e 2005] e depois incorporada ao documento do padrão IEEE 802.11 de 2007 [IEEE Standard 802.11 2007].

Tabela 2.2 Combinação Válida de Tipos e Subtipos [IEEE Standard 802.11 2007].

Tipo	Descrição Tipo	Subtipo	Descrição Subtipo
01	Controle	1000	*Block Ack Request (BlockAckReq)*
01	Controle	1001	*Block Ack (BlockAck)*
01	Controle	1010	*Power Save (PS)-Poll*
01	Controle	1011	*Request to Send (RTS)*
01	Controle	1100	*Clear to Send (CTS)*
01	Controle	1101	*Acknowledgement (ACK)*
01	Controle	1110	*Contention-Free (CF)-End*
01	Controle	1111	*CF-End + CF-Ack*

2.1.7.1 BAR (*Block Ack Request*)

Os quadros BAR e BA, introduzidos pela emenda IEEE 802.11e [IEEE Standard 802.11e 2005], são usados para permitir a confirmação de um bloco de quadros usando apenas um quadro de confirmação. O quadro BAR é usado para requisitar a confirmação de recepção de um bloco de quadros.

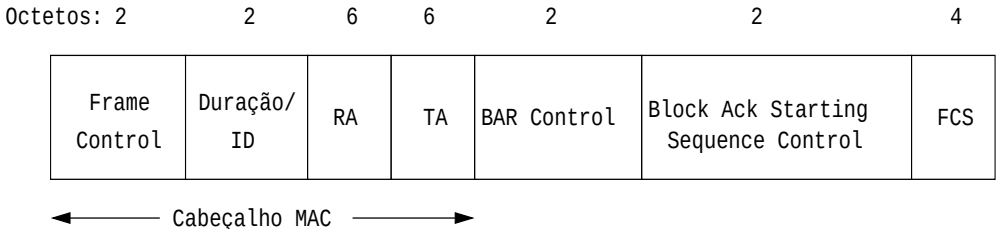


Figura 2.7 *Block Ack Request* no Padrão IEEE 802.11.

O quadro BAR, ilustrado na Figura 2.7, possui 24 *bytes* de comprimento e é formado por 7 campos: FC (*Frame Control*), *Duração*, *Endereço 1* (RA), *Endereço 2* (TA), BAR *control*, *Block Ack Starting Sequence Control* e FCS (*Frame Check Sequence*). O campo BAR *control* possui 2 *bytes* e é usado para a negociação de 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. Os demais campos possuem o mesmo tamanho e descrição já apresentados para os quadros RTS.

O mecanismo de confirmação em bloco de quadros, BA e BAR, também pode ser explorado através da falsificação de informações contidas no quadro BAR. Um estudo sobre o uso malicioso dos quadros BAR é apresentado em [Koenings et al. 2009] e [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. Eles demonstram que um único quadro BAR manipulado pode causar uma negação de serviço na rede por 10 segundos.

2.1.7.2 BA (*Block Ack*)

O quadro BA, introduzidos pela emenda IEEE 802.11e [IEEE Standard 802.11e 2005], é usado em conjunto com o BAR no mecanismo capaz de permitir a confirmação de um bloco de quadros usando apenas um quadro de confirmação. O quadro BA é utilizado como resposta ao quadro de requisição BAR. BA e BAR, em conjunto, são usados para aperfeiçoar a eficiência do protocolo, seu uso parte da premissa de que quanto menor for o quadro, menor a eficiência do transporte devido ao custo de cabeçalho e de envio de quadros de confirmação. O mecanismo fornece ganhos significativos e permite que o emissor envie vários pacotes de dados em sequência, até o tamanho do buffer que for previamente combinado. Os quadros BAR são enviados pelo emissor depois da transmissão de um fluxo de dados. Os quadros BA, por sua vez, contêm um *bitmap* que indica os pacotes recebidos.

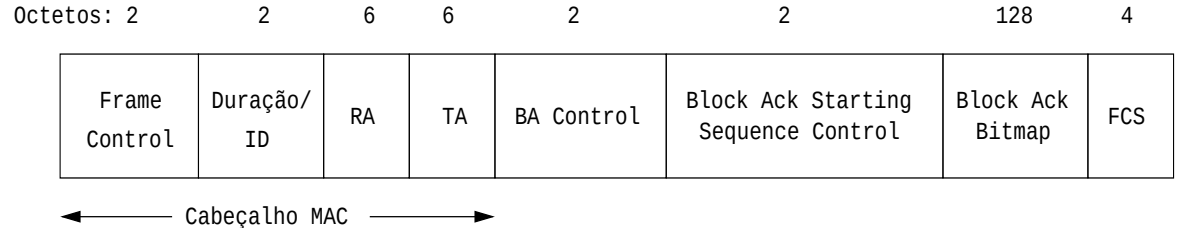


Figura 2.8 *Block Ack* no Padrão IEEE 802.11.

O quadro BA, ilustrado na Figura 2.8, 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 foram recebidos, permite indicar a recepção de até 64 quadros. Os demais campos possuem tamanho e descrição similares aos apresentados para o quadro RTS.

2.2 CCMP (PROTOCOLO DE MODO CTR COM CBC-MAC)

A emenda IEEE 802.11i [IEEE Standard 802.11i 2004], finalizada em julho de 2004, veio com a definição de um novo método de cifragem, o CCMP, baseado no *Advanced Encryption Standard* (AES) [NIST 2001], um padrão certificado pelo governo americano e aprovado pelo *U.S. National Institute of Standards and Technology* (NIST) anunciado como *Federal Information Processing Standard*-197 (FIPS-197).

O padrão IEEE 802.11 [IEEE Standard 802.11 2007] republicado em 2007 incorpora a emenda IEEE 802.11i.

O CCMP foi concebido para prover confidencialidade de dados, autenticação, integridade e proteção contra *replay*.

Apesar de ser considerado completamente seguro, a adoção do CCMP na época enfrentava certa resistência, pois trazia o inconveniente de que muitas interfaces de redes ainda não suportavam o funcionamento do padrão.

2.2.1 Uso do CCMP em Quadros de Dados

Fazendo-se uso de cifragem baseada no AES, poder-se-ia usar um grande número de diferentes algoritmos e modos de operação.

O modo que foi escolhido no padrão definido pelo IEEE foi o modo contador (*Counter Mode - CTR*) com CBC-MAC (*Cipher Block Chaining Message Authentication Code*) [Whiting et al. 2003] [Dworkin 2004].

Contador com CBC-MAC (CCM) é um modo de operação combinado, no qual a mesma chave que é usada na cifragem, para confidencialidade, também é usada para gerar um valor de verificação seguro, para verificação de integridade. Ele permite fazer a cifragem e a integridade em um mesmo processo. O modo contador (CTR) fornece o sigilo dos dados (cifragem) enquanto o CBC-MAC é responsável pela integridade e autenticidade.

Todo o processo AES usado dentro do CCMP usa o AES com uma chave de 128 *bits* e um bloco de tamanho também de 128 *bits*.

O CCM é definido na RFC 3610 [Whiting et al. 2003], é um modo genérico que pode ser usado com qualquer algoritmo de cifragem orientado a blocos. Dois parâmetros precisam ser definidos, são eles M e L, no CCMP temos:

- M = 8, que indica que o tamanho do campo g̃lsglo:mic é de 8 octetos;
- L = 2, indica que o campo *Length* é de 2 octetos, que é suficiente para o maior MPDU possível do padrão IEEE 802.11.

Estes dois parâmetros serão responsáveis pelo valor de outras informações necessárias. A Tabela 2.3 apresenta os valores de codificação dos parâmetros M e L usados no CCMP.

Tabela 2.3 Codificação dos Parâmetros L e M [Whiting et al. 2003].

Nome	Descrição	Tamanho	Codificação
M	Número de octetos do campo autenticação	3 *bits*	(M-2)/2
L	Número de octetos do campo *length*	3 *bits*	L-1

O CCM requer uma chave temporária diferente para cada nova sessão, também requer um valor de *nonce* único para cada quadro protegido por uma determinada chave temporária, e o CCMP usa um *packet number* (PN) de 48 *bits* para a construção do *nonce*. O reuso de um mesmo PN com a mesma chave temporária vai contra todas as garantias de segurança.

2.2.1.1 Entradas para o processamento do CCM

O CCM é uma cifra de bloco genérica para cifragem e autenticação, no padrão IEEE 802.11 é usada com o AES para formar o CCMP.

Para o processamento quatro entradas são necessárias para o CCM:

1. Chave: a chave temporal (128 *bits*);
2. *Nonce*: O *nonce* tem seu comprimento em termos de octetos atrelado ao parâmetro L pela fórmula 15-L que para o padrão IEEE 802.11 corresponde a 13 octetos. Uma alerta deve ser feito, quando utilizando uma chave qualquer, o valor de *nonce* deve

ser único. Isto é, o conjunto de valores *nonce* usados com qualquer chave dada não deve ser duplicado. Usar o mesmo *nonce* para duas mensagens diferentes cifradas com a mesma chave destrói as propriedades de segurança deste modo.

3. Corpo do quadro: o corpo do quadro tem de 1 a 2296 octetos

4. AAD: o *AAD* consiste de uma *string* que tem entre 22 e 30 octetos. Ele pode ser usado para autenticar cabeçalhos de quadros, se não se deseja autenticar dados adicionais pode ser colocado como entrada uma *string* de comprimento zero [Whiting et al. 2003].

Tabela 2.4 Entradas para o CCM.

Nome	Descrição	Tamanho
K	Chave de cifra de bloco	128 *bits*
N	Nonce	13 octetos
m	Mensagem para autenticar	1 a 2296 octetos
a	Dados adicionais de autenticação	22 a 30 octetos

O processamento do CCM fornece autenticação e integridade para o corpo do quadro e o *AAD*, assim como fornece também confidencialidade ao corpo do quadro. A saída do CCM consiste de dados cifrados e 8 octetos adicionais de MIC.

2.2.1.2 Número do Pacote (PN)

O *PN* é incrementado por um número positivo para cada MPDU. O PN nunca deverá se repetir para uma série de MPDUs que usem a mesma chave temporal TK, sob pena de acabar com todas as garantias de segurança. O *PN* tem 48 *bits*.

2.2.1.3 Construção do AAD

O comprimento do AAD pode variar dependendo da presença ou não dos campos *QC* e *A4*. Se os campos *QC* e *A4* o AAD tem o formato ilustrado na Figura 2.9.

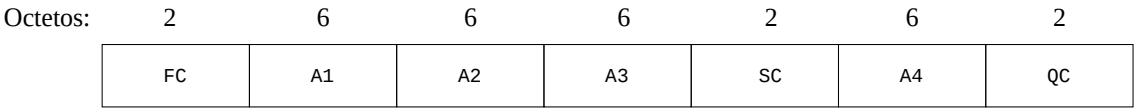


Figura 2.9 Formato do AAD.

2.2.1.4 Construção do *Nonce* CCM

O *nonce* é formado pela concatenação do *Octeto de Prioridade*, *Endereço A2* e o número do pacote (PN).

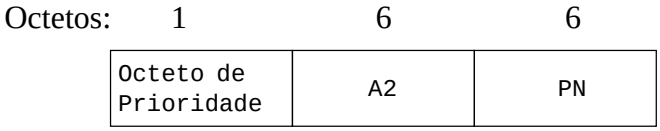


Figura 2.10 *Nonce* no 802.11.

2.2.2 Processo de Encapsulamento CCMP

A Figura 2.11 mostra o processo de encapsulamento CCMP por meio de um diagrama de blocos.

O CCMP cifra o *payload* de um texto claro MPDU e encapsula o texto cifrado através dos seguintes passos:

1. Incrementa o PN para obter um novo PN para cada MPDU, então o PN nunca se repete para a mesma TK;

2. Usa os campos do cabeçalho MPDU para construir o AAD para o CCM. O CCM provê proteção de integridade para os campos incluídos no AAD;

3. Constrói o CCM *nonce* através do PN, *A2* e da *Prioridade* do MPDU onde *A2* é o *Endereço 2* do MPDU;

4. Coloca o novo PN e o *key id* nos 8 octetos do cabeçalho CCMP;

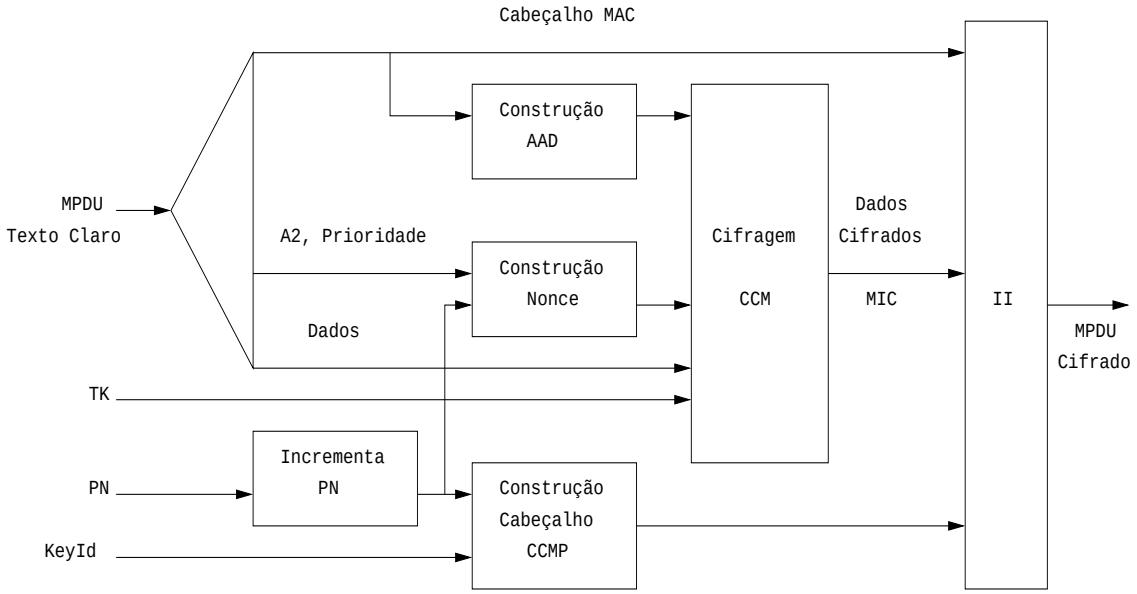


Figura 2.11 Diagrama em Bloco do Processo de Encapsulamento CCMP [IEEE Standard 802.11 2007].

5. Usa a *TK*, *AAD*, *nonce*, e dados MPDU para formar o texto cifrado e o MIC. Este passo é conhecido como processamento inicial CCM;

6. Forma o MPDU cifrado combinando o cabeçalho original MPDU, o cabeçalho CCMP, os dados cifrados e o MIC.

A Figura 2.12 mostra o processo de encapsulamento CCMP para um quadro de dados. Para o entendimento da proposta deste trabalho é fundamental entender a parte superior na qual é feito o cálculo do MIC, pois esse processo será útil no entendimento do mecanismo proposto.

O processamento dos dados realizados pelos blocos AES no Cálculo do MIC (na parte superior da Figura 2.12) e na Cifragem (ilustrada na parte inferior da Figura 2.12) usam a mesma chave temporária (para o CCMP é chamada simplesmente *Temporal Key* (TK)).

O cálculo do MIC e o processo de cifragem seguem por caminhos paralelos como mostrado na Figura 2.12.

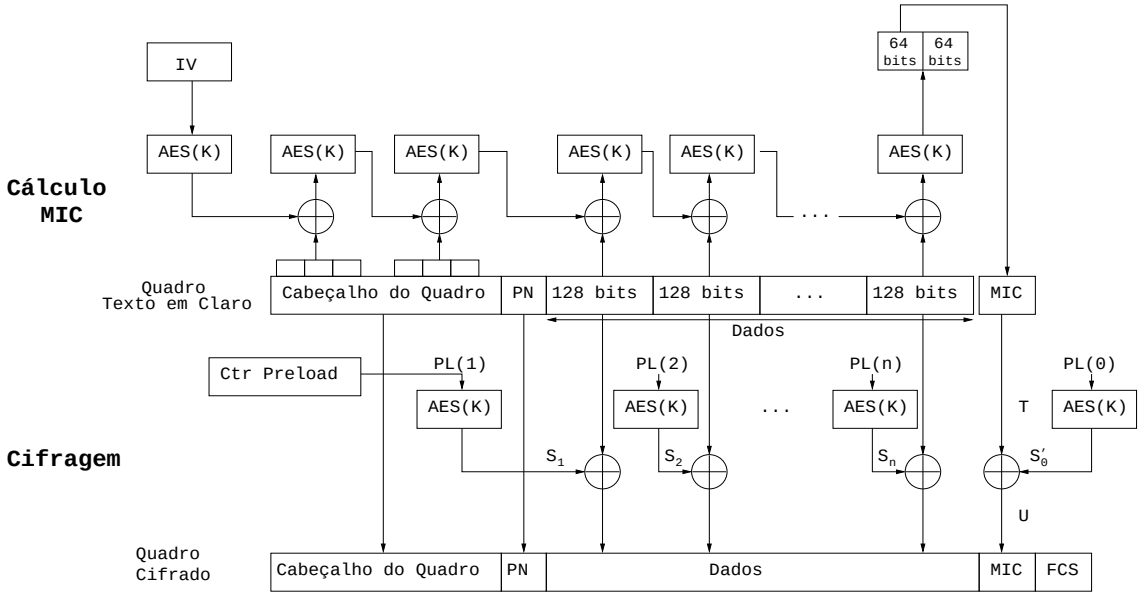


Figura 2.12 Processo de Encapsulamento CCMP [Eaton 2002].

2.2.2.1 Autenticação

O primeiro passo é calcular o campo de autenticação T. Inicialmente é definida uma sequência de blocos B_0, B_1, ..., B_n e então aplicado o CBC-MAC a esses blocos. O primeiro bloco B_0 é também conhecido como vetor de inicialização (IV) ele é formado conforme demonstra a Tabela 4.1:

Tabela 2.5 Bloco B_0.

Número do Octeto	Conteúdo
0	Flags
1 ... (15 - L)	Nonce
(16 - L) ... 15	l(m)

Onde o campo *Flags* ocupa 1 *byte* e também possui formatação pré-definida ilustrada na Tabela 2.6. O *Nonce* teve o seu formato anteriormente ilustrado, vale ressaltar que o seu valor é único e nunca deverá ser repetido com o uso de uma mesma chave criptográfica.

Na Tabela 2.6 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

Tabela 2.6 Campos *Flags* Autenticação.

Número do Bit	Conteúdo
7	Reservado (sempre zero)
6	Adata
5 ... 3	M'
2 ... 0	L'

de autenticação de dados adicionais, ou *AAD*, quando igual a 1. Caso a técnica não seja utilizada, *Adata* deve ser zero. Os 3 *bit* 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.

Após o IV, são adicionados (opcionalmente) os blocos de autenticação de dados adicionais (AAD), em seguida são adicionados os blocos das mensagens. Os blocos das mensagens são formados pela divisão da mensagem em blocos de 128 *bits* e então completado o último bloco com zeros se necessário.

O resultado é uma sequência de blocos $B_0, B_1, ..., B_n$, onde n+1 é o número total de blocos da mensagem. O CBC-MAC é calculado por:

Algoritmo 2.2.1: T (K, B, n, M)

$X_1 \leftarrow E(K, B_0)$

para $i = 1$ **até** n **faça**

$\quad X_{(i+1)} \leftarrow E(K, X_i \oplus B_i)$

$T \leftarrow M$ *primeiros bytes de* $X_{(n+1)}$

onde E() é a função criptográfica usada, K é a chave criptográfica, M é o número de *bytes* do campo autenticação e T é o código de autenticação.

2.2.2.2 Cifragem

Para a cifragem é usado o modo contador (CTR). Primeiramente são definidos os blocos que irão passar pelo processo de cifragem:

para i = 0 **até** n **faça**

$S_i \leftarrow E(K, A_i)$

Os valores de A_i são formatados de maneira semelhante ao IV, onde o campo A_i (campo CTR) é codificado nos *bytes* mais significativos por:

Tabela 2.7 Bloco A_i.

Número do Octeto	Conteúdo
0	Flags
1 ... (15 - L)	Nonce
(16 - L) ... 15	Contador i

O campo *Flags* é formatado da seguinte maneira:

Tabela 2.8 Campos *Flags* Cifragem.

Número do Bit	Conteúdo
7	Reservado (sempre zero)
6	Reservado (sempre zero)
5 ... 3	Zero
2 ... 0	L'

O primeiro *bit* de ordem mais alta é reservado para uso futuro e deve ser sempre zero. O segundo *bit* de ordem mais alta corresponde ao *Adata* no bloco B_0, mas que não tem utilidade aqui, fica reservado e deve ser setado para zero. Os *bits* 3,4 e 5 também são setados para zero, assegurando que todos os blocos A são distintos de B_0, pois B_0 tem codificação igual a codificação de M que é diferente de zero nesta posição. Os 3 *bit* seguintes contém L' usando a mesma codificação que é usada em B_0.

A mensagem é cifrada através do XOR efetuado entre os octetos da mensagem m com os primeiros *l(m)* octetos da concatenação de $S_1, S_2, S_3, ..., S_n$. Note que S_0 não é usada para cifrar mensagens.

O primeiro valor a ser empregado no processo de cifragem mostrado na Figura 2.12 é o *Ctr Preload* similar ao IV empregado no cálculo do MIC, possui 128 *bits*, mas usa um contador inicializado em 1 em vez de um *l(m)* resultando em um contador diferente para cifrar cada quadro.

O valor de autenticação do texto cifrado U é calculado por meio da cifragem de T, calculado durante o processo de autenticação, com o bloco S_0 e truncado até o comprimento desejado (S'_0).

U $\leftarrow$ T $\oplus$ *primeiros M bytes* (S_0)

O resultado final consiste da mensagem cifrada seguida por um valor de autenticação cifrado U.

2.3 RESUMO

Este capítulo descreveu os quadros de controle, mostrando o formato destes e sua utilidade dentro de uma rede local sem fio IEEE 802.11, além de exemplificar possíveis ataques a cada um dos quadros de controle e o como este ataque afetaria à disponibilidade da rede.

O capítulo explicou ainda o processo de cifragem, realizado pelo modo contador, e o processo do cálculo do código de autenticação de mensagem (MAC), realizado pelo CBC-MAC. Juntos, modo contador e o CBC-MAC formam o CCM, no padrão IEEE 802.11, o CCM é usado com AES para formar o CCMP [IEEE Standard 802.11i 2004].

O conhecimento do funcionamento do CCMP, apresentado neste capítulo, permitirá entender a proposta deste trabalho, que será detalhada no Capítulo 4 e é bastante semelhante ao cálculo do MAC para quadros de dados que é realizado pelo CBC-MAC dentro do CCMP.

CAPÍTULO 3

TRABALHOS RELACIONADOS

Os estudos voltados para a segurança de redes sem fio - padronizados inicialmente no 802.11 [IEEE Standard 802.11 1999]- propuseram o WEP para proteger as mensagens de dados. A Wi-Fi Alliance propôs o WPA e, em seguida o WPA2, a fim de substituir o frágil WEP. O WPA trazia aperfeiçoamentos na verificação da integridade das mensagens e um novo mecanismo de atualização de chaves a cada sessão. O WPA2 introduziu um novo algoritmo criptográfico baseado no AES [IEEE Standard 802.11 2007] que trouxe ganhos de segurança ainda maiores, mas tanto o WPA quanto o WPA2, assim como o WEP, tinham como objetivo a proteção dos quadros de dados.

O IEEE, através do grupo de trabalho w, publicou em 2009 o IEEE Std 802.11w-2009 [IEEE Standard 802.11w 2009], esse padrão fornece mecanismos para que estações possam trocar quadros de gerenciamento protegidos, de forma que ataques de negação de serviço por desconexão falsa usando as vulnerabilidades dos quadros de gerenciamento deixem de ser realizáveis. A proteção construída para os quadros de gerenciamento é compatível com a solução de segurança criada para proteger os quadros de dados (publicada como emenda IEEE 802.11i [IEEE Standard 802.11i 2004] e depois incorporada ao padrão republicado em 2007 [IEEE Standard 802.11 2007]), mas nenhuma dessas soluções fornece a proteção de que necessitam os quadros de controle.

Como será visto, não é de hoje que pesquisadores perceberam a importância de proteger todos os quadros das redes sem fio, sob pena de sofrer ataques justamente através dos quadros que estão de alguma forma desprotegidos. Em relação aos quadros de controle, estas pesquisas não só não foram suficientes para a criação, por parte do IEEE, de um grupo de trabalho voltado à proteção destes quadros, mas também ainda apresentam muitas possibilidades de aperfeiçoamento.

3.1 BELLARDO E SAVAGE

Em um trabalho intitulado 802.11 *Denial-of-Service Attacks: Real vulnerabilities and Practical Solutions*, John Bellardo e Stefan Savage [Bellardo and Savage 2003] apresentaram propostas para minimizar os efeitos negativos causados à rede devido à ataques de DoS causados pela exploração maliciosa do mecanismo RTS/CTS.

Uma das propostas de Bellardo e Savage consiste na limitação do valor máximo informado no campo *Duração* dos quadros de controle. Essa proposta pretende mitigar os efeitos da recepção de um quadro RTS malicioso enviado para realizar a reserva do canal e com isso negar acesso a dispositivos legítimos. De acordo com a proposta, o recebimento de qualquer quadro RTS com um valor no campo *Duração* maior que o valor estabelecido teria o seu valor reduzido de imediato para o valor máximo permitido.

Outra proposta deste trabalho, 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, neste caso, encerraria-se a reserva do canal as estações voltariam imediatamente a concorrer pelo uso do canal. Este mecanismo falhava e se tornava insuficiente perante ataques mais elaborados em que fossem enviados dados espúrios após o envio de um quadro RTS. Bellardo e Savage já haviam mencionado também, a possibilidade de realizar-se um ataque às estações que estivessem no modo PS do IEEE 802.11 e que tivessem seus quadros armazenados na AP enquanto a sua interface estivesse desligada.

3.2 QURESHI

O trabalho publicado por Zaffar Qureshi [Qureshi et al. 2007] e sua equipe, voltou-se para o problema da falta de proteção dos quadros de controle PS-Poll que culmina com a perda, por parte da estação vítima que está com sua interface de rede desligada, dos quadros armazenados no AP. Os autores apresentam uma proposta que utiliza um campo de *Association ID* (AID) com uma valor pseudoaleatório que é cifrado usando chaves pré-estabelecidas, desta forma essas chaves não poderiam ser falsificadas ou previstas por

um atacante. No entanto, apesar do trabalho oferecer uma alternativa simples e sem necessidade de hardware adicional, e ter sua força apoiada no uso de uma nova chave de cifragem a cada nova mensagem, ela não pode ser estendida a todos os outros quadros de controle, os quadros de controle RTS e CTS, por exemplo, não possuem o campo AID, a bem da verdade, nenhum outro quadro apresenta o campo *Association ID*, tornando-a assim, uma solução para um problema pontual.

3.3 RAY E STAROBINSKI

Falamos no Capítulo 2.1 sobre o Problema do Nó Escondido, para combatê-lo, muitas vezes o mecanismo *request-to-send/clear-to-send* (RTS/CTS) é utilizado com a finalidade de evitar colisões e, portanto, atingir alto *throughput* na rede. O mecanismo RTS/CTS pode bloquear uma rede se for utilizado maliciosamente, pois qualquer nó pode receber um pacote RTS e atrasar sua transmissão por um período de tempo (equivalente ao tempo do campo *Duração*) sem se perguntar se a transmissão de dados para a qual o canal foi reservado está realmente ocorrendo. A esse bloqueio malicioso que causa negação de serviço na rede, Ray e Starobinski [Ray and Starobinski 2007] deram o nome de *False Blocking*. Como proposta para solucionar o problema de *False Blocking* foram sugeridas e analisadas três diferentes técnicas:

- a primeira técnica consiste na criação de quadros de controle auxiliares como ocorre em outros protocolos, de forma que estes quadros auxiliares servissem para validar um quadro RTS;

- a segunda estratégia seria o aumento dos intervalos de *backoff*, a ideia do aumento dos intervalos vem da observação de que o problema do *False Blocking* é aumentado quando a distância de retransmissão de sucessivos quadros RTS é muito pequena;

- a terceira e última proposta é chamada de validação RTS, nela, um nó ao ouvir um quadro de controle RTS só suspende a sua transmissão por um longo período se uma transferência de dados entre nós estiver ocorrendo após um RTS, caso contrário, se

nenhuma transmissão de dados iniciar, o nó não aguardará mais, com isso, terá atrasado sua transmissão só por um curto espaço de tempo.

Os autores chegaram a conclusão de que a primeira técnica quebraria a compatibilidade com os sistemas legados e a segunda técnica tem uma eficácia muito limitada.

A terceira técnica é uma técnica não-criptográficas de mitigação de ataque ao mecanismo RTS/CTS, que segundo os autores, estabilizaria o *throughput* em valores de carga alta sendo uma alternativa viável. Através de simulações apresentadas no trabalho, demonstrou-se que a validação RTS é uma técnica promissora, reduzindo o atraso médio. Perceba que esta última alternativa proposta por [Ray and Starobinski 2007] é muito semelhante a técnica proposta em [Bellardo and Savage 2003], com a diferença de ser aplicada ao contexto de redes sem fio *multihop*. As duas técnicas, diante de um ataque malicioso mais inteligente, em que após o envio de um RTS falso fossem enviados dados quaisquer, seriam ineficazes e o nó ficaria bloqueado (DoS).

3.4 KHAN E HASAN

Em [Khan and Hasan 2008] é apresentada uma autenticação baseada em números pseudoaleatórios para conter ataques de negação de serviço. Este trabalho foi a primeira proteção criptográfica que propôs uma abrangência que permitisse atender a lacuna de proteção existente em relação aos quadros de controle e aos quadros de gerenciamento, estes últimos ainda não contavam com a proteção trazida pela emenda IEEE 802.11w [IEEE Standard 802.11w 2009]. O mecanismo proposto visa a ser uma solução robusta que efetivamente consiga conter os ataques de DoS baseados na manipulação maliciosa de quadros de gerenciamento e controle usando autenticação baseada em números pseudoaleatórios. O mecanismo proposto neste trabalho envolve substituir o FCS que é preenchido com um CRC-32 por um FCS que é preenchido com um CRC-16 e usar os 16 *bits* poupados para autenticação. A troca do CRC-16 pelo CRC-32 não tem impacto significativo na detecção (0,0015% de diferença).

O código de autenticação que preenche os 16 *bits* restantes é gerado com o uso de uma PRF (*Pseudo Random Function*). As PRFs usadas no padrão 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. O uso de apenas 16 *bits* para o código de autenticação torna frágil a proteção do mecanismo proposto pelos autores.

Os 16 *bits* obtidos que serão usados para autenticar a mensagem farão com que ela só seja processada se o número for válido, senão a mensagem será descartada.

Nessa proposta, portanto, 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 para manter o tamanho original desses quadros.

Khan e Hasan reconhecem que o mecanismo não é definitivo, não é uma contramedida completa contra ataques a quadros RTS, CTS e ACK. De fato, uma análise mais apurada nos mostra alguns detalhes sobre a proposta que precisam ser tratados:

- o pequeno tamanho do elemento de autenticação é um problema;
- ataques de *replay* continuam sendo possíveis.

3.5 RACHEDI E BENSLIMANE

Trabalho focado principalmente em algumas vulnerabilidades dos quadros de controle CTS e ACK. Os autores Rachedi e Benslimane [Rachedi and Benslimane 2009], em seu trabalho, classificam os ataques ao CTS e ACK como *cross-layer* pois o ataque sai da camada MAC e se propaga para camadas superiores. Os ataques enumerados no trabalho são ataque de CTS falso e ataque de ACK falso. O ataque de CTS falso pode bloquear os nós na mesma região de transmissão do atacante, mas pode também bloquear os nós fora do alcance da transmissão do atacante e dentro do alcance de interferência. Pode-se dizer que o impacto deste ataque não está limitado ao alcance da transmissão, mas sim ao alcance de interferência do atacante. Outro importante problema com este ataque, é que ainda que se detecte o falso CTS, não se detecta o atacante, pois quadro CTS não tem sequer endereço de origem. O ataque de falso ACK consiste em validar o pacote para o emissor, embora o pacote não seja recebido corretamente pelo receptor. O impacto desta validação falsa do pacote é que o emissor não retransmitirá o pacote porque ele recebeu

um ACK. É possível ainda um ataque usando ACK falso dividido em duas partes. Na primeira parte, o atacante cria uma colisão com um quadro transmitido para um nó B. Em uma segunda parte, o atacante envia um falso ACK para o nó emissor A. Os autores afirmam que o falso ACK é mais difícil de implementar do que o falso CTS, porém o impacto negativo do falso ACK é maior. Os autores fazem três propostas para evitar o sucesso destes ataques:

- adicionar o endereço do transmissor nos quadros ACK e CTS;
- enviar um *hash* criptográfico do quadro de dados junto ao ACK;
- proteger os quadros ACK, CTS e RTS com um elemento EHMAC que pode ter entre 10 e 20 *bytes*.

O primeiro ponto que fragiliza a proposta feita em [Rachedi and Benslimane 2009] é o fato de não existir qualquer artifício que possa impedir, ou pelo menos dificultar, os ataques de *replay*. Os autores se preocuparam em mencionar a proteção de apenas parte dos quadros de controle, não ficando claro, se foi encontrado algo que pudesse impedir e estender a proteção a todos os quadros de controle. Especificamente em relação aos pontos propostos, temos que:

- adicionar o endereço de transmissor não remove vulnerabilidade, no máximo dificulta a ação do atacante que precisará por vezes forjar o endereço do transmissor;
- o envio de um *hash* criptográfico gerado com o HMAC-SHA, por exemplo, necessitaria de 20 *bytes* e geraria um excessivo aumento no tamanho dos quadros, além do fato do HMAC-SHA1 possuir algumas fraquezas [Kim et al. 2006] [Rechberger and Rijmen 2008];
- a terceira e última opção proposta geraria um aumento no tamanho dos quadros de pelo menos 10 *bytes*, sem resolver o problema dos ataques de *replay*, assim como as opções anteriores.

3.6 MYNENI E HUANG

Em 2010 foi publicado um trabalho que visa proteger de forma criptográfica todos os quadros de controle. O trabalho [Myneni and Huang 2010] propõem proteger os quadros de controle, incluindo os novos quadros (BA e BAR), por meio de um código de autenticação de mensagem (MAC), no trabalho publicado os autores se concentram nos quadros RTS e CTS, pois esses, segundo eles, são os maiores alvos de ataque. Como primeiro passo, é utilizado o *framework* IAPP para distribuição e gerenciamento de chave. Usando a chave distribuída e gerenciada pelo *framework* IAPP, gera-se um código de autenticação de mensagem (MAC) para *frames* de controle. Para conter ataques de *replay* é apresentado um mecanismo para gerar um número de sequência que assegura que a geração do código MAC é única.

O código de autenticação de mensagem (MAC) é gerado usando o HMAC [H.Krawczyk et al. 1997] sobre o algoritmo de função *hash* SHA-1 de criptografia [Eastlake and Jones 2001]. A razão para usar SHA-1 como função de *hash* criptográfica, para os autores, é que muitas estações já têm essa função de *hash* criptográfica em seus *softwares* ou *hardwares*. Usando um algoritmo existente há uma redução no custo global de atualização do sistema, portanto, SHA-1 é o preferido, apesar das melhorias para o SHA-1 que já foram propostas.

Para amenizar o aumento no tamanho dos quadros e já que o campo MAC pode ser usado no lugar do FCS, o FCS *frame check sequence* - que é um campo presente nos quadros RTS e CTS do padrão IEEE 802.11 - é removido na proposta de Myneni e Huang sem prejuízo da checagem de erro.

O trabalho apresentado por Myneni e Huang [Myneni and Huang 2010] embora seja um grande avanço principalmente por ser um mecanismo de segurança extensível a todos os quadros de controle e por ser capaz de proteger contra ataques de *replay* apresenta alguns inconvenientes. Para a implementação da proposta são necessárias várias etapas que adicionam muitos passos, o uso do *framework* IAPP para distribuição e gerenciamento de chave, depois o uso do HMAC-SHA-1 para gerar o MAC que tem 160 *bits*, como isso ainda é insuficiente diante de ataques de *replay*, eles optaram pelo uso de um número de sequência de 32 *bits*. No total, nesta proposta, há um incremento de 192 *bits* que se reduz

a um aumento de 160 *bits* no tamanho do quadro, pois os autores optaram por retirar o FCS que representa 32 *bits* no comprimento do quadro de controle no padrão IEEE 802.11. Para ilustrar melhor, só em relação ao custo sobre o comprimento do quadro, em um quadro CTS que tem 112 *bits*, o acréscimo de 160 *bits* representa um incremento de mais de 142% do tamanho do quadro CTS definido no padrão IEEE 802.11. Além do que, o uso do algoritmo HMAC-SHA-1, já existente em alguns dispositivos, é questionável do ponto de vista da segurança do processo, devido às fragilidades encontradas nesta função de *hash* criptográfico [Kim et al. 2006] [Rechberger and Rijmen 2008].

3.7 RESUMO

Neste capítulo, seis trabalhos foram analisados. Os trabalhos analisados representam pesquisas que não só mencionaram a possibilidade de realização de ataques à disponibilidade das redes sem fio por meio da exploração das vulnerabilidades dos quadros de controle, mas também propuseram mecanismos para conter os ataques. A Tabela 3.1 mostra os tipos de quadros que cada um dos trabalhos protege, de forma que se o trabalho protege contra os ataques de falsificação de quadros o campo está marcado com X e se protege contra os ataques de repetição (*replay*) está marcado com 0.

Tabela 3.1 Tabela Resumitiva dos Trabalhos Relacionados.

	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

CAPÍTULO 4

O MECANISMO PROPOSTO PARA A PROTEÇÃO DOS QUADROS DE CONTROLE

Este trabalho já apresentou, no Capítulo 2, os quadros de controle do IEEE 802.11 e os ataques existentes contra eles, bem como diversos trabalhos relacionados que propõem fornecer um mecanismo de segurança a estes quadros de controle. Neste capítulo, na Seção 4.1, serão apresentados os formatos dos 8 novos tipos de quadros de controle. A Seção 4.2 apresentará a forma de calcular o campo MAC, que será adicionado ao final dos novos tipos de quadros de controle e permitirá verificar a integridade e a autenticidade destes quadros.

4.1 NOVOS QUADROS DE CONTROLE

O mecanismo proposto neste trabalho 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 e em suas abreviaturas receberão um S na frente, simbolizando tratar-se de um quadro de controle seguro. Um quadro de controle ACK protegido pelo mecanismo será denominado SACK, por exemplo. 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*.

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 (uma) 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.

4.1.1 SPS-Poll (Secure PS-Poll)

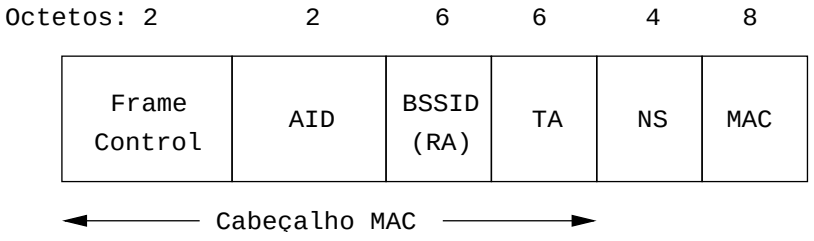


Figura 4.1 *Secure PS-Poll.*

O quadro SPS-Poll, ilustrado na Figura 4.1, possui 28 *bytes* de comprimento e é formado por 6 campos: FC (*Frame Control*), AID (*Association ID*), *Endereço 1*, *Endereço 2*, NS (Número de Sequência) e MAC (*Message Authentication Code*). O campo FC possui 2 *bytes* e permite identificar o tipo de quadro e provê algumas informações de controle. O campo AID representa um identificador de associação da estação e possui 2 *bytes*. Os campos *Endereço 1* e *2* possuem 6 *bytes* cada e representam, respectivamente, o endereço do receptor e do transmissor. O campo NS possui 4 *bytes* seguido do campo MAC de 8 *bytes*.

4.1.2 SRTS (Secure Request to Send)

O SRTS, mostrado na Figura 4.2, possui 28 *bytes* de comprimento, sendo dividido em 6 campos: FC (*Frame Control*), *Duração*, *Endereço 1*, *Endereço 2*, NS (Número de Sequência) e MAC (*Message Authentication Code*). O campo FC possui 2 *bytes* e permite

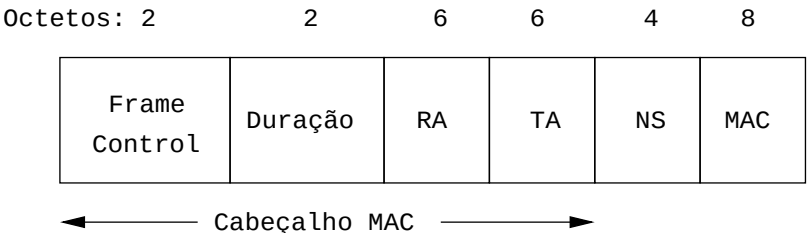


Figura 4.2 *Secure RTS.*

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 NS possui 4 *bytes* seguido do campo MAC de 8 *bytes*.

4.1.3 SCTS (Secure Clear to Send)

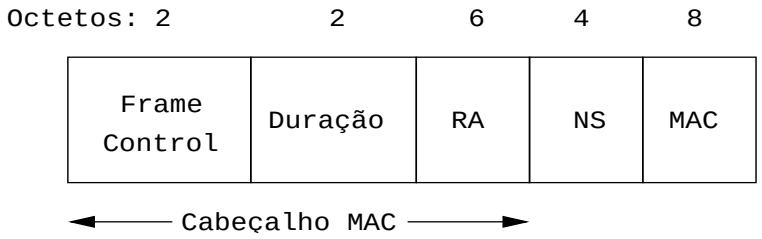


Figura 4.3 *Secure CTS.*

O SCTS, ilustrado na Figura 4.3, possui 22 *bytes* de comprimento, sendo dividido em 5 campos: FC (*Frame Control*), *Duração*, *Endereço 1*, NS (Número de Sequência) e MAC (*Message Authentication Code*). O campo FC possui 2 *bytes* e 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]. O campo *Endereço 1* possui 6 *bytes* e representa o endereço do receptor. O campo NS possui 4 *bytes* seguido do campo MAC (*Message Authentication Code*) de 8 *bytes*.

4.1.4 SACK (Secure Acknowledgement)

Os quadros ACK (*Acknowledgement*) são usados para confirmar o recebimento de alguns tipos de quadros, esse processo de confirmação é necessário na camada MAC e faz dos quadros de controle ACK os quadros que trafegam em maior quantidade nas redes sem fio IEEE 802.11.

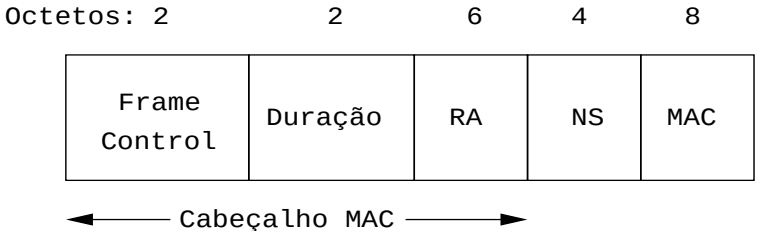


Figura 4.4 *Secure ACK.*

Os quadros SACK, ilustrados na Figura 4.4, possuem a mesma função dos quadros ACK tratando-se apenas de uma versão que utiliza o mecanismo de segurança proposto. Possuem 22 *bytes* de comprimento, sendo dividido em 5 campos: FC (*Frame Control*), *Duração*, *Endereço 1*, NS (Número de Sequência) e MAC (*Message Authentication Code*). O campo FC possui 2 *bytes*, 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]. O campo *Endereço 1* possui 6 *bytes* e representa o endereço do receptor. O campo NS possui 4 *bytes* seguido do campo MAC (*Message Authentication Code*) de 8 *bytes*.

4.1.5 SCF-End (Secure Contention Free End)

O IEEE 802.11 [IEEE Standard 802.11 2007] define duas funções de coordenação do canal, DCF (usada na maior parte dos dispositivos) e PCF. 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*).

A versão segura dos quadros CF-End, SCF-End, é mostrada na Figura 4.5, possui 28

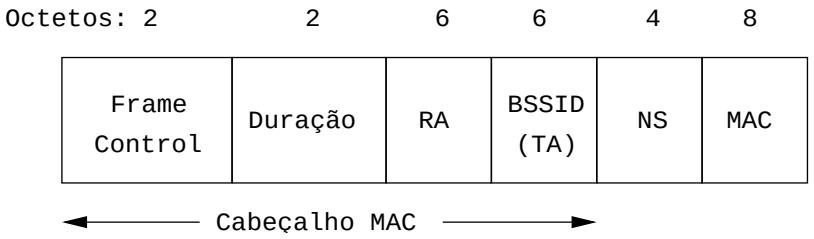


Figura 4.5 *Secure CF-End.*

bytes de comprimento e é dividida em 6 campos: FC (*Frame Control*), *Duração*, *Endereço 1*, *Endereço 2*, NS (Número de Sequência) e MAC (*Message Authentication Code*). Em particular nesses 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 SRTS.

4.1.6 SCF-End+CF-Ack (Secure CF-End+Contention Free Ack)

Conforme visto, 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 recebidos.

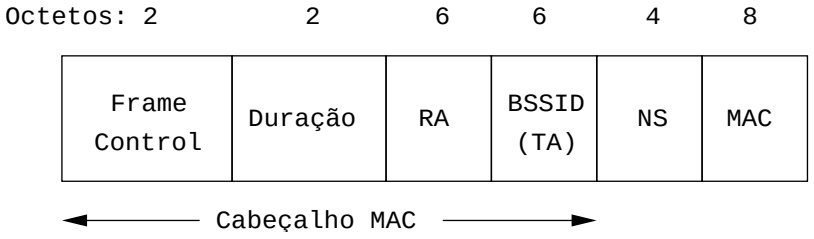


Figura 4.6 *Secure CF-End+CF-Ack.*

O SCF-End+CF-Ack, ilustrado na Figura 4.6, possui 28 *bytes* de comprimento, dividido em 6 campos: FC (*Frame Control*), *Duração*, *Endereço 1*, *Endereço 2*, NS (Número de Sequência) e MAC (*Message Authentication Code*). Os campos deste quadro são preenchidos de forma similar ao preenchimento efetuado para os quadros CF-End, descrito anteriormente.

4.1.7 SBAR (Secure Block Ack Request)

Os quadros BAR e BA, introduzidos pela emenda IEEE 802.11e [IEEE Standard 802.11e 2005], são usados para permitir a confirmação de um bloco de quadros usando apenas um quadro de confirmação. O quadro BAR é usado para requisitar a confirmação de recepção de um bloco de quadros.

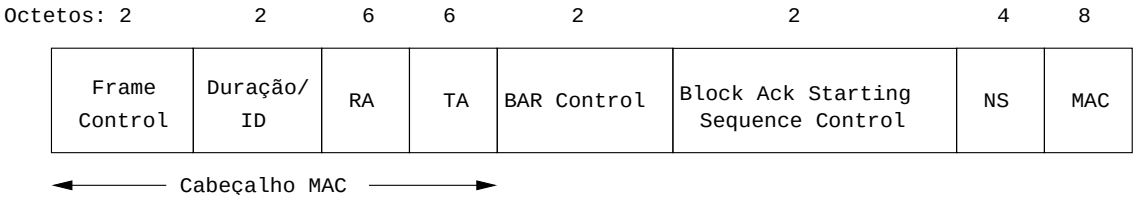


Figura 4.7 *Secure BAR.*

O quadro SBAR, ilustrado na Figura 4.7, possui 32 *bytes* de comprimento e é formado por 8 campos: FC (*Frame Control*), *Duração*, *Endereço 1*, *Endereço 2*, BAR *control*, *Block Ack Starting Sequence Control*, NS (Número de Sequência) e MAC (*Message Authentication Code*). O campo BAR *control* possui 2 *bytes* e é usado para a negociação de 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. Os demais campos possuem o mesmo tamanho e descrição já apresentados para os quadros SRTS.

4.1.8 SBA (Secure Block Ack)

O quadro BA, introduzidos pela emenda IEEE 802.11e [IEEE Standard 802.11e 2005], é usado em conjunto com o BAR no mecanismo capaz de permitir a confirmação de um bloco de quadros usando apenas um quadro de confirmação. O quadro BA é utilizado como resposta ao quadro de requisição BAR. Os quadros BAR são enviados pelo emissor depois da transmissão de um fluxo de dados. Os quadros BA, por sua vez, contêm um *bitmap* que indica os pacotes recebidos.

O quadro SBA, ilustrado na Figura 4.8, possui 160 *bytes* de comprimento e inclui 9

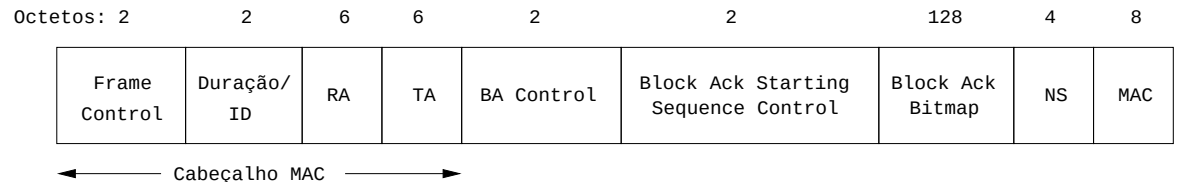


Figura 4.8 *Secure BA.*

campos: FC (*Frame Control*), *Duração*, *Endereço 1*, *Endereço 2*, BA *control*, *Block Ack Starting Sequence Control*, *Block Ack Bitmap*, NS (Número de Sequência) e MAC (*Message Authentication Code*). 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 foram recebidos. Os demais campos possuem tamanho e descrição similares aos apresentados para o quadro SRTS.

4.2 CÁLCULO DO VALOR DO CAMPO MAC

Como foi visto no início deste capítulo, a versão segura dos quadros de controle consiste na retirada do campo FCS e, em seu lugar, colocar o campo NS de 4 *bytes* seguido do campo MAC de 8 *bytes*. É justamente sobre a geração do valor do campo MAC que esta seção tratará.

O campo MAC é quem possibilitará, ao nó receptor, verificar a autenticidade e a integridade do quadro de controle recebido, é por conta desta capacidade de se utilizar o campo MAC também para a verificação de integridade, que se torna dispensável manter um campo FCS (cuja função é detectar erros) o qual é preenchido com um *Cyclic Redundancy Code* de 32 *bits* (CRC-32). Para a construção dos quadros de controle seguros é suficiente utilizar o CBC-MAC do CCMP, pois este, através do cálculo do código de autenticação (campo MAC) permitirá verificar a autenticidade e a integridade do quadro de controle recebido.

O algoritmo do CBC-MAC (Algoritmo 2.2.1, na Seção 2.2.2.1) ao receber uma mensa-

gem B, dividida em uma sequência de blocos, fará essa mensagem passar por uma função de criptografia por blocos E() que utiliza uma chave criptográfica K e dará como resultado T. T será o código de autenticação (MAC) e, corresponde aos 8 *bytes* mais significativos dos 16 *bytes* obtidos pelo CBC-MAC.

O cálculo de T é feito de acordo com o Algoritmo 2.2.1, já apresentado e repetido nesta seção. 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 valor de 16 *bytes* cujos 8 *bytes* mais significativos serão o valor de T.

4.2.1 Bloco B_0 ou IV

O primeiro bloco a entrar no processo B_0, também conhecido como vetor de inicialização (IV) é formado como mostra a Tabela 4.1. 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.

Para oferecer a segurança aos quadros de controle o bloco B_0 é construído segundo a Tabela 4.1, onde:

- *Flag* - possui 1 *byte*. Contém as informações previstas para o campo *flags* definido em [Whiting et al. 2003] e possui valor igual a $(00011011)_2$. 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.

Tabela 4.1 Composição do Bloco B_0 [Whiting et al. 2003].

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

4.2.2 Processo de Encapsulamento dos Quadros de Controle

Após obter o valor do vetor de inicialização, é possível o início do processo de encapsulamento dos quadros de controle seguros.

No caso do CCMP quando usado no 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 (MAC) 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 4.9 ilustra esse processo. O bloco inicial a ser criptografado possui 128 *bits* e é representado pelo IV (*Initialization Vector*), cuja composição já foi explicada.

O processo de construção do MAC utiliza o CBC-MAC com o AES como cifra de bloco no Algoritmo 2.2.1, 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

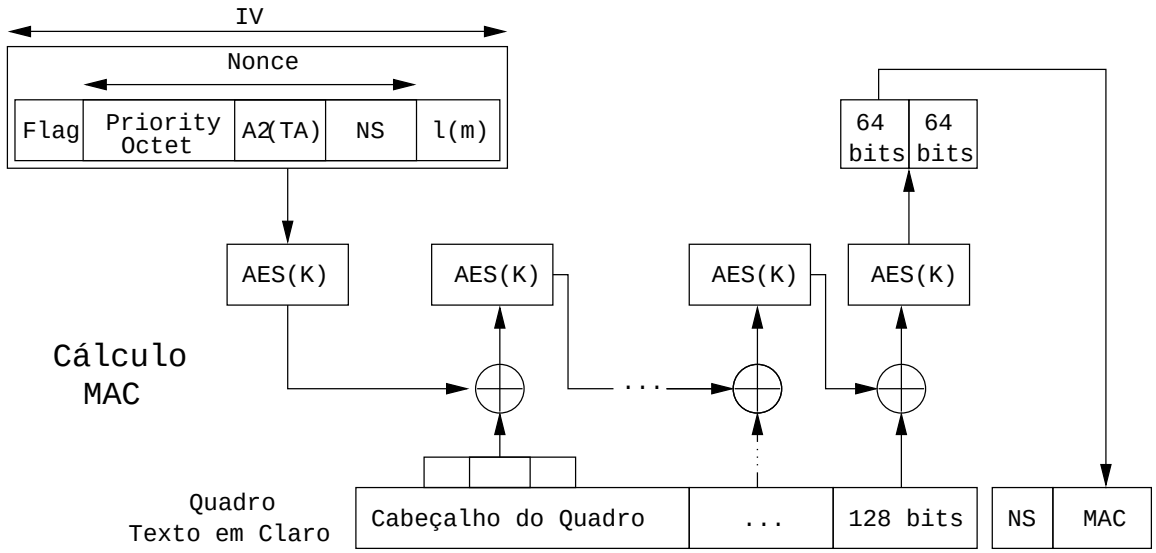


Figura 4.9 Geração do Valor do Campo MAC.

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 possa construir o código de autenticação e que qualquer nó receptor seja capaz de verificar a autenticidade e integridade do quadro, é necessário que uma chave K em comum entre esses nós seja estabelecida. Este processo de geração, distribuição e renovação será explicado no Capítulo 5.

4.2.3 Processo de Recepção e Verificação dos Quadros de Controle

Ao receber um quadro de controle no formato proposto neste trabalho, o nó da rede sem fio deve recalcular o MAC e comparar o valor obtido com aquele informado no campo MAC. Para isso, este nó receptor deverá possuir a chave K e o IV. A chave K deverá ser de conhecimento de todas as estações da rede, a chave K é uma chave de grupo. 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 é transportado em texto 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 RESUMO

No capítulo, foram conhecidos oito novos tipos de quadros de controle, os quadros de controle seguros. Estes novos quadros diferenciam-se dos quadros de controle originais por possuir em vez de um campo FCS, dois outros campos: um campo de número de sequência e um campo de código de autenticação da mensagem.

Dentro do mecanismo que torna o quadro de controle seguro, foi visto que o NS tem o intuito de proteger contra ataques de replay e o valor gerado, denominado código de autenticação de mensagem (MAC), fornecer a autenticidade e a integridade.

O capítulo mostrou que para a verificação do código de autenticação da mensagem, deve-se recalcular o valor do MAC, após o recebimento do quadro de controle seguro, se o valor obtido for diferente do valor do campo MAC presente no quadro de controle seguro, este quadro de controle deverá ser descartado por tratar-se de um quadro falsificado, que sofreu algum tipo de manipulação ou erro. Outra possibilidade, mostrada no capítulo, do quadro de controle ser descartado é se for identificado que trata-se de um quadro de controle repetido, neste caso, a repetição do quadro de controle seguro é perceptível por meio da análise do número de sequência.

CAPÍTULO 5

SEGURANÇA, AUMENTO NO TAMANHO DOS QUADROS E ESTUDO DE CASO

O objetivo geral do trabalho realizado é propor um mecanismo capaz de proteger todos os quadros de controle. Além disso, o trabalho busca trazer para a rede um menor aumento no tamanho dos quadros que o trabalho proposto por [Myneni and Huang 2010] que é o único, dentre os trabalhos pesquisados, que protege todos os quadros de controle, inclusive os protege dos ataques de *replay*. O último objetivo, porém não menos importante, é ter compatibilidade com os mecanismos de segurança que já estejam presentes em todos os dispositivos que são compatíveis com o padrão IEEE 802.11.

Na Seção 5.1, será mostrado que o mecanismo proposto é compatível com os dispositivos que já possuem a implementação de todo o padrão IEEE 802.11 [IEEE Standard 802.11 2007]. A Seção 5.1 mostrará ainda que o mecanismo é seguro, desde que respeitada a forma de construção. Ao fim deste capítulo, na Seção 5.3, será mostrado o impacto do aumento do tamanho dos quadros de controle gerados em uma rede, do ponto de vista do aumento do tráfego, comparando inclusive com a proposta de Myneni [Myneni and Huang 2010].

5.1 SEGURANÇA

5.1.1 Compatibilidade

Conforme foi visto no Capítulo 4, para geração do código de autenticação (MAC) para os quadros de controle, aproveita-se a implementação do CBC-MAC no CCMP. Foi explicitado ainda, que há a necessidade de uma chave K comum aos nós participantes da rede

para que um nó da rede possa construir o MAC e para qualquer outro nó possa verificar a autenticidade e integridade do quadro que contém o MAC.

O processo de estabelecimento de uma comunicação segura WPA2 consiste também da criação, distribuição e regular atualização das chaves temporárias.

Em dispositivos que suportam o WPA2 são definidas duas hierarquias de chaves [IEEE Standard 802.11 2007]:

- *Pairwise key hierarchy*, para proteger tráfego *unicast*;
- GTK uma hierarquia que consiste de uma única chave para proteger tráfego *multicast* e *broadcast*.

As duas hierarquias de chaves vistas consistem de dois *handshakes*:

- *4-Way-Handshake* que permite a derivação de uma chave PTK e o envio, em texto cifrado, da chave GTK para o nó;
- *Group Key Handshake* cujo intuito é distribuir uma nova chave GTK a todos os clientes da rede sem a necessidade de reautenticar estes clientes.

Para a proposta deste trabalho, a chave de grupo GTK derivada durante o processo do *4-Way-Handshake* e renovada periodicamente usando o *Group Key Handshake*, será de muita utilidade.

A escolha em se usar a chave de grupo (*Group Encryption Key* que faz parte da chave hierárquica GTK) deve-se ao fato de que todos os nós devem ser capazes de verificar a autenticidade dos quadros enviados em *broadcast*, ou mesmo enviados em *unicast*, mas que tenham o objetivo realizar reserva do canal por um período de tempo especificado no campo *Duração*. A chave de grupo é a chave usada para a criptografia de tráfego destinado a múltiplos nós da rede, e pelo fato de todos os nós da rede já a possuírem, é a chave a ser empregada para geração e posterior verificação do MAC.

A GTK deve ser um número aleatório gerado a partir de uma *Group Master Key* que é distribuída, em texto cifrado, durante o *4-Way Handshake* e que pode ser atualizada por meio de um *Group Key Handshake* [IEEE Standard 802.11 2007]. Ainda de

acordo com o padrão, a chave GTK poderá ser atualizada por conta da desassociação ou desautenticação de algum nó da rede, ou um evento que possa disparar o *Group Key Handshake*.

O uso do mecanismo deste trabalho requer a renovação da chave de grupo por meio do *Group Key Handshake* para evitar que um nó utilize um mesmo número de sequência com uma mesma GTK da rede após esgotarem-se os números de sequência.

Com a utilização de elementos funcionais presentes nos dispositivos compatíveis com o padrão IEEE 802.11 [IEEE Standard 802.11 2007], busca-se garantir que os dispositivos possam utilizar o mecanismo proposto, de forma que seja necessária apenas a atualização dos softwares dos dispositivos. A capacidade de todos os dispositivos de rede sem fio em se comunicar trocando quadros de controle seguros, dependerá de uma negociação prévia, de forma análoga a que acontece com dispositivos compatíveis com o IEEE 802.11w para os quadros de gerenciamento robustos.

As partes envolvidas na comunicação devem ser capazes de gerar os quadros de controle robustos e devem deter as chaves (obtidas no 4-*Way Handshake* e renovadas no *Group Key Handshake*).

5.1.2 Segurança do Mecanismo Utilizado

Na adoção de um mecanismo de segurança, sempre há grande preocupação com o grau de segurança fornecido, esta preocupação pode ser dividida, em grande parte, em duas áreas: o tamanho da chave e a natureza do algoritmo.

Quanto ao tamanho da chave, a segurança do mecanismo tem ligação com a segurança do WPA2, em redes protegidas por este assim como em redes protegidas pelo WPA. É possível a obtenção das chaves PTK e GTK por meio de ataques 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 [Moskowitz 2003]. Esta é uma vulnerabilidade que não é do protocolo e pode ser contornada pelo uso de *passphrases* maiores que 20 caracteres.

Quanto ao algoritmo, o mecanismo proposto utiliza o AES com algoritmo básico CBC-

MAC, isso permite que sejam recebidos quadros de controle que após serem separados precisem de preenchimento, até que todos os blocos atinjam o tamanho fixo estabelecido para o bloco. Ao final do processo, os 8 (oito) *bytes* mais significativos é que são enviados como código de autenticação (MAC).

Em [Rogaway 2011] foi realizada uma avaliação dos modos de operação de algumas cifras de bloco, mais especificamente no Capítulo 7 de [Rogaway 2011] tratou-se do CBC-MAC utilizando 6 (seis) algoritmos diferentes e 3 (três) métodos de preenchimento. Rogaway demonstrou que da forma que está sendo empregado o CBC-MAC no mecanismo proposto neste trabalho, com o Algoritmo do tipo 1 e método de Preenchimento também do tipo 1, pode-se trabalhar com mensagens de comprimento de 0 a infinito, com blocos e chave de tamanho fixo que o CBC-MAC apresenta propriedades de segurança suficientemente adequadas.

A chave utilizada possui comprimento de 128 *bits*, utilizada no AES, a complexidade de tempo de um ataque de força bruta é $O(2^{128})$. Até bem pouco tempo atrás não havia ataque mais rápido que 2^{128}, mas recentemente foi publicado em [Bogdanov et al. 2011] um ataque mais rápido de recuperação de chave, que contra a versão de 128 *bits* possui complexidade de tempo $O(2^{126,1})$.

5.1.3 Segurança do Mecanismo Proposto Frente aos Trabalhos Relacionados

O trabalho [Myneni and Huang 2010] propõe um formato de quadros de controle que gera o seu código de autenticação de mensagem (MAC) usando o algoritmo HMAC sobre a função de *hash* criptográfica SHA-1. O SHA-1 começou a apresentar diversos ataques que trouxeram descrédito a esta função de *hash* criptográfico [Wang et al. 2005] [Manuel 2008]. Apesar dos conhecidos problemas do SHA-1, não estava claro que isso causaria diminuição da segurança do uso do HMAC sobre o SHA-1, foi então que também começaram a surgir estudos demonstrando fraquezas do HMAC-SHA-1 [Kim et al. 2006] e [Rechberger and Rijmen 2008]. Estas descobertas, demonstram que o mecanismo utilizado em [Myneni and Huang 2010] já apresentava fraquezas documentadas quando o mecanismo proposto por Myneni e Huang foi publicado. Se por um lado as fragilidades demonstram que a

segurança do mecanismo proposto em [Myneni and Huang 2010] se baseava em algoritmos já vulneráveis, por outro, demonstra a melhoria, no que diz respeito a segurança, que há na proposta apresentada neste trabalho, que utiliza mecanismos comprovadamente seguros [Rogaway 2011].

No Capítulo 3 foram mencionadas algumas propostas de proteção que foram agrupadas na Tabela 3.1. Na Tabela 3.1 foi acrescentada a linha que resume a proteção oferecida pela proposta deste trabalho formando a Tabela 5.1 .

Tabela 5.1 Comparativo das Diversas Propostas.

	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	X/0	X/0	X/0	X/0	X/0	X/0	X/0	X/0

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.

Por meio da Tabela 5.1, é possível observar que os trabalhos que protegem simultaneamente todos os quadros de controle e que oferecem também proteção contra ataques de *replay* são o de [Myneni and Huang 2010] e o trabalho proposto aqui.

5.2 AUMENTO DO TAMANHO DOS QUADROS DE CONTROLE CAUSADO PELO ACRÉSCIMO DOS ELEMENTOS DE SEGURANÇA

Pelo fato do trabalho em [Myneni and Huang 2010], assim como o proposto nesta pesquisa, proteger todos os quadros de controle, inclusive contra os ataques de *replay*, foi realizada uma comparação mais aprofundada dos dois trabalhos.

O impacto causado pela adoção do mecanismo proposto por Myneni e Huang acrescenta 160 *bits* ao tamanho do quadro original, enquanto o mecanismo proposto neste trabalho causa um impacto de 64 *bits*.

Para facilitar o entendimento do que esses dois valores representam de aumento em relação ao tamanho original dos quadros foi construída a Tabela 5.2 que apresenta o tamanho dos quadros de controle do IEEE 802.11, do mecanismo proposto neste trabalho e da proposta apresentada em [Myneni and Huang 2010], além do aumento percentual dos quadros nestes novos formatos com relação ao tamanho do quadro de controle do padrão. Note que o mecanismo proposto neste trabalho introduz, por quadro de controle, um aumento 2,5 vezes menor do que aquele introduzido pela proposta em [Myneni and Huang 2010].

Tabela 5.2 Comparativo do Tamanho dos Quadros de Controle.

Quadro de Controle	Tamanho Atual (*bits*)	Tamanho na Proposta (*bits*)	Aumento % Proposta	Tamanho Myneni (*bits*)	Aumento % Myneni
RTS	160	224	40	320	100
CTS	112	176	57,14	272	142,86
ACK	112	176	57,14	272	142,86
PS-Poll	160	224	40	320	100
CF-End	160	224	40	320	100
CF-End+ CF-Ack	160	224	40	320	100
BAR	192	256	33,33	352	83,33
BA	1216	1280	5,26	1376	13,16

A proposta deste trabalho, por conta da compatibilidade, buscou utilizar elementos funcionais que já estivessem presentes nos dispositivos compatíveis com o padrão IEEE 802.11, isso reduz o custo de atualização e permite, muitas vezes, que só atualizações do software tomem lugar e permitam o funcionamento do mecanismo. O trabalho de Myneni e Huang usa HMAC-SHA-1 porque, segundo os autores, muitos adaptadores já tem esse algoritmo de *hash* criptográfico, ou em *software*, ou em *hardware*, o que também traria

os benefícios de redução do custo de atualização.

O benefício de acrescentar um menor número de *bits* aos quadros de controle ficam evidentes na Tabela 5.2 e as razões para utilização de mecanismos presentes nos dispositivos foram brevemente explicados. Outro ponto importante, e que já foi comentado no Capítulo 3 diz respeito à segurança dos mecanismos. A proposta deste trabalho utiliza o AES cujo ataque mais rápido de recuperação da chave foi publicado em [Bogdanov et al. 2011] e possui complexidade de tempo $O(2^{126,1})$, por outro lado o SHA-1 já apresenta falhas encontradas por criptoanalistas [Wang et al. 2005] que ensejaram a criação do SHA-2. Combinado com o HMAC no HMAC-SHA-1, foram mostradas fraquezas deste mecanismo nos trabalhos [Kim et al. 2006] e [Rechberger and Rijmen 2008].

5.3 ESTUDO DE CASO

A proposta desta seção é verificar dentro do tráfego de uma rede sem fio em produção, como seria o impacto da adoção dos mecanismos sugeridos em [Myneni and Huang 2010] e no mecanismo proposto neste trabalho, em relação ao funcionamento normal desta rede.

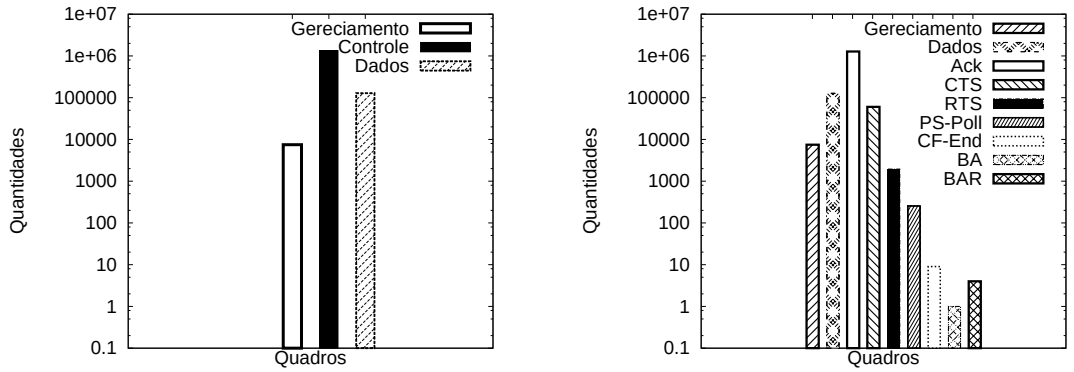
5.3.1 Experimento 1 - Rede Sem Fio CIn/UFPE

A rede escolhida, devido ao seu grande e variado tráfego, foi a rede sem fio do Centro de Informática da UFPE. Dentro do período de apenas 1 (uma) hora de captura, gerou-se um arquivo *trace* com aproximadamente 1.500.000 quadros capturados. Os quadros foram filtrados para que os quadros capturados fossem provenientes de um determinado AP escolhido, ou direcionado a ele.

Sabe-se que o aumento do tamanho dos quadros gera um custo para a rede. Com este estudo, espera-se mensurar o quanto que o aumento do tamanho dos quadro causará de impacto na rede sem fio em análise. Este impacto, causado pelo aumento do tamanho dos quadros de controle terá efeito na queda da vazão, na menor quantidade de informação útil por volume de *bytes* transmitido, no aumento do atraso e também em um possível aumento do número de colisões.

De acordo com trabalhos anteriores [Myneni and Huang 2010] mesmo com o acréscimo de campos para validação de 20 *bytes*, o custo é desprezível.

A Figura 5.1(a) apresenta a quantidade capturada dos 3 (três) tipos de quadros definidos pelo padrão IEEE 802.11. Note que há uma predominância dos quadros de controle. A Figura 5.1(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.

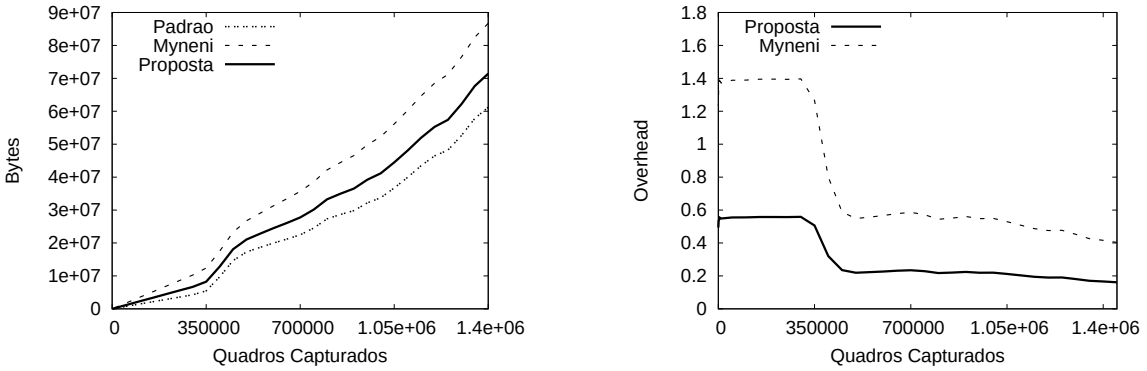


(a) (b)

Figura 5.1 Distribuição da Quantidade dos Quadros.

Com a informação da distribuição da quantidade dos quadros, foram acrescentados aos quadros de controle o valor relativo ao aumento do tamanho dos quadros, de acordo com a Tabela 5.2, de forma que um quadro RTS que originalmente teria 160 *bits*, passa a ter 224 *bits* utilizando o mecanismo proposto neste trabalho e passa a ter 320 *bits* utilizando o mecanismo proposto em [Myneni and Huang 2010]. Desta forma é possível estabelecer uma comparação entre o tráfego original do padrão IEEE 802.11 e os dois mecanismos de segurança. A Figura 5.2(a) apresenta o número cumulativo de *bytes* transferidos em função da quantidade de quadros. Note que o mecanismo proposto neste trabalho possui um menor aumento de volume de tráfego (expresso em *bytes*) para a mesma quantidade de quadros capturados em relação a proposta de Myneni e Huang.

Para tornar mais evidente o impacto causado pelas duas propostas em relação ao tráfego da rede sem fio sem a utilização dos mecanismos, a Figura 5.2(b) apresenta o *overhead* normalizado do tráfego, considerando as duas propostas avaliadas. Na Fi-



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

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

Figura 5.2 Comparação entre Propostas.

gura 5.2(b) entenda-se por *overhead* o aumento percentual de *bits* devido ao uso de elementos de segurança NS e MAC. Note que até aproximadamente os 300.000 primeiros quadros capturados, o mecanismo proposto neste trabalho tem um impacto próximo de 57%, enquanto a proposta do Myneni tem um impacto de quase 143%. O impacto inicial relativamente alto, deve-se ao grande tráfego de quadros de controle do tipo ACK (onde o impacto por quadro é de 142,86% de acordo com a Tabela 5.2). A medida que o volume de quadros transmitidos aumenta, observa-se que que o impacto do mecanismo proposto tende a 20% enquanto o impacto do mecanismo proposto por Myneni tende a 40%, o que evidencia a superioridade do mecanismo proposto neste trabalho também no que diz respeito ao menor impacto na rede, conforme era esperado, já que esse impacto é reflexo do aumento do tamanho dos quadros que já havia sido determinado anteriormente.

Em relação ao impacto obtido devido principalmente à grande presença de quadros ACK, pode-se entender a importância do uso dos quadros BAR e BA para o desempenho da rede e é possível entender ainda, que quanto maiores os quadros que precisam de confirmação, menor será o impacto proporcional ao volume de quadros enviados.

5.3.2 Experimento 2 - Tráfego Gerado com Iperf

Foi realizado também um experimento utilizando uma rede cujo tráfego era gerado através do Iperf [1].

A Figura 5.3(a) apresenta a quantidade capturada dos 3 tipos de quadros definidos pelo padrão IEEE 802.11. Percebe-se que há um equilíbrio entre os quadros de controle e os quadros de dados. A Figura 5.3(b) detalha os tipos de quadros de controle capturados, através dela, pode-se ver novamente um equilíbrio, desta vez, entre os quadros de controle Ack e os quadros de dados.

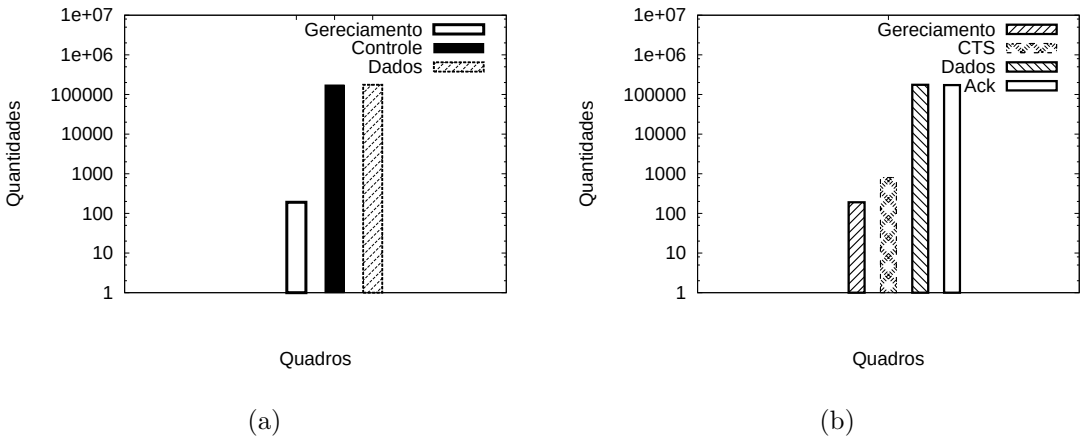
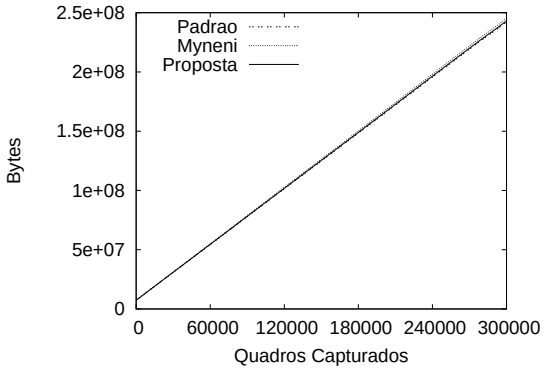


Figura 5.3 Distribuição da Quantidade dos Quadros do Tráfego Analisado.

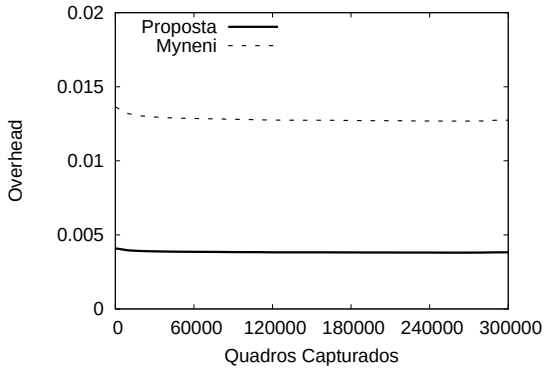
O procedimento adotado para a análise é o mesmo utilizado anteriormente na análise do tráfego capturado na rede sem fio do Centro de Informática da UFPE. Na distribuição da quantidade dos quadros, foram acrescentados aos quadros de controle o valor relativo ao aumento do tamanho dos quadros de controle devido ao uso dos campos de número de sequência e de código de autenticação de mensagem, de acordo com a Tabela 5.2. Desta forma é possível estabelecer uma comparação entre o tráfego original do padrão IEEE 802.11 e os dois mecanismos de segurança avaliados. A Figura 5.4(a) apresenta o número cumulativo de *bytes* transferidos em função da quantidade de quadros. A diferença, apresentada na Figura 5.4(a) é praticamente imperceptível, porque o impacto do aumento do tamanho dos quadros de controle é mínimo neste tráfego gerado pelo

[1]Iperf - http://dast.nlanr.net/Projects/Iperf/.

Iperf, conforme podemos comprovar através da Figura 5.4(b) que apresenta o aumento normalizado do tráfego considerando as duas propostas avaliadas.



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



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

Figura 5.4 Comparação do Comportamento das Propostas Diante do Novo Tráfego.

A Figura 5.4(b) mostra que o *overhead* é muito pequeno, cerca de 1,3% para a proposta de [Myneni and Huang 2010] e cerca de 0,4% para o mecanismo proposto neste trabalho, entenda-se por *overhead* o aumento percentual de *bits* devido ao uso de elementos de segurança NS e MAC.

Os resultados obtidos, na análise da rede sem fio do Centro de Informática da UFPE e na análise do tráfego gerado pelo Iperf, mostram que o mecanismo proposto onera a rede com um impacto negativo (causado pelo aumento do tamanho dos quadros de controle) significativamente menor do que a outra proposta avaliada.

5.4 RESUMO

Este capítulo mostrou que a segurança do mecanismo inicia-se pela geração das chaves. A chave utilizada no mecanismo proposto é gerada no 4-*Way Handshake* e renovada no *Group Key Handshake*, denomina-se GTK.

Para a geração do código de autenticação de mensagens (MAC) está sendo empregado o CBC-MAC com o AES, além disso, é utilizado ainda um número de sequência.

O mecanismo proposto protege todos os quadros de controle, o que o torna, já de

início, mais completo do que cinco dos seis trabalhos relacionados e, por esse critério, tão completo com o sexto e último trabalho relacionado analisado.

Foi mencionado que o HMAC-SHA-1 apresenta vulnerabilidades publicadas em [Kim et al. 2006] [Rechberger and Rijmen 2008], isto demonstra que o trabalho [Myneni and Huang 2010] utiliza um mecanismo vulnerável, diferentemente deste trabalho, mais robusto, que utiliza o CBC-MAC com AES cujo ataque mais rápido de recuperação de chave encontrado tem complexidade de tempo $O(2^{126,1})$.

No que diz respeito ao impacto causado pelo aumento do tamanho dos quadros de controle, mais uma vez o mecanismo proposto demonstrou superioridade, com o acréscimo de apenas 8 *bytes*, bem menos que os 20 *bytes* da proposta [Myneni and Huang 2010]. Este menor impacto foi ratificado em dois experimentos, um dentro da rede do CIn/UFPE e outro através da utilização do tráfego gerado por meio do Iperf.

CAPÍTULO 6

CONCLUSÕES

O IEEE 802.11 padronizou o primeiro mecanismo de segurança, o WEP; em seguida, surgiram WPA e WPA2. Os ataques que poderiam comprometer o sigilo das informações que trafegavam na rede pareciam ter acabado.

Em redes locais sem fio que seguem o padrão IEEE 802.11, até setembro de 2009, quando foi publicado o padrão IEEE 802.11w, apenas os quadros de dados recebiam alguma proteção estabelecida em um padrão. No entanto, os dois outros tipos de quadros que trafegam em uma rede sem fio - quadros de gerenciamento e quadros de controle - não recebiam qualquer proteção. Após a publicação do padrão IEEE 802.11w, os quadros de gerenciamento tiveram também uma proteção padronizada. Até o momento, o IEEE não criou nenhum grupo de trabalho para estudar mecanismos e criar um padrão que tenha o objetivo de proteger os quadros de controle.

Diante da ausência de um mecanismo que vise proteger os quadros de controle, esta dissertação mostrou alguns dos ataques possíveis a estes quadros e a importância de protegê-los para manter a disponibilidade da rede sem fio.

Foram mostrados trabalhos que propuseram mecanismos para proteção de quadros de controle específicos, trabalhos que visam à proteção parcial de todos os quadros de controle (parcial porque não protegem contra ataque de *replay*). Foi apresentado ainda, um trabalho que fornece proteção mais abrangente, atingindo todos os quadros de controle inclusive contra ataques de *replay*, porém este último acrescenta 160 *bits* ao tamanho do quadro.

A contribuição que esta dissertação trouxe foi a propositura de um mecanismo que permita dar segurança aos quadros de controle, por meio da adição de dois novos campos: um número de sequência e um código de autenticação de mensagem que alteram o formato

original dos quadros de controle. Estes dois novos campos permitem proteger os quadros de controle contra os ataques, inclusive os de *replay*, com um maior grau de segurança e um menor *overhead* para o funcionamento da rede sem fio.

O mecanismo criado utiliza as chaves geradas durante o *4-Way-Handshake*, acrescenta um número de sequência que vai junto ao quadro de controle em texto claro. Este mecanismo utiliza o CBC-MAC, que já está presente nos dispositivos compatíveis com o WPA2, para a geração do campo MAC - o campo MAC também é acrescentado ao quadro. A partir da chave, do número de sequência, da mensagem recebida e de outros elementos necessários para a execução do CBC-MAC o quadro é então encapsulado e está pronto para o envio. Ao chegar ao destinatário, ele estará apto a recalcular o MAC, verificar se aquele quadro é legítimo e, se não se trata de uma repetição. Caso o quadro seja legítimo e não se trate de uma repetição, o destinatário poderá agir conforme o quadro solicita, se for identificado que o quadro não é legítimo ou trata-se de um quadro repetido ele é descartado e, nenhuma ação solicitada pelo quadro é executada.

Como trabalhos futuros pretende-se: (i) Implementar a proposta no NS-3 e verificar outros custos associados à implementação; (ii) Considerar a possibilidade de estes ataques terem origem na rede interna e buscar alternativas para evitar o ataque por parte de indivíduos que possuem a chave de grupo.

Esta dissertação gerou uma publicação no XI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais promovido pela Sociedade Brasileira de Computação (SBC), em novembro de 2011, intitulada “Um Mecanismo de Proteção de Quadros de Controle para Redes IEEE 802.11” [Corrêa Jr. and Gonçalves 2011].

REFERÊNCIAS BIBLIOGRÁFICAS

[Bai et al. 2009] Bai, Y., Yu, Y., and Chen, L. (2009). Enhanced Protection Mechanism for Improving Co-Existence of IEEE 802.11b and IEEE 802.11g Wireless LANs. In *Proceedings of the 69th IEEE Vehicular Technology Conference, VTC Spring 2009,26-29 April 2009, Hilton Diagonal Mar, Barcelona, Spain*. IEEE.

[Bellardo and Savage 2003] Bellardo, J. and Savage, S. (2003). 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In *Proceedings of the 12th conference on USENIX Security Symposium (SSYM)*, pages 2–2, Berkeley, CA, USA. USENIX Association.

[Bogdanov et al. 2011] 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, South Korea, December 4-8, 2011. Proceedings*, pages 344–371.

[Borisov et al. 2001a] Borisov, N., Goldberg, I., and Wagner, D. (2001a). (In)Security of The WEP algorithm. `http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html`.

[Borisov et al. 2001b] Borisov, N., Goldberg, I., and Wagner, D. (2001b). Intercepting Mobile Communications: The Insecurity of 802.11. In *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom)*, pages 180–189, New York, NY, USA. ACM.

[Cam-Winget et al. 2007] Cam-Winget, N., Smith, D., and Walker, J. (2007). IEEE 802.11-07/2163r0 - A-MPDU security issues.

[Chen and Muthukkumarasamy 2006] Chen, B. and Muthukkumarasamy, V. (2006). Denial of Service Attacks Against 802.11 DCF Abstract. In *Proceedings of the IADIS International Conference Applied Computing*.

[Corrêa Jr. and Gonçalves 2011] Corrêa Jr., M. A. C. and Gonçalves, P. A. S. (2011). Um Mecanismo de Proteção de Quadros de Controle para Redes IEEE 802.11. In *Proceedings of the XI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG)*.

[da Conceição et al. 2006] da Conceição, A. F., Li, J., and Florêncio, D. A. (2006). Voice Transmission over IEEE 802.11 Networks: Main Issues and Restrictions. In *Proceedings of the 12th Brazilian Symposium on Multimedia and the Web (WebMedia)*, pages 233–242, New York, NY, USA. ACM.

[Dworkin 2004] Dworkin, M. (2004). Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. NIST - Special Publication 800-38C.

[Eastlake and Jones 2001] Eastlake, D. and Jones, P. (2001). RFC 3174 - US Secure Hash Algorithm 1 (SHA1).

[Eaton 2002] Eaton, D. (2002). Diving into the 802.11i Spec: A Tutorial.

[Fluhrer et al. 2001] Fluhrer, S. R., Mantin, I., and Shamir, A. (2001). Weaknesses in the Key Scheduling Algorithm of RC4. *Lecture Notes in Computer Science*, 2259.

[H.Krawczyk et al. 1997] H.Krawczyk, M.Bellare, and R.Canneti (1997). RFC 2104 - HMAC: Keyed-Hashing for Message Authentication.

[IEEE Standard 802.11 1999] 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 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 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 802.11g 2003] IEEE Standard 802.11g (2003). 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: Further Higher Data Rate Extension in the 2.4 GHz Band.

[IEEE Standard 802.11i 2004] 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 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 802.11n 2009] IEEE Standard 802.11n (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 5: Enhancements for Higher Throughput.

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

[Kim et al. 2006] 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 et al. 2009] Koenings, B., Schaub, F., Kargl, F., and Dietzel, S. (2009). Channel Switch and Quiet attack: New DoS attacks exploiting the 802.11 standard. In *The 34th IEEE Conference on Local Computer Networks (LCN)*, Zurich, Switzerland.

[Malekzadeh et al. 2010] 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.*, 2010:5:1–5:15.

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

[Moskowitz 2003] Moskowitz, R. (2003). Weakness in Passphrase Choice in WPA Interface. `http://wifinetnews.com/archives/002452.html`.

[Myneni and Huang 2010] Myneni, S. and Huang, D. (2010). IEEE 802.11 Wireless LAN Control Frame Protection. In *CCNC'10: Proceedings of the 7th IEEE conference on Consumer communications and networking conference*, pages 844–848, Piscataway, NJ, USA. IEEE Press.

[NIST 2001] NIST (2001). Specification for the Advanced Encryption Standard (AES), FIPS 197.

[Qureshi et al. 2007] 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 *Proceedings of the 11th Conference on 11th WSEAS International Conference on Communications - Volume 11*, pages 7–11, Stevens Point, Wisconsin, USA. World Scientific and Engineering Academy and Society (WSEAS).

[Rachedi and Benslimane 2009] 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 and Starobinski 2007] 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 and Rijmen 2008] Rechberger, C. and Rijmen, V. (2008). New Results on NMAC/HMAC when Instantiated with Popular Hash Functions. *Universal Computer Science*, pages 347–376.

[Rogaway 2011] Rogaway, P. (2011). Evaluation of Some Blockcipher Modes of Operation. Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan.

[Stubblefield et al. 2001] Stubblefield, A., Ioannidis, J., and Rubin, A. D. (2001). Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. Technical report, AT&T Labs.

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

[Wang et al. 2005] Wang, X., Yin, Y. L., and Yu., H. (2005). Finding collisions in the full SHA-1. In *Advances in Cryptology (CRYPTO)*, volume 3621 of *Lecture Notes in Computer Science*, pages 17–36. Springer-Verlag.

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