Universidade Federal de Pernambuco

Centro de Informática

Pós-graduação em Ciência da Computação

UM ESQUEMA DE SEGURANÇA PARA QUADROS DE CONTROLE EM REDES IEEE 802.11

Ivan Luiz de França Neto

DISSERTAÇÃO DE MESTRADO

Recife

14 de Agosto de 2015

Universidade Federal de Pernambuco

Centro de Informática

Ivan Luiz de França Neto

UM ESQUEMA DE SEGURANÇA PARA QUADROS DE CONTROLE EM 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: *Paulo André da Silva Gonçalves*

Recife

14 de Agosto de 2015

Este trabalho é dedicado a Deus, à minha família e a todos que contribuíram com o mesmo.

AGRADECIMENTOS

Agradeço a Deus pela minha vida e saúde. Foram nos momentos mais díficeis que aprendi a confiar nEle e no Seu cuidado. Tenho aprendido o quanto a vida nessa Terra é passageira (os anos voam) e que nada se compara a vida eterna que ele tem preparado. Amar ao próximo como a si mesmo é o que as pessoas desse mundo mais precisam.

Agradeço aos meus pais pelos princípios e valores que me foram transmitidos durante toda minha formação. Obrigado pelo amor e por toda dedicação de vocês. Obrigado por todo esforço para me dar a melhor educação possível. Serei eternamente grato e, por isso, dedico minhas conquistas a vocês, pois elas não são minhas, mas são NOSSAS. Também dedico esse trabalho aos meus irmãos, Felipe e Hugo, e a minha namorada. Paulinha, você foi um dos melhores presentes que recebi de Deus. Obrigado por todo apoio, cuidado e amor.

Como em qualquer trabalho acadêmico, o papel do orientador é muito importante para o resultado alcançado. Agradeço muito ao professor Paulo Gonçalves pelo direcionamento durante a pesquisa e por todos os comentários construtivos durante as reuniões de acompanhamento. Parabéns pela dedicação, atenção e cuidado que tem com cada membro do seu grupo de pesquisa. Obrigado por toda experiência transmitida desde os tempos de Iniciação Científica. Essa conquista também é dedicada a cada integrante do grupo de pesquisa. Aprendi muito com vocês também.

E disse ao homem: Eis que o temor do Senhor é a sabedoria, e apartar-se do mal é a inteligência.

— JÓ 28:28

RESUMO

Os quadros de controle IEEE 802.11 desempenham funções importantes na rede sem fio. Dentre elas estão o controle de acesso ao meio de comunicação, a recuperação de quadros armazenados no Ponto de Acesso e a confirmação do recebimento de blocos de quadros ou de certos tipos de quadros. Apesar da importância dos quadros de controle, eles são vulneráveis a ataques de forjação, manipulação e reinjeção devido à inexistência de mecanismos de proteção. Este trabalho propõe um esquema de segurança para quadros de controle em redes IEEE 802.11 a fim de evitar esses ataques. A proposta se diferencia dos trabalhos relacionados por prover um alto grau de segurança em todos os seus módulos com baixo impacto na vazão da rede. Além disso, a proposta não incorre nas fraquezas que eles possuem na contenção dos ataques de reinjeção e no processo de geração e distribuição de chaves.

Palavras-chave: Redes sem fio, quadros de controle, negação de serviço, geração e distribuição de chave, ataque de replicação

ABSTRACT

IEEE 802.11 control frames play important roles in the wireless network. Among them are the medium access control, the retrieve of buffered frames in the Access Point, and the acknowledgment of block of frames or certain types of frames. Despite their importance, control frames remain vulnerable to forging, tampering, and replay attacks due to lack of protection mechanisms. This work proposes a security scheme for IEEE 802.11 control frames to prevent such attacks. Our proposal differs from related work by providing a high level of security in all modules along with low impact on network throughput. Furthermore, the proposal avoid the weaknesses that they have in the restraint the replay attacks and in the key generation and distribution process.

Keywords: Wireless network, control frame, denial of service, key generation and distribution, replay attack

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

AES *Advanced Encryption Standard*. 20

AMK Authenticity Master Key. 36

AP *Access Point*. 2, 7, 13, 29, 35–37, 41, 45

ATK Authenticity Temporal Key. 33, 35–37, 39, 41–43, 45

CBC-MAC *Cipher Block Chaining-Message Authentication Code*. 21, 28

CMAC *Cipher-based MAC*. 20, 22, 41, 43, 44, 59

DoS *Denial-of-Service*. 1

FCS *Frame Check Sequence*. 6, 8, 26

GTK *Group Temporal Key*. 18, 19, 28, 29, 35–37, 57

HMAC *Hash function-based MAC*. 27, 28, 44, 57

IAPP *Inter-Access Point Protocol*. 27, 29, 31, 56

IEEE *Institute of Electrical and Electronics Engineers*. 1–3, 5, 14

MAC *Message Authentication Codes*. 2, 21, 22, 27, 41, 43, 45

NS Número de Sequência. 32, 33, 39, 46

PTK *Pairwise Temporal Key*. 18, 26, 29, 36, 57

RA Receiver Address. 6, 8

RSNA Robust Security Network Association. 35

SHA-1 *Secure Hash Algorithm-1*. 27, 57

SHA-256 *Secure Hash Algorithm-256*. 28, 31, 56

TA Transmitter Address. 6, 8, 34, 41, 55

TMT *Theoretical Maximum Throughput*. 47, 49

CAPÍTULO 1

INTRODUÇÃO

As redes sem fio baseadas no padrão IEEE 802.11 [IEEE Standard 802.11 2012] oferecem diversas vantagens quando comparadas as redes cabeadas, como a mobilidade oferecida aos usuários, a facilidade e a velocidade de implantação, a flexibilidade e o baixo custo [Gast 2002]. Além disso, essas redes estão cada vez mais populares e um número crescente de residências, edifícios de escritórios e espaços públicos tais como *shoppings*, aeroportos e centros urbanos estão sendo equipados por elas, para conectar dispositivos à Internet. Nessas redes, a conectividade e as garantias de disponibilidade de acesso constante são fatores de fundamental importância.

O padrão IEEE 802.11 [IEEE Standard 802.11 2012] para redes locais sem fio provê especificações para as camadas física e enlace. Esse padrão define três tipos de quadros para a camada enlace: controle, dados e gerenciamento. Os quadros de controle são utilizados para controlar o acesso ao meio e para confirmação do recebimento de alguns tipos de quadros. Os quadros de dados são utilizados para transportar dados das camadas superiores. Os quadros de gerenciamento são utilizados, dentre outras coisas, para o estabelecimento da comunicação entre as estações e o Ponto de Acesso.

Nas redes sem fio baseadas no padrão IEEE 802.11, assim como em qualquer outra tecnologia que utiliza o canal sem fio para envio de dados, a segurança é um fator essencial para garantir o sigilo e a integridade dos dados, bem como a autenticação dos clientes legítimos. Desta forma, ao longo dos anos, alguns protocolos de segurança foram definidos para atuarem na camada enlace dessas redes protegendo os quadros de dados [IEEE Standard 802.11i 2004] e de gerenciamento [IEEE Standard 802.11w 2009]. Apesar de prover diferentes níveis de segurança, as WLANs baseadas no padrão IEEE 802.11 permanecem vulneráveis a ataques de negação de serviço ou DoS (*Denial of Ser-*

vice), devido à falta de proteção e autenticação dos quadros de controle.

1.1 MOTIVAÇÃO

Os quadros de controle possuem papeis importantes nas redes sem fio baseadas no padrão IEEE 802.11. Dentre eles estão o controle de acesso ao meio de comunicação, a recuperação de quadros armazenados no Ponto de Acesso ou AP (*Access Point*) e a confirmação do recebimento de blocos de quadros ou de certos tipos de quadros [IEEE Standard 802.11 2012]. Apesar da importância dos quadros de controle, eles são vulneráveis a ataques de forjação, manipulação e reinjeção (*replay*) devido à inexistência de mecanismos para a proteção dos mesmos.

Em geral, a consequência desses ataques é algum tipo de negação de serviço (*DoS*) ao AP e estações que compõem a rede sem fio. Alguns exemplos incluem os ataques *CTS* (*Clear to Send*) *replay* e *RTS* (*Request to Send*) *replay*, os quais obrigam entidades legítimas da rede a postergarem desnecessariamente suas transmissões [Myneni e Huang 2010]. Outro exemplo é o envio de um *ACK* falso, validando quadros enviados por um nó remetente, mesmo que tais quadros não tenham sido recebidos corretamente pelo nó destinatário. [Rachedi e Benslimane 2009]. Devido a falta de mecanismos de proteção para os quadros de controle, diferentes tipos de esquemas de defesa têm sido propostos ao longo dos anos a fim de evitar, mitigar ou ao menos detectar as tentativas de ataques [Qureshi et al. 2007, Zhang et al. 2008, Khan e Hasan 2008, Rachedi e Benslimane 2009, Myneni e Huang 2010, Jr. e Gonçalves 2011, Malekzadeh, Ghani e Subramaniam 2012].

Este trabalho propõe um esquema de segurança para a proteção dos quadros de controle de redes IEEE 802.11. O esquema proposto busca evitar a negação de serviço consequente das tentativas de forjação, manipulação e reinjeção desses quadros. Os ataques considerados são aqueles provenientes de entidades maliciosas não pertencentes à rede. Para prover segurança, o esquema proposto faz uso de números de sequência individuais e códigos de autenticação de mensagem ou MACs (*Message Authentication Codes*). A proposta se diferencia dos trabalhos relacionados por prover um alto grau de segurança

em todos os seus módulos com baixo impacto na vazão e no *overhead* da comunicação. Além disso, a proposta não incorre nas fraquezas que eles possuem na contenção dos ataques de reinjeção e no processo de geração e distribuição de chaves.

1.2 OBJETIVOS

O objetivo geral dessa dissertação de mestrado é a proposição de um esquema de segurança para proteção dos quadros de controle das redes IEEE 802.11 contra ataques de forjação, manipulação e reinjeção desses quadros. Esse esquema deve fornecer segurança em todos os seus módulos, sem adicionar um *overhead* significativo na comunicação. Nesse sentido, deseja-se especificamente:

1. Estudar o padrão IEEE 802.11 e os módulos de segurança disponíveis no padrão;
2. Estudar os principais ataques direcionados aos quadros de controle nas redes IEEE 802.11;
3. Estudar as soluções que buscam proteger os quadros de controle nas redes IEEE 802.11;
4. Propor um esquema de proteção aos quadros de controle que se adeque ao objetivo geral;
5. Realizar experimentos e avaliar o impacto da solução na vazão da rede.

1.3 ORGANIZAÇÃO

O restante deste trabalho está organizado da seguinte forma: o Capítulo 2 apresenta as principais funcionalidades dos quadros de controle IEEE 802.11 e alguns ataques conhecidos aos quadros de controle para a negação de serviço na rede. Nesse capítulo também são apresentados os protocolos de acesso ao meio de comunicação e os processos de Geração e Distribuição de Chaves presentes no padrão IEEE 802.11. O Capítulo 3 apresenta os trabalhos relacionados. O Capítulo 4 apresenta o esquema de segurança proposto. O

Capítulo 5 apresenta o impacto dos esquemas de proteção estudados na vazão da rede. Por fim, o Capítulo 6 apresenta as conclusões.

CAPÍTULO 2

CONCEITOS BÁSICOS

Este capítulo descreve os conceitos básicos relativos às redes IEEE 802.11 e ao Código de Autenticação de Mensagem CMAC (*Cipher-based MAC*) [Dworkin 2005] [Barker e Roginsky 2011] [Barker et al. 2012]. A Seção 2.1 apresenta os quadros de controle presentes em uma rede IEEE 802.11 e alguns ataques de forjação, manipulação e reinjeção desses quadros. A Seção 2.3 apresenta os protocolos de acesso ao meio de comunicação definidos no padrão IEEE 802.11. A função desses protocolos é determinar quando determinada estação pode transmitir seus quadros na rede. A Seção 2.4 apresenta os principais processos de geração e distribuição de chaves definidos pelo padrão IEEE 802.11. Tais processos são utilizados para garantir a integridade e a confidencialidade dos dados que trafegam na camada de enlace. Por fim, a Seção 2.5 apresenta os mecanismos de Geração e Verificação do Código de Autenticação de Mensagens CMAC. O CMAC é utilizado para garantir a integridade e a autenticidade das mensagens trocadas entre duas partes comunicantes.

2.1 QUADROS DE CONTROLE IEEE 802.11

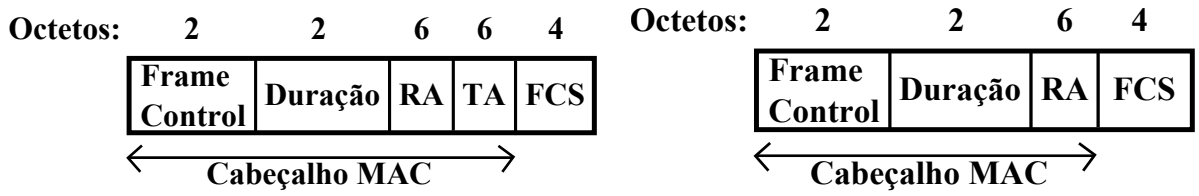
Os quadros de controle na revisão mais atual do padrão IEEE 802.11 [IEEE Standard 802.11 2012] possuem 9 subtipos: RTS (*Request to Send*), CTS (*Clear to Send*), ACK (*Acknowledgment*), PS-Poll (*Power Save Poll*), CF-End (*Contention-Free End*), CF-End+CF-ACK (*Contention-Free End + ACK*), BAR (*Block Ack Request*), BA (*Block Ack*) e *Control Wrapper*. As funcionalidades deles são descritas nesta seção.

2.1.1 RTS (Request to Send) e CTS(Clear to Send)

O mecanismo RTS/CTS serve para minimizar a ocorrência de colisões no meio de comunicação. Ele define um *handshake* antes de duas entidades da rede trocarem dados. Uma estação que faz uso de tal mecanismo e está disposta a transmitir dados a um destinatário, envia inicialmente um quadro RTS. O destinatário, por sua vez, responde ao RTS recebido com um quadro CTS. Todas as demais entidades da rede que ouvem o RTS ou o CTS são silenciadas por um período de tempo suficiente para a troca dos dados e confirmação de recebimento dos mesmos. Na prática, o mecanismo RTS/CTS é utilizado quando o quadro de dados a ser enviado possui um tamanho maior que um limiar pré-definido [IEEE Standard 802.11 2012]. Seu uso para quadros de dados curtos adiciona um *overhead* significativo de comunicação que não justifica o seu emprego.

O IEEE 802.11 também define um mecanismo conhecido por *CTS-to-self*, onde determinada entidade pode reservar o acesso ao meio de comunicação através da transmissão de um quadro CTS destinado a ela mesma. Esse mecanismo é menos custoso para rede do que o mecanismo RTS/CTS. No entanto, não lida de forma satisfatória no tratamento do problema do nó escondido e na prevenção de colisões. A escolha do mecanismo mais apropriado depende das condições da rede em questão [IEEE Standard 802.11 2012].

As Figuras 2.1(a) e 2.1(b) apresentam o formato de um quadro RTS e de um quadro CTS, respectivamente. O quadro RTS é composto por cinco campos. O campo FC (*Frame Control*) possui 2 bytes e informa o tipo e o subtipo do quadro, além de outras informações de controle. O campo Duração possui 2 bytes e informa o período de tempo (em microssegundos) que o canal ficará reservado. O campo RA (*Receiver Address*) possui 6 bytes e informa o endereço do nó receptor. O campo TA (*Transmitter Address*) possui 6 bytes e informa o endereço do nó transmissor. O campo FCS (*Frame Check Sequence*) possui 4 bytes e é usado na checagem da integridade dos quadros recebidos. O quadro CTS possui 4 campos, todos presentes em um quadro RTS. O quadro CTS só não possui o campo TA (*Transmitter Address*), que informa o endereço do nó transmissor. Portanto, um quadro RTS e um quadro CTS possuem, respectivamente, 20 e 14 bytes de comprimento.



(a) Quadro RTS. (b) Quadro CTS.

Figura 2.1 Quadros de controle RTS e CTS.

2.1.2 ACK (Acknowledgement)

Um nó receptor em uma rede IEEE 802.11 deve confirmar o recebimento de determinados tipos de quadros através do envio de um quadro ACK ao nó transmissor. Como apresentado na Figura 2.2, um quadro ACK não carrega informações sobre o endereço do nó transmissor, mas apenas do nó receptor. O tamanho do quadro ACK é de 14 bytes.

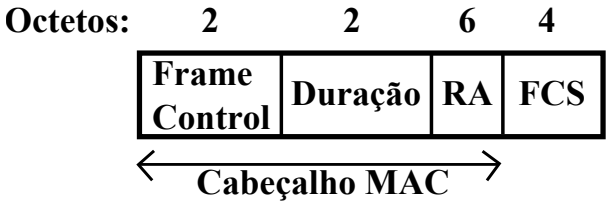


Figura 2.2 Quadro de controle ACK.

2.1.3 PS-POLL (Power Save Poll)

As redes IEEE 802.11 definem um mecanismo de Gerenciamento de Energia (*Power Management*). Uma estação pode estar em um dos dois modos de gerenciamento de energia possíveis: o modo AM (*Active mode*) e o modo PS (*Power Save*). Uma estação que se encontra no modo AM pode receber quadros a qualquer momento. Já uma estação no modo PS, se encontra em um estado de repouso e não deve receber quadros. Quando uma estação se encontra no modo PS (*Power Save*), o AP não deve transmitir os quadros que chegam para a referida estação. O AP deve armazená-los e transmiti-los somente no momento em que a estação informar que está pronta para recebê-los. Tal informação é fornecida por meio de um quadro PS-Poll ao AP.

O quadro PS-Poll é composto por cinco campos, como apresentado na Figura 2.3: FC (*Frame Control*), AID (*Association ID*), BSSID (RA), TA (*Transmitter Address*) e FCS (*Frame Check Sequence*). O campo AID possui 2 bytes e é utilizado para armazenar o ID de associação da estação, os dois bits mais sgnificativos do valor contido neste campo devem ser setados para 1. O campo BSSID (*Basic Service Set Identification*) possui 6 bytes e identifica a BSS (*Basic Service Set*), que em uma rede infraestruturada é o endereço MAC (*Medium Access Control*) do AP da BSS. As funcionalidades dos demais campos já foram citadas anteriormente. Um quadro PS-Poll possui 20 bytes de comprimento.

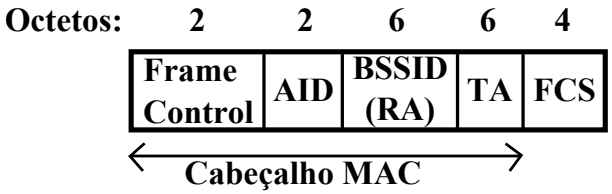


Figura 2.3 Quadro de controle PS-Poll.

2.1.4 CF-End (Contention Free End) e CF-End+CF-ACK (CF-End+Contention Free Ack)

O IEEE 802.11 define um método de acesso ao meio opcional denomidado PCF (*Point Coordination Function*). Nesse método de acesso, o AP determina qual estação atualmente tem o direito de transmitir. Quando a operação PCF se encerra, o AP informa o fim desse período através da transmissão de um quadro CF-End ou CF-End+CF-ACK. O quadro CF-End+CF-ACK é usado quando há algum quadro recebido que necessita de confirmação no momento em que o PCF é encerrado.

Os quadros de controle CF-End e CF-End+CF-ACK são idênticos. Como apresentado na Figura 2.4, eles são formados por cinco campos: FC (*Frame Control*), Duração, RA (*Receiver Address*), BSSID (TA) e FCS (*Frame Check Sequence*). O campo RA é o endereço *broadcast* do grupo e o campo duração é setado para 0, pois não é utilizado durante a utilização do método PCF. As funcionalidades dos demais campos já foram

citadas anteriormente. Os quadros CF-End e CF-End+CF-ACK possuem 20 bytes de comprimento cada um.

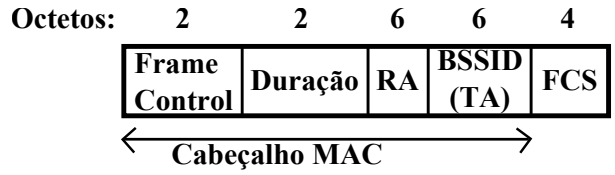


Figura 2.4 Quadros de controle CF-End e CF-End+CF-ACK.

2.1.5 BAR (Block Ack Request) e BA (Block Ack)

O padrão IEEE 802.11 define o mecanismo *Block Ack*, o qual agrega diversas confirmações em um único quadro de controle. Com isso, a eficiência no uso do canal de comunicação é melhorada. O mecanismo *Block Ack* é composto por três fases: (1) *Setup*, (2) Transferência dos dados e da confirmação *Block Ack* e (3) *Tear Down*. A Figura 2.5 apresenta o gráfico de sequência de mensagens trocadas em cada fase. Esse mecanismo é inicializado na fase de *Setup*. Durante essa fase, quadros Requisição/Resposta ADDBA (*add Block Acknowledgment*) são trocados entre o nó transmissor e o nó receptor. É nessa fase que as estações alocam recursos e negociam, por exemplo, a quantidade máxima de quadros de dados transmitida em um bloco.

Finalizada a fase de *setup*, a estação transmissora pode iniciar o envio de blocos de quadros de dados para a estação receptora. Quando todos os quadros de um bloco forem transmitidos, a estação transmissora deve solicitar à estação receptora a confimação de que o bloco enviado foi recebido corretamente. Essa solicitação é realizada com o envio de um quadro de controle do tipo BAR (*Block Ack Request*). Uma vez que a estação receptora tenha recebido corretamente todos os quadros de dados pertencentes ao bloco, ao receber o quadro de controle BAR, esta deve enviar à estação transmissora um quadro de controle do tipo BA (*Block Ack*), confirmando o recebimento dos quadros pertencentes ao bloco.

Quando o nó transmissor não tem mais dados a enviar, este deve comunicar ao nó

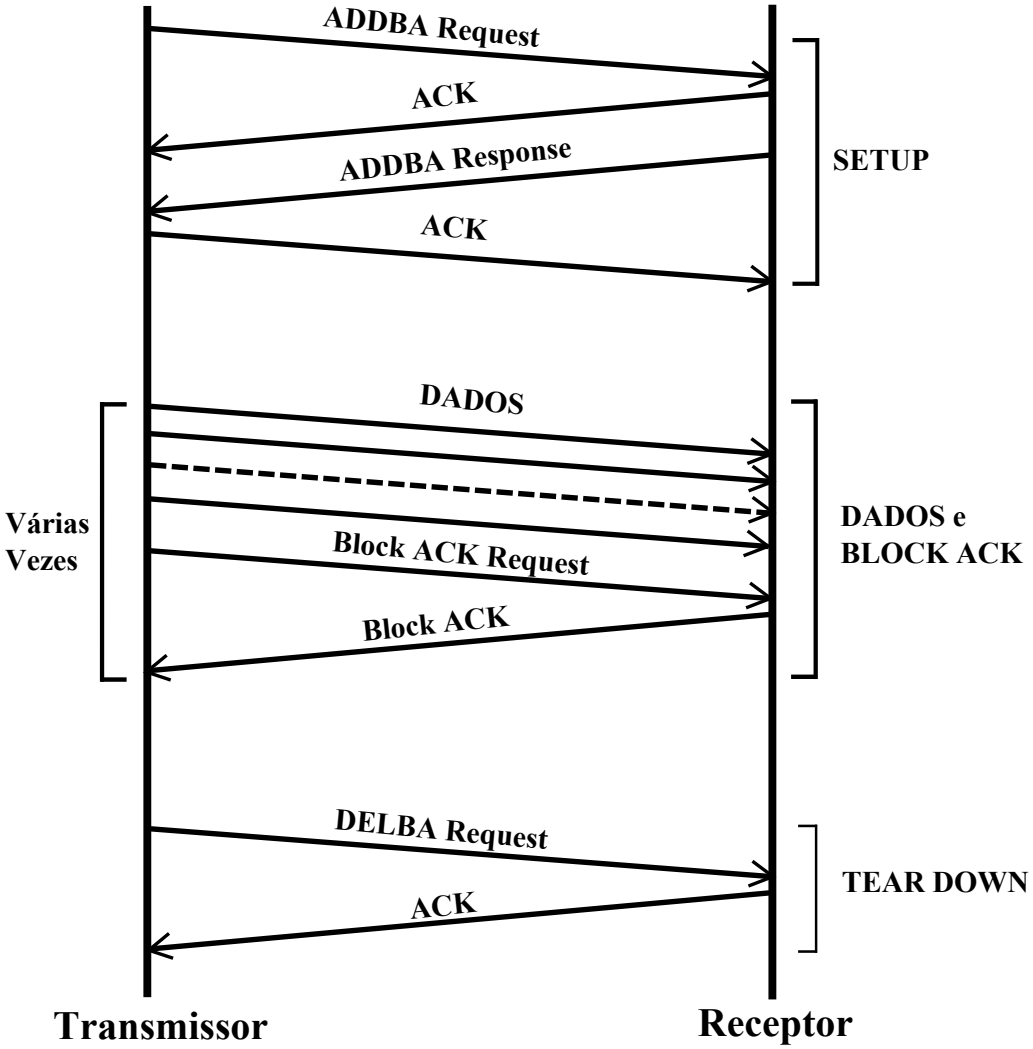


Figura 2.5 Sequência de mensagens trocadas no mecanismo *Block ACK*.

receptor o encerramento do uso do mecanismo *Block Ack*. Essa comunicação é realizada durante a fase *Tear Down* por meio do envio do quadro *DELBA* (*delete Block Acknowledgment*) *Request*. O nó receptor, ao receber esse quadro, deve liberar todos os recursos alocados durante a fase de *Setup*.

A Figura 2.6 apresenta o formato do quadro de controle BAR. O quadro BAR é composto por sete campos: FC (*Frame Control*), Duração, RA (*Receiver Address*), TA (*Transmitter Address*), BAR *Control*, BAR *Information* e FCS (*Frame Check Sequence*). O campo BAR *Control* possui 2 bytes e uma de suas funções é informar os parâmetros de *QoS* utilizados, como o TID (*Traffic Identifier*). O campo BAR *Information* possui

comprimento variável e carrega o número de sequência do primeiro quadro do bloco.

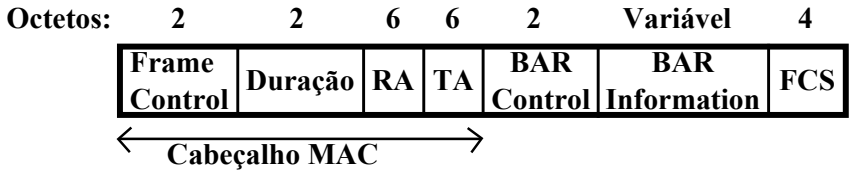


Figura 2.6 Quadro de controle BAR.

A Figura 2.7 apresenta o formato do quadro de controle BA. O quadro BA também é composto por sete campos: FC (*Frame Control*), Duração, RA (*Receiver Address*), TA (*Transmitter Address*), BA *Control*, BA *Information* e FCS (*Frame Check Sequence*). O campo BA *Information* possui comprimento variável e indica, por exemplo, o *status* de recepção dos quadros do bloco. As funcionalidades dos demais campos já foram citadas anteriormente.

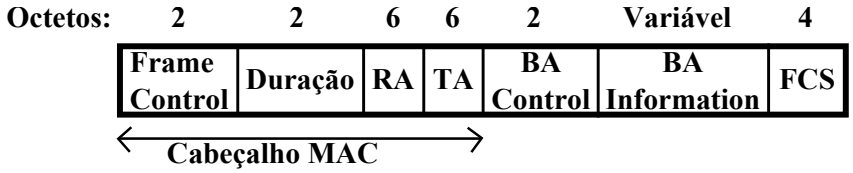


Figura 2.7 Quadro de controle BA.

O comprimento de um quadro BAR depende do tipo da variante do quadro BAR, o qual pode ser classificado em: *Basic*, *Compressed* e *Multi-TID*. Os quadros *Basic* e *Compressed* BAR possuem 24 bytes de comprimento. Da mesma forma, o comprimento de um quadro BA depende do tipo da variante do quadro BA, que também pode ser classificado em: *Basic*, *Compressed* e *Multi-TID*. Os quadros *Basic* e *Compressed* BA possuem, respectivamente, 152 bytes e 32 bytes de comprimento. O comprimento dos quadros *Multi-TID* BAR e *Multi-TID* BA é variável.

2.1.6 Control Wrapper

Esse quadro foi criado com a emenda IEEE 802.11n [IEEE Standard 802.11n 2009], a qual define as transmissões *High Throughput* (HT). O quadro *Control Wrapper* é usado

para transportar outros quadros de controle (com exceção do quadro *Control Wrapper*) juntamente com um campo HT *Control*, o qual é necessário para a realização de certas operações definidas no IEEE 802.11n.

A Figura 2.8 apresenta o formato do quadro de controle *Control Wrapper*. Esse quadro é composto por sete campos: FC (*Frame Control*), Duração/ID, *Endereço 1*, *Carried Frame Control*, HT *Control*, *Carried Frame* e FCS (*Frame Check Sequence*). O campo *Endereço 1* possui 6 bytes e é gerado de acordo com as regras que definem o valor do campo *Endereço 1* no quadro de controle transportado. O campo *Carried Frame Control* contém o valor do campo *Frame Control* do quadro de controle transportado. O campo *Carried Frame* contém alguns dos campos do quadro de controle que está sendo transportado. As funcionalidades dos demais campos já foram citadas em seções anteriores. O comprimento de um quadro *Control Wrapper* depende do quadro de controle que está sendo transportado.

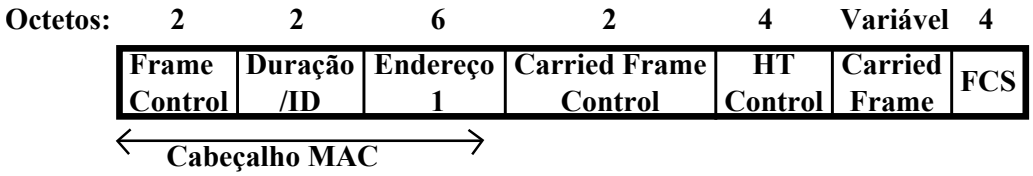


Figura 2.8 Quadro de controle *Control Wrapper*.

2.2 ATAQUES AOS QUADROS DE CONTROLE

Devido à inexistência de mecanismos para a proteção dos quadros de controle, as redes IEEE 802.11 se tornam vulneráveis a diversos tipos de ataques de forjação, manipulação e reinjeção desses quadros. Os ataques considerados são aqueles provenientes de entidades maliciosas não pertencentes à rede. Esta seção apresenta os principais ataques e suas consequências.

2.2.1 Ataques aos quadros RTS e CTS

Um dos ataques ao mecanismo RTS/CTS é a injeção de quadros RTS e CTS falsificados na rede. Nesse ataque, uma estação maliciosa cria e envia quadros RTS e CTS falsos a fim de bloquear o uso do canal de comunicação pelos nós vizinhos através de uma falsa reserva [Ray e Starobinski 2007]. Atacantes mais experientes podem ainda manipular o valor contido no campo *Duração* desses quadros. Esse valor instrui as estações vizinhas por quanto tempo o canal não poderá ser utilizado por elas. O valor máximo possível para tal campo é de 32.767 microssegundos.

Outro tipo de ataque associado ao mecanismo RTS/CTS é o ataque de reinjeção [Myneni e Huang 2010]. Nesse ataque, a estação maliciosa ouve o canal para capturar quadros RTS ou CTS enviados por estações legítimas e os retransmitir na rede. As estações que ouvem as retransmissões postergam indevidademente suas transmissões.

2.2.2 Ataques ao quadro ACK

Outro tipo de ataque é a injeção de ACK falsificado na rede [Chen e Muthukkumarasamy 2006] [Rachedi e Benslimane 2009]. Nesse ataque, uma estação maliciosa gera um quadro ACK falsificado destinado a um transmissor de dados na rede. Caso o ataque tenha sucesso, isso confirma o recebimento de quadros que podem não ter sido recebidos corretamente pelo receptor. Assim, não haverá retransmissão dos quadros em questão devido à falsa confirmação.

2.2.3 Ataques ao quadro PS-Poll

Um ataque de negação de serviço baseado em quadros PS-Poll é apresentado em [Qureshi et al. 2007]. Nesse ataque, uma estação maliciosa forja e envia quadros PS-Poll ao AP se passando por uma estação legítima que se encontra em modo PS (*Power Save*). O AP é forçado a transmitir os dados armazenados para estação legítima que, por estar em modo PS, não receberá os quadros a ela destinados.

2.2.4 Ataques aos quadros CF-End e CF-End+CF-ACK

Em [Malekzadeh, Ghani e Subramaniam 2010] é apresentado o impacto de ataques de negação de serviço a partir da manipulação dos quadros de controle CF-End e CF-End+CF-ACK. Durante a realização dos ataques foi possível perceber que o serviço fornecido pela rede sem fio ficou indisponível e que as transmissões legítimas foram interrompidas, devido a sobrecarga da rede.

2.2.5 Ataques aos quadros BAR e BA

Em [Koenings et al. 2009] é apresentado um ataque que explora o mecanismo *Block Ack*. Uma estação maliciosa pode facilmente forjar a mensagem *Delete Block Acknowledgement* (*DELBA*) utilizada para finalizar a comunicação estabelecida entre duas estações durante o processo *Block Ack*. Dessa forma, a estação maliciosa pode finalizar prematuramente o processo *Block Ack* estabelecido entre estações legítimas, liberando os recursos alocados por essas estações e acarretando na perda de quadros.

2.3 PROTOCOLOS DE ACESSO AO MEIO DE COMUNICAÇÃO DEFINIDOS NO PADRÃO IEEE 802.11

Os nós pertencentes à uma rede IEEE 802.11 devem coordenar o acesso ao meio de comunicação compartilhado. O padrão IEEE 802.11 fornece dois métodos de controle de acesso ao meio: o *Distributed Coordination Function* (DCF), que é um método distribuído, e o *Point Coordination Function* (PCF), que é centralizado. A função dos dois métodos é determinar quando uma estação pode transmitir quadros na rede. Se em determinado momento o meio de comunicação está ocupado com alguma estação transmitindo quadros, então outra estação que também deseja utilizar o canal deve postergar suas transmissões até que o meio de comunicação fique ocioso.

Quando uma estação percebe que o canal está ocioso, esta não irá transmitir imediatamente. A estação deve esperar certo intervalo de tempo, antes de iniciar sua transmissão.

Esse intervalo de tempo é denominado de espaçamento interquadros (*Interframe Space* - IFS). Dentre os IFSs definidos no padrão IEEE 802.11, os mais importantes são:

- *Short IFS* - (SIFS): O SIFS é o menor dos espaçamentos interquadros, fornecendo um alto nível de prioridade, permitindo que alguns quadros acessem o meio antes de outros. O ACK e o CTS, por exemplo, usam o intervalo SIFS;
- *DCF IFS* - (DIFS): Todas as estações que operam sobre o método de acesso DCF utilizam o intervalo DIFS para transmitir quadros de dados e quadros de gerenciamento;
- *PCF IFS* - (PIFS): PIFS é o intervalo tempo que o ponto de acesso deve esperar quando deseja operar o modo *Point Coordination Function* (PCF). Como a duração de um PIFS é menor que a de um DIFS, o ponto de acesso obtém o controle do meio de comunicação antes que as estações iniciem a transmissão de seus quadros utilizando o modo *Distributed Coordination Function* (DCF).

2.3.1 Distributed Coordination Function (DCF)

O método *Distributed Coordination Function* (DCF) deve ser implementado em todos os nós da rede. Por ser um método de controle de acesso ao meio distribuído, a decisão de qual estação tem o direito de transmitir em determinado momento é tomada pelas próprias estações. Devido a essa natureza distribuída, as estações podem transmitir quadros simultaneamente, ocasionando colisões. A fim de reduzir o número de colisões na rede e garantir que apenas uma estação transmita quadros em um dado momento, o DCF emprega uma combinação de mecanismos de detecção de portadora (*Carrier Sense* - CS).

O principal mecanismo de detecção de portadora utilizado no padrão é o *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA). O CSMA/CA é projetado para reduzir a probabilidade de colisão quando mais de uma estação compartilha determinado meio de comunicação. Nesse protocolo cada estação deve primeiramente examinar o canal

para determinar se ele está ocupado com a transmissão de quadros de outra estação. A camada física do IEEE 802.11 fornece essa informação a camada MAC.

A Figura 2.9 apresenta o mecanismo básico do CSMA/CA. Se determinada estação percebe que o canal está livre por um período de tempo igual a determinado espaçamento interquadros (IFS), então seus quadros podem ser transmitidos no canal. No entanto, se a estação detecta que o canal está ocupado, esta deve postergar seu acesso até que se perceba, mais tarde, que o canal está livre novamente. Assim que percebe que o canal está ocioso por um período de tempo igual a determinado IFS, a estação calcula um tempo de *backoff* aleatório e inicia a contagem regressiva desse tempo enquanto o canal estiver ocioso. Quando o temporizador chega a zero, a estação transmite seu quadro. Esse temporizador é utilizado para evitar que múltiplas estações inciem suas transmissões logo após um período IFS de inatividade na rede. O procedimento de *backoff* reduz o número de colisões entre quadros.

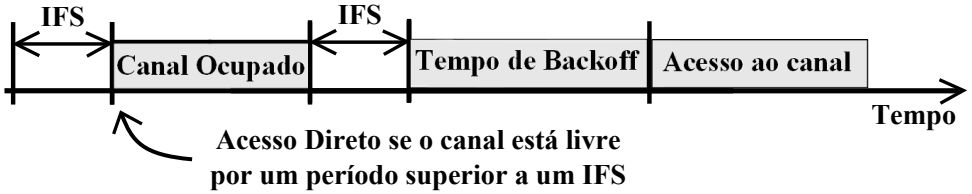


Figura 2.9 Mecanismo básico do CSMA/CA.

O DCF também fornece informações de reserva do canal através do campo *Duração*, presente no cabeçalho MAC dos quadros IEEE 802.11. Este procedimento ajuda a reduzir o número de colisões, permitindo que as estações realizem suas transmissões de forma eficiente. Se uma estação deseja transmitir um quadro de dados, esta deve indicar explicitamente, através do campo *Duração*, o período de tempo durante o qual o seu quadro será transmitido pelo canal. O valor desse campo é utilizado pelas estações que são afetadas pela transmissão para determinar o tempo durante o qual deverão adiar o seu acesso ao meio. Essa contagem é realizada por meio de um temporizador, denominado *Network Allocation Vector* (NAV). Desta forma, o NAV mantém uma predição de tráfego futuro no canal, baseado na informação contida no campo *Duração* dos quadros IEEE 802.11

2.3.1.1 Mecanismo Request-to-Send/Clear-to-Send (RTS/CTS)

O padrão IEEE 802.11 também inclui um mecanismo opcional de acesso ao meio: Request-to-Send/Clear-to-Send (RTS/CTS). Como apresentado na Seção 2.1.1, uma estação pode reservar o acesso ao meio de comunicação por meio do envio dos quadros de controle RTS e CTS. Como apresentado na Figura 2.10, quando uma estação transmissora deseja enviar um quadro de dados, ela pode, primeiramente, enviar um quadro RTS a estação receptora informando a duração do quadro de dados e do quadro ACK. A estação receptora, ao receber um quadro RTS responde com um quadro CTS autorizando a transmissão. Todas as outras estações, ao receberem os quadros RTS e CTS, sabem que o canal ficará reservado para uma transmissão por um período de tempo que é indicado no campo *Duração* dos quadros RTS e CTS. Desta forma, cada estação que ouve o CTS e o RTS atualiza seu temporizador NAV, adiando o seu acesso ao meio.

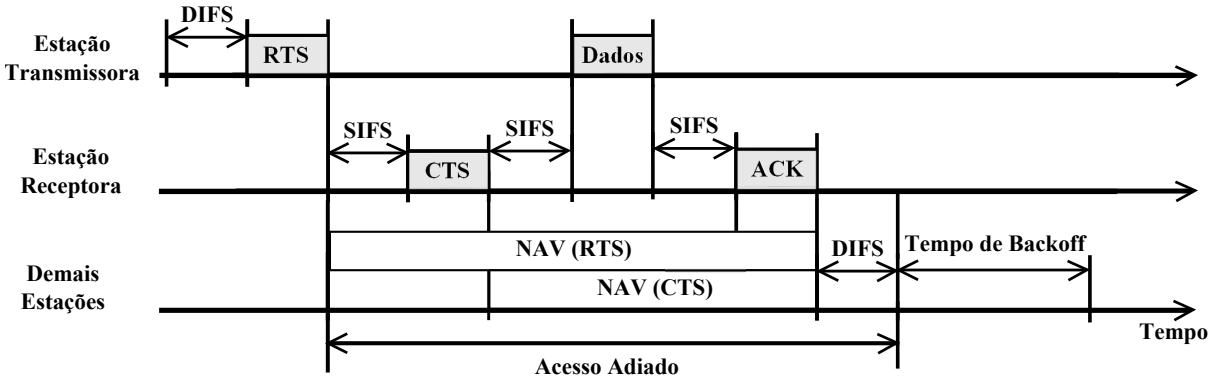


Figura 2.10 Mecanismo RTS/CTS [IEEE Standard 802.11 2012].

2.3.2 Point Coordination Function (PCF)

O padrão IEEE 802.11 também fornece um método de acesso ao meio opcional, denominado *Point Coordination Function* (PCF). Esse método de acesso utiliza um ponto coordenador ou *Point Coordinator* (PC), o qual determina qual estação atualmente tem o direito de transmitir. O PC deve operar no Ponto de Acesso (AP). O período de tempo durante a operação de uma PCF é chamado de *Contention-Free Period* (CFP),

cuja duração é controlada pelo Ponto de Acesso. O fim de um CFP deve ser informado pelo AP, através da transmissão de um quadro de controle CF-End ou CF-End+CF-ACK, como apresentado na Seção 2.1.4. Utilizando o Ponto de Acesso como nó central controlador, esse método evita a ocorrência de colisões entre as estações pertencentes à rede.

2.4 GERAÇÃO E DISTRIBUIÇÃO DE CHAVES NO PADRÃO IEEE 802.11

Uma vez que os dados transmitidos em uma rede sem fio trafegam em um meio que não é seguro, o padrão IEEE 802.11 fornece diversos protocolos de segurança que tem por objetivo evitar a captura indevida do tráfego de dados dessas redes. O objetivo desses protocolos é fornecer mecanismos de autenticação às estações legítimas e garantir a integridade e a confidencialidade dos dados que trafegam na camada de enlace. É durante a fase de autenticação de uma estação, que são definidas as chaves de segurança utilizadas na comunicação posterior. Nesta seção são apresentados as chaves de segurança utilizadas no padrão IEEE 802.11 e os principais processos utilizados na geração e na distribuição dessas chaves: o *4-Way Handshake* e o *Group Key Handshake*.

2.4.1 4-Way Handshake

O principal mecanismo da etapa de autenticação é o processo de *4-Way Handshake* entre a estação e o ponto de acesso. Nesse processo, apresentado na Figura 2.11, a estação e o ponto de acesso se autenticam mutuamente e derivam uma chave PTK (*Pairwise Transient Key*) comum e exclusiva a eles. A PTK é utilizada, entre outras coisas, no processo de encriptação dos quadros de dados enviados em *unicast*.

Durante o *4-Way Handshake*, o ponto de acesso também envia à estação, em texto cifrado, as chaves GTK (*Group Temporal Key*) e $IGTK$ (*Integrity Group Temporal Key*). Essas chaves são encriptadas com a KEK (*Key Encryption Key*), que faz parte da PTK. Com relação a $IGTK$, que fornece segurança aos quadros de gerenciamento da rede, esta só é enviada quando a emenda IEEE 802.11w [IEEE Standard 802.11w 2009] está sendo

utilizada. Tanto a GTK quanto a $IGTK$ são compartilhadas por todas as estações da rede. A GTK é empregada no processo de encriptação dos quadros de dados enviados em *broadcast* e *multicast* e a $IGTK$ é utilizada para fornecer integridade aos quadros de gerenciamento.

Com relação as mensagens trocadas durante o *4-Way Handshake*, as duas primeiras são utilizadas para que o ponto de acesso e a estação derivem a PTK. A terceira mensagem é utilizada pelo ponto de acesso para enviar as chaves GTK e $IGTK$ à estação. Por fim, a estação comunica ao ponto de acesso, através da quarta mensagem, que a autenticação foi realizada com sucesso.

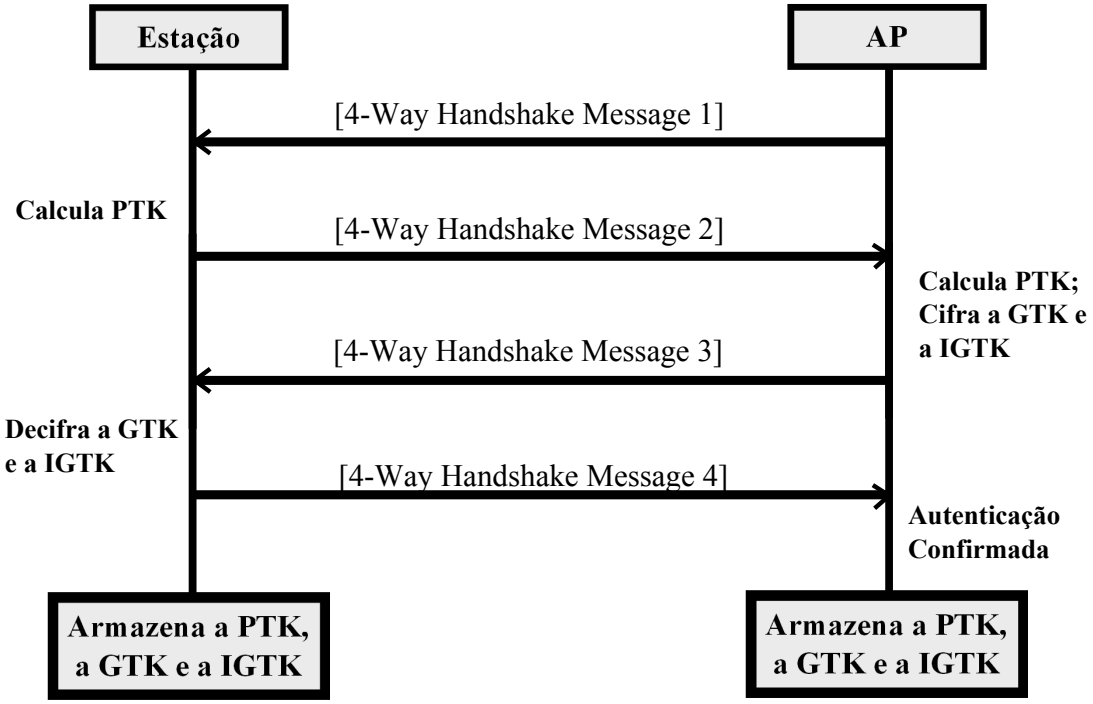


Figura 2.11 4-Way Handshake [IEEE Standard 802.11 2012].

2.4.2 Group Key Handshake

Além do *4-Way Handshake*, o padrão IEEE 802.11 especifica o *Group Key Handshake*, apresentado na Figura 2.12. Esse último é um processo utilizado na distribuição das chaves GTK e $IGTK$. Quando um cliente sai da rede o ponto de acesso precisa distribuir

novas chaves GTK e $IGTK$ às demais estações que permaneceram na rede. Com o objetivo de distribuir essas chaves sem a necessidade de reautenticar todas as estações, o ponto de acesso utiliza o processo *Group Key Handshake*. Desta forma, as estações que deixaram a rede não terão mais acesso as mensagens enviadas em *broadcast* ou *multicast*. A primeira mensagem do *Group Key Handshake* é utilizada para enviar, em texto cifrado, a GTK e a $IGTK$ à estação. A segunda mensagem é utilizada pela estação para confirmar o *handshake*.

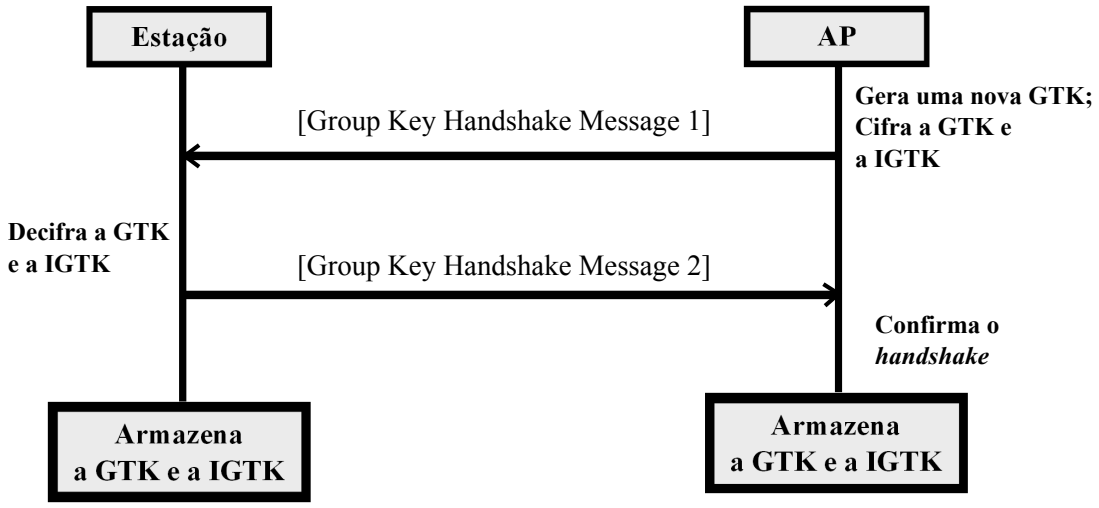


Figura 2.12 Group Key Handshake [IEEE Standard 802.11 2012].

2.5 CMAC

O CMAC (*Cipher-based MAC*) [Dworkin 2005] [Barker e Roginsky 2011] [Barker et al. 2012] é um Código de Autenticação de Mensagem (*Message Authentication Code* - MAC) baseado em cifras de bloco, tais como o AES. Códigos de Autenticação de Mensagem são utilizados para garantir a integridade e a autenticidade das mensagens trocadas, no sentido de que cada parte comunicante deve ser hábil a identificar quando uma mensagem recebida foi exatamente a mensagem enviada pela outra parte. Isto só é possível se as partes comunicantes possuírem alguma chave secreta compartilhada que o atacante não conhece.

No CMAC uma chave secreta compartilhada, K, deve ser utizada para garantir a

segurança do mecanismo. Essa chave deve ser gerada uniformemente de forma aleatória, ser secreta e usada exclusivamente no CMAC. O CMAC recebe como entrada uma mensagem M de comprimento $Mlen$ (em bits). Ao contrário do CBC-MAC, que só pode ser empregado com segurança quando o comprimento das mensagens sendo autenticadas é fixo, não há qualquer restrição com relação ao comprimento das mensagens autenticadas pelo CMAC. O Código de Autenticação de Mensagem (MAC) gerado pelo CMAC é denotado por T, cujo comprimento é $Tlen$ (em bits).

2.5.1 Geração de Subchaves

O processo de geração do MAC T envolve a utilização de duas subchaves, $K1$ e $K2$, derivadas a partir da chave secreta compartilhada K. O comprimento de cada subchave é o tamanho do bloco da cifra de bloco utilizada, denotado por b. Desta forma, se o AES é utilizado como cifra de bloco, cada subchave deve possuir 128 bits de comprimento. As subchaves são fixas para qualquer invocação do CMAC com uma mesma chave K. Logo, as subchaves podem ser pré-computadas e armazenadas com a chave K, enquanto esta última ainda estiver em uso.

Um dos elementos utilizados no processo de geração das subchaves é uma cadeia de bits denotada por R_b, onde b é o comprimento (em bits) de um bloco. R_b é uma representação de um polinômio binário irredutível de grau b, isto é, o primeiro lexograficamente entre todos os polinômios com o menor número possível de termos não zero. Se este polinômio é expresso como $u^b + c_{b-1}u^{b-1} + ... + c_2u^2 + c_1u + c_0$, onde os coeficientes $c_{b-1}, c_{b-2}, ..., c_2, c_1, c_0$ são ou 0 ou 1, então R_b é a cadeia de bits $c_{b-1}c_{b-2}...c_2c_1c_0$. No caso do AES, $R_{128} = 0^{120}10000111$ [Dworkin 2005].

O Algoritmo 2.5.1 apresenta o pseudocódigo da geração das subchaves $K1$ e $K2$. Na linha 2, a cifra de bloco é aplicada a um bloco que consiste unicamente de bits '0'. Na linha 6, a primeira subchave é derivada da cadeia resultante por aplicar um deslocamento a esquerda de um bit e, condicionalmente na linha 8, por aplicar o XOR a constante R_{128}. Na linha 10, a segunda subchave é derivada de maneira semelhante a primeira.

Algoritmo 2.5.1 Geração das subchaves $K1$ e $K2$

1: **procedure** SUBK(K)
2: $L = AES_k(0^{128})$
3:
4: // $MSB_s(L)$ retorna uma cadeia dos s bits mais a esquerda da cadeia de bits L
5: **if** $MSB_1(L) = 0$ **then**
6: $K1 = L << 1$;
7: **else**
8: $K1 = (L << 1) \oplus R_{128}$;
9: **end if**
10: **if** $MSB_1(K1) = 0$ **then**
11: $K2 = K1 << 1$;
12: **else**
13: $K2 = (K1 << 1) \oplus R_{128}$;
14: **end if**
15: **return** $K1$ e $K2$;
16: **end procedure**

2.5.2 Geração e Verificação do MAC

O processo de autenticação de mensagens do CMAC é composto por duas etapas: a Geração e a Verificação do MAC. O Algoritmo 2.5.2 apresenta a etapa de Geração do MAC, onde K é a chave secreta compartilhada, M é a mensagem que está sendo autenticada e $Tlen$ é o comprimento do MAC. A mensagem M é formatada em uma sequência de n blocos (*linha 8*). Os blocos $M_1, M_2, ..., M_{n-1}$ possuem o mesmo comprimento do bloco da cifra de bloco utilizada (b bits). O último bloco da cadeia (M_n^*) deve ser mascarado com uma das subchaves empregadas no mecanismo (*linhas 10 a 14*). Há duas situações possíveis:

- Se o comprimento da mensagem (M) é um múltiplo do comprimento do bloco da cifra de bloco utilizada (b bits), então todos os blocos da mensagem terão um com-

Algoritmo 2.5.2 Geração do MAC

1: **procedure** CMAC(K,M,$Tlen$)
2: **if** $Mlen = 0$ **then**
3: $n = 1$; // n indica a quantidade de blocos em que a mensagem M será quebrada
4: **else**
5: $n = \lceil Mlen/b \rceil$; // b é o comprimento, em bits, de um bloco do AES
6: **end if**
7:
8: $M = M_1||M_2||...||M_{n-1}||M_n^*$; // $M_1, M_2, ..., M_{n-1}, M_n^*$ é uma sequência de cadeias de bits, onde $M_1, M_2, ..., M_{n-1}$ são blocos de comprimento b.
9:
10: **if** M_n^* é um bloco de comprimento b **then**
11: $M_n = K1 \oplus M_n^*$;
12: **else**
13: $M_n = K2 \oplus (M_n^*||10^j)$ // onde $j = nb - Mlen - 1$;
14: **end if**
15:
16: $C_0 = 0^b$;
17: **for** $i = 1$ *to* n **do**
$C_i = AES_K(C_{i-1} \oplus M_i)$;
18: **end for**
19:
20: $T = MSB_{Tlen}(C_n)$;
21: **return** T;
22: **end procedure**

primento b (em bits). Neste caso, o bloco final (M_n^*) é mascarado com a subchave $K1$ (*linha 11*).

- Se o comprimento da mensagem (M) não é um múltiplo do comprimento do bloco

da cifra de bloco utilizada (b bits), então o comprimento do bloco final (M_n^*) é menor que b. Desta forma, um *padding* composto por um único bit '1' seguido de bits '0' é adicionado ao bloco M_n^*, de forma que o comprimento do bloco resultante seja igual a b. O bloco final ($M_n^*||10^j$) é mascarado com a subchave $K2$ (*linha 13*).

Depois que o último bloco da mensagem é mascarado com uma das subchaves, a técnica CBC (*Cipher block Chaining*) é aplicada a mensagem formatada (*linhas 16 a 18*). A saída final do CBC é truncada de acordo com o comprimento do MAC ($Tlen$) (*linha 20*). Os dois casos de geração do MAC são apresentados na Figura 2.13.

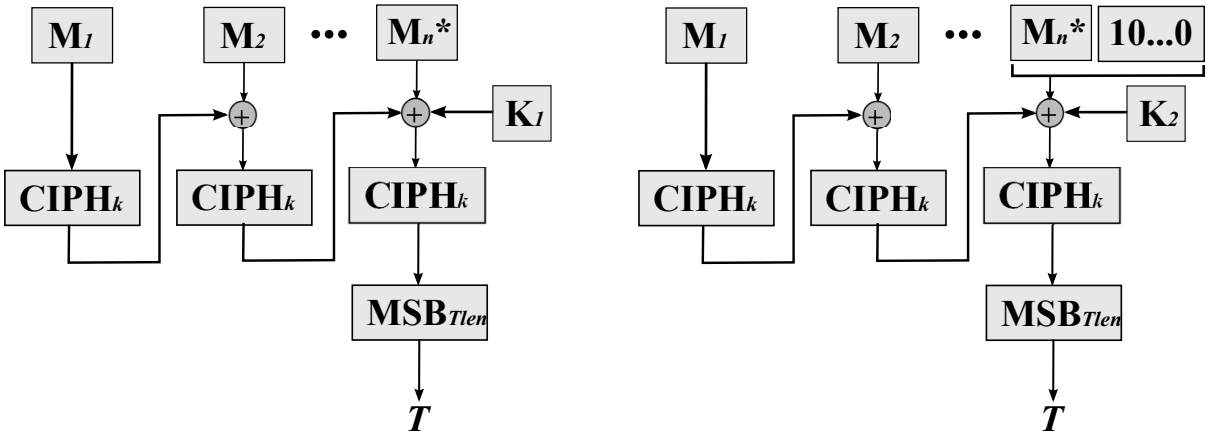


Figura 2.13 Os dois casos de Geração do MAC [Dworkin 2005].

Uma entidade, ao receber uma mensagem contento o MAC T, pode verificar a autenticidade e a integridade da mesma acionando o algoritmo de Verificação do MAC. O Algoritmo 2.5.3 apresenta a etapa de Verificação, onde K é a chave secreta compartilhada, M é a mensagem que está sendo autenticada e T é o Código de Autenticação de Mensagem (MAC) presente na mensagem recebida. O algoritmo de Geração do MAC é aplicado à mensagem M (*linha 2*), e o MAC resultante (T') é comparado com o MAC recebido (T) pela entidade (*linha 3*). Se o retorno da função $VER(K, M, T)$ é o valor "VÁLIDA"a mensagem recebida é aceita como sendo íntegra e autêntica. Caso contrário, essa não corresponde a mensagem originalmente enviada pela entidade transmissora.

Algoritmo 2.5.3 Verificação do MAC

```
1: procedure VER(K,M,T)
2:     T' = CMAC(K, M, Tlen);
3:     if T = T' then
4:         return VÁLIDA;
5:     else
6:         return INVÁLIDA;
7:     end if
8: end procedure
```

2.6 RESUMO

Neste capítulo foram apresentados os quadros de controle, suas funções e os principais tipos de ataques a que estão sujeitos. Além disso, foram apresentados os protocolos de acesso ao meio de comunicação (*Distributed Coordination Function* e *Point Coordination Function*) e os principais processos de geração e distribuição de chaves (*4-Way Handshake* e *Group Key Handshake*) definidos no padrão IEEE 802.11.

Por fim, foram apresentadas as etapas de Geração e Verificação do MAC definidas no CMAC. O CMAC permite que uma entidade receptora autentique as mensagens recebidas de outra entidade. Esse processo é utilizado para garantir que a mensagem recebida não foi alterada ou adulterada durante a transmissão.

CAPÍTULO 3

TRABALHOS RELACIONADOS

Dentre os trabalhos relacionados que buscam proteger os quadros de controle das redes IEEE 802.11, dois focos de pesquisa foram identificados. Existem trabalhos que fornecem soluções pontuais para se detectar e evitar ataques específicos realizados contra determinados tipos de quadros de controle [Bellardo e Savage 2003, Chen, Ding e Varshney 2003, Ray e Starobinski 2007, Qureshi et al. 2007, Zhang et al. 2008, Rachedi e Benslimane 2009] e trabalhos que propõem soluções para conter os ataques de negação de serviço contra todos os tipos de quadros de controle [Khan e Hasan 2008, Myneni e Huang 2010, Jr. e Gonçalves 2011, Malekzadeh, Ghani e Subramaniam 2012]. Neste capítulo são apresentados os trabalhos pertencentes ao segundo grupo, uma vez que estes fornecem esquemas de segurança para todos os quadros de controle e mantêm um foco de pesquisa semelhante ao proposto neste trabalho.

3.1 KHAN E HASAN

A primeira tentativa de proteger todos os quadros de controle contra ataques de *DoS* foi proposta em [Khan e Hasan 2008]. O esquema fornece uma solução criptográfica baseada no uso de números pseudoaleatórios (*Pseudo Random Number* - PRN). O campo FCS (*Frame Check Sequence*), presente nos quadros IEEE 802.11 e empregado para verificação de integridade, é utilizado para transmitir os 16 bits utilizados pelo esquema na autenticação dos quadros de controle. Dessa forma, o comprimento dos quadros de controle não é alterado. A chave criptográfica utilizada na autenticação é a PTK (*Pairwise Transient Key*), empregada no IEEE 802.11i [IEEE Standard 802.11i 2004] para criptografia

de quadros de dados enviados em *unicast*.

Esse esquema fornece proteção para todos os quadros de controle e mantem o tamanho original dos quadros. No entanto, o uso de apenas 16 bits para prover a autenticação dos quadros torna frágil a proteção oferecida. Além disso, ataques de reinjeção não são tratados pela proposta.

3.2 MYNENI E HUANG

O esquema proposto em [Myneni e Huang 2010] faz uso do HMAC-SHA-1 para proteger todos os quadros de controle do padrão IEEE 802.11. O esquema adiciona 160 bits de Código de Autenticação de Mensagem ou MAC em cada quadro de controle. A chave utilizada na geração do MAC é distribuída e gerenciada pelo *framework* IAPP *(Inter-Access Point Protocol)*. Além disso, o campo FCS (*Frame Check Sequence*) dos quadros é removido da proposta dado que o MAC também pode ser utilizado para verificação de integridade. Um número de sequência global de 32 bits, atualizado pelas estações a cada N microssegundos, é utilizado a fim de conter ataques de reinjeção.

Um dos problemas relacionados a este esquema é o uso do algoritmo HMAC-SHA1, que vem sendo questionado do ponto de vista de segurança devido às fragilidades encontradas no *hash* criptográfico. De acordo com alguns trabalhos, ataques de colisão nas funções *hash* subjacentes podem ser usados para enfraquecer a segurança do HMAC [Contini e Yin 2006, Kim et al. 2006, Rechberger e Rijmen 2008]. Além disso, a proposta adiciona 160 bits ao tamanho dos quadros de controle, o que representa um *overhead* considerável, principalmente para quadros de controle como o ACK e o CTS que possuem apenas 112 bits de comprimento.

3.3 JR. E GONÇALVES

O esquema proposto em [Jr. e Gonçalves 2011] busca proteger os quadros de controle do padrão IEEE 802.11 através do uso de um Código de Autenticação de Mensagem de 64 bits e de um número de sequência global de 32 bits. A geração do código de autenticação

é feita utilizando-se o CBC-MAC (*Cipher Block Chaining-Message Authentication Code*). A chave utilizada no processo de autenticação é chave criptográfica *GTK* (*Group Temporal Key*), a qual já é empregada pelo protocolo de segurança IEEE 802.11i no processo de encriptação de quadros de dados enviados em *broadcast* e *multicast*. O campo FCS também é removido da proposta sem prejuízo para a verificação de erro, uma vez que o Código de Autenticação de Mensagem também garante a integridade do quadro. O aumento de 64 bits no tamanho do quadro de controle resulta em um *overhead* significativamente menor do que aquele observado nos esquemas propostos em [Myneni e Huang 2010] e [Malekzadeh, Ghani e Subramaniam 2012].

Apesar de apresentar um baixo *overhead* e utilizar diversos esquemas de segurança já disponíveis nos hardwares atuais, o esquema proposto em [Jr. e Gonçalves 2011] apresenta algumas fraquezas relacionadas à segurança. Um dos problemas está relacionado ao uso do CBC-MAC. O CBC-MAC básico é seguro apenas quando o comprimento das mensagens sendo autenticadas é fixo. Se o objetivo é autenticar mensagens de comprimento variado, como no caso dos quadros de controle, o uso do CBC-MAC básico é suscetível a ataques de forjação bastante simples [Menezes, Oorschot e Vanstone 1996].

O esquema também utiliza o endereço do nó transmissor (*Transmitter Address* - TA), contido no cabeçalho MAC do quadro de controle, para calcular o Código de Autenticação de Mensagem correspondente. Como apresentado na Seção 2.1, os quadros de controle ACK e CTS não possuem o endereço do nó transmissor em seu cabeçalho MAC. Desta forma, a integridade e autenticidade dos quadros de controle CTS e ACK não podem ser verificadas por todos os nós da rede que utilizam esse esquema.

3.4 MALEKZADEH, GHANI E SUBRAMANIAM

Dois esquemas de proteção para os quadros de controle IEEE 802.11 são propostos em [Malekzadeh, Ghani e Subramaniam 2012]. O primeiro, denominado *O-hmac2*, utiliza o algoritmo original HMAC-SHA-256 para geração do MAC e adiciona 256 bits de autenticação em cada quadro de controle. Já o segundo, o *M-hmac2*, gera o MAC a partir de um HMAC-SHA-256 modificado e adiciona 128 bits de autenticação. O campo FCS

dos quadros de controle é mantido e um campo *timestamp* de 32 bits é adicionado para conter ataques de reinjeção. O *overhead* adicionado por ambas as propostas é expressivo. O *O-hmac2* adiciona 288 bits ao tamanho do quadro de controle e o *M-hmac2* adiciona 160 bits.

3.5 FRAQUEZAS ASSOCIADAS À GERAÇÃO E À DISTRIBUIÇÃO DA CHAVE DE AUTENTICAÇÃO

Uma das principais fraquezas identificadas em todos os trabalhos relacionados está associada à geração e à distribuição da chave utilizada no processo de autenticação. Os esquemas propostos em [Khan e Hasan 2008] e [Jr. e Gonçalves 2011] fazem uso, respectivamente, das chaves criptográficas PTK e GTK já empregadas no IEEE 802.11i. Essas chaves, além de serem utilizadas no processo de encriptação dos quadros de dados das redes IEEE 802.11, passam a ser utilizadas também no processo de autenticação dos quadros de controle. O uso de uma mesma chave para dois processos criptográficos diferentes pode enfraquecer a segurança proporcionada por um ou ambos os processos e deve ser evitado [Katz e Lindell 2007]. Logo, limitar o uso de uma chave diferente por processo reduz os danos provocados em função da descoberta da chave [Barker et al. 2012].

Em [Myneni e Huang 2010], o uso do *framework* IAPP para a geração e a distribuição da chave de autenticação adiciona um *overhead* significativo em função do número de APs e estações conectadas, uma vez que uma nova chave deve ser gerada e distribuída sempre que uma estação se conecta ao AP ou se desconecta dele. Além disso, esse *framework* não é mais usado pelo padrão IEEE 802.11. Já o esquema proposto em [Malekzadeh, Ghani e Subramaniam 2012] considera a existência de uma chave pré-compartilhada e não aborda o processo de geração e distribuição dessa chave.

3.6 FRAQUEZAS ASSOCIADAS À PROTEÇÃO CONTRA OS ATAQUES DE REINJEÇÃO

Outra fraqueza apresentada pelos trabalhos relacionados está associada ao mecanismo de proteção contra os ataques de reinjeção. Nenhum mecanismo para contenção desse tipo de ataque é proposto em [Khan e Hasan 2008]. Logo esse esquema é vulnerável a ataques de reinjeção. Os esquemas propostos em [Myneni e Huang 2010] e [Jr. e Gonçalves 2011] empregam um número de sequência global. Em [Myneni e Huang 2010], esse número deve ser atualizado pelas estações em intervalos de tempo definidos. Se esse intervalo de tempo for muito grande, uma estação maliciosa pode realizar ataques de reinjeção. Já em [Jr. e Gonçalves 2011] o número de sequência é atualizado a cada quadro de controle transmitido. Essa última abordagem exige que cada nó da rede esteja ao alcance dos demais nós, pois se dois nós em uma rede não se ouvem, o número de sequência armazenado por cada nó pode ser inconsistente. Além disso, para que o emprego de um número de sequência global funcione adequadamente em ambos os esquemas, é necessário que todas as estações da rede estejam sincronizadas.

Em [Malekzadeh, Ghani e Subramaniam 2012] é proposto o uso de *timestamp*. A segurança de uma mecanismo baseado em *timestamp* se baseia no uso de um tempo de referência comum. Portanto, a sincronização das estações também é necessária. Quando um nó receptor recebe um quadro, este deve checar se o *timestamp* incluído está dentro de uma janela aceitável do tempo atual. Além da necessidade de sincronização das estações, ataques de reinjeção ainda podem ser possíveis, desde que o ataque seja realizado de forma suficientemente rápida, dentro da janela de tempo definida [Katz e Lindell 2007] [Menezes, Oorschot e Vanstone 1996].

3.7 RESUMO

Neste Capítulo foram apresentados os trabalhos relacionados que propõem soluções para conter os ataques de negação de serviço contra todos os tipos de quadros de controle [Khan e Hasan 2008, Myneni e Huang 2010, Jr. e Gonçalves 2011,

Malekzadeh, Ghani e Subramaniam 2012]. A Tabela 3.1 resume as principais características de cada trabalho apresentado.

Tabela 3.1 Resumo dos Trabalhos Relacionados.

	Overhead	**Ataques de Replicação**	**Autenticação**	**Gerenciamento de Chaves**
(Khan e Hasan 2008)	0 bits	Não evita	*Pseudo Random Number* (16 bits)	Utiliza a PTK
(Myneni e Huang 2010)	160 bits	Número de Sequência Global	HMAC-SHA1	*Framework* IAPP
(Jr. e Gonçalves 2011)	64 bits	Número de Sequência Global	CBC-MAC	Utiliza a GTK
M-hmac2 **(Malekzadeh, Ghani e Subramaniam 2012)**	160 bits	*Timestamp*	HMAC-SHA-256 modificado	Chave pré-compartilhada
O-hmac2 **(Malekzadeh, Ghani e Subramaniam 2012)**	288 bits	*Timestamp*	HMAC-SHA256	Chave pré-compartilhada

CAPÍTULO 4

ESQUEMA DE PROTEÇÃO PROPOSTO

Este trabalho propõe um esquema de proteção para todos os tipos de quadros de controle definidos no padrão IEEE 802.11 contra ataques de forjação, manipulação e reinjeção. Os ataques considerados são os provenientes de entidades maliciosas não pertencentes à rede. Todos os quadros de controle do esquema proposto possuem dois novos campos em relação ao formato original: o campo MAC de 64 bits e o campo NS (Número de Sequência) de 32 bits. O campo MAC permite que os nós receptores possam verificar a autenticidade e a integridade dos quadros de controle recebidos. Assim sendo, o campo FCS (*Frame Check Sequence*) de 32 bits é removido dos quadros de controle sem qualquer prejuízo. O campo NS é utilizado para garantir que os nós sejam capazes de detectar ataques de reinjeção. A Figura 4.1 confronta a versão original definida pelo padrão IEEE 802.11 e a versão segura dos quadros de controle.

(a) Versão original. (b) Versão segura da proposta.

Figura 4.1 Formato dos quadros de controle.

O esquema proposto consiste em três módulos que em conjunto garantem a proteção dos quadros de controle. O primeiro é o módulo de *Geração e Distribuição de Chaves*, que define a chave que será utilizada no processo de autenticação dos quadros de controle. Este módulo se ajusta aos processos de distribuição de chaves presentes no IEEE 802.11. O segundo módulo é o módulo de *Prevenção contra Ataques de Reinjeção*, que define um mecanismo de proteção contra ataques de reinjeção, baseado no uso de números de sequência individuais. Por fim, o terceiro é o módulo de *Geração e Verificação do MAC*,

que inclui o algoritmo de computação do MAC e define os procedimentos necessários para o envio e a recepção de um quadro de controle.

A Figura 4.2 apresenta o fluxograma com os passos realizados durante a construção da versão segura de um quadro de controle antes do seu envio na rede. O módulo de *Prevenção contra Ataques de Reinjeção*, que gerencia os números de sequência do nó, informa qual número de sequência deve ser utilizado no campo NS do quadro do controle. O módulo de *Geração do MAC* computa o MAC (Message Authentication Code), que é utilizado para garantir a autenticidade e a integridade do quadro de controle enviado. O módulo de *Geração do MAC* calcula o MAC a partir: (1) do *Cabeçalho MAC* do quadro de controle; (2) do número de sequência gerado a partir do módulo de *Prevenção contra Ataques de Reinjeção*; (3) e da chave de segurança (ATK), gerenciada pelo módulo de *Geração e Distribuição de Chaves*. A versão segura do quadro de controle é formada pela concatenação do *Cabeçalho MAC* com os campos NS e MAC.

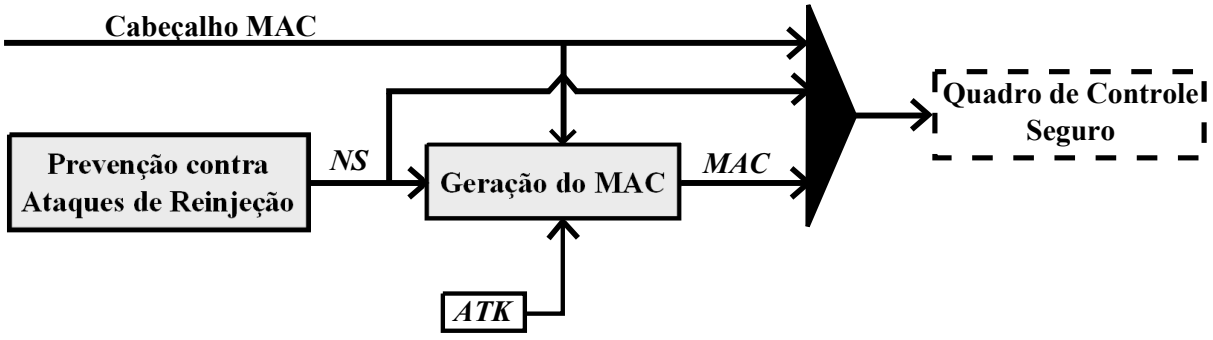


Figura 4.2 Envio de um quadro de controle.

A Figura 4.3 apresenta o fluxograma com os passos realizados durante o recebimento de um quadro de controle. Esse mecanismo verifica se o quadro de controle recebido é um quadro legítimo, ou seja, autêntico e que não se trata de uma reinjeção. O módulo de *Prevenção contra Ataques de Reinjeção* utiliza o conteúdo do campo NS para verficar se o quadro é uma reinjeção. Se o quadro é uma replicação este deve ser descartado. Caso contrário, o módulo de *Verificação do MAC* é acionado a fim de verificar a autenticidade e a integridade do quadro de controle. O módulo de *Verificação do MAC* recebe como entrada o quadro de controle e a chave de segurança (ATK). Se o quadro não é autêntico

este deve ser descartado. Caso contrário, este é considerado um quadro legítimo.

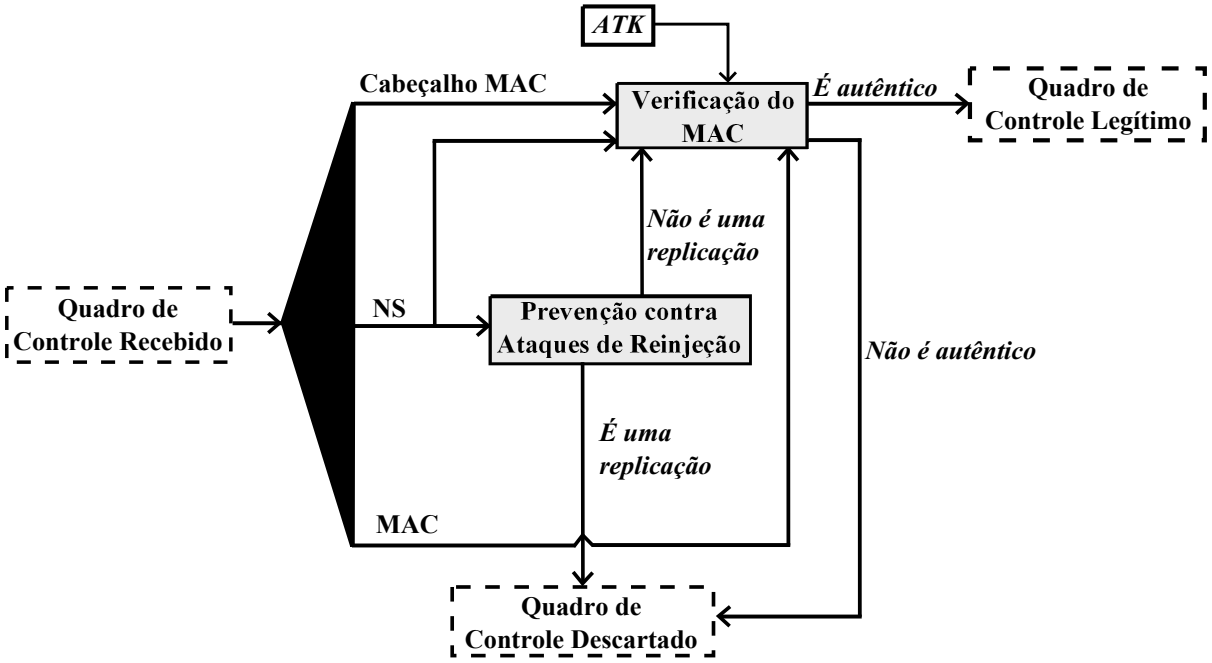


Figura 4.3 Recebimento de um quadro de controle.

Em particular aos quadros de controle ACK e CTS, os quais não possuem o endereço do nó transmissor em seu *Cabeçalho MAC*, um campo TA (*Transmitter Address*) de 6 bytes é adicionado em seu cabeçalho, uma vez que a informação de que nó transmitiu determinado quadro de controle é necessária no módulo de *Prevenção contra Ataques de Reinjeção*, apresentado na Seção 4.2. Além disso, nenhum mecanismo adicional de geração e distribuição de chaves do que o já existente no padrão IEEE 802.11 se faz necessário como é explicado na Seção 4.1.

As Seções 4.1, 4.2 e 4.3 deste capítulo apresentam os três módulos que compõem o esquema de segurança proposto, assim como a integração entre eles. Na Seção 4.4 é realizada uma análise da segurança do esquema de proteção.

4.1 MÓDULO DE GERAÇÃO E DISTRIBUIÇÃO DE CHAVES

O módulo de *Geração e Distribuição de Chaves* se ajusta à infraestrutura de geração e distribuição de chaves presente no padrão IEEE 802.11i. O padrão IEEE 802.11i define

dois processos de geração e distribuição de chaves, o *4-Way Handshake* e o *Group Key Handshake*.

O objetivo do *4-Way Handshake* é autenticar mutuamente a estação e o ponto de acesso. Durante o *4-Way Handshake*, a estação e o ponto de acesso derivam a PTK (*Pairwise Transient Key*), que é utilizada na encriptação dos quadros de dados enviados em *unicast*. O AP também envia as chaves GTK (*Group Temporal Key*) e $IGTK$ (*Integrity Group Temporal Key*) à estação. A GTK é empregada no processo de encriptação dos quadros de dados *broadcast* e *multicast*. A $IGTK$ é utilizada para fornecer integridade aos quadros de gerenciamento. Já o *Group Key Handshake* é invocado sempre que uma estação deixa a rede, tal que novas chaves GTK e $IGTK$ sejam distribuídas a todas as estações que permaneceram na rede, sem a necessidade de reautentica-las.

O módulo de *Geração e Distribuição de Chaves* da proposta define uma nova hierarquia de chaves, além das já definidas pelo RSNA (*Robust Security Network Association*) do IEEE 802.11i. Essa nova hierarquia, denominada *Authenticity Key Hierarchy*, consiste em uma única chave de 128 bits de comprimento (*Authenticity Temporal Key - ATK*). Esta chave é derivada pelo AP (*Access Point*) e distribuída a todas estações na rede. A ATK (*Authenticity Temporal Key*) é a chave utilizada no processo de autenticação dos quadros de controle e, portanto, deve ser secreta e gerada uniformemente de forma aleatória. A Figura 4.4 apresenta a *Authenticity Key Hierarchy*.

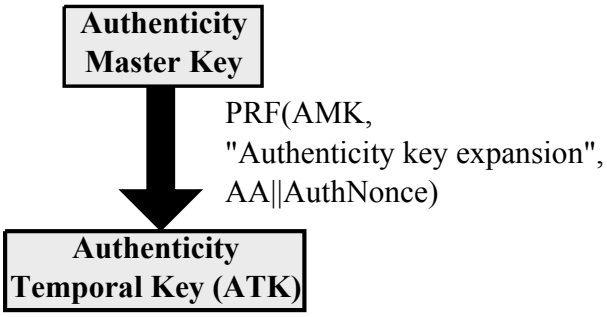


Figura 4.4 Authenticity Key Hierarchy.

Este módulo é divido em três etapas: *Geração da Chave*, *Distribuição da Chave* e *Renovação da Chave*. Cada uma das etapas é detalhada nas seções a seguir.

4.1.1 Etapa de Geração da Chave

A chave ATK é derivada pelo AP a partir de uma função pseudoaleatória (PRF), presente no IEEE 802.11i [IEEE Standard 802.11i 2004], de tal forma que:

$$ATK = PRF_{128}(AMK, \text{“}Authenticity\ key\ expansion\text{”}, AA \mid\mid AuthNonce), \quad (4.1)$$

onde AMK (*Authenticity Master Key*) é uma chave auxiliar que deve ser configurada no AP, *Authenticity key expansion* é uma *string* fixa, AA é o endereço MAC do AP e $AuthNonce$ é um número gerado aleatoriamente pelo AP, tendo o objetivo de garantir que a chave ATK é diferente a cada derivação. A técnica utilizada para configurar a AMK no AP está fora do escopo desse trabalho.

4.1.2 Etapa de Distribuição da Chave

No padrão IEEE 802.11i, quando uma nova estação se conecta ao AP, um *4-Way Handshake* é realizado entre a estação e o AP e ambos se autenticam mutuamente. Durante o *4-Way Handshake*, a estação e o AP derivam uma chave denominada PTK (*Pairwise Transient Key*), comum e exclusiva a eles. A PTK é utilizada para criptografia de quadros de dados enviados em *unicast*. Além da PTK, o AP também envia à estação a chave GTK (*Group Transient Key*), a qual é compartilhada por todas as estações da rede e empregada no processo de encriptação dos quadros de dados enviados em *broadcast* e *multicast*.

Além do envio das chaves PTK e GTK, também é necessário que a chave ATK seja enviada à estação através do *4-Way Handshake*. A Figura 4.5 apresenta o *Adapted 4-Way Handshake*. A ATK é enviada para a estação através da *4-Way Handshake Message 3*. A fim de garantir o sigilo da ATK, esta será encriptada com partes da PTK antes de ser enviada pelo AP à estação, de forma semelhante ao que ocorre com a GTK.

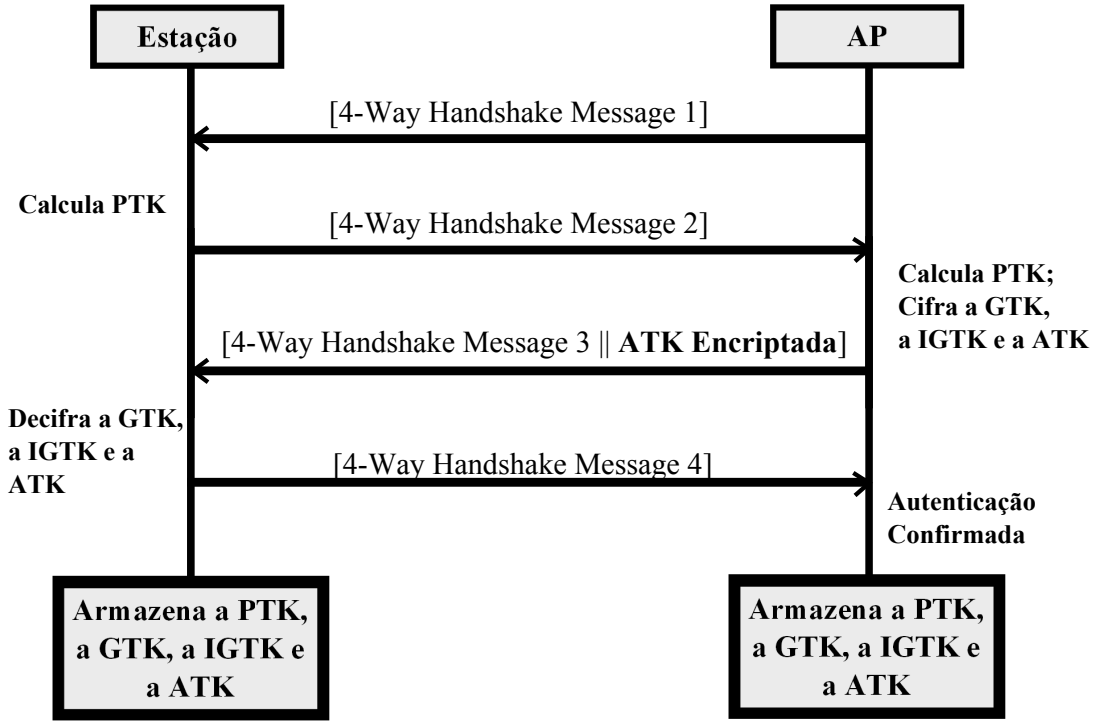


Figura 4.5 Adapted 4-Way Handshake.

4.1.3 Etapa de Renovação da Chave

Quando o AP necessita renovar a chave GTK (*Group Temporal Key*) e distribui-la a todas as estações da rede, este invoca o *Group Key Handshake* definido no padrão IEEE 802.11i. O *Group Key Handshake* é invocado sempre que uma estação sai da rede, a fim de que uma nova GTK seja distribuída para todas as estações da rede, sem a necessidade de reautenticá-las.

A fim de garantir que a ATK só é conhecida por estações pertencentes à rede, esse módulo se ajusta ao processo *Group Key Handshake*. Desta forma, a ATK também é renovada e distribuída às estações por meio desse processo. A Figura 4.6 apresenta o *Adapted Group Key Handshake*. A ATK é renovada e distribuída juntamente com a *Group Key Handshake Message 1*.

A fim de garantir o sigilo da ATK e a segurança do esquema de proteção proposto, tal chave também deve ser renovada e distribuída pelo AP às estações em outras duas situações. No primeiro caso, a ATK deve ser renovada a fim de evitar que determinado

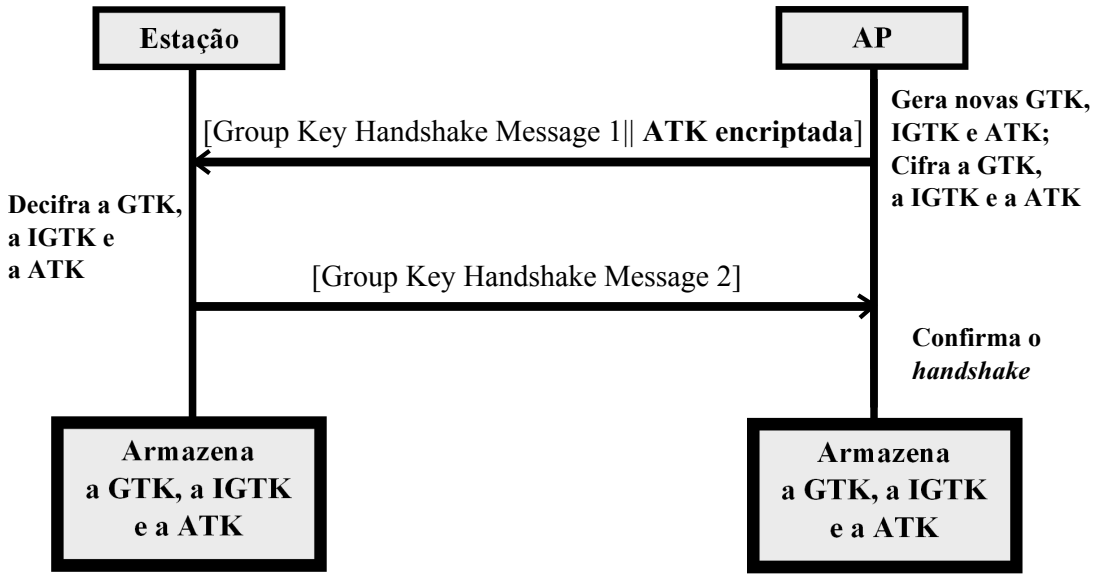


Figura 4.6 Adapted Group Key Handshake.

nó repita a utilização de determinado número de sequência com a mesma ATK. Tal procedimento, detalhado na Seção 4.2, evita de forma efetiva os ataques de reinjeção. Na segunda situação, a ATK é renovada para proteger o sistema contra ataques capazes de detectar e explorar colisões no MAC dos quadros de controle. Tais ataques são capazes de produzir MACs válidos para quadros falsos. Dessa forma, como apresentado na Seção 4.4, a ATK deve ser renovada quando o número de mensagens trocadas na rede com a mesma ATK ultrapassa um limiar de 2^{48} mensagens. Nas duas situações apresentadas, a ATK é renovada e distribuída por meio do *Group Key Handshake*, como apresentado na Figura 4.6.

O módulo apresentado nessa seção se ajusta aos protocolos de geração e distribuição de chaves do padrão IEEE 802.11i. A chave ATK, utilizada no processo de autenticação dos quadros de controle, é gerada, distribuída e renovada de forma segura através do módulo de *Geração e Distribuição de Chaves* dessa proposta. Desta forma, nenhuma infraestrutura adicional de geração e distribuição de chaves se faz necessária, além da já existente no padrão IEEE 802.11 [IEEE Standard 802.11 2012].

4.2 MÓDULO DE PREVENÇÃO CONTRA ATAQUES DE REINJEÇÃO

Em um canal sem fio, um atacante dentro do raio de alcance de um nó transmissor legítimo é capaz de capturar quadros de controle legítimos e retransmiti-los dentro da rede, causando resultados inesperados. Esse ataque é conhecido como ataque de reinjeção. A fim de evitar a ocorrência de tais ataques, o esquema de proteção proposto nesse trabalho introduz o módulo de *Prevenção contra Ataques de Reinjeção*.

Esse módulo utiliza números de sequência individuais de 32 bits de comprimento. Cada nó transmissor possui um contador de 32 bits, denominado TC (*Transmission Counter*), o qual é inicializado com o valor *1*. O campo NS do quadro de controle é preenchido com o valor armazenado nesse contador. O contador TC é incrementado de uma unidade cada vez que um quadro de controle é enviado pelo nó. A fim de garantir a segurança desse módulo, o número de sequência de qualquer que seja o nó nunca poderá ser repetido durante a utilização da mesma ATK. Desta forma, quando o valor do contador TC chega a *0*, a ATK deve ser renovada a partir de uma chamada ao processo *Adapted Group Key Handshake*, como apresentado na Figura 4.6. Além disso, quando a chave ATK é renovada, o contador TC de cada nó é reinicializado, passando a conter o valor *1* novamente.

Cada nó receptor deve manter um conjunto de N contadores de 32 bits. Cada contador, denominado RC (*Reception Counter*), é inicializado com o valor *0* e está associado a cada um dos N nós presentes na rede. Para cada quadro de controle recebido de um nó transmissor, o nó receptor compara o valor contido no campo NS do quadro de controle com o valor armazenado no contador RC associado ao nó transmissor. Se o valor contido no campo NS do quadro de controle é menor ou igual ao valor armazenado no contador RC, associado ao nó transmissor, então um ataque de reinjeção está sendo realizado e o quadro de controle deve ser descartado. No entanto, se o valor contido no campo NS é maior que o valor armazenado no contador RC, então o quadro de controle recebido não é uma reinjeção. Se for constatado que o quadro é realmente autêntico, então o contador RC associado ao nó transmissor é atualizado com o valor contido no campo NS do quadro de controle recebido. Além disso, toda vez que a chave ATK for renovada, o conjunto de

N contadores RC de cada nó é reinicializado, passando a conter o valor *0* novamente.

Algoritmo 4.2.1 Etapas de Geração, Distribuição e Renovação da Chave

```
1: procedure GeraçãodaChave
2:     ATK ← PRF_128(AMK, "Authenticity key expansion" || AA || AuthNonce)
3: end procedure
4:
5: // Esta função é utilizada para inicializar os contadores de uma estação em particular
6: procedure inicializarContadores
7:     TC ← 1
8:     for all nós na rede do
9:         RC[Nó Transmissor] ← 0
10:    end for
11: end procedure
12:
13: procedure DistribuiçãodaChave
14:    if Uma estação se conecta ao AP then
15:        call Adapted 4-Way Handshake // Invocado pelo AP
16:        call inicializarContadores // Invocado apenas pela estação
17:    end if
18: end procedure
19:
20: procedure RenovaçãodaChave
21:    if Uma estação se desconecta do AP or Transmission Counter (TC) é zero or
       Número de menssagens trocadas na rede > 2^48 then
22:        call Adapted Group Key Handshake // Invocado pelo AP
23:        call inicializarContadores // Invocado por todos os nós na rede
24:    end if
25: end procedure
```

O pseudocódigo com a integração do módulo de *Prevenção contra Ataques de*

Reinjeção com o módulo de *Geração e Distribuição de Chaves* é apresentado pelo Algoritmo 4.2.1. A ATK é gerada pelo AP a partir da etapa de *Geração da Chave* (*linha 2*). Quando determinada estação se conecta ao AP, a ATK é distribuída à estação por meio do *Adapted 4-Way Handshake* (*linha 15*) e os contadores TC (*Transmission Counter*) e RC (*Reception Counter*) da estação são inicializados (*linha 16*). Quando (1) uma estação se desconecta do AP; ou (2) o contador TC de determinada estação chega a 0; ou (3) o número de mensagens trocadas na rede com uma mesma ATK é maior que 2^{48} mensagens; então a ATK deve ser renovada pelo AP e distribuída às estações por meio do *Adapted Group Key Handshake* (*linha 22*) e os contadores TC e RC de todos os nós da rede devem ser reinicializados (*linha 23*).

A informação de qual nó está transmitindo é obtida a partir do campo TA (*Transmitter Address*), o qual está presente no cabeçalho MAC do quadro de controle. Todos os quadros de controle definidos no padrão IEEE 802.11, com exceção do ACK e do CTS, possuem o endereço do nó transmissor em seu cabeçalho MAC. Portanto, para que esse módulo funcione adequadamente, o campo TA é adicionado ao cabeçalho MAC dos quadros de controle ACK e CTS.

4.3 MÓDULO DE GERAÇÃO E VERIFICAÇÃO DO MAC

Esse módulo adota um mecanismo de autenticação dos quadros de controle a fim de evitar que atacantes sejam capazes de manipular e forjar quadros de controle legítimos. O algoritmo para computação do MAC (*Message Authentication Code*) adotado é o CMAC [Dworkin 2005] com o AES. O CMAC é um algoritmo de computação de MAC baseado em cifra de blocos. Trata-se de uma variação do CBC-MAC, que não incorre nas fraquezas deste último e que pode ser empregado com segurança na autenticação de mensagens de comprimento variado [Barker e Roginsky 2011] [Barker et al. 2012]. Além disso, o CMAC integra o padrão IEEE 802.11. A chave secreta utilizada na geração e na verificação do MAC é a chave ATK, a qual é derivada pelo AP, como apresentado na Seção 4.1. Esse módulo é composto por duas etapas: *Geração do MAC* e *Verificação do MAC*.

4.3.1 Geração do MAC

O pseudocódigo com os passos realizados durante o envio de um quadro de controle, de acordo com o esquema de proteção proposto, é apresentado no Algoritmo 4.3.1.

Algoritmo 4.3.1 Enviar quadros de controle

1: **procedure** ENVIARQUADRO(*CabeçalhoMAC*)
2: $NS \leftarrow TC$
3: $TC \leftarrow TC + 1$
4: $quadroControleSeguro \leftarrow CabeçalhoMAC||NS$
5: $MAC \leftarrow$ **call** CMAC(ATK, $quadroControleSeguro$, 64)
6: $quadroControleSeguro \leftarrow CabeçalhoMAC||NS||MAC$
7: **return** $quadroControleSeguro$
8: **end procedure**

Um nó transmissor ao enviar um quadro de controle, deve primeiro concatenar o cabeçalho MAC do quadro de controle com o número de sequência (NS) (*linha 4*), que corresponde ao valor armazenado em seu *Transmission Counter* (TC) (*linha 2*). Como apresentado na Seção 4.2, o contador TC deve ser incrementado a cada quadro de controle enviado (*linha 3*). Em seguida, o nó transmissor deve computar o MAC do quadro de controle, através do algoritmo CMAC (*linha 5*). O CMAC recebe os seguintes parâmetros: a chave secreta compartilhada (ATK); a versão segura dos quadros de controle (*quadroControleSeguro*), como apresentado na Figura 4.1 (b), com a exclusão do campo MAC; e o comprimento da saída final do CMAC ($Tlen$). A saída final do CMAC é truncada de modo que apenas os primeiros 64 bits ($Tlen$) são utilizados como código de autenticação no esquema proposto. A versão segura do quadro de controle é obtida pela concatenação do $CabeçalhoMAC$ com os campos NS e MAC (*linha 6*).

4.3.2 Verificação do MAC

O pseudocódigo com os passos realizados durante a verificação da autenticidade de um quadro de controle recebido é apresentado no Algoritmo 4.3.2.

Algoritmo 4.3.2 Receber quadros de controle

```
1:  // CabeçalhoMAC||NS||MAC é o formato de um quadro de controle na versão segura
2:  procedure receberQuadro(CabeçalhoMAC||NS||MAC)
3:      if NS do quadroControleSeguro ≤ RC[Nó Transmissor] then
4:          Descartar o quadro de controle recebido;  // O quadro de controle é uma
    reinjeção
5:      else
6:          statusVerificacão ← call VER(ATK, CabeçalhoMAC||NS||MAC)
7:          if statusVerificacão = "VÁLIDA" then
8:              RC[Nó Transmissor] ← NS;  // O quadro de controle é autêntico
9:          else
10:             Descartar o quadro de controle recebido;  // O quadro de controle não é
    autêntico
11:         end if
12:     end if
13:     return statusVerificacão
14: end procedure
```

Um nó, ao receber um quadro de controle e verificar que este quadro não está no formato da versão segura dos quadros de controle, deve descarta-lo. Se o quadro de controle está no formato da versão segura, o nó receptor invocará o módulo de *Prevenção contra Ataques de Reinjeção*, apresentado na Seção 4.2, para checar se o quadro é uma repetição (*linha 3*). Se o quadro é uma repetição este deve ser descartado (*linha 4*). Se o quadro não é uma repetição, o nó deve invocar o algoritmo de Verificação do MAC definido no CMAC (*linha 6*), a fim de validar a autenticidade e a integridade do quadro de controle recebido. O algoritmo de Verificação do MAC recebe os seguintes parâmetros: a chave secreta compartilhada (ATK) e a versão segura do quadro de controle recebido ($CabeçalhoMAC||NS||MAC$). Se a saída da função VER é o valor "VÁLIDA"(*linha 7*), então o quadro de controle é aceito como sendo autêntico e íntegro. Além disso, o contador RC do nó é atualizado com o valor do campo NS (*linha 8*). Se a saída da função VER

não é o valor "VÁLIDA"(*linha 9*), o quadro de controle não é considerado autêntico e deve ser descartado (*linha 10*).

4.4 ANÁLISE DE SEGURANÇA

A segurança da proposta se baseia na segurança dos mecanismos adotados em cada módulo e na forma como os mesmos são empregados em conjunto com o padrão IEEE 802.11. Com relação ao mecanismo de autenticação adotado, a escolha do AES-CMAC se baseia em critérios de eficiência e segurança.

Quanto à eficiência, o uso do CMAC com AES é mais apropriado que o uso de algoritmos que são baseados em funções *hash*, como o HMAC, por exemplo. Em sistemas que lidam com mensagens curtas de até 32 bytes [Denis e Johnson 2007], o CMAC é mais rápido e produz menor latência que o HMAC. Conforme apresentado em [Patel 2003], tal ineficiência do HMAC pode ser significativa na autenticação de mensagens que cabem dentro de um ou dois blocos do HMAC. O HMAC passa a ser mais eficiente que o CMAC quando lida com mensagens de maior comprimento. As versões seguras dos quadros de controle possuem um comprimento de no máximo 28 bytes, com exceção de algumas variantes dos quadros de controle BA e BAR e do quadro *Control Wrapper*, que possuem comprimento variável. Portanto, o uso do CMAC se mostra mais apropriado no requisito eficiência.

Com relação à segurança, alguns trabalhos sugerem que ataques de colisão nas funções *hash* subjacentes podem ser usados para enfraquecer a segurança do HMAC [Contini e Yin 2006, Kim et al. 2006, Rechberger e Rijmen 2008]. Exemplos de ataques de distinção, forjação e recuperação parcial ou completa de chaves no HMAC-SHA-1, são apresentados em [Rechberger e Rijmen 2008]. Esse ataque emprega um número reduzido de passos (até 62 dos 80 passos da SHA-1). Já a segurança proporcionada pelo AES-CMAC é construída sob a força do algoritmo criptográfico AES [Song et al. 2006] [Barker et al. 2012]. Uma análise mais profunda da segurança do CMAC pode ser encontrada em [Iwata e Kurosawa 2003].

Com relação ao comprimento do MAC, um atacante sem acesso à chave pode ser capaz

de adivinhar o MAC correto para uma mensagem com probabilidade de *1* em 2^{Tlen}, onde $Tlen$ é o comprimento do MAC. Para a maioria das aplicações, se $Tlen$ é menor que o comprimento da chave de autenticação e seu valor é de no mínimo 64 bits, a proteção oferecida é suficiente para fazer este ataque economicamente inviável [Tilborg e Jajodia 2011].

A segurança do sistema também é afetada por ataques que são baseados na detecção de pares de mensagens distintas que produzem o mesmo MAC antes de sua truncação. Tais pares representam colisões. Um atacante pode explorar uma colisão para produzir um MAC válido para uma nova mensagem. Para aplicações de propósito geral, a recomendação padrão é limitar o uso da chave para não mais do que 2^{48} mensagens quando o AES é utilizado [Dworkin 2005]. Este procedimento protege o sistema contra ataques de forjação do MAC. Portanto, como apresentado na Seção 4.1.3, o AP sempre renova a chave ATK quando o número total de mensagens trocadas na rede utilizando-se uma mesma chave ultrapassa esse limiar de 2^{48} mensagens. Esse limiar pode ser reduzido a fim de fornecer uma segurança maior para o sistema em questão, caso seja necessário.

Com relação à chave utilizada no CMAC, esta deve ser gerada uniformemente de forma aleatória, ser secreta e usada exclusivamente no CMAC [Dworkin 2005]. Como apresentado na Seção 4.1, a chave ATK é derivada de forma segura pelo AP, através de uma função pseudoaleatória, e é usada exclusivamente no CMAC. Com relação ao segredo da chave, o *4-Way Handshake* e o *Group Key Handshake* usam partes da PTK (*Pairwise Transient Key*) para proteger a ATK quando esta última é transmitida para as estações. Além disso, o comprimento da ATK é de 128 bits, o que é considerado seguro atualmente [Barker e Roginsky 2011] [Barker et al. 2012].

Códigos de autenticação de mensagem, de uma maneira geral, não oferecem proteção contra ataques de reinjeção, pois um quadro de controle legítimo e seu MAC podem ser capturados e retransmitidos dentro da rede. O uso de um esquema baseado em *timestamp*, como o apresentado em [Malekzadeh, Ghani e Subramaniam 2012], ou de um número de sequência global, como apresentado em [Myneni e Huang 2010] e [Jr. e Gonçalves 2011], foi descartado pela necessidade de manter todas as estações sincronizadas. Além disso, esses esquemas continuam vulneráveis a ataques de reinjeção, como apresentado no

Capítulo 3. Assim, o esquema proposto se vale de números de sequência individuais inseridos no campo NS (Número de Sequência) dos quadros de controle para conter os ataques de reinjeção. Esse esquema não necessita que as estações estejam sincronizadas, evitando de forma efetiva os ataques de reinjeção.

4.5 RESUMO

Neste capítulo foi apresentado o novo formato dos quadros de controle do esquema proposto. Os novos quadros possuem dois novos campos em relação ao formato original: o campo MAC de 64 bits e o campo NS (Número de Sequência) de 32 bits. Além disso, o campo FCS é removido dos quadros de controle. A remoção não tem prejuízo para a verificação de erro, uma vez que o Código de Autenticação de Mensagem também garante a integridade do quadro de controle.

Também foram apresentados os três módulos que compõem o esquema de proteção proposto: (1) *Geração e Distribuição de Chaves*, (2) *Prevenção contra Ataques de Reinjeção* e (3) *Geração e Verificação do MAC*. O Módulo de *Geração e Distribuição de Chaves* define a chave que será utilizada no processo de autenticação dos quadros de controle e se ajusta aos processos de distribuição de chaves presentes no padrão IEEE 802.11. O Módulo de *Prevenção contra Ataques de Reinjeção* define um mecanismo de proteção contra ataques de reinjeção, através do uso de números de sequência individuais. Por fim, o Módulo de *Geração e Verificação do MAC* define os procedimentos necessários para que o envio e a recepção de um quadro de controle sejam realizados com segurança. O capítulo apresentou ainda uma análise de segurança do esquema proposto.

CAPÍTULO 5

AVALIAÇÃO DE DESEMPENHO

Este capítulo avalia o impacto dos esquemas de segurança estudados na vazão da rede. A vazão máxima teórica (*Theoretical Maximum Throughput* - TMT) é definida pela seguinte equação [Xiao e Rosdahl 2002] [Jun, Peddabachagari e Sichitiu 2003]:

$$TMT \ = \ (\frac{8 \cdot L_{DATA}}{T}) \ \ (Mbps) \quad , \tag{5.1}$$

onde L_{DATA} é o comprimento do *payload* do quadro de dados (em *bytes*) e T é o tempo (em microssegundos) necessário para transmitir esse quadro.

O cálculo da vazão depende do método de controle de acesso ao meio (*Medium Access Control* - MAC), da taxa do canal e da técnica de espalhamento espectral adotada (e.g. FHSS, DSSS, HR/DSSS, ERP, OFDM). A Figura 5.1 apresenta o diagrama de tempo para o método CSMA/CA.

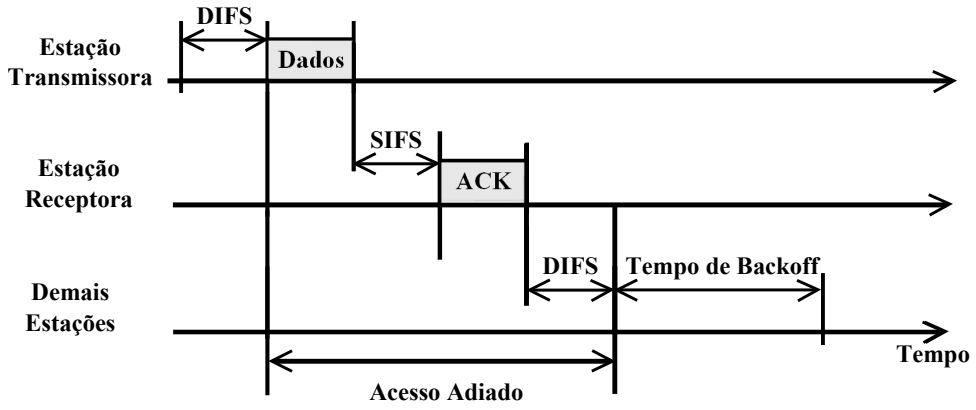


Figura 5.1 Diagrama de tempo para o CSMA/CA [IEEE Standard 802.11 2012].

Quando o método de controle de acesso CSMA/CA é utilizado:

$$T = T_{DADOS} + T_{SIFS} + T_{ACK} + T_{DIFS} + T_{CW} \quad (\mu s) \quad , \tag{5.2}$$

onde T_{DADOS} e T_{ACK} representam, respectivamente, o atraso de transmissão do quadro de dados e do ACK. T_{SIFS} e T_{DIFS} representam a duração de um SIFS (*Short Interframe Space*) e de um DIFS (*Distributed Coordination Function Interframe Space*), respectivamente. O tempo médio de *backoff* é representado por T_{CW}.

A Figura 5.2 apresenta o diagrama de tempo para o método RTS/CTS. Quando o método de controle de acesso ao meio RTS/CTS é utilizado:

$$T = T_{RTS} + 3T_{SIFS} + T_{CTS} + T_{DATA} + T_{ACK} + T_{DIFS} + T_{CW} \quad (\mu s) \quad , \tag{5.3}$$

onde T_{RTS} e T_{CTS} representam, respectivamente, o atraso de transmissão do RTS e do CTS.

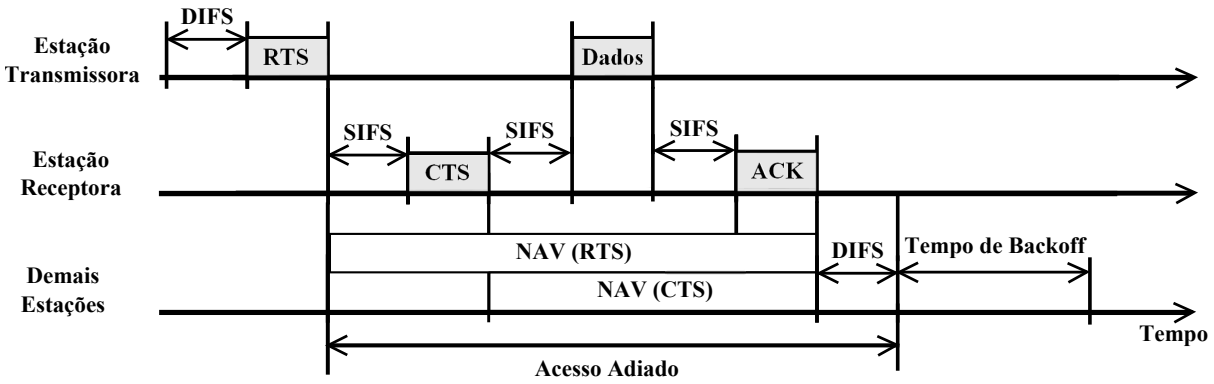


Figura 5.2 Time diagram for the RTS/CTS [IEEE Standard 802.11 2012].

Considerando o uso da técnica de espalhamento espectral ERP-OFDM (IEEE 802.11g), o tempo de transmissão dos quadros, em microssegundos, é dado por [IEEE Standard 802.11 2012]:

$$T_{FRAME} = T_{PREAMBLE} + T_{SIGNAL} + T_{SYM} \cdot Ceiling(\frac{16 + 8 \cdot (L_{FRAME}) + 6}{N_{DBPS}}) + SignalExtension \quad , \tag{5.4}$$

onde $T_{PREAMBLE}$ é o tempo de transmissão do preâmbulo físico, T_{SIGNAL} é o tempo de transmissão do *PHY header*, T_{SYM} é o tempo de transmissão de um símbolo OFDM e L_{FRAME} corresponde ao comprimento, em *bytes*, do quadro cujo atraso de transmissão está sendo calculado. O N_{DBPS} representa o número de bits de dados por símbolo OFDM e depende da taxa do canal empregada. O resultado da função *Ceiling* indica o número de símbolos OFDM (N_{SYM}) utilizados na transmissão do quadro. O número de bits transmitidos deve ser um múltiplo do N_{DBPS}. Caso necessário, o comprimento da mensagem deve ser estendido para se tornar um múltiplo deste. $SignalExtension$ é um período sem transmissões. Por fim, o tempo médio de *backoff* T_{CW} é dado por:

$$T_{CW} = (\frac{T_{slot} \cdot CW_{min}}{2}) \ , \tag{5·5}$$

onde T_{slot} é o tempo de um slot e CW_{min} é o tamanho mínimo da janela de *backoff*. Ambos dependem da camada física (PHY).

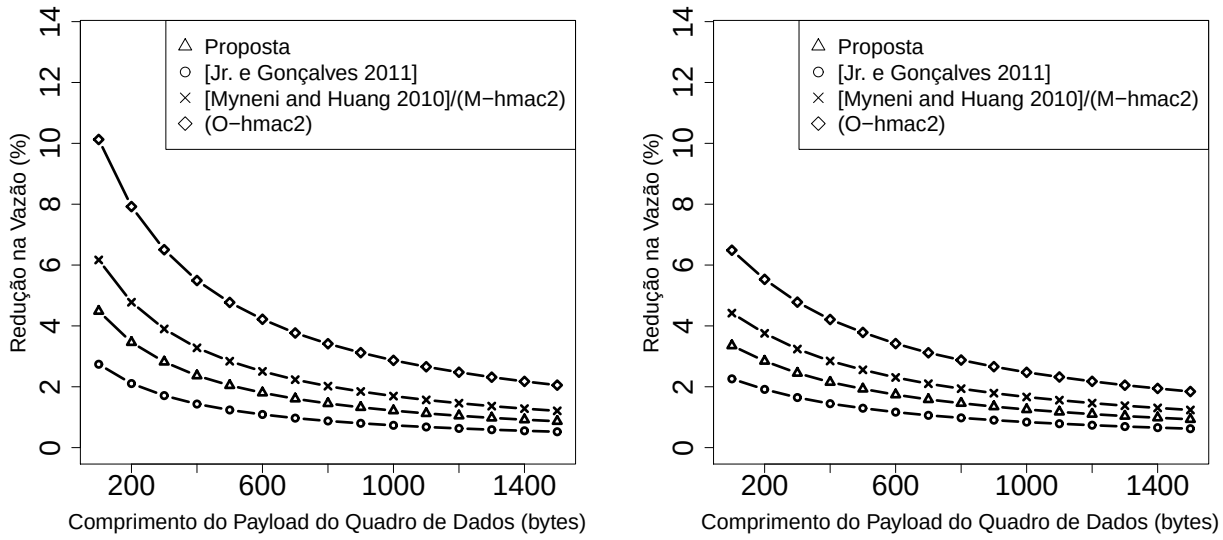
A Tabela 5.1 apresenta os valores dos parâmetros utilizados para o cálculo da TMT considerando-se uma camada física IEEE 802.11g.

Tabela 5.1 Parâmetros do IEEE 802.11g.

Parâmetro	Valor	Parâmetro	Valor
T_{slot}	$20\mu s$	CW_{min}	15
$T_{PREAMBLE}$	$16\mu s$	T_{SIGNAL}	$4\mu s$
T_{DIFS}	$50\mu s$	T_{SYM}	$4\mu s$
T_{SIFS}	$10\mu s$	$SignalExtension$	$6\mu s$

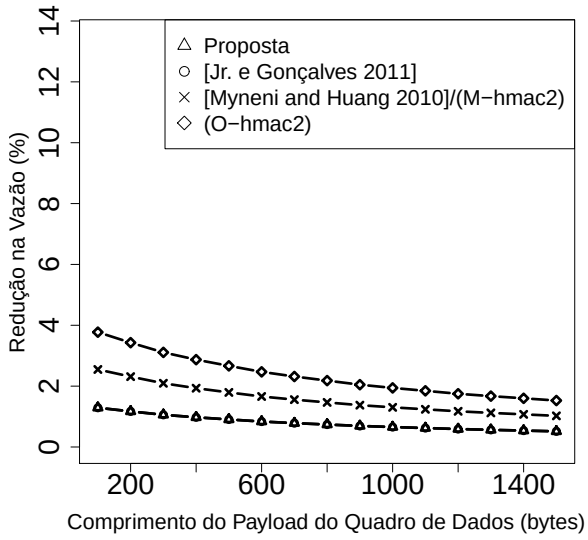
5.1 ESTUDO DE CASO

Esta seção avalia a redução da vazão da rede, devido ao uso dos esquemas de segurança estudados. Assume-se que cada quadro de dados é confirmado por um ACK e sem a ocorrência de colisões. Assume-se também uma camada física IEEE 802.11g. O modelo TMT é utilizado para o cômputo da vazão da rede.



(a) Taxa do canal de 6 Mbps

(b) Taxa do canal de 12 Mbps



(c) Taxa do canal de 24 Mbps

Figura 5.3 Redução da Vazão da Rede (CSMA/CA).

A Figura 5.3 apresenta a redução da vazão da rede devido ao uso de cada esquema de proteção estudado, considerando que a rede emprega o CSMA/CA. O impacto é analisado em todas as taxas obrigatórias do canal: 6, 12 e 24 Mbps. Independente da taxa do canal e do tamanho do *payload* do quadro de dados, o esquema proposto neste

trabalho apresenta um impacto na vazão da rede inferior ao apresentado pelo esquema proposto em [Myneni e Huang 2010] e pelos esquemas *O-hmac2* e *M-hmac2* propostos em [Malekzadeh, Ghani e Subramaniam 2012]. Quando comparada com o esquema proposto em [Jr. e Gonçalves 2011] e considerando as taxas do canal de 6 e 12 Mbps, a prosposta apresenta um impacto na vazão da rede superior. No entanto, como pode ser observado na Figura 5.3(c), quando a taxa do canal é de 24 Mbps o esquema proposto em [Jr. e Gonçalves 2011] e o esquema proposto nesse trabalho apresentam o mesmo impacto na vazão da rede.

O fato da proposta apresentar um impacto na vazão da rede superior ao apresentado pelo esquema proposto em [Jr. e Gonçalves 2011] quando a taxa do canal é de 6 ou 12 Mbps, mas apresentar o mesmo impacto quando a taxa do canal é de 24Mpbs se deve a conversão dos bits dos quadros de controle ACK e CTS em símbolos OFDM, realizados através da função *Ceiling* presente na Equação 5.4. Como apresentado no Capítulo 3, os quadros de controle ACK e CTS no esquema proposto em [Jr. e Gonçalves 2011] apresentam 176 bits de comprimento. Já o comprimento desses quadros no esquema proposto nesse trabalho é de 224 bits, uma vez que o endereço do nó transmissor (TA) é adicionado ao cabeçalho MAC desses quadros. A Tabela 5.2 apresenta o valor da função *Ceiling* para os quadros ACK e CTS considerando os dois esquemas de proteção. O resultado dessa função representa a quantidade de símbolos OFDM necessários para transmitir um quadro. Como pode ser observado, quando a taxa do canal é de 6 ou 12 Mbps, o esquema proposto em [Jr. e Gonçalves 2011] utiliza uma quantidade menor de símbolos que a proposta. Desta forma, o impacto na vazão da rede é menor. No entanto, quando a taxa do canal é de 24 Mbps, ambos os esquemas utilizam a mesma quantidade de símbolos OFDM, ocasionando o mesmo impacto na vazão.

Tabela 5.2 Quantidade de símbolos OFDM necessários para transmitir um ACK ou um CTS.

Esquema de Proteção	6 Mbps	12 Mbps	24 Mbps
[Jr. e Gonçalves 2011]	9	5	3
Proposta	11	6	3

O pior caso de redução da vazão é observado quando uma taxa de 6 Mbps é utilizada, como apresentado na Figura 5.3(a). Nesse caso, quando o tamanho do *payload* do quadro de dados é 100 bytes, a vazão é reduzida apenas 2,73% e 4,48% para o esquema proposto em [Jr. e Gonçalves 2011] e neste trabalho, respectivamente. Uma redução de 6,16% é observada tanto para o esquema proposto em [Myneni e Huang 2010] quanto para o *M-hmac2* [Malekzadeh, Ghani e Subramaniam 2012]. Já para o *O-hmac2* [Malekzadeh, Ghani e Subramaniam 2012], a redução apresentada é de 10,12% a uma taxa de 6 Mbps.

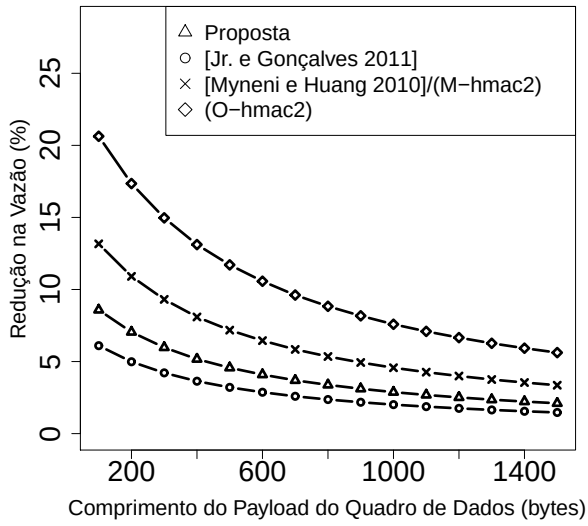
Considerando uma taxa de 12 Mbps, o impacto na vazão da rede foi reduzido em comparação com os resultados obtidos a uma taxa de 6 Mbps. Como apresentado na Figura 5.3(b), quando o tamanho do *payload* do quadro de dados é 100 bytes, a vazão é reduzida apenas 2,25% e 3,35% para o esquema proposto em [Jr. e Gonçalves 2011] e neste trabalho, respectivamente. Uma redução de 4,41% é observada tanto para o esquema proposto em [Myneni e Huang 2010] quanto para o *M-hmac2* e de 6,48% para o *O-hmac2*.

O melhor caso de redução da vazão ocorre para uma taxa de 24 Mbps para todos os esquemas, como apresentado na Figura 5.3(c). Quando o tamanho do *payload* do quadro de dados é 100 bytes, por exemplo, a redução observada é de apenas 1,29% para o esquema proposto em [Jr. e Gonçalves 2011] e neste trabalho, de 3,77% para o *O-hmac2* e de 2,54% para o esquema proposto em [Myneni e Huang 2010] e para o *M-hmac2*.

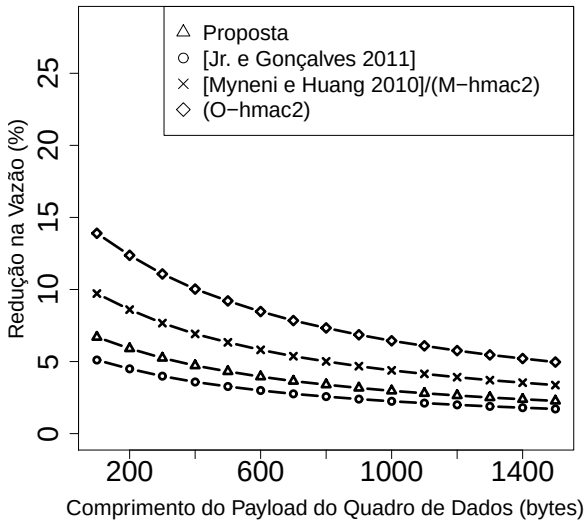
A Tabela 5.3 resume a redução da vazão apresentada na Figura 5.3, quando o tamanho do *payload* do quadro de dados é 100 bytes.

Tabela 5.3 Redução da Vazão quando o tamanho do *payload* do quadro de dados é 100 bytes (CSMA/CA).

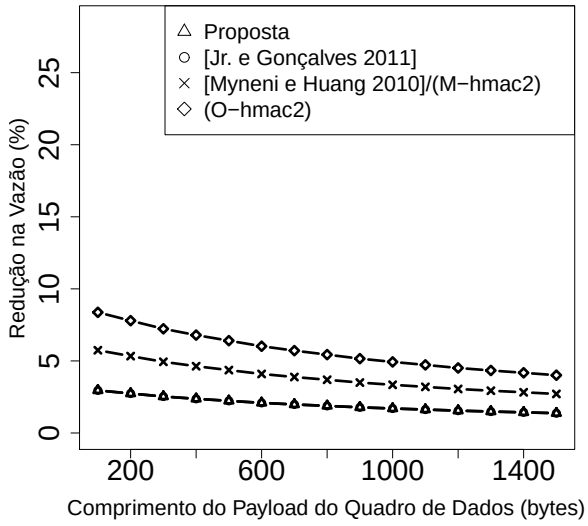
Esquema de Proteção	6 Mbps	12 Mbps	24 Mbps
[Jr. e Gonçalves 2011]	2,73%	2,25%	1,29%
Proposta	4,48%	3,35%	1,29%
[Myneni e Huang 2010]	6,16%	4,41%	2,54%
[Malekzadeh, Ghani e Subramaniam 2012]	10,12%	6,48%	3,77%



(a) Taxa do canal de 6 Mbps



(b) Taxa do canal de 12 Mbps



(c) Taxa do canal de 24 Mbps

Figura 5.4 Redução da Vazão da Rede (RTS/CTS).

A Figura 5.4 apresenta o impacto dos esquemas de proteção estudados na vazão da rede, quando se emprega o mecanismo RTS/CTS. Nesse cenário, o pior caso de redução da vazão também é observado quando uma taxa de 6 Mbps é utilizada, como é apresentado na Figura 5.4(a). Nesse caso, quando o tamanho do *payload* do quadro de dados é 100

bytes, por exemplo, a vazão é reduzida apenas 6,10% e 8,58% para o esquema proposto em [Jr. e Gonçalves 2011] e neste trabalho, respectivamente. Uma redução de 13,16% é observada tanto para o esquema proposto em [Myneni e Huang 2010] quanto para o *M-hmac2*. Já para o *O-hmac2*, a redução apresentada é de 20,63% a uma taxa de 6 Mbps.

Considerando uma taxa de 12 Mbps, o impacto na vazão da rede foi reduzido em comparação com os resultados obtidos a uma taxa de 6 Mbps. Como apresentado na Figura 5.4(b), quando o tamanho do *payload* do quadro de dados é 100 bytes, a vazão é reduzida apenas 5,10% e 6,69% para o esquema proposto em [Jr. e Gonçalves 2011] e neste trabalho, respectivamente. Uma redução de 9,71% é observada tanto para o esquema proposto em [Myneni e Huang 2010] quanto para o *M-hmac2* e de 13,89% para o *O-hmac2*.

O melhor caso de redução da vazão ocorre para uma taxa de 24 Mbps para todos os esquemas, como apresentado na Figura 5.4(c). Quando o tamanho do *payload* do quadro de dados é 100 bytes, por exemplo, a redução observada é de apenas 2,95% para o esquema proposto em [Jr. e Gonçalves 2011] e neste trabalho, de 8,37% para o *O-hmac2* e de 5,74% para o esquema proposto em [Myneni e Huang 2010] e para o *M-hmac2*.

A Tabela 5.4 resume a redução da vazão apresentada na Figura 5.4, quando o tamanho do *payload* do quadro de dados é 100 bytes.

Tabela 5.4 Redução da Vazão quando o tamanho do *payload* do quadro de dados é 100 bytes (RTS/CTS).

Esquema de Proteção	6 Mbps	12 Mbps	24 Mbps
[Jr. e Gonçalves 2011]	6,10%	5,10%	2,95%
Proposta	8,58%	6,69%	2,95%
[Myneni e Huang 2010]	13,16%	9,71%	5,74%
[Malekzadeh, Ghani e Subramaniam 2012]	20,63%	13,89%	8,37%

Como apresentado nas Figuras 5.3 e 5.4, à medida que a taxa do canal aumenta, o impacto dos esquemas de proteção estudados na vazão da rede tende a diminuir. Esse resultado é esperado, uma vez que à medida que a taxa do canal aumenta, o número de

símbolos OFDM necessários para transmitir um quadro de controle diminui. Desta forma, em taxas mais altas o número de símbolos OFDM necessário para transmitir um quadro de controle modificado pelos esquemas estudados se aproxima do número de símbolos OFDM necessário para transmitir um quadro de controle em seu formato original.

5.2 PRINCIPAIS DIFERENÇAS ENTRE OS ESQUEMAS DE PROTEÇÃO ESTUDADOS

A Tabela 5.5 apresenta um resumo das principais características do esquema de proteção proposto comparando-o com cada esquema de proteção estudado. Com relação ao *overhead*, o esquema proposto em [Khan e Hasan 2008] não altera o comprimento dos quadros de controle e, portanto, não tem impacto na vazão da rede. No entanto, esse esquema é superado pelo esquema proposto neste trabalho em aspectos de segurança. Diferentemente da proposta neste trabalho, o esquema proposto em [Khan e Hasan 2008] possui as seguintes fraquezas: 1) não trata os ataques de reinjeção e 2) usa apenas 16 bits para prover a autenticação, o que torna frágil a proteção oferecida.

Dentre os trabalhos que alteram o comprimento dos quadros de controle, o esquema proposto neste trabalho e em [Jr. e Gonçalves 2011] introduzem o menor *overhead* e, portanto, apresentaram os melhores resultados em termos do impacto na vazão da rede. O esquema proposto em [Jr. e Gonçalves 2011] leva uma certa vantagem com relação ao impacto na vazão, pois o esquema proposto nesse trabalho, além de introduzir 64 bits de autenticação, adiciona um campo TA de 6 bytes ao cabeçalho MAC dos quadros de controle ACK e CTS. Contudo, o esquema proposto leva vantagem em aspectos de segurança e de funcionamento do processo de verificação da autenticidade dos quadros. Diferentemente da proposta neste trabalho, o esquema proposto em [Jr. e Gonçalves 2011] possui as seguintes fraquezas: 1) usa o CBC-MAC básico como mecanismo de autenticação e, portanto, é sucetível a ataques de forjação, 2) emprega um número de sequência global, que gera inconsistências quando dois ou mais nós da rede não se ouvem e 3) os quadros ACK e CTS não podem ser autenticados em todos os nós da rede, o que impede o funcionamento adequado do esquema de autenticação.

Tabela 5.5 Resumo das principais características de cada proposta estudada.

	Overhead	**Ataques de Replicação**	**Autenticação**	**Gerenciamento de Chaves**
Proposal	**112 bits** (Ack + CTS) e **64 bits** (Para os demais tipos de quadros de controle)	Número de Sequência Individual	AES-CMAC	Se ajusta a Infraestrutura presente no padrão IEEE 802.11i
(Khan e Hasan 2008)	0 bits (Para todos os tipos de quadros de controle)	Não evita	*Pseudo Random Number* (16 bits)	Utiliza a PTK
(Jr. e Gonçalves 2011)	64 bits (Para todos os tipos de quadros de controle)	Número de Sequência Global	CBC-MAC	Utiliza a GTK
(Myneni e Huang 2010)	160 bits (Para todos os tipos de quadros de controle)	Número de Sequência Global	HMAC-SHA1	Framework IAPP
M-hmac2 **(Malekzadeh, Ghani e Subramaniam 2012)**	160 bits (Para todos os tipos de quadros de controle)	*Timestamp*	HMAC-SHA-256 modificado	Chave pré-compartilhada
O-hmac2 **(Malekzadeh, Ghani e Subramaniam 2012)**	288 bits (Para todos os tipos de quadros de controle)	*Timestamp*	HMAC-SHA256	Chave pré-compartilhada

Os demais esquemas estudados além de introduzirem um *overhead* significativo, também fornecem uma proteção contra ataques de reinjeção que exige a sincronização das estações, como apresentado no Capítulo 3. Logo, ataques de reinjeção ainda são possíveis, se realizados dentro de uma janela aceitável do tempo atual. Com relação ao algoritmo de autenticação, o esquema proposto em [Myneni e Huang 2010] faz uso do HMAC-SHA-1, que vem sendo questionado devido às fragilidades encontradas no *hash* criptográfico [Rechberger e Rijmen 2008].

Como apresentado anteriormente, todos os trabalhos relacionados apresentam fraquezas associadas à geração e à distribuição da chave utilizada no processo de autenticação. Os esquemas propostos em [Khan e Hasan 2008] e [Jr. e Gonçalves 2011] fazem uso da chave criptográfica PTK e GTK, respectivamente. Tais chaves já são utilizadas pelo IEEE 802.11, enfraquecendo a segurança proporcionada por ambos os esquemas. O esquema proposto em [Myneni e Huang 2010] requer um sistema de geração e distribuição de chaves que não é suportado pelo IEEE 802.11, além de adicionar um *overhead* significativo na rede à medida que o número de estações presentes no canal de comunicação aumenta, como foi constatado pelos autores. Já o esquema proposto em [Malekzadeh, Ghani e Subramaniam 2012] não aborda o processo de geração e distribuição de chaves na rede.

5.3 RESUMO

Neste Capítulo foi apresentado o modelo da vazão máxima teórica (*Theoretical Maximum Throughput* - TMT) utilizado para o cômputo da vazão da rede. Esse modelo foi utilizado no estudo de caso realizado na Seção 5.1. Para o cálculo da vazão foi considerada a utilização dos métodos de controle de acesso ao meio CSMA/CA e RTS/CTS. Foi assumida uma camada física IEEE 802.11g, e todas as taxas obrigatórias do canal foram analisadas. Na Seção 5.1 foi apresentado o impacto na vazão da rede devido ao uso de cada esquema de proteção estudado. Foi observado que à medida que a taxa do canal aumenta, o impacto dos esquemas de proteção estudados na vazão da rede tende a diminuir. Por fim, na Seção 5.2 foram apresentadas as principais diferenças entre os

esquemas de proteção estudados com relação ao *overhead*, impacto na vazão e aspectos de segurança.

CAPÍTULO 6

CONCLUSÃO

Diversos ataques à disponibilidade das redes sem fio baseadas no padrão IEEE 802.11 podem ser facilmente realizados através do uso de quadros de controle. Isso ocorre devido ao fato do padrão IEEE 802.11 não possuir qualquer tipo de mecanismo de proteção para esses quadros. Este trabalho lidou com essa problemática apresentando um esquema de segurança para os quadros de controle IEEE 802.11.

A solução proposta se diferencia dos trabalhos relacionados em três aspectos. Primeiro, por apresentar um módulo de geração e distribuição de chaves que se ajusta aos protocolos de geração e distribuição de chaves presente no padrão IEEE 802.11i. Desta forma, a chave utilizada na autenticação dos quadros de controle é gerada e distribuída de forma segura, sem que qualquer infraestrutura de distribuição de chaves, além da fornecida pelo padrão IEEE 802.11i, se faça necessária. Segundo, este trabalho também se diferencia, por contar com um módulo de prevenção de ataques de reinjeção que não exige sincronização dos nós da rede e que, portanto, não é vulnerável a ataques de reinjeção. Finalmente, o esquema proposto neste trabalho apresenta um baixo impacto na vazão da rede, quando comparado aos esquemas de segurança estudados, independente da taxa do canal e do tamanho do *payload* do quadro de dados.

O esquema proposto utiliza vários elementos que já são especificados no padrão IEEE 802.11, tais como a função pseudoaleatória (PRF), os processos de distribuição de chave (*4-Way Handshake* e *Group Key Handshake*) e o algoritmo de computação do MAC (AES-CMAC). Além disso, as alterações apresentadas pelo esquema não comprometem o funcionamento do IEEE 802.11.

REFERÊNCIAS BIBLIOGRÁFICAS

[Barker et al. 2012]BARKER, E. et al. Recommendation for Key Management - Part 1: General (Revision 3). In: *NIST Special Publication 800-57*. [S.l.: s.n.], 2012.

[Barker e Roginsky 2011]BARKER, E.; ROGINSKY, A. Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths. In: *NIST Special Publication 800-131A*. [S.l.: s.n.], 2011.

[Bellardo e Savage 2003]BELLARDO, J.; SAVAGE, S. 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In: *Proc. of 2th USENIX Security Symposium (SSYM)*. [S.l.]: Washington, DC, USA, 2003. p. 15–28.

[Chen e Muthukkumarasamy 2006]CHEN, B.; MUTHUKKUMARASAMY, V. Denial of Service Attacks Against 802.11 DCF Abstract. 2006. 2006.

[Chen, Ding e Varshney 2003]CHEN, D.; DING, J.; VARSHNEY, P. Protecting wireless networks against a denial of service attack based on virtual jamming. In: *Proc. of the ACM 9th International Conference on Mobile Computing and Networking (MobiCom 03)*. [S.l.]: San Diego, CA, USA, 2003. p. 14–19.

[Contini e Yin 2006]CONTINI, S.; YIN, Y. L. Forgery and partial key-recovery attacks on hmac and nmac using hash collisions. In: *ADVANCES IN CRYPTOLOGY - ASIACRYPT'06, LNCS 4284*. [S.l.]: Springer-Verlag, 2006. p. 37–53.

[Denis e Johnson 2007]DENIS, T.; JOHNSON, S. *Cryptography for Developers*. [S.l.]: Syngress Publishing, 2007.

[Dworkin 2005]DWORKIN, M. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. In: *NIST Special Publication 800-38B*. [S.l.: s.n.], 2005.

[Gast 2002]GAST, M. *802.11 Wireless Networks: The Definitive Guide*. [S.l.]: OŔeilly, 2002.

[IEEE Standard 802.11 2012]IEEE Standard 802.11. *IEEE Standards for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. 2012.

[IEEE Standard 802.11i 2004]IEEE Standard 802.11i. *IEEE Standard for Information Technology – Telecommunications and Information Exchange between System – 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*. 2004.

[IEEE Standard 802.11n 2009]IEEE Standard 802.11n. *IEEE Standard for Information technology – Telecommunications and Information Exchange between System – 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*. 2009.

[IEEE Standard 802.11w 2009]IEEE Standard 802.11w. *IEEE Standard for Information technology – Telecommunications and Information Exchange between System – 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*. 2009.

[Iwata e Kurosawa 2003]IWATA, T.; KUROSAWA, K. Stronger Security Bounds for OMAC, TMAC and XCBC. In: *INDOCRYPT*. [S.l.]: Springer, 2003. (Lecture Notes in Computer Science), p. 402–415.

[Jr. e Gonçalves 2011]JR., M. Corrêa; GONcALVES, P. A. S. Um Mecanismo de Proteção de Quadros de Controle para Redes IEEE 802.11. In: *Proc. of SBSeg*. [S.l.: s.n.], 2011.

[Jun, Peddabachagari e Sichitiu 2003]JUN, J.; PEDDABACHAGARI, P.; SICHITIU, M. L. Theoretical Maximum Throughput of IEEE 802.11 and its Applications. In: *In Proceedings of the IEEE International Symposium on Network Computing and Applications*. [S.l.: s.n.], 2003. (NCA '03), p. 249–257.

[Katz e Lindell 2007]KATZ, J.; LINDELL, Y. *Introduction to Modern Cryptography*. [S.l.]: Chapman and Hall/CRC Press, 2007.

[Khan e Hasan 2008]KHAN, M.; HASAN, A. Pseudo random number based authentication to counter denial of service attacks on 802.11. In: *Proc. of 5th IFIP International Conference on Wireless and Optical Communications Networks (WOCN)*. [S.l.: s.n.], 2008. p. 1–5.

[Kim et al. 2006]KIM, J. et al. On the security of hmac and nmac based on haval, md4, md5, sha-0 and sha-1 (extended abstract). In: *Proceedings of the 5th international conference on Security and Cryptography for Networks*. Berlin, Heidelberg: Springer-Verlag, 2006. (SCN'06), p. 242–256. ISBN 3-540-38080-9, 978-3-540-38080-1.

[Koenings et al. 2009]KOENINGS, B. et al. Channel Switch and Quiet attack: New DoS Attacks Exploiting the 802.11 Standard. In: *Proc. of the 34th IEEE Conference on Local Computer Networks (LCN)*. [S.l.]: Zurich, Switzerland, 2009.

[Malekzadeh, Ghani e Subramaniam 2010]MALEKZADEH, M.; GHANI, A. A. A.; SUBRAMANIAM, S. Design of cyberwar laboratory exercises to implement common security attacks against ieee 802.11 wireless networks. *J. Comp. Sys., Netw., and Comm.*, 2010. Hindawi Publishing Corp., New York, NY, United States, v. 2010, p. 5:1–5:15, jan. 2010. ISSN 1687-7381. Disponível em: <http://dx.doi.org/10.1155/2010/218271>.

[Malekzadeh, Ghani e Subramaniam 2012]MALEKZADEH, M.; GHANI, A. A. A.; SUBRAMANIAM, S. A new security model to prevent denial-of-service attacks and vio-

lation of availability in wireless networks. *Int. J. Communication Systems*, 2012. v. 25, n. 7, p. 903–925, 2012.

[Menezes, Oorschot e Vanstone 1996]MENEZES, A.; OORSCHOT, P. van; VANSTONE, S. *Handbook of Applied Cryptography*. [S.l.]: CRC Press, 1996.

[Myneni e Huang 2010]MYNENI, S.; HUANG, D. IEEE 802.11 Wireless LAN Control Frame Protection. In: *Proc. of the 7th IEEE Conference on Consumer communications and Networking Conference (CCNC)*. [S.l.]: Piscataway, NJ, USA. IEEE Press, 2010. p. 844–848.

[Patel 2003]PATEL, S. An efficient mac for short messages. In: *Revised Papers from the 9th Annual International Workshop on Selected Areas in Cryptography*. London, UK, UK: Springer-Verlag, 2003. (SAC '02), p. 353–368. ISBN 3-540-00622-2. Disponível em: <http://dl.acm.org/citation.cfm?id=646558.694905>.

[Qureshi et al. 2007]QURESHI, Z. I. et al. A Solution to Spoofed PS-Poll Based Denial of Service Attacks in IEEE 802.11 WLANs. In: *Proc. of the 11th WSEAS International Conference on Communications*. [S.l.]: Stevens Point, Wisconsin, USA. World Scientific and Engineering Academy and Society (WSEAS), 2007. p. 7–11.

[Rachedi e Benslimane 2009]RACHEDI, A.; BENSLIMANE, A. Impacts and Solutions of Control Packets Vulnerabilities with IEEE 802.11 MAC. *Wireless Comm. and Mobile Comp.*, 2009. v. 9, n. 4, p. 469–488, 2009.

[Ray e Starobinski 2007]RAY, S.; STAROBINSKI, D. On False Blocking in RTS/CTS-Based Multihop Wireless Networks. *IEEE Transactions on Vehicular Technology*, 2007. v. 56, n. 2, p. 849–862, 2007.

[Rechberger e Rijmen 2008]RECHBERGER, C.; RIJMEN, V. New Results on NMAC/HMAC when Instantiated with Popular Hash Functions. *Universal Computer Science*, 2008. v. 14, n. 3, p. 347–376, 2008.

[Song et al. 2006]SONG, J. et al. *RFC 4493 - The AES-CMAC Algorithm.* June 2006.

[Tilborg e Jajodia 2011]TILBORG, H. C. van; JAJODIA, S. *Encyclopedia of Cryptography and Security*. [S.l.]: Springer, 2011.

[Xiao e Rosdahl 2002]XIAO, Y.; ROSDAHL, J. Throughput and Delay Limits of IEEE 802.11. *IEEE Communications Letters*, 2002. v. 6, n. 8, p. 355–357, 2002.

[Zhang et al. 2008]ZHANG, Z. et al. Jamming ACK attack to wireless networks and a mitigation approach. In: *Proc. of the IEEE GLOBECOM)*. [S.l.]: New Orleans, LO, USA, 2008. p. 1–5.