Kécyo Keviny Gonçalves de Mendonça
Orientador: Esp. Fredison Muniz de Sousa
Co-orientador: Esp. Pablo de Abreu Vieira

Análise da Vulnerabilidade do Mecanismo RTS/CTS a Ataques de Negação de Serviço em Redes Wireless IEEE 802.11

Picos - PI
27 de Novembro de 2017

Kécyo Keviny Gonçalves de Mendonça
Orientador: Esp. Fredison Muniz de Sousa
Co-orientador: Esp. Pablo de Abreu Vieira

Análise da Vulnerabilidade do Mecanismo RTS/CTS a Ataques de Negação de Serviço em Redes Wireless IEEE 802.11

Monografia submetida ao curso de Bacharelado em Sistemas de Informação, da Universidade Federal do Piauí, sob orientação do Prof. Esp. Fredison Muniz de Sousa, como exigência parcial para obtenção do título de bacharel em Sistemas de Informação

Universidade Federal do Piauí
Campus Senador Helvídio Nunes de Barros
Bacharelado em Sistemas de Informação

Picos - PI
27 de Novembro de 2017

FICHA CATALOGRÁFICA
Serviço de Processamento Técnico da Universidade Federal do Piauí
Biblioteca José Albano de Macêdo

M539a Mendonça, Kécyo Keviny Gonçalves de

Análise da vulnerabilidade do mecanismo RTS/CTS a ataques de negação de serviço em redes Wireless IEEE 802.11 / Kécyo Keviny Gonçalves de Mendonça.– 2017.
CD-ROM : il.; 4 ¾ pol. (47f.)
Trabalho de Conclusão de Curso (Curso Bacharelado em Sistemas de Informação) – Universidade Federal do Piauí, Picos, 2018.
Orientador(A): Prof. Esp. Fredison Muniz de Sousa
Coorinentador: Prof. Esp. Pablo de Abreu Vieira

1. Rede Sem Fio. 2.Wireless. 3.Protocolo de Controle de Acesso ao Meio. I. Título.

CDD 004.62

ANÁLISE DA VULNERABILIDADE DO MECANISMO RTS/CTS A ATAQUES DE NEGAÇÃO DE SERVIÇO EM REDES WIRELESS IEEE 812.11

KECYO KEVINY GONÇALVES DE MENDONÇA

Monografia Aprovado
como exigência parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Data de Aprovação

Picos – PI. 05 de dezembro de 2017

Profº. Esp. Fredison Muniz de Sousa
Orientador

Prof. Esp. Ismael de Holanda Leal
Membro

Patricia Vieira da Silva Barros
Profª. *Ma.* Patricia Vieira da Silva Barros
Membro

Agradecimentos

Agradeço principalmente a Deus por ter me dado forças para não desistir da caminhada.

A minha família que nunca pouparam esforços, sempre dando o suporte necessário para alcançar meus objetivos, durante toda minha vida, em especial, aos meus pais Silvamar e Fabricia, por sempre me apoiarem em todas as decisões que tomei na vida.

Aos meus amigos e colegas de curso e da vida que estiveram presentes, incentivando e dando conselhos que contribuíram para a melhoria deste trabalho.

Em especial a *"Família SI"*, composta por: Leonardo de Jesus, Rafael Araújo, Jaqueline Campelo, Diego Fernando, Diego Vasconcelo (Kirito), Carlos Henrique, Guilherme Dutra, Antônio de Carvalho e Fabrício Sousa. Porquê sem eles eu não teria conseguido chegar onde cheguei durante todos estes anos de curso.

A minha grande amiga Daiany Vasconcelos, que mesmo de longe sempre me apoiou e incentivou no que fosse necessário.

A minha amiga Kaori Nakahashi, pelos anos de amizades e por sempre me ajudar no que fosse preciso.

A minha querida amiga Frida Franco, que mesmo com todas as brincadeiras e zoações contra minha pessoa, é uma pessoa que eu gosto e considero muito.

Ao meu orientador professor Me. Fredison Muniz, por me auxiliar e incentivar no desenvolvimento desde trabalho.

Ao professor Pablo Abreu, que mesmo não estando mais presente como parte do corpo docente da universidade, me ajudou para que fosse possível a conclusão desde trabalho.

Aos meus grandes amigos e parceiros de jogatina, Laio Samuel (LaioSam), Victor Macêdo (Akeeme), e Edenisio Galvão (Chiwuwa) pelas horas de diversão e descontração no lolzim.

Agradeço também a todas as outras pessoas que de alguma forma contribuíram para que eu pudesse desenvolver este trabalho.

"A menos que modifiquemos a nossa maneira de pensar, não seremos capazes de resolver os problemas causados pela forma como nos acostumamos a ver o mundo."
(Albert Einstein)

Resumo

As tecnologias e aplicações sem fio vem recebendo uma grande atenção nos últimos anos. O protocolo de controle de acesso ao meio (MAC) é o elemento principal que determina a eficiência na partilha da largura de banda de comunicação limitada do canal sem fio, em redes de área local sem fio (WLANs). O padrão IEEE 802.11 emprega o mecanismo RTS/CTS (Request to Send/Clear to Send) como um mecanismo opcional para prevenção de colisões na rede, esse mecanismo é amplamente utilizado em redes wireless que apresentem o problema do nó oculto. Embora esse mecanismo seja eficiente na redução de colisões, o mesmo também gera um *overhead* (sobrecarga) significativo na rede quando utilizado. Dessa forma, sabendo que o uso desse mecanismo é aconselhável apenas para frames (quadros) grandes, uma estação maliciosa poderia introduzir frames desse tipo na rede, com o objetivo de forçar o uso desnecessário desse mecanismo, a fim sobrecarregar a rede. Diante da inexistência de métodos de proteção, esse mecanismo se torna altamente suscetível a ataques de negação de serviço, ataque estes que tem por objetivo tornar recursos de um sistema indisponíveis para usuários legítimos. O presente trabalho tem como proposta de pesquisa apresentar e verificar a eficácia de um novo tipo de ataque de negação de serviço direcionado ao mecanismo de prevenção de colisões RTS/CTS, analisando o impacto que o mesmo pode gerar em redes sem fio baseadas no padrão IEEE 802.11. Os resultados obtidos demonstraram que o ataque conseguiu degradar de forma significativa o desempenho da rede, a ponto deixar a indisponível, mesmo que por uma quantidade pequena de tempo. Com o intuito de diminuir o impacto desse tipo de ataque, foram propostas duas possíveis contramedidas para a prevenção e mitigação dessa vulnerabilidade.

Palavras-chaves: RTS/CTS. Negação de Serviço. Padrão 802.11. Colisões.

Abstract

Wireless technologies and applications have been getting a lot of attention in recent years. The Medium Access Control Protocol (MAC) is the primary element that determines the efficiency in sharing the wireless channel's limited communication bandwidth over wireless local area networks (WLANs). The IEEE 802.11 standard employs the RTS / CTS (Request to Send / Clear to Send) mechanism as an optional mechanism to prevent network collisions, this mechanism is widely used in wireless networks that present the hidden node problem. Although this mechanism is efficient in reducing collisions, it also generates a significant overhead in the network when used. In this way, knowing that the use of this mechanism is advisable only for large frames, a malicious station could introduce frames of this type in the network, in order to force the unnecessary use of this mechanism in order to overload the network. In the absence of protection methods, this mechanism becomes highly susceptible to denial-of-service attacks, which is intended to make a system's resources unavailable to legitimate users. The present work has as a research proposal to present and verify the effectiveness of a new type of denial of service attack directed to the mechanism of prevention of collisions RTS / CTS, analyzing the impact that can generate in wireless networks based on the IEEE standard 802.11. The results showed that the attack was able to significantly degrade the performance of the network, to the point that it was unavailable, even for a small amount of time. In order to reduce the impact of this type of attack, two possible countermeasures were proposed to prevent and mitigate this vulnerability.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

AP *Access Point.*

CSMA/CA *Carrier Sense Multiple access With Collision Avoidance*

CTS *Clear to Send.*

DFC *Distributed Coordination Function.*

DIFS *DCF Interframe Spacing*

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

DDoS *Distributed Denial-of-Service, ou negação de serviço distrubuída.*

FC *Frame Control*

FCS *Frame Check Sequence*

HMAC *Hash-based Message Authentication Code.*

IEEE *Institute of Electrical and Electronic Engineers*

MAC *Media Access Control*

OSI *Open Systems Interconnection*

PIFS *PCF Interframe Space*

RA *Receiver Address*

RF *Radio Frequência*

RSSI *Received Signal Strength Indication*

RTS *Request to Send*

SHA *Secure Hash Algorithm*

SIFS *Shortest Interframe spacing*

SSID *Service Set IDentifier*

TA *Transmiter Address*

WIFI *Wireless Fidelity*

Sumário

1 Introdução

Nos últimos anos, com o crescente avanço tecnológico, pudemos notar um aumento significativo de dispositivos computacionais com acesso à internet conectados a redes sem fio, que mais popularmente são conhecidas como redes Wi-Fi . Estudos recentes da Cetic.br, o braço de pesquisas do Comitê Gestor da Internet, apontam que em 2015 pouco mais da metade dos brasileiros acessava a internet com regularidade via redes *wireless.*

Como é notado, tais redes vem ganhando cada vez mais espaço, tendo em vista sua mobilidade e praticidade aliados ao seu baixo custo e facilidade de implementação. Como consequência dessa alta popularização, seu uso é cada vez mais comum nos mais variados ambientes, como: (Universidades, aeroportos, shoppings e etc.).

Contudo, do mesmo modo que o uso dessa tecnologia cresce gradativamente, ataques à essas redes tem ganhado cada vez mais notoriedade. Dentre os diversos ataques direcionados a essa infraestrutura, um dos mais utilizados e que merece atenção, é o ataque de negação de serviço – Denial of Service (DoS), que consiste na tentativa de tornar o serviço fornecido pela rede indisponível (SANDSTROM, 2001).

Esses tipos de ataque consomem os recursos de servidores e roteadores impedindo assim que usuários legítimos tenham acesso a um determinado serviço, o que torna os mesmos bastante preocupantes.

De acordo com vários autores, diversos fatores podem motivar um ataque de negação de serviço, desde usuários bem-intencionados que fazem o uso desse tipo de ataque para encontrar soluções para vulnerabilidades existentes, até usuários mal-intencionados, que buscam interromper serviços através desse tipo de ataque. Devido facilidade de implementação aliado a sua efetividade, a prática desse tipo de ataque vem se tornando cada vez mais comum.

1.1 Contexto e Problema

O padrão wireless IEEE 802.11 define um protocolo de controle de acesso ao meio (MAC), que é responsável por garantir o compartilhamento de acesso ao meio através da uma função de coordenação distribuída (DFC). Essa função define dois mecanismos para controle de colisões: um básico e um opcional.

O mecanismo básico para controle de colisões é o CSMA/CA - (*Carrier-Sense Multiple Access*), que "escuta"o canal para determinar se existem transmissões acontecendo naquele meio, caso não existam, então a transmissão é feita, caso contrário a estação continua escutando o canal até que seja o mesmo esteja livre para transmissão.

Contudo, redes wireless de grandes extensões sofrem com um problema conhecido como estação escondida, ou estação oculta, que é quando duas ou mais estações em uma mesma

rede, tentam fazer uma transmissão a um ponto de acesso, porém essas duas estações não estão no mesmo raio de sinal, dessa forma escutam o canal e concluem erroneamente que o canal está livre e tentam transmitir ao mesmo tempo, ocasionando assim uma colisão de pacotes.

Para resolver esse problema o IEEE propôs um mecanismo opcional, que consiste no uso de dois quadros de controle para prevenção de colisões, os quadros RTS (*Request to Send*) e CTS (*Clear to Send*), no qual antes de iniciar uma transmissão a estação envia um frame RTS, solicitando permissão para poder iniciar o processo de transmissão, e aguarda um CTS confirmando que o meio está livre e a transmissão pode ser iniciada, caso a estação esteja livre para o recebimento. Desse modo, todas as demais estações que estiverem no mesmo raio de alcance de sinal do AP(*Access Point*), escutarão o frame CTS concluindo assim que uma transmissão está prestes a ser iniciada, e que devem adiar suas transmissões por um determinado período de tempo.

Dessa maneira o mecanismo resolve o problema do terminal escondido e praticamente elimina o problema de colisões em redes wireless. Porém o uso desse mecanismo além de gerar um *overhead*(sobrecarga) na rede reduz sua taxa de transferência, uma vez que para cada transmissão dois quadros de controle adicionais são enviados.

Portanto o uso desse mecanismo só é aconselhável para *frames* (quadros) considerados grande, visto que nesse tipo de pacotes a probabilidade de colisões são grandes, por conta na demora na sua transmissão. Para definir a partir de que tamanho de frame o mecanismo será ativado, é proposto um mecanismo denominado RTS *Threshold* (limiar RTS).

De acordo com (MORIMOTO, 2008) o valor padrão desse limiar pode variar de 0 até o seu tamanho máximo que é definido em 2347 bytes, se o valor do limiar for muito baixo, significa dizer que o recurso RTS/CTS será usado com mais frequência, ocasionando uma possível queda no desempenho da rede. Tendo em vista o conhecimento prévio dessas informações, é possível identificar uma possível vulnerabilidade existente nesse mecanismo, onde um usuário mal intencionado poderia introduzir na rede frames de tamanho máximo em um curto período de tempo, gerando dessa forma uma inundação de quadros RTS/CTS, resultando em um overhead bastante significativo e ocasionando uma possível negação de serviço na rede. 0

1.2 Objetivos

1.2.1 Objetivo Geral

Tendo em vista a problemática apresentada no capítulo de introdução, o presente trabalho tem como objetivo principal apresentar e analisar um novo tipo de ataque de negação de serviço direcionado ao mecanismo de prevenção de colisão RTS/CTS, bem como avaliar o potencial impacto gerado pelo mesmo às redes sem fio baseadas no protocolo

IEEE 802.11.

1.2.2 Objetivos Específicos

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

- Verificar a eficácia de um novo tipo de ataque direcionado ao mecanismo RTS/CTS.
- Realizar experimentos e avaliar o impacto do ataque no desempenho da rede.
- Propor possíveis métodos de prevenção e mitigação do ataque.
- Melhorar o desempenho da rede

1.3 Organização do Trabalho

A organização do trabalho foi feita de acordo como descrito a seguir:

O capítulo 2 apresenta o Referencial Teórico, que contém todos os conceitos básicos sobre assuntos relacionados com o trabalho em questão, afim de auxiliar o leitor a se familiarizar com o assunto.

O capítulo 3 apresenta uma visão geral dos trabalhos científicos relacionados ao tema proposto neste presente trabalho, bem como uma análise geral sobre os mesmos.

O capitulo 4 mostras de maneira resumida o problema a ser trabalhado, bem como os testes feitos para analisar os efeitos gerados na rede após o ataque proposto nesta abordagem.

No capítulo 5 é realizada uma discussão sobre o resultado dos testes realizados.

Já no capítulo 6 são abordados algumas sugestões para possíveis métodos para mitigação do ataque proposto no presente trabalho.

Por fim no capítulo 7 são apresentadas as considerações finais e a conclusão, dos resultados obtidos no trabalho, fazendo uma recapitulação dos objetivos e se eles foram satisfeitos ou não.

2 Referencial Teórico

2.1 Redes de Computadores

Segundo (MORAES; CIRONE, 2003), entende-se por redes de computadores um conjunto de dois ou mais dispositivos, que são chamados de nós[1] , que usam protocolos em comum para compartilhar informação e recursos entre si, por meio de uma conexão, podendo ser por fio de cobre, fibra ótica, ondas de rádio e também via satélite, ou até mesmo por uma conexão híbrida, que use mais de um meio de conexão ao mesmo tempo.

As redes de computadores surgiram para suprir a necessidade de troca de informações com segurança entre máquinas distintas, por meio de protocolos regras ou convenções. Independentemente do tamanho e do grau de complexidade, o objetivo básico de uma rede é garantir que todos os recursos disponíveis sejam compartilhados rapidamente, com segurança e de forma confiável. Para tanto, uma rede de computadores deve possuir regras básicas e mecanismos capazes de garantir o transporte seguro das informações entre os elementos constituintes (RIBEIRO et al., 2014).

2.2 Sistemas Distribuídos

(COLOURIS; DOLLIMORE; KINDBERG, 2007) conceitua sistemas distribuídos como um “Sistema no qual os componentes de Hardware e Software localizados em uma rede de computadores se comunicam e coordenam suas ações somente por troca de mensagens.

Tanto para (COLOURIS; DOLLIMORE; KINDBERG, 2007) como (TANENBAUM, 2003) a principal diferença entre uma rede de computadores e um sistema distribuído é que, num sistema distribuído, a existência de vários computadores autônomos interconectados é evidente para o usuário, onde o mesmo não necessita saber da existência de múltiplos processadores. Ele simplesmente digita um comando e este comando é executado. A tarefa de escolher o melhor processador, mover e buscar arquivos, tratando os resultados, é tarefa do sistema de rede ou sistema operacional.

2.3 Redes Wireless

As redes IEEE 802.11 são redes locais sem fio capazes de interligar dispositivos em uma mesma infraestrutura de rede, porém sem a necessidade de cabos para a transmissão de dados, visto que essa transmissão ocorre por meio de ondas de rádio ou infravermelho. Com

[1] Em redes de computadores nós são pontos de interseção, conexão ou união de vários elementos, sejam eles computadores ou equipamentos de uma rede(MORAES; CIRONE, 2003)

isso as redes wireless vem sendo cada vez mais utilizadas pelos mais variados dispositivos eletrônicos portáteis, tendo em vista sua portabilidade.

O funcionamento das redes wireless ocorre quando é estabelecido uma comunicação de dados através de pontos específicos de uma rede, onde os dados são modulados e transmitidos através de ondas eletromagnéticas.

Justamente pelo meio de transmissão dos dados das redes sem fios trafegarem pelo ar, ela se torna menos segura que as redes cabeadas, já que o atacante basta está na área de alcance do sinal para conseguir interceptar o trafego de dados na rede (OLIVEIRA, 2010).

Atualmente o foco das redes de computadores sem fio (Wireless) se encontra no contexto das redes locais de computadores (Wireless Local Area Network - WLAN), tanto em soluções proprietárias como no padrão do IEEE. Algumas empresas como IBM, CISCO, Telecom e 3COM, colocaram em prática alguns padrões proprietários, porém hoje essas e outras empresas baseiam seus produtos no padrão do IEEE devido às vantagens que o padrão aberto oferece: interoperabilidade, baixo custo, demanda de mercado, confiabilidade de projeto, entre outras (TELECO, 2008).

As redes wireless possuem algumas vantagens e desvantagens em relação às redes cabeadas, que podem ser vistas na tabela 1.

2.4 Segurança da Informação

A segurança é um fator chave quando se fala de informação, tendo em vista que a informação é um dos bens mais valiosos tanto para organizações quanto para pessoas comuns.

A norma ABNT NBR ISO/IEC 27002 enfatiza que a Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

A identificação dos ativos físicos, tecnológicos e processos que estão atrelados ou manipulam as informações e suas classificações quanto aos possíveis riscos é um processo fundamental, haja vista a importância desses ativos para as instituições. A gestão do risco de cada ativo será um norteador para as ações da Segurança da Informação (STANDARD, 2015)

Segundo (LOUREIRO, 2008), A segurança da Informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

Para garantir a segurança da informação devem ser adotados três princípios básicos, o princípio da confidencialidade, onde somente pessoas autorizadas podem ter acesso a determinada informação. O princípio da integridade que afirma que os dados não podem

Tabela 1: Vantagens e desvantagens do uso de redes wireless em relação a redes cabeadas.

Vantagens	Desvantagens
Mobilidade - oferecem a liberdade de deslocamento mantendo-se a conexão.	***Qualidade de serviço*** - a qualidade do serviço provido ainda é menor que a das redes cabeadas.
Simplicidade - configuração fácil e rápida e simples da rede, sem cabos a serem instalados.	***Interferência*** - as interferências no sinal nas redes Wi-Fi sempre serão aspectos de preocupação perante os usuários.
Flexibilidade - podem ser instaladas em locais praticamente impossíveis para cabos e facilitam configurações temporárias e remanejamentos.	***Distorção por percursos múltiplos (Multipath)*** – devido as reflexões do sinal transmitido provocado por diferentes superfícies ao longo do trajeto, o sinal percebido pelo receptor é distorcido, piorando a qualidade do sinal.
Baixo Custo – se considerado o custo global da rede e não o preço individual dos equipamentos, as WLANs reduzem os custos de instalação porque dispensam cabeamento, por isso, a economia é ainda maior em ambientes sujeitos a mudanças frequentes	***Segurança*** - em uma rede sem fio é mais difícil garantir a segurança, uma vez que o meio de transmissão é aberto a qualquer um que esteja no perímetro geográfico do transmissor. Esta segurança é feita, normalmente, através de criptografia, o que acarretará no aumento de custos e degradação de desempenho.
Interoperabilidade - entre os equipamentos WLANs de marcas diferentes.	***Handoff*** - devido à possibilidade de deslocamento do terminal sem fio, o sistema deve garantir a conectividade conciliando o handoff entre as fronteiras de transmissão e o roteamento do tráfego.

ser criados, alterados ou removidos sem autorização. Alguns mecanismos de integridade são a assinatura[2] digital e algoritmos de hash[3] . E o princípio da disponibilidade que fala que informação está disponível a pessoas autorizadas sempre que necessário. Protocolos de alta disponibilidade podem garantir isso.

Com a crescente popularização de redes wireless públicas os usuários diariamente são expostos a riscos que podem comprometer a integridade e confidencialidade das informações, com isso a aplicação de políticas de segurança da informação nesses locais seria de extrema importância, tendo em vista que a adoção dessas práticas ajudaria a proteger e minimizar os riscos e poderiam vir a ocorrer nesses ambientes.

2.5 Ataques de Negação de Serviço

Os ataques DoS, ou ataques de negação de serviço são feitos não com o objetivo de invadir o sistema, mas sim com o propósito de torná-lo indisponível. O que os torna preo-

[2] Método de segurança usado para validar documentos digitais(INFORWESTER, 2016).

[3] Algoritmo que mapeia dados grandes e de tamanho variável para pequenos dados de tamanho fixo (TECHTUDO, 2012)

cupantes é que eles podem ser lançados contra qualquer host[4] conectado à Internet. Não é necessário que serviços com vulnerabilidades de segurança estejam ativos(MORIMOTO, 2008).

Nesta seção são apresentadas as formas existentes de negação de serviço. São abordadas ainda as características da arquitetura da Internet que possibilitam a execução destes ataques, bem como são apresentados os principais fatores que motivam os atacantes a interferir em um serviço.

2.5.1 Tipos de Ataques de Negação de Serviço

2.5.1.1 Denial of Service DoS

De acordo com (LAUFER et al., 2005) o ataque do tipo DoS (*Denial Of Service*), também conhecido como ataque de negação de serviço, é uma tentativa de fazer com que aconteça uma sobrecarga em um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus utilizadores. Para isso, o atacante utiliza técnicas enviando diversos pedidos de pacotes para o alvo com a finalidade de que ele fique tão sobrecarregado que não consiga mais responder a nenhum pedido de pacote. Assim, os utilizadores não conseguem mais acessar dados do computador por ele estar indisponível e não conseguir responder a nenhum pedido.

Diferentemente de ataques DDoS[5], nesse tipo de ataque apenas um único computador faz vários pedidos, afim de sobrecarregar servidores e redes. Esse ataque é o mais simples de negação de serviço não sendo o mais efetivo, tendo em vista que esse ataque utiliza apenas um atacante, e desta maneira o ataque só é efetivo se direcionado a servidores fracos, redes com pouca banda, ou computadores com baixas especificações.

2.5.1.2 Distributed Denial of Service DDoS

Ataque DDoS é um tipo de ataque DoS, porem de dimensões bem maiores, pois esse tipo de ataque se utiliza de vários computadores para atacar uma máquina especifica, distribuindo a ação entre essas várias maquinas. Tais ataques tem grande visibilidade na mídia, pois é um dos ataques mais comuns na internet.

Os ataques de negação de serviços distribuídos necessitam de uma grande quantidade de computadores que façam parte do ataque, para isso uma das melhores formas encontradas pelos "atacantes" é de fazer o uso de programas de ataque DDoS por meio de vírus ou softwares maliciosos visando infectar e disseminar pequenos programas para ataques DoS, com o intuito de "escravizar" uma grande quantidade de maquinas. Geralmente os usuários das maquinas escravizadas nem sabem que sua máquina está sendo utilizadas para

[4] Por definição, *host* é qualquer computador ou máquina conectado a uma rede, que conta com número de IP e nome definidos(TECHTUDO, 2012).

[5] Ataque de negação distribuído, onde uma máquina usa várias outras com com objetivo de sobrecarregar um sistema ou serviço(TECMUNDO, 2011).

tais ataques, com isso os "atacantes" conseguem camuflar a máquina principal do ataque, já que a quantidade de maquinas que participam do ataque é muito grande(OLIVEIRA et al., 2007).

OLIVEIRA et al. explica que uma das formas mais comuns de DDoS se utiliza de botnets que de forma sucinta é uma rede formada por diversos computadores infectados, onde essas maquinas serão controladas remotamente para fazer ataques DDoS.

Quando um computador é infectado e passa a fazer parte de uma rede DDoS, ou botnet, esta máquina passa a ser chamada de "zumbi", onde após a contaminação, tais maquinas recebem comandos de outras máquinas denominadas de "mestres", que por sua vez recebem orientações e instruções do atacante.

As máquinas zumbis, são responsáveis por gerar o tráfego que irá resultar na negação do serviço e podem ser controladas por um ou vários mestres, com isso a identificação e rastreamento do autor do ataque se torna bastante difícil.

Depois de infectadas as máquinas enviam vários pacotes de dados a um alvo, até que este determinado alvo não consiga processar e responder tantas requisições e com isso começam a negar serviço.

A figura 2 mostra a topologia de um ataque DDoS.

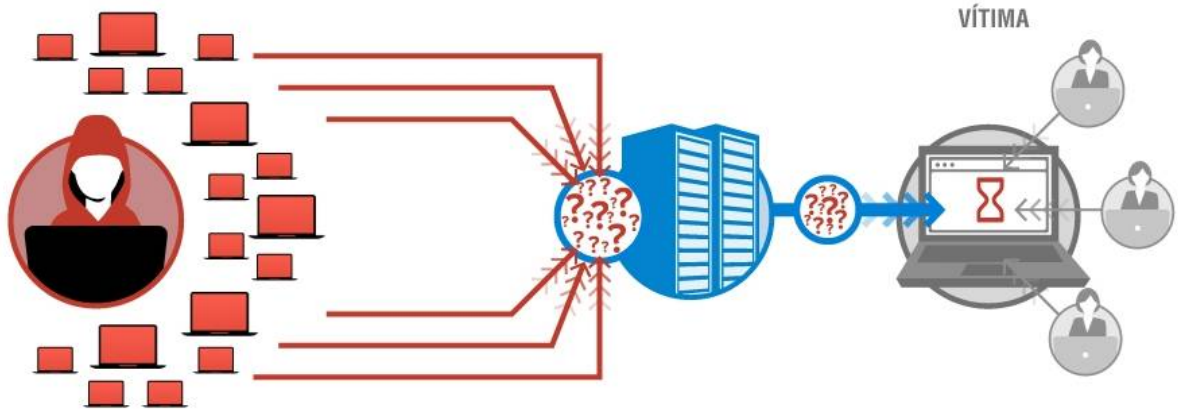

Figura 1: - Topologia de um ataque DDoS

Fonte:verisign.com

2.6 Sub-camada de Acesso ao Meio MAC

Originalmente IEEE definiu um protocolo de acesso ao meio da subcamada MAC, denominado DFWMAC (Distributed Foundation Wireless Médium Access Control), que suporta dois métodos de acesso, um distribuído e um centralizado, que é opcional. Este protocolo também trata de problemas relacionados com roaming (BIANCHI, 2000).

O padrão IEEE 802.11 define ainda dois mecanismos de acesso ao meio, o DFC (Distributed Coordenation Function), que é o mecanismo padrão onde as estações devem competir entre si para obter acesso ao meio (contention mode) e o PFC (Point Coordenation Function), que funciona de forma centralizada onde o AP é o responsável o "pooling"com as estações que estão na rede (contention free-mode), verificando qual estação deseja realizar a transmissão e deste modo evitando que as estações disputem entre si (GAST, 2005)

2.6.1 (DFC (Distributed Coordenation Function)

A DCF é o mecanismo de acesso fundamental no IEEE 802.1 I MAC, mais conhecida como CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) com reconhecimento, e tem como principal objetivo previnir colisões. Esse mecanismo funciona de maneira diferente da função CSMA/CD que é empregada em redes cabeadas, e controla as colisões quando elas ocorrem.

Para que essa prevenção de colisões seja possível, a estação sente o meio para determinar se o canal está ocioso por um período maior que o tempo de DIFS (distributed interframe space). Se o meio estiver livre, então a estação transmite o quadro, caso contrário ela aguarda o final da transmissão. Porém existem casos em que ocorrem colisões durante a transmissão, nesse caso a estação permanece analisando o canal até que ele fique disponível por um espaço de tempo igual a DIFS e então inicializa um contador que possui uma duração aleatória (backoff).(SOARES; GUIDO; COLCHER, 1995)

Após cada transmissão com ou sem colisão, a rede fica em um modo onde as estações só podem começar a transmitir em intervalos de tempo a elas pré-alocados. Dessa forma ao findar uma transmissão, as estações alocadas ao primeiro intervalo têm o direito de transmitir. Se não o fazem, o direito passa as estações alocadas ao segundo intervalo, e assim sucessivamente até que ocorra uma transmissão, quando todo o processo reinicia.

A figura 2 ilustra o funcionamento básico do método DFC, onde pode ser notado que cada estação "sente"o meio durante um intervalo de tempo antes de iniciar propriamente a transmissão. A duração deste intervalo de tempo determina a prioridade de acesso ao meio, e no 802.11 são especificados três parâmetros de "prioridade", SIFS, PIFS e DIFS.

(TELECO, 2008) define esses três parâmetros como:

- Inter Frame Space (DIFS) – espaço entre quadros da DCF. Este parâmetro indica o maior tempo de espera, monitorando o meio, aguardando no mínimo um intervalo de silêncio para transmitir os dados.

- Priority Inter Frame Space (PIFS) – espaço entre quadros da PFC. Tempo de espera entre o DIFS e o SIFS (prioridade média). Envia quadros de contenção de superquadros e é usado para o serviço de acesso com retardo.

- Short Inter Frame Space (SIFS) – é usado para transmissão de quadros carregando respostas imediatas (curtas), como ACK.

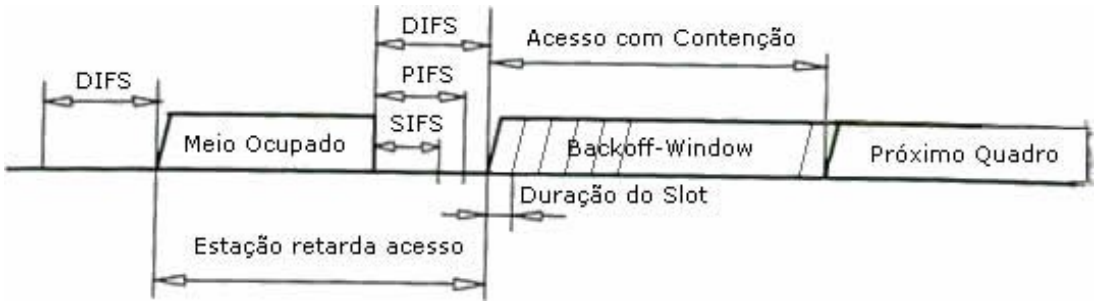

Figura 2: - DFWMAC Básico

Fonte:André Pimenta Mathias – UFRJ.

Devido à necessidade de eficiência para realização das transmissões, o DCF que possui a função de coordenar o funcionamento de uma rede sem fio, trabalha com segmentação de tempo, através de slots de tempo. Assim, a estação inicia a transmissão no início do segmento e é necessário que a duração deste slot permita que todas as estações percebam a existência de uma (MENDES, 2008).

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

A IEEE 802.11 define ainda um esquema de acesso opcional para a redução de colisões no meio de comunicação, esse método faz o uso de quadros de pedidos (Request to Send RTS) e permissões (Clear to Send - CTS) para a transmissão de dados.

A figura 3 mostra a estrutura de um frame RTS, que possui 20 bytes de comprimento, sendo dividido em 5 campos: FC (Frame Control), Duração, Endereço 1 (RA), Endereço 2 (TA) e FCS (Frame Check Sequence). O campo FC possui 2 bytes e permite identificar o tipo de quadro e provê algumas informações de controle. O campo Duração possui 2 bytes e informa o tempo de reserva do canal. Seu valor máximo é de 32.767 microssegundos (IEEE, 2010).

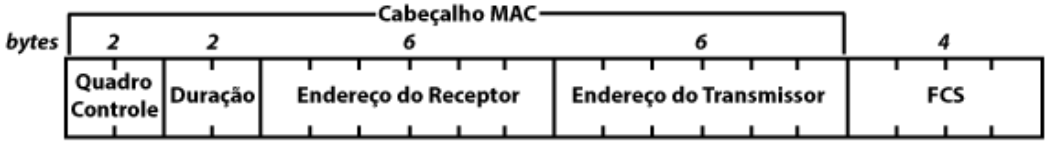

Figura 3: - Frame RTS - (IEEE, 2010)

Fonte: Elaborada pelo autor, conforme IEE 802.11.

Os campos Endereço 1 e 2 possuem 6 bytes cada e representam, respectivamente, o endereço do receptor e do transmissor. O campo FCS possui 4 bytes e é preenchido com um CRC-32 para a detecção de erros.

Diferentemente do quadro RTS, o quadro CTS possui apenas 14 bytes de comprimento, sendo dividido em 4 campos: FC (Frame Control), Duração, Endereço 1 (RA) e FCS (Frame Check Sequence). O campo FC possui 2 bytes e permite identificar o tipo de quadro e provê algumas informações de controle. O campo Duração possui 2 bytes e informa o tempo de reserva do canal, tendo seu valor máximo de 32.767 microssegundos(IEEE, 2010).

A estrutura básica do quadro CTS pode ser observado na figura 4.

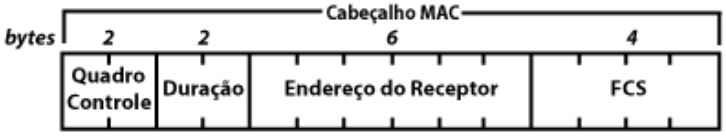

Figura 4: - Frame CTS - (IEEE, 2010)

Fonte: Elaborada pelo autor, conforme IEE 802.11.

O mecanismo RTS/CTS foi proposto para tratar o problema conhecido como estação escondida (hidden node).

Esse método foi proposto para tratar o problema conhecido como estação escondida (hidden node), que é ilustrado na figura 5.

Figura 5: - Problema do terminal escondido

Fonte: Elaborada pelo autor, conforme IEE 802.11.

Existem 3 terminais A, B e C. B está ao alcance dos sinais transmitidos por A e C, mas estes estão fora de alcance um do outro. Se o terminal A estiver transmitindo para B e o terminal C deseja também transmitir para B, o terminal C concluirá erroneamente que o canal está livre, uma vez que ele está fora do alcance de A que no momento é o terminal que está fazendo a transmissão para B. Se C começar a transmitir vai interferir

com a recepção em B ocasionando uma colisão de pacotes. Neste caso C é denominado o terminal escondido para A.

Com o mecanismo RTS/CTS esse problema é resolvido, tendo em vista que quando uma estação transmissora deseja enviar um quadro de dados, ela pode primeiramente enviar um quadro RTS à 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 dessa forma o seu acesso ao meio(NETO, 2015).

A figura 6 ilustra como é feita a comunicação.

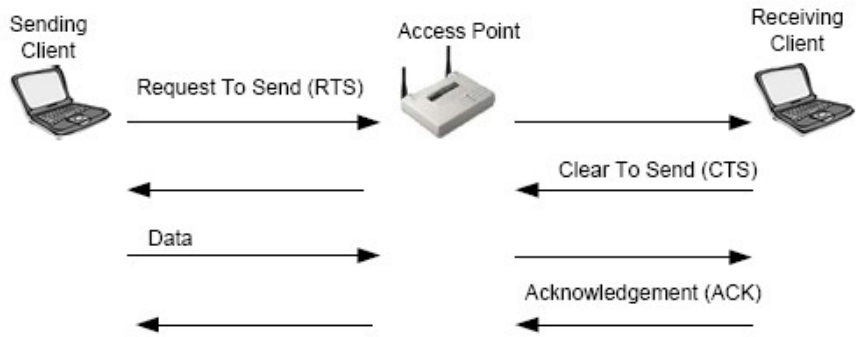

Figura 6: - Comunicação RTS/CTS

Fonte:(TELECO, 2008).

O uso do RTS/CTS praticamente elimina o problema de colisões, mas em compensação reduz a taxa de transferência da rede, já que passa a ser necessário transmitir dois frames adicionais para cada frame de dados.

Devido a isso, o uso desse mecanismo é recomendável apenas para frames grandes, que demoram mais para serem transmitidos e são mais suscetíveis a colisões. Frames pequenos continuam sendo transmitidos diretamente reduzindo o overhead da rede, contudo ainda existem riscos de ocorrerem colisões na transmissão.

O uso desse mecanismo pode ser feito de 3 formas, a primeira forma é "Desligado", nesse caso o mecanismo é completamente desabilitado e a rede opera somente com o mecanismo padrão CSMA/CA. A segunda forma de utilização do mecanismo é "Ligado", onde cada estação antes de iniciar qualquer transmissão enviará requisição através de um quadro RTS e será respondido com um CTS, porém esse não é o uso mais adequado, tendo em vista que dessa forma a rede sofrerá uma grande perca de desempenho. A última forma é a "Ativado com um gatilho", que é a forma mais eficiente de utilização do mecanismo

RTS/CTS, pois nela é possível ativar o mecanismo somente após o tamanho do pacote ultrapassar um limiar predefinido.

Esse limiar é conhecido como RTS Threshold, e permite justamente definir a partir de que tamanho de frame o sistema é usado. Por default, o tamanho máximo de frame (definido na opção Fragmentation Threshold) é de 2346 bytes e o RTS Threshold é de 2347 bytes. Esta é uma forma polida de desativar o recurso, já que se o RTS Threshold é maior do que o tamanho máximo dos frames, significa que a regra nunca será aplicada(SHEU et al., 2002).

Esse parâmetro permite delimitar a partir de que tamanho de frame o mecanismo RTS/CTS vai ser usado. Para auxiliar nesse controle existe ainda um outro mecanismo denominado Limiar de fragmentação que define o tamanho máximo de frame que será transmitido pelo ponto de acesso, ou seja, quando um pacote de dados ultrapassar esse valor ele será fragmentado e enviado em frames separados.

Por padrão o limite máximo do Limiar de fragmentação é de 2346 bytes, já o valor máximo do RTS Threshold é de 2347. Dessa forma para desabilitar a troca de RTS/CTS bastaria apenas setar o valor do limiar de fragmentação menor do que o Limiar RTS, pois com isso o frame nunca irá atingir o limiar para ativação do RTS Threshold, pois o pacote seria fragmentado assim que atingisse o limiar de fragmentação.

2.6.3 Ataques aos quadros RTS e CTS

Os ataques direcionados ao mecanismo RTS/CTS, consistem principalmente em alterar os valores contidos no campo de duração desses quadros de controle, visando reservar o canal de transmissão por um tempo adicional, gerando assim uma queda de desempenho na rede afetada por esse tipo de ataque.(SAWWASHERE; NIMBHORKAR, 2014)

(RAY; STAROBINSKI, 2007) Aborda um desses ataques, que é o ataque de injeção de quadros RTS/CTS falsos. No qual uma estação maliciosa cria e envia quadros RTS e CTS falsos afim de bloquear o uso do canal de comunicação pelos nós vizinhos, através de uma falsa reserva desse canal.

(NETO, 2015) salienta que se Atacantes mais experientes podem ainda manipular o valor contido no campo de duração desses quadros. Esse valor instrui as estações vizinhas por quanto tempo o canal não poderá ser utilizado por elas.

Outro ataque a esse tipo de quadro, é o ataque de reinjeção abordado por (MYNENI; HUANG, 2010). Onde a estação escuta o canal com o objetivo de capturar quadros RTS ou CTS enviados por nós legítimos da rede e retransmitir esses quadros na rede.

Ataques direcionados a esse mecanismo só são possíveis porque o padrão 802.11 não implementa nenhum mecanismo de autenticação aos quadros de controle, os tornando assim vulneráveis a ataques de negação de serviço.

3 Trabalhos Relacionados

Desde 1997 com a criação do padrão IEEE 802.11 até os dias atuais segurança em redes sem fio é amplamente discutida e estudada. Do mesmo modo que, os ataques a este tipo de rede também evoluem com a mesma intensidade (COLOURIS; DOLLIMORE; KINDBERG, 2007).

Neste capítulo, serão apresentados ao todo nove trabalhos, onde todas as abordagens são relacionadas a ataques e vulnerabilidades existentes nos quadros de controle, que exploram a principalmente falta de mecanismos para a garantia de integridade dos mesmos em redes baseadas no padrão 802.11.

Em (RAY; STAROBINSKI, 2007) é utilizada uma abordagem estatística para detectar um ataque NAV na camada MAC em redes wireless. Onde uma vez que todo nó retransmite um quadro CTS em resposta a um quadro de RTS, o atacante pode modificar o campo de duração NAV para o tamanho máximo, e com isso monopolizar o meio, para que outras estações não possam acessar o mesmo, este problema foi denominado como ataque de NAV.

Para identificar este ataque, os autores utilizaram se de algumas informações estatísticas, como: média e desvio padrão da rede. Porém esta técnica é bastante ineficaz, tendo em vista que um usuário mal-intencionado, pode simplesmente explorar a falha tentando mantes as estatísticas da rede como normal, impossibilitando assim a identificação do ataque.

(NAGARJUN et al., 2013) Analisaram um ataque aos quadros de controle RTS/CTS que explora o mecanismo de reserva média das redes wireless, através do campo de duração. O seguinte ataque consiste em modificar o campo de duração contido nos quadros RTS/CTS, onde uma vez que os nós legítimos da rede responderão a uma requisição RTS com uma confirmação CTS, e nisso um invasor poderia explorar os nós legítimos para propagar CTS com o campo de duração manipulado, reservando assim o canal por um tempo adicional

Além disso eles propuseram ainda algumas variantes destes ataques, com o objetivo principal de provar a vulnerabilidade dos quadros de controle a esse tipo de ataque. Por fim eles criaram uma ferramenta com ambiente gráfico, com a capacidade de criar ambientes de testes para ataques aos quadros RTS/CTS e após isso gerar gráficos adequados para analisar o comportamento destes ataques.

Já (BELLARDO; SAVAGE, 2003) buscou fazer uma descrição e identificação de vulnerabilidades nos serviços de gerenciamento e acesso de mídia 802.11, que são vulneráveis a ataques de negação de serviço.

Para verificar e comprovar a eficácia de tais ataques, é feita uma simulação destes ataques através da ferramenta ns2 (Network Simulator 2). Essa simulação consistiu em

enviar quadros RTS/CTS e quadros de reconhecimento (ACK) com a duração máxima. Ao final da simulação ficou comprovado que o canal pode ser completamente bloqueado durante este ataque, consequentemente gerando uma negação de serviço na rede. Por fim descrevem e implementam contramedidas, não criptográficas para serem implementadas para sanar as vulnerabilidades encontradas durante os testes.

No decorrer do trabalho eles mostram que atualmente a maioria dos dispositivos não implementam adequadamente as especificações da camada MAC do padrão 802.11, pois estão definindo incorretamente o NAV.

Estes autores concluíram ainda que o ataque de detecção de portador virtual é muito mais complexo de se identificar, quando comparado ao ataque de autenticação MAC 802.11.

O trabalho de (MALEKZADEH; SUBRAMANIAM AZIM, 2011) tem como principal objetivo demonstrar o efeito que ataques de negação de serviço tem sobre uma rede. Para isso os autores primeiramente fazem uma simulação do ataque utilizando o simulador de redes OMNeT++ e após os testes serem feitos em ambiente simulado, os mesmos também são reproduzidos em um cenário real, com o objetivo principal de validar os testes feitos em ambiente simulado, demonstrando que os resultados alcançados, são aceitáveis.

Para os testes em ambiente simulado, os autores inicialmente verificaram o throughput e o delay da rede com tráfego gerado a partir de segmentos TCP *(Transmission Control Protocol)* e UDP *(User Datagram Protocol).*

Verificando se os resultados dos testes, pode se constatar uma queda bastante acentuada no throughput para 0Bps e um aumento bastante relevante no delay, que passou de 0 para aproximadamente 6 segundos, durante o tempo em que o teste foi executado. Outro fator que foi levado em conta na realização da simulação foi a quantidade de pacotes perdidos, durante a simulação que foi de 37,90%, que pode ser considerado uma quantidade bastante elevada, se comparada a uma situação normal.

Após a análise dos resultados da realização dos testes os autores puderam constatar que é completamente viável e condizente o resultado dos testes em ambiente simulado com os testes feitos em um cenário real.

Com o objetivo de fornecer uma solução para proteger todos os quadros de controles contra ataques do tipo frame control. (MYNENI; HUANG, 2010) sugerem a proteção dos quadros de controle, por meio de um código de autenticação (MAC), que utiliza um método de geração e distribuição de dados empregado no protocolo 802.11f que possui 160 bits. Inicialmente o ponto de acesso, procura por outros pontos de acessos no canal, se se após essa busca não for encontrado nenhum AP no canal, será gerado um número K, que é enviado via conexão TCP a outras estações. Além desse número K, é gerado um número de sequência S, que toma por base a duração da reserva do canal contido nos frames RTS/CTS.

Porém esta técnica ainda não resolveu completamente o problema, pois os quadros de

controle estavam vulneráveis a ataques de replay. Desta forma eles preferiram por usar um número de sequência de 32 bits. Com isso no total essa proposta adicionou 192 bits, representando mais de 170% do tamanho de um quadro CTS no padrão de redes wireless, que possui 112 bits.

Consequentemente essa proposta torna se de certa forma inviável, já que adiciona um overhead bastante significativo na rede. Além disso através dos resultados obtidos nas simulações, foi possível observar que antes do ataque o throughput da rede era de 28.4 Mbps e após a realização do ataque esse mesmo parâmetro caiu para 27.6 Mbps um valor bastante pequeno, desse modo é possível constatar que os ataques realizados não obtiveram resultados satisfatórios.

O trabalho de (JÚNIOR; GONÇALVES, 2012) busca a proteção não apenas os quadros de controle RTS/CTS, mas sim todos os quadros de controle, para isso eles usaram um código de autenticação de mensagens de 64 bits, em conjunto com um número de sequência global de 32 bits. De forma que a geração do código de autenticação é feita utilizando o algoritmo conhecido como CBC-MAC (Cipher Block Caining-Message Authentication Code). Para a autenticação dos quadros os autores fazem o uso de uma chave criptográfica já empregada pelo protocolo IEEE 802.11i para a encriptação dos dados.

Para reduzir a quantidade de bits gerados após a modificação dos quadros do controle os autores removem o campo de FCS, que serve para checar a sequência dos quadros, esse campo pode ser removido sem nenhum prejuízo para a perca, pois com o método proposto é adicionado um código de autenticação de mensagens, para garantir a integridade do quadro.

A proposta apresentada por eles gera um overhead de apenas 64 bits, que pode ser considerado pequeno se comparado a outras propostas. Porém da proposta apresentada gerar um overhead baixo o esquema proposto por Jr. e Gonçalves 2011, se mostrou vulnerável a algumas falhas de segurança, tendo em vista que o mesmo utiliza o CBMAC, que de acordo com França 2015 é seguro apenas é seguro apenas quando o comprimento das mensagens sendo autenticadas é fixo.

Semelhantemente a (JÚNIOR; GONÇALVES, 2012) o trabalho proposto por (NETO, 2015)também propõe um esquema de segurança para todos os quadros de controle em redes wireless IEEE 802.1. de acordo com o autor, essa proposta se diferencia das outras por prover um alto grau de segurança, além de geram um baixo overhead, gerando assim um baixo impacto na rede. Esse trabalho possui proteção a ataques de reinjeção não possuindo vulnerabilidades no processo de geração de distribuição de chaves.

O método elaborado pelo autor consiste em adicionar dois novos campos aos quadros de controles já existentes, esses campos são os de MAC (Message Authentication Code), que tem o valor de 64 bit e o campo de NS (Número de Sequência Individual) de 32 bits. no qual o primeiro campo permitirá que os nós receptores possam fazer uma verificação da autenticidade e da integridade dos quadros de controle. Assim como em Jr e Gonçalves

2011 o campo de FCS é também removido sem geral nenhum prejuízo, em que o campo NS é encarregado de garantir que os nós serão capazes de detectar ataques de reinjeção. O método conta ainda com três módulos para garantir a proteção dos quadros de controle. Os módulos são: módulo de geração e distribuição de chaves, que estabelece a chave utilizada para autenticação, o segundo é o módulo contra ataques de reinjeção que representa um mecanismo de proteção contra ataques de reinjeção, e por fim o terceiro módulo, é o módulo de geração e verificação do MAC, que estipula os procedimentos para o envio e recepção de um quadro de controle.

Após os testes o autor mostrou que o impacto na vazão da rede foi reduzido em relação a outros métodos quando se emprega o mecanismo RTS/CTS. A tabela a seguir mostra de forma resumida os trabalhos apresentados nesta seção, bem como sua abordagem e por fim os resultados alcançados pelos seus autores.

(RIBEIRO et al., 2014) Aborda o problema de ataques de negação de serviço em redes sem fio 802.11, e utiliza o simulador OMNeT++ para fazer uma simulação do ataque e analisar o impacto gerado por esse tipo de ataque a esse tipo de rede. Posteriormente é apresentada uma abordagem para mitigação de um ataque desse tipo, buscando obter resultado expressivos para a melhoria das redes sem fio.

Para os testes os autores escolherem o ataque de negação de serviço a quadros de controle RTS/CTS, onde é abordada uma vulnerabilidade desses quadros de controle a ataques de inundação, que consiste enviar uma grande quantidade de quadros RTS em um curto espaço de tempo, buscando congestionar o servidor. Dessa forma, o ataque terá domínio completo do canal, negando serviço aos demais hosts na rede sem fio.

Após os resultados dos testes os autores puderam constatar que a medida que o ataque era executado o throughput da rede era reduzido, e esse número caia ainda mais a medida que o número de hosts era aumentado na rede. Foi possível constatar ainda que o método de mitigação proposto foi bastante eficaz, pois após o mesmo ser executado o throughput da rede voltou a subir.

Foi notado ainda que durante os testes, em alguns momentos o throughput da rede chegou a zero por alguns segundos, indicando que um congestionamento total na rede, interrompendo totalmente o tráfego na rede.

Por fim (ZOU; DENG, 2010) investigam as vulnerabilidades existentes na camada MAC das redes wireless. O trabalho foca mais especificamente em um ataque que consiste em forjar quadros CTS, onde o atacante envia pacotes CTS (Clear to Send) com valores NAV altos com o objetivo de monopolizar o canal de transmissão e consequentemente causar um ataque de negação de serviço na rede.

Os autores focam nesse tipo de ataque devido ao fato de que o IEEE não provê nenhum esquema de segurança para esses tipos de quadro, os tornando vulneráveis a diversos tipos de ataque

Ainda neste trabalho, os autores apresentam abordagem para detectar estas mensagens

de controle forjadas, no qual é feita a detecção de interferência permitindo que um nó alvo envie uma mensagem, que instrui os nós vizinhos a ignorar a mensagem de controle forjada. Dessa forma o canal volta a ficar livre para o tráfego normal de dados. Para comprovar o beneficio do método proposto é utilizado o simulador de redes ns2, que é um simulador de redes bastante utilizado na pesquisa e no ensino.

Como é pode ser visto, basicamente dois tipos de ataques são abordados: ataques que consistem na falsificação dos quadros de controle, e ataques que fazem o uso da reinjeção de pacotes na rede, porém todos tem o mesmo objetivo, que é gerar uma perca de desempenho na rede.

A principal diferença entre os trabalhos citados e a proposta deste trabalho, está no fato de que diferentemente dos trabalhos relacionados, o ataque apresentado no trabalho proposto consiste em explorar de maneira legítima uma possível vulnerabilidade do mecanismo RTS/CTS, porém sem modificar nem reinjetar quadros de controle falsos na rede, como é feito nas abordagens citadas. O presente trabalho busca apenas introduzir frames legítimos com o tamanho máximo em um curto período de tempo, resultando dessa forma em uma ativação desnecessária do mecanismo, degradando de maneira significativa o desempenho da rede.

A Tabela 2 mostra de maneira resumida a abordagem e os resultados dos trabalhos relacionados desta seção.

Tabela 2: Resumo dos trabalhos relacionados

Trabalho	Tipo de ataque	Proposta
Ray e Starobinski	Falsificação de quadros RTS/CTS	Validação,de RTS através um sensor da portadora.
Nagarjun et.al.	Modificação do campo de duração do quadro RTS	Verificar o impacto de ataques DoS em redes wireless 802.11
Bellardo e Savage	Negação de serviço por inundação de quadros RTS	Limitação do valor máximo do campo de duração
Malekzadeh e Subramaniam	Modificação do campo de duração do quadro RTS	Utiliza o,algoritmo HMAC-SHA-256 para autenticação dos quadros de controle
Mynemi e Huang	Reinjeção de quadros RTS	Mecanismo para gerar um número de sequência único, utilizado para a identificação de quadros falsos.
Jr. e Gonçalves	Falsificação/ Reinjeção de quadros RTS	Uso de um código de autenticação de mensagens de 64 bits e de um número de sequência global de 32 bits.
Neto	Falsificação/ Reinjeção de quadros RTS	Uso de um código de autenticação de mensagens de 64 bits e de um número de sequência individual de 32 bits.
Ribeiro et al.	Negação de serviço por inundação de quadros RTS	Após receber o pacote, faz uma verificação do tempo solicitado, comparando com o tamanho do pacote.
Zou e Deng	Ataque de falsificação de quadros CTS	Detecta a interferência na rede e envia uma mensagem aos nós vizinhos para ignorar o quadro de controle falsificado.

4 Descrição e Avaliação da Proposta

4.1 Descrição

O ataque abordado no presente trabalho consiste na injeção de pacotes de tamanho máximo da rede em um curto espaço de tempo com o intuito de ativar desnecessariamente o mecanismo de prevenção de colisões RTS/CTS, para causar uma inundação de quadros de requisição RTS.

Nesta situação, acontece um congestionamento de reserva de canal por causa do alto número de quadros de requisições. Em consequência disso, a rede sofrerá uma perca considerável de desempenho, podendo até mesmo negar serviço a outros hosts presentes na rede em questão.

4.2 Avaliação

A fim de atingir os objetivos de analisar a efetividade de um ataque de negação de serviço direcionado ao mecanismo RTS/CTS, bem como analisar o impacto do mesmo no desempenho de redes wireless 802.11, foram feitos diversos testes e simulações envolvendo diferentes cenários e situações, em que uma rede sem fio pode enfrentar em meio a estes ataques. Esta seção descreve a estrutura, topologia e a análise dos resultados obtidos em cada cenário de testes.

4.2.1 Estrutura do experimento

Para simulação do ataque primeiramente foi necessário a criação de uma rede wireless, padrão 802.11 com a topologia no modo infraestrutura, ou seja, todos os dispositivos na rede se comunicavam entre si através de um AP (Access Point), onde o mesmo estava equipado com o firmware Open WRT [1] que foi utilizado principalmente por contar com a capacidade de modificação do parâmetro RTS Threshold.

Para análise de desempenho foi utilizado o software Jperf [2] que funciona em modo cliente servidor, dessa forma foram utilizadas duas máquinas para desempenhar esses papéis na rede, e de acordo com a necessidade da simulação empregada em cada cenário, algumas outras máquinas foram introduzidas gradualmente na rede.

[1] Distribuição do GNU/Linux, altamente customizável, direcionada a sistemas embarcados

[2] Versão do Iperf com interface gráfica que um software utilizado para testar a largura de banda, podendo realizar injeção de pacotes para medir o desempenho de redes de computadores.

Para medir o impacto do ataque à rede, foram analisadas duas métricas, o *throughput*[3] e contagem de pacotes descartados *(drops)* na rede.

Outros parâmetros e configuração em relação aos testes, são descritos mais detalhadamente nos cenários de simulações que serão abordados a seguir.

4.2.2 Cenário I

No cenário I foi feito apenas um teste preliminar, que tinha como objetivo medir o troughput médio da rede, para posteriormente servir como base e parâmetro de comparação, para os cenários de simulações de ataques na rede.

Para este teste não foi necessário nenhuma estação conectada a rede, além dois dois hosts utilizados pela ferramenta Jperf.Como esse foi um teste apenas um teste preliminar para medir o throughput médio da rede, o mecanismo RTS Threshold estava inativo, tendo em vista que não havia necessidade de se utilizar o mesmo.

A topologia deste cenário pode ser vista na figura 7.

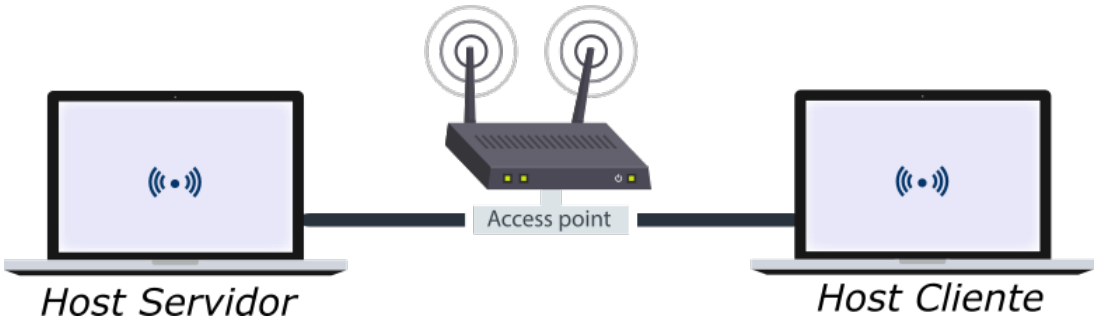

Figura 7: - Topologia utilizada para testes do cenário I.

O resultado obtido neste teste pode ser observado na figura 8, que mostra o gráfico gerado pela ferramenta após o término do teste.

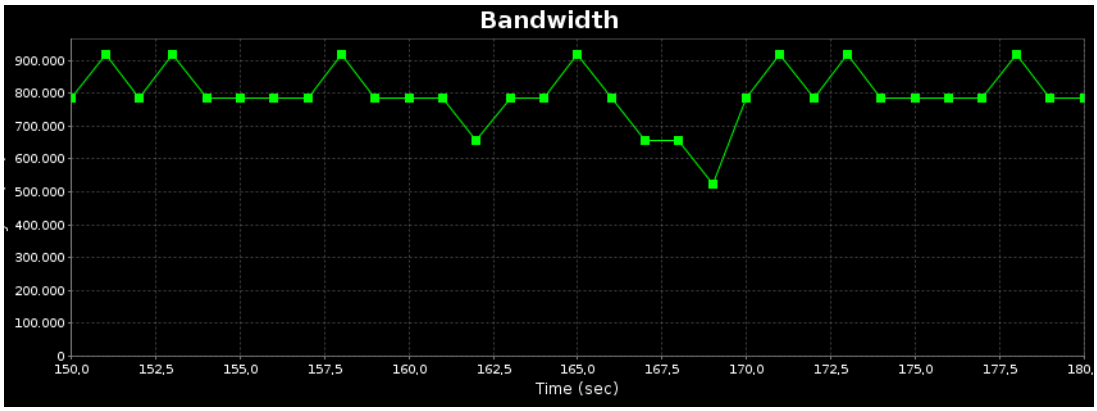

Figura 8: - Gráfico gerado pela ferramenta ao fim da simulação do primeiro cenário.

[3] é a quantidade de dados transferidos de um lugar a outro, ou a quantidade de dados processados em um determinado espaço de tempo(DICIONARIOINFORMAL.COM, 2013)

De acordo com o gráfico e resultados gerados pela ferramenta, é possível notar que a rede atingiu um troughput médio de 791896 Bytes/sec. Analisando os resultados do teste em questão, é possível notar ainda que apesar de algumas oscilações, a rede obteve um fluxo constante na largura de banda durante o decorrer do teste.

Com o resultado desse teste foi possível obter uma base de comparação para os testes feitos nos cenários seguintes.

4.2.3 Cenário II

Para esta simulação, foi necessário inicialmente ativar o mecanismo RTS Threshold no AP*Access Point)*, onde o mesmo foi configurado com o valor de 100 bytes, ou seja, qualquer quadro que fosse maior que esse limiar ativaria o uso do mecanismo RTS/CTS.

Dessa forma, novamente a ferramenta Jperf foi executada, tanto no host cliente quanto no host servidor para monitorar o *troughput* da rede. A partir disso, uma terceira estação foi introduzida na rede, onde esta máquina executava de ping para o AP, com tamanhos de pacotes de 200 bytes, ou seja, pacotes com o tamanho superior ao limiar RTS, induzindo assim o uso do mecanismo RTS/CTS a cada transmissão de dados, entre a estação maliciosa e o AP.

A topologia utilizada neste cenário, pode ser visualizada na figura 9.

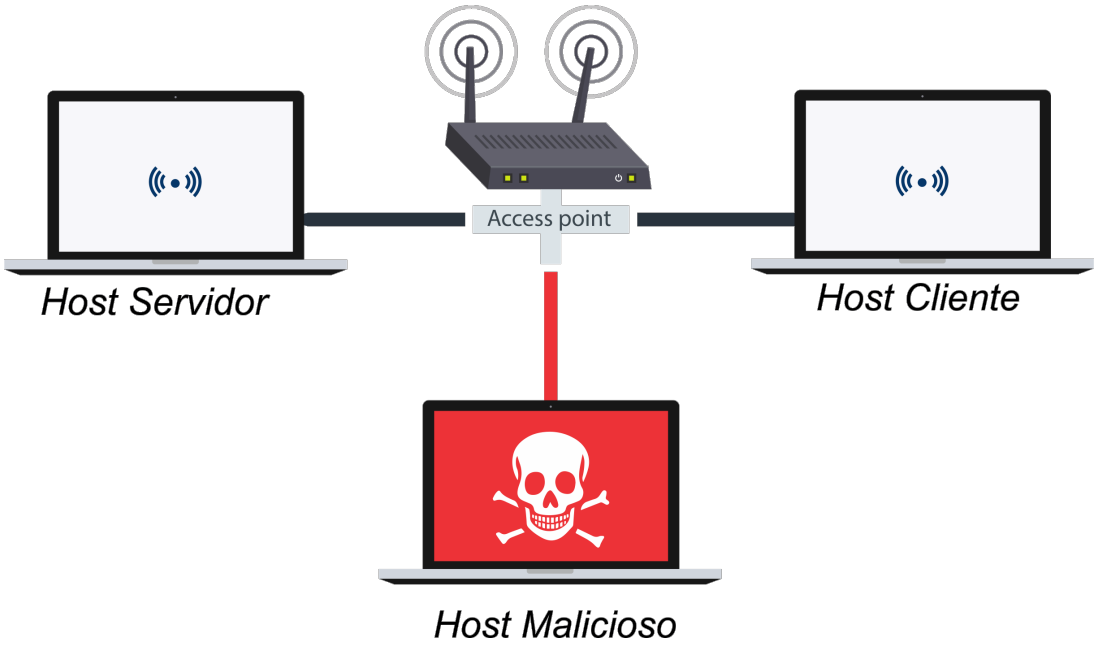

Figura 9: - Topologia utilizada para a simulação do cenário II.

O resultado gerado pelo Jperf desta simulação pode ser observado na figura 10.

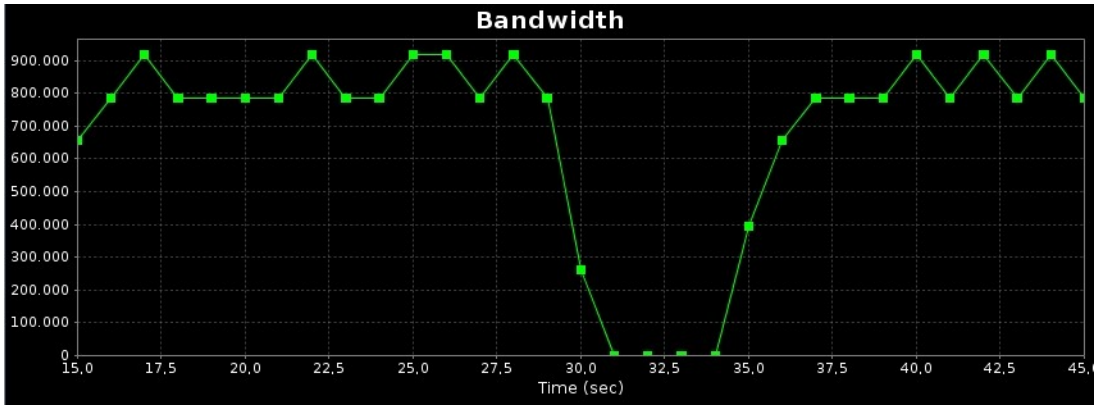

Figura 10: - Gráfico gerado pela ferramenta ao fim da simulação do segundo cenário.

Analisando os resultados gerados pela ferramenta, ao final dos testes foi obtido um troughput médio de 751512 Bytes/sec Bytes, aproximadamente 5% em relação ao throughput médio da rede no cenário em que a mesma não estava sendo atacada. Observando os mesmos resultados, é possível observar ainda que a variação do throughput sob ataque DoS varia a partir do início do ataque, onde o throughput chega a praticamente zero Bps por alguns segundos.

Contudo, embora neste cenário a simulação do ataque tenha conseguido degradar a rede, essa perda de desempenho foi bastante pequena.

Analisando este fato a conclusão pensada para a perda de desempenho ter sido mínima, está no fato de ocorrer no baixo tráfego de dados da rede, tendo em vista que para esta simulação foi introduzida apenas uma estação na rede, com isso a colisão de pacotes nesta situação é inexistente, já que o único tráfego gerado na rede é proveniente da estação maliciosa, dessa forma a perca de desempenho observada é causada apenas pelo overhead gerado pelo uso do mecanismo RTS/CTS.

4.2.4 Cenário III

A simulação feita neste cenário teve como objetivo reavaliar a o ataque simulado do cenário dois, tendo em vista que os testes desenvolvidos no cenário II tiveram resultados inconclusivos, haja vista que o baixo tráfego da rede impossibilitou uma melhor análise dos resultados.

Dessa forma a simulação feita neste cenário foi semelhante à descrita no cenário 2, porém nesta simulação além da estação maliciosa, foram adicionados mais 6 hosts lícitos na rede, com o objetivo de avaliar se realmente a quantidade de hosts estaria diretamente relacionada a quantidade de colisões ocorridas na rede, e se o ataque executado neste cenário seria de fato mais efetivo do que o ataque executado no cenário 2.

A topologia utilizada neste cenário, pode ser visualizada na figura 11.

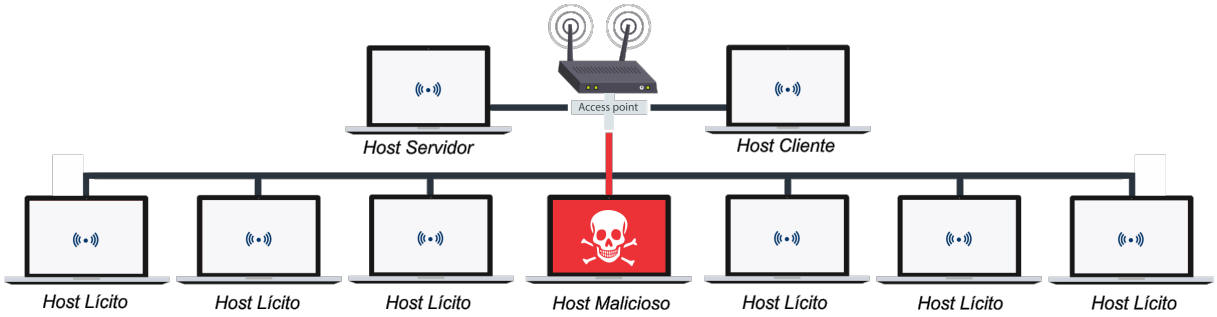

Figura 11: - Topologia utilizada para a simulação do cenário III.

Ao final dos testes realizados o jperf gerou o gráfico ilustrado na figura 12

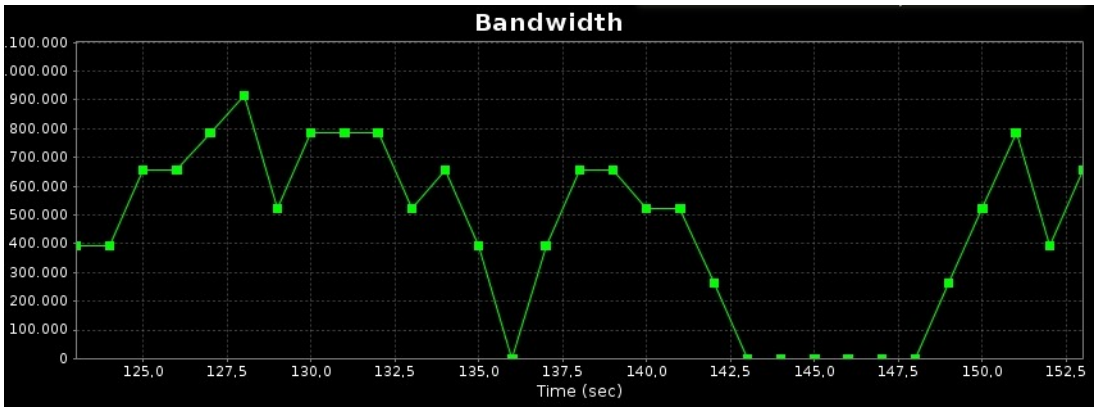

Figura 12: - Gráfico gerado pela ferramenta ao fim da simulação do terceiro cenário.

Com a análise dos resultados gerados ficou comprovado o fato observado no cenário 2, ou seja a quantidade de hosts presentes na rede e tráfego gerado pelas mesmas, influenciou diretamente na queda de desempenho da rede, tendo em vista que após a introdução de mais nós na rede o troughput médio da rede caiu consideravelmente, passando 751512 Bytes/sec conforme descrito no cenário 2, para apenas 655360 Bytes/sec, ou seja a rede teve uma perca de desempenho total de aproximadamente 17,3%. Outro fator bastante interessante a se observar no gráfico gerado dos testes do cenário 3, é a instabilidade da rede durante o ataque. Além disso, novamente em alguns períodos de tempo o troughput chega a zero, ocasionando dessa forma uma completa negação de serviço à rede.

4.2.5 Cenário IV

Os testes feitos no cenário IV tiveram como objetivo de simular o ataque de negação de serviço proposto neste trabalho, porém de forma distribuída, ou seja, diferentemente das simulações feitas nos cenários dois e três, a simulação feita neste cenário ao invés de ter apenas uma estação maliciosa efetuando o ataque à rede, teve várias estações atacando ao

mesmo tempo. O teste feito neste cenário teve também como objetivo analisar como uma rede wireless IEEE 802.11 se comportaria, em meio a um ataque de negação de serviço distribuido direcionado ao mecanismo de prevenção de colisões RTS/CTS.

Neste cenário as estações licitas do cenário III passaram também a atacar a rede, assim sendo, ao invés da rede contar apenas uma estação maliciosa, passou a ter 7, ou seja, todas as estações lícitas utilizadas no cenário anterior foram utilizadas para efetuar o ataque à rede, onde as mesmas foram encarregadas de efetuar pings contra o AP com quadros de 200 bytes, forçando a rede novamente usar o mecanismo RTS/CTS em todas as transmissões.

A topologia utilizada neste cenário, pode ser visualizada na figura 13.

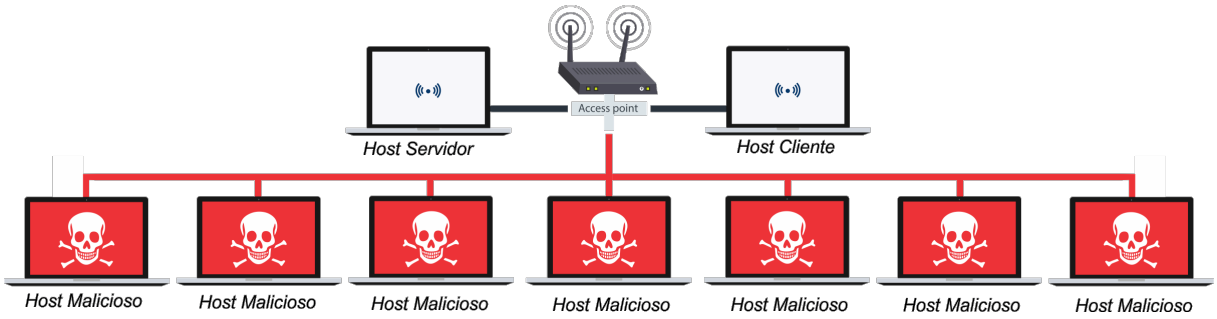

Figura 13: - Topologia utilizada para a simulação do cenário IV.

Ao término dos testes realizados no cenário IV foi gerado novamente o gráfico pela ferramenta Jperf como pode se observado na figura 14.

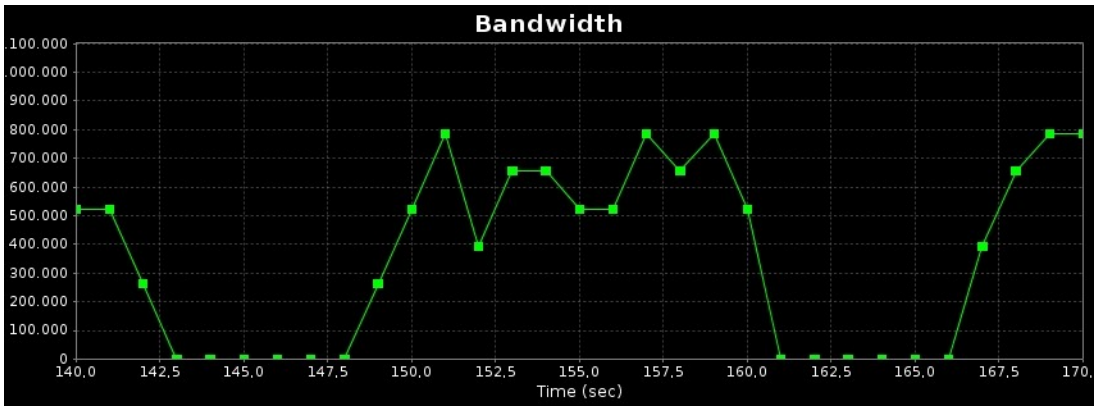

Figura 14: - Gráfico gerado pela ferramenta ao fim da simulação do quarto cenário.

Novamente observando o gráfico e os resultados gerados pela ferramenta foi possível observar que o resultado obtido neste cenário foi bastante semelhante ao resultado gerado no cenário III, já que o resultado do throughput médio da rede passou de 655360 Bytes/sec no cenário III, para 642912 Bytes/sec, em média uma diferença de apenas 1,9% em relação aos dois cenários. Já em relação ao cenário em que a rede não estava sofrendo ataque, a perca de desempenho foi de 18,4%.

Porém mesmo que a queda de desempenho em relação ao cenário anterior tenha sido pequena, observando o gráfico é possível observar que no cenário 4 os períodos de tempo em que o throughput da rede chegaram a zero foram maiores, isso se dá pela quantidade maior de hosts atacando a rede ao mesmo tempo, pois dessa forma a rede não consegue processar a alta quantidade de ataques e passa a negar serviço por alguns períodos de tempo.

O que pode justificar o fato da queda de desempenho ter sido baixa em relação ao cenário anterior, é o mesmo fato observado no cenário dois, ou seja, a falta de nós legítimos gerando tráfego na rede. Para comprovar este fato observado foi necessário a execução de mais um cenário de testes conforme é descrito a seguir.

4.2.6 Cenário V

O Cenário 5 foi o último cenário de testes, e teve como objetivo verificar se a quantidade de tráfego da rede, tem impacto direto na perca de desempenho quando a rede está sendo atacada. Dessa forma, para este cenário foram adicionadas a rede de testes mais 4 hosts lícitos, com isso a rede passou a ter 7 hosts maliciosos encarregados de atacar a rede explorando a vulnerabilidade do mecanismo RTS/CTS, e 4 hosts lícitos encarregados apenas de gerar tráfego legítimo na rede.

a topologia da simulação desse cenário pode ser vista abaixo, na figura 15.

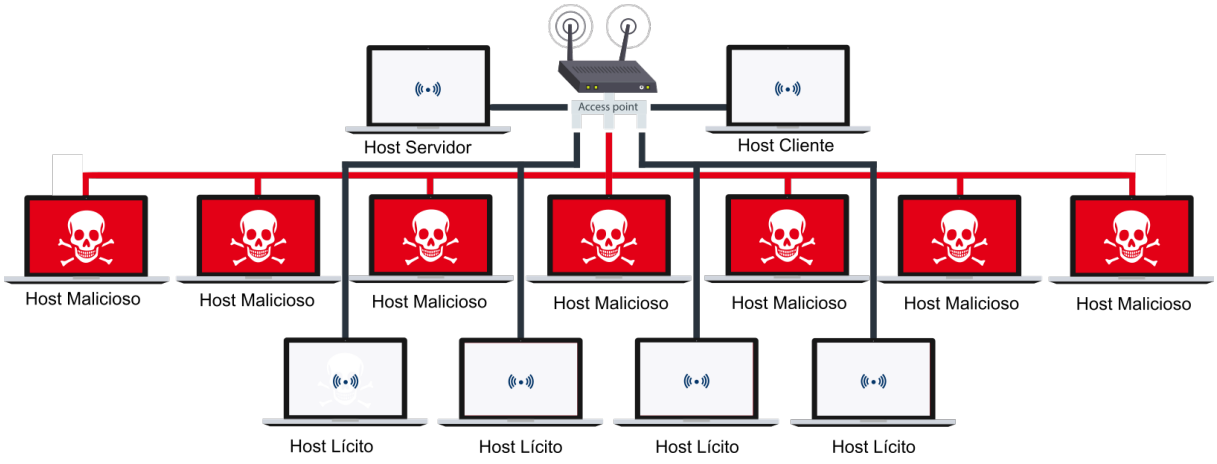

Figura 15: - Topologia utilizada para a simulação do cenário V.

Após a realização da simulação a ferramenta Jperf gerou o gráfico que pode ser visto na figura 16.

Considerando os resultados obtidos após a simulação deste cenário de testes, é possível observar que o throughput da rede teve uma queda bastante acentuada, em relação ao cenário IV que não possuía nenhuma gerando tráfego lícito, uma vez que o resultado médio

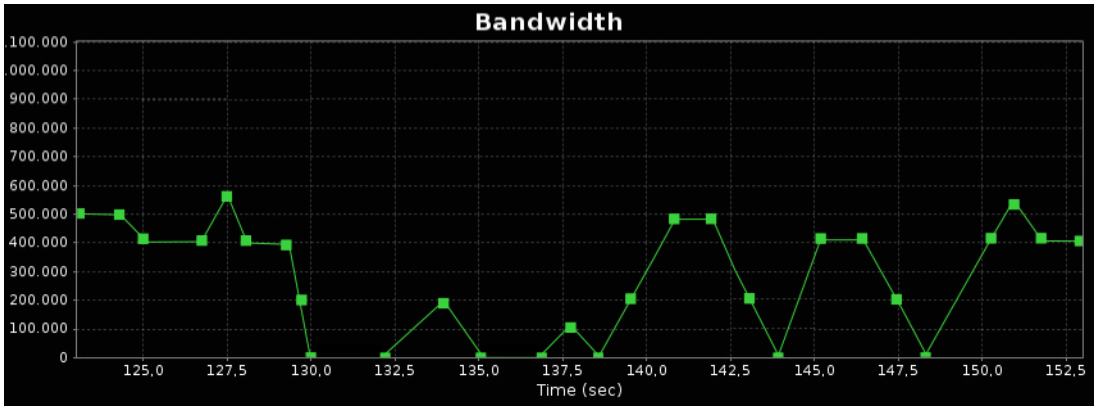

Figura 16: - Gráfico gerado pela ferramenta ao fim da simulação do quinto cenário.

obtido neste teste foi de 563843 bytes/sec, aproximadamente 12,3% de perca em relação ao cenário anterior. É importante observar ainda, que a medida que foram introduzidos hosts lícitos na rede, o desempenho da mesma caiu consideravelmente durante o ataque de negação de serviço distribuído, atingindo aproximadamente 29% de perca de desempenho total da rede.

Neste cenário embora os períodos de tempo de negação de serviço total da rede tenham sido menores, os mesmos ocorreram com maior frequência, se comparados em relação ao período anterior, o que mostra a dificuldade da rede em manter a sua estabilidade em meio ao ataque ao mecanismo.

Diante deste fato é possível comprovar que a quantidade de hosts gerando tráfego na rede impacta diretamente na efetividade do ataque.

Outra métrica que pode ser utilizada para avaliar o impacto do ataque na rede, é a quantidade de pacotes descartados durante as transmissões.

A tabela 3 mostra a quantidade de pacotes durante a execução dos testes de cada cenário.

Tabela 3: Porcentagem de perca de pacotes de cada cenário de testes.

Cenário	**Pacotes Perdidos (%)**
I	0
II	0,59
III	3,85
IV	28,4
V	35,5

Tendo em vista que no cenário de avaliação do troughput médio da rede, não houve nenhum descarte de pacotes, fica evidente que o ataque mostrado tem uma influência direta no descarte dos pacotes.

Conforme a tabela é possível analisar que o ataque que mais causou descarte de pacotes foi o ataque simulado no cenário V, obtendo um total de aproximadamente 35,5% de pa-

cotes descartados. Isso se justifica pelo fato de no ultimo cenário ocorrerem mais situações em que o troughput da rede chegou a 0, nesse caso a rede passa a negar completamente serviço, e em consequência disso os pacotes são descartados.

4.2.7 Resumo dos resultados obtidos

De acordo com os testes feitos e com os resultados obtidos, fica evidente a eficácia do ataque proposto, bem como sua efetividade em causar danos consideráveis no desempenho da rede, tendo em vista que a medida que a simulação do ataque era feita o desempenho da mesma caia consideravelmente, tendo momentos em que o throughput da rede chegava a zero, afetando assim a disponibilidade da rede.

O gráfico da figura 17 mostra o troughput de cada cenário de testes.

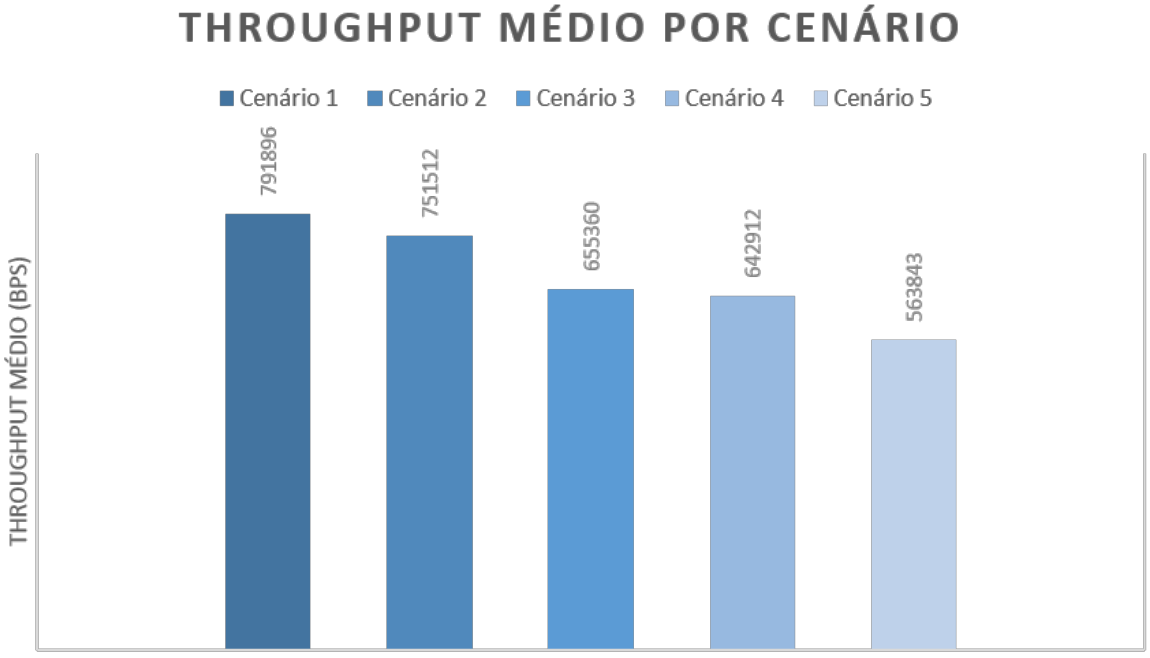

Figura 17: - Throughput médio de cada cenário.

Esse fator é preocupante, pois mesmo que isso acontecesse por pequenos períodos de tempo, nesses momentos a rede se tornaria completamente indisponível para qualquer estação lícita que desejasse fazer qualquer transmissão na rede.

5 Possíveis Métodos de Mitigação do Ataque

Este capítulo irá descrever possíveis métodos e abordagens para mitigação do ataque proposto o presente trabalho. Porém para que que os métodos abordados tenham eficácia, é necessário que o gerente de redes tenha conhecimento prévio da rede, afim de traçar um perfil para que seja possível conhecer o trafego normal de quadros RTS/CTS na rede, e com isso seja possível aplicar os métodos aqui abordados.

5.0.1 Localização da estação maliciosa por potência de sinal

A primeira proposta de contramedida para o ataque proposto neste trabalho, faz o uso de uma técnica conhecida como RSSI (Received Signal Strength Indication), que é uma técnica que se baseia em mensurar a potência do sinal de RF (Rádio Frequência) para estimar a posição de um dispositivo em uma rede wireless.

De acordo com (BAHL; PADMANABHAN; BALACHANDRAN, 2000), o mapeamento de RSSI é técnica que mais tem se destacado nos sistemas de localização indoor. Esta técnica, consiste em realizar um mapeamento por meio da medição da potência do sinal de rádio frequência em todo raio de amplitude que a rede wireless contempla e armazenar em um banco de dados, juntamente com o SSID de cada AP da área em questão. Dessa forma posteriormente estes dados poderão ser comparados em tempo real com um dispositivo a ser localizado, que no caso deste trabalho, seria uma estação maliciosa na rede, onde o resultado mais aproximado dessa comparação determina a posição estimada do dispositivo na rede.

A figura 18 ilustra um exemplo de um mapeamento RSSI

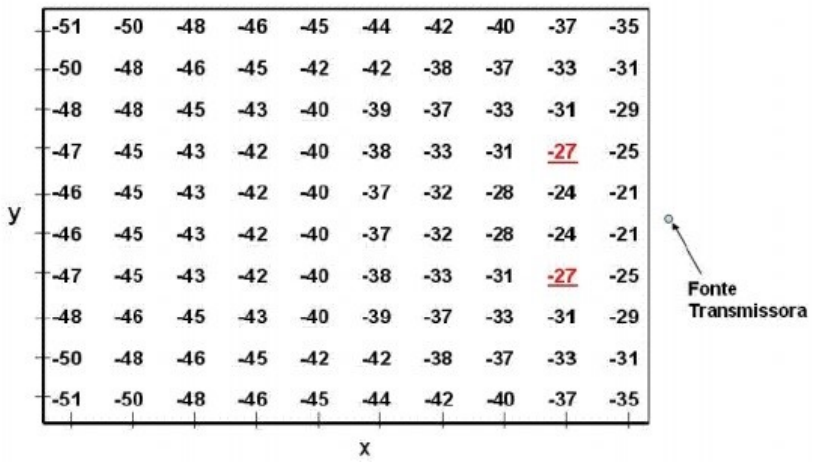

Figura 18: - Mapeamento RSSI

Fonte:(FAGUNDES, 2008).

Contudo, esta técnica só seria indicada para redes de pequeno e médio porte, pois de acordo com (FAGUNDES, 2008) mapeamentos mais extensos podem causar erros dependendo da distância, tendo em vista que a precisão de localização se torna comprometida em situações que o sinal RF sofre com o fenômeno conhecido como multipercurso, onde a variação pode chegar a 10db, não sendo possível uma localização precisa do dispositivo.

Outra adversidade relacionado a adesão dessa técnica pra solução do problema proposto nessa abordagem, está no fato de que em caso de ataques distribuídos a técnica de localização por força de sinal não seria a mais adequada. Dessa forma um segundo método para mitigação do ataque será abordado.

5.0.2 Método Sistemático prevenção de ataques

A segunda abordagem consiste em um método sistemático para detecção e contenção do ataque proposto neste trabalho. Este método é dividido em 2 módulos: um módulo de detecção, e um módulo para contenção do ataque.

A descrição do método, será descrita detalhadamente ao decorrer desta seção.

Descrição da abordagem

Quando um nó recebe um quadro de requisição RTS de outro nó, é feita uma análise através do módulo de detecção, para constatar se a requisição é proveniente de um nó malicioso ou não. Se o módulo de detecção, detectar uma intenção maliciosa de um nó, então o pedido de requisição não é respondido, e o módulo de contenção é ativado.

Para facilitar o entendimento do método, os módulos empregados no método de prevenção serão descritos a seguir.

Módulo de detecção

O módulo de prevenção se assemelha a um snifer de rede, ou seja ele é capaz de interceptar, registrar e analisar todos os quadros de requisição que chegam a cada nó, e determina se aquele determinado quadro é um quadro proveniente de uma estação maliciosa ou não. Para isso o módulo de detecção recorre a uma "black list" (lista negra), que contém o endereço de estações maliciosas já identificadas previamente.

Após isso o módulo, faz uma simples comparação, do endereço do remetente, que está contido no cabeçalho do quadro de requisição, e os endereços contidos na lista. Se o endereço comparado constar na lista, então aquela requisição é declarada como maliciosa, portanto o nó receptor não responderá ao quadro de requisição, encerrando assim a comunicação com o nó malicioso.

Para que o processo descrito seja efetivo, a lista das estações maliciosas deve está sempre atualizada. Para que isso seja possível é feito o uso de um mecanismo denominado de "Request Threshold" (Limiar de Requisição), que é utilizado em conjunto com o modo

de detecção, e funciona de forma análoga ao mecanismo RTS Threshold, porém ao invés de ser ativo de acordo com o tamanho do pacote, o mesmo é ativo, conforme uma quantidade de requisições de RTS de uma mesma estação durante um curto período de tempo. Onde o valor desse limiar é definido pelo administrador da rede.

Dessa forma se o modulo de detecção através do mecanismo "Request Threshold" detectar um comportamento anômalo de requisições de quadro RTS de uma mesma estação, o mesmo será responsável por ativar o módulo de contenção.

Módulo de Contenção

O módulo de contenção, funciona de maneira bem simples, ele é responsável por identificar o endereço do nó malicioso através do campo do remetente contido no cabeçalho do quadro RTS, e verificar se o mesmo já consta na "black list". Se o endereço do nó malicioso ainda não constar na lista, o módulo de contenção irá adiciona-lo.

Dessa maneira qualquer estação maliciosa que tentar injetar quadros de tamanho máximo na rede, com o objetivo de ativar o mecanismo RTS de forma desnecessária, para sobrecarregar a rede, terá suas requisições rejeitadas, e consequentemente a rede não sofrerá perca de desempenho ocasionada pelo ataque proposto nesta abordagem.

A figura 19 ilustra o funcionamento deste método.

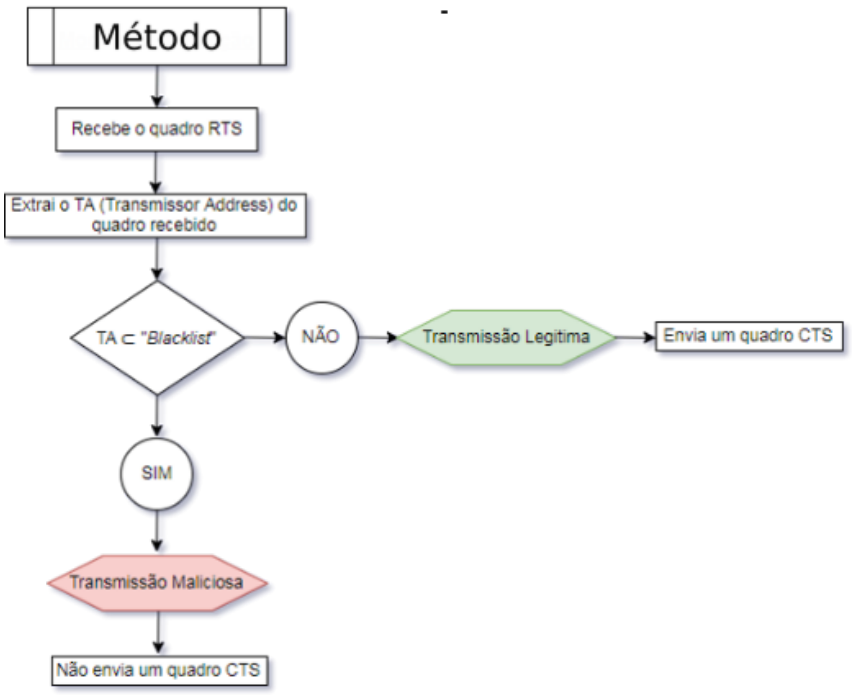

Figura 19: - Método sistemático para detecção e contenção do ataque

Fonte: Elaborada pelo autor.

6 Conclusão

As redes wireless baseadas no protocolo 802.11 cada vez mais tem seu uso aplicado nos mais variados campos, essa popularidade se deve a uma série de fatores, onde o principal é a sua mobilidade. Dessa forma o desempenho dessa tecnologia é um fator que deve ser mantido e sempre melhorado. Estre tralho apresentou um novo ataque de negação de serviço direcionado ao mecanismo de prevenção de colisões RTS/CTS que tinha como objetivo degradar o desempenho da rede. Onde foram realizados testes e simulações, evidenciando a efetividade do mesmo. Ficou comprovado ainda que ataques direcionados a esse mecanismo podem afetar o throughput da rede e o atraso da transmissão além de aumentar o congestionamento na rede.

Além de demonstrar o ataque, foram descritas e analisadas emíricamente, possíveis contramedidas para solução do Problema. Nas simulações realizadas, foi demonstrado através dos resultados obtidos, que um ataque de negação de serviço, que explore o mecanismo RTS/CTS, mesmo feito em pequena escala, ocasiona grande prejuízo ao funcionamento de toda a rede.

6.1 Trabalhos Futuros

Tendo em vista o fato de que o presente trabalho teve como foco principal o estudo e análise de uma vulnerabilidade presente no mecanismo de detecção de colisões RTS/CTS, bem como analisar os impactos que um ataque direcionado a essa vulnerabilidade gerariam em uma rede wireless 802.11. As propostas apresentadas como possíveis formas de prevenção e mitigação desse ataque, foram abordadas apenas de forma empírica.

Diante deste fato, é vista a necessidade de testar e validar a eficácia desses métodos propostos, bem como analisar os custos associados à implementação e avaliar a viabilidade da implantação de ambos os métodos como técnicas de prevenção de ataques direcionados ao mecanismo RTS/CTS em rede wireless 802.11.

Referências

BAHL, P.; PADMANABHAN, V. N.; BALACHANDRAN, A. Enhancements to the radar user location and tracking system. *Microsoft Research*, v. 2, n. MSR-TR-2000-12, p. 775–784, 2000. Citado na página 41.

BELLARDO, J.; SAVAGE, S. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In: WASHINGTON DC. *USENIX security symposium*. [S.l.], 2003. v. 12, p. 2–2. Citado na página 26.

BIANCHI, G. Performance analysis of the ieee 802.11 distributed coordination function. *IEEE Journal on selected areas in communications*, IEEE, v. 18, n. 3, p. 535–547, 2000. Citado na página 20.

COLOURIS, G.; DOLLIMORE, J.; KINDBERG, T. Sistemas distribuídos: conceitos e projetos. _ *Porto Alegre: Bookman*, 2007. Citado 2 vezes nas páginas 16 e 26.

DICIONARIOINFORMAL.COM. *Significado de Throughput.* 2013. Disponível em: <http://www.dicionarioinformal.com.br/significado/throughput/7536/>. Citado na página 33.

FAGUNDES, L. P. Técnicas de localização de dispositivos móveis em redes wifi-tdoa. 2008. Citado 2 vezes nas páginas 41 e 42.

GAST, M. *802.11 wireless networks: the definitive guide*. [S.l.]: "O'Reilly Media, Inc.", 2005. Citado na página 21.

IEEE. Ieee standard for information technology–telecommunications and information exchange between systems–local and metropolitan area networks–specific requirements–part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6: Wireless access in vehicular environments. *IEEE Std*, v. 802, n. 11, 2010. Citado 3 vezes nas páginas 8, 22 e 23.

INFORWESTER. *O que é Certificação Digital?* 2016. Disponível em: <https://www-.infowester.com/assincertdigital.php/>. Citado na página 18.

JÚNIOR, M. A. C.; GONÇALVES, P. A. d. S. Um mecanismo de protecao de quadros de controle para redes ieee 802.11. Universidade Federal de Pernambuco, 2012. Citado na página 28.

LAUFER, R. P. et al. Negação de serviço: Ataques e contramedidas. *Livro Texto dos Mini-cursos do V Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, 2005. Citado na página 19.

LOUREIRO, S. Segurança da informação: Preservação das informações estratégicas com foco em sua segurança.[sl], 12 2008. 66 p. *Monografia de Conclusão de Curso (Especialização)-Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília*, 2008. Citado na página 17.

MALEKZADEH; SUBRAMANIAM AZIM, A. G. S. A. M. M. Design of cyberwar laboratory exercises to implement common security attacks against ieee 802.11 wireless networks. *Journal of Computer Systems, Networks, and Communications*, Hindawi Publishing Corporation, v. 2010, 2011. Citado na página 27.

MENDES, C. C. S. Gerenciamento de recursos em redes sem fio ieee802. 11. *Master's degree dissertation. Universidade Tecnológica Federal do Paraná. Curitiba*, 2008. Citado na página 22.

MORAES, A. F.; CIRONE, A. C. Redes de computadores: Da ethernet àinternet. *Editora Erica, São*, 2003. Citado na página 16.

MORIMOTO, C. E. Redes, guia prático. *Porto Alegre: Sul Editores*, v. 4, p. M857r, 2008. Citado 2 vezes nas páginas 14 e 19.

MYNENI, S.; HUANG, D. Ieee 802.11 wireless lan control frame protection. In: IEEE. *Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE*. [S.l.], 2010. p. 1–5. Citado 2 vezes nas páginas 25 e 27.

NAGARJUN, P. et al. Simulation and analysis of rts/cts dos attack variants in 802.11 networks. In: IEEE. *Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on*. [S.l.], 2013. p. 258–263. Citado na página 26.

NETO, I. L. d. F. Um esquema de segurança para quadros de controle em redes ieee 802.11. Universidade Federal de Pernambuco, 2015. Citado 3 vezes nas páginas 24, 25 e 28.

OLIVEIRA, A. T. *ANALISE DAS VULNERABILIDADES DAS REDES SEM FINA CIDADE DE VITORIA DA CONQUISTA - BA*. [S.l.]: Universidade Estadual do Sudoeste da Bahia – UESB, 2010. Citado na página 17.

OLIVEIRA, E. et al. Avaliacao de proteção contra ataques de negação de serviço distribuídos (ddos) utilizando lista de ips confiáveis. *VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, 2007. Citado na página 20.

RAY, S.; STAROBINSKI, D. On false blocking in rts/cts-based multihop wireless networks. *IEEE Transactions on Vehicular Technology*, IEEE, v. 56, n. 2, p. 849–862, 2007. Citado 2 vezes nas páginas 25 e 26.

RIBEIRO, A. C. et al. An approach to mitigate denial of service attacks in ieee 802.11 networks. *Journal of Computer Sciences*, p. 128–137, 2014. Citado 2 vezes nas páginas 16 e 29.

SANDSTROM, H. A survey of the denial of service problem. *BSc Programmes in Engineering Computer Engineering*, 2001. Citado na página 13.

SAWWASHERE, S. S.; NIMBHORKAR, S. U. Survey of rts-cts attacks in wireless network. In: IEEE. *Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on*. [S.l.], 2014. p. 752–755. Citado na página 25.

SHEU, S.-T. et al. The impact of rts threshold on ieee 802.11 mac protocol. In: IEEE. *Parallel and Distributed Systems, 2002. Proceedings. Ninth International Conference on*. [S.l.], 2002. p. 267–272. Citado na página 25.

SOARES, L. F. G.; GUIDO, L.; COLCHER, S. Redes de computadores: das lans, mans e wans às redes atm. Campus, 1995. Citado na página 21.

STANDARD, A. Iso/iec 27002. *Information technology-security techniques-code of practice for information security controls,(AS ISO/IEC 27002: 2015), Standards Australia*, 2015. Citado na página 17.

TANENBAUM, A. *S. Redes de Computadores. São Paulo: Ed.* [S.l.]: Campus, 2003. Citado na página 16.

TECHTUDO. *O que é Hash?* 2012. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/07/o-que-e-hash.html>. Citado 2 vezes nas páginas 18 e 19.

TECMUNDO. *DDoS: como funciona um ataque distribuído por negação de serviço.* 2011. Disponível em: <https://www.tecmundo.com.br/seguranca/10970-ddos-como-funciona-um-ataque-distribuido-por-negacao-de-servico.htm>. Citado na página 19.

TELECO. *Características do Wi-Fi.* 2008. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialww1/pagina_4.asp/>. Citado 3 vezes nas páginas 17, 21 e 24.

ZOU, X.; DENG, J. Detection of fabricated cts packet attacks in wireless lans. In: SPRINGER. *QSHINE*. [S.l.], 2010. p. 105–115. Citado na página 29.

TERMO DE AUTORIZAÇÃO PARA PUBLICAÇÃO DIGITAL NA BIBLIOTECA "JOSÉ ALBANO DE MACEDO"

Identificação do Tipo de Documento

( ) Tese

( ) Dissertação

(X) Monografia

( ) Artigo

Eu, **Kécyo Keviny Gonçalves de Mendonça**, autorizo com base na Lei Federal nº 9.610 de 19 de Fevereiro de 1998 e na Lei nº 10.973 de 02 de dezembro de 2004, a biblioteca da Universidade Federal do Piauí a divulgar, gratuitamente, sem ressarcimento de direitos autorais, o texto integral da publicação **Análise da vulnerabilidade do mecanismo RTS/CTS a ataques de negação de serviço em redes Wireless IEEE 802.11** de minha autoria, em formato PDF, para fins de leitura e/ou impressão, pela internet a título de divulgação da produção científica gerada pela Universidade.

Picos-PI 06 de fevereiro de 2018.

Assinatura