URLAN SALGADO DE BARROS

O IMPACTO DE ATAQUES DE REDUÇÃO DA QUALIDADE DE SERVIÇO EM REDES WI-FI COM CONTROLE DE POTÊNCIA DE TRANSMISSÃO

Monografia de Graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para obtenção do título de Bacharel em Ciência da Computação.

LAVRAS
MINAS GERAIS - BRASIL
2008

URLAN SALGADO DE BARROS

O IMPACTO DE ATAQUES DE REDUÇÃO DA QUALIDADE DE SERVIÇO EM REDES WI-FI COM CONTROLE DE POTÊNCIA DE TRANSMISSÃO

Monografia de Graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para obtenção do título de Bacharel em Ciência da Computação.

Área de Concentração:
Redes de Computadores - Segurança Computacional

Orientador:
Prof. Luiz H. A. Correia & Profa. Michele N. Lima

LAVRAS
MINAS GERAIS - BRASIL
2008

.

Ficha Catalográfica preparada pela Divisão de Processos Técnicos
da Biblioteca Central da UFLA

Barros,Urlan Salgado de

O impacto de ataques de redução da qualidade de serviço em redes Wi-Fi com controle de potência de transmissão /Urlan Salgado de Barros. Lavras - Minas Gerais, 2008. 73p : il.

Monografia de Graduação - Universidade Federal de Lavras. Departamento de Ciência da Computação.

1. Segurança. 2. Wi-Fi. 3. Controle de Potência de Transmissão. 4. NS2. I. BARROS, U. S. II. Universidade Federal de Lavras. III. Título.

URLAN SALGADO DE BARROS

O IMPACTO DE ATAQUES DE REDUÇÃO DA QUALIDADE DE SERVIÇO EM REDES WI-FI COM CONTROLE DE POTÊNCIA DE TRANSMISSÃO

Monografia de Graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para obtenção do título de Bacharel em Ciência da Computação.

Aprovada em *20 de novembro de 2008*

Prof. Bráulio Adriano de Mello

Prof. João Carlos Giacomin

Prof. Luiz H. A. Correia & Profa. Michele N. Lima
(Orientador)

LAVRAS
MINAS GERAIS - BRASIL

Dedico a oportunidade que me foi dada.

Agradecimentos

Agradeço à minha mãe Lenir, que sempre me apoiou, me dando carinho, afeto e amor. Sem ela eu com certeza não seria nada. Agradeço ao meu pai Urias, por sempre ter me ajudado, mesmo com aquele jeito carrancudo, para que eu pudesse me manter aqui, estudando e com isso podendo aprender mais. Agradeço ao meu irmão Fred, que sempre esteve ao meu lado, conversando, rindo e xingando, quando fosse necessário.

Agradeço aos meus orientadores Luiz Henrique, Michele e Aldri, por terem me dado essa oportunidade de poder aprender mais, mesmo eu sempre tendo me esforçado bastante e por sempre terem me orientado, mesmo quando fossem necessárias algumas catracadas.

Agradeço à minha namorada Karla, pelo amor, carinho e afeto incondicionais e pelos momentos de paciência enquanto eu escrevia este trabalho. Agradeço à minha sogra Nina, pelos momentos de descontração e pelo almoço nos finais de semana.

Agradeço a todos os meus amigos do Cocobongo Golo and Prosa Unlimited: Rodrigo (Cocão), Alysson, Diego (Tião), Tony, Alessandro (Bode), José Francisco (Zefera), Alan (Ossuda), Sidney, Cadu, Wesley, Gustavo e Fred (Corvo).

Agradeço ao meu amigo Tiago (Kurumin), pelas dicas e pelas discussões a respeito de Redes, Segurança, Sistemas Operacionais e se mulheres com rosto claro e cabelo preto são morenas ou não.

Agradeço ao Fred pelas discussões a respeito de Computação, pelas horas de brincadeira e pelas risadas ao nos perguntar qual o kernel do FreeBSD.

Agradeço ao pessoal do Centro de Informática da UFLA: Ana, Júlio, Marcão, Rafael Santana, Haroldo, Ney, Valmir, Cida, Erasmo, Thiago Ramos e Anderson pelas brincadeiras e pela paciência que tiveram comigo, por sempre me aturarem por lá.

Agradeço a todas as pessoas do DCC pelas boas conversas e pelas boas discussões.

Agradeço a toda turma do Predinho Rosa, especialmente as pessoas que dividiram apartamento comigo.

Agradeço aos companheiros Eduardo, Arthur Furlan, Wellton e Anderson pelas dicas sobre a ferramenta ns2.

Agradeço a todos aqueles que me ajudaram de alguma maneira mas que, por pura incapacidade mental minha de relembrar das coisas, não pude dedicar uma linha para eles neste trabalho.

Resumo

As redes sem fio tem sido usadas por proverem mobilidade aos usuários e por estarem em todos os lugares. Vários mecanismos, como o IEEE 802.11, comumente chamado *Wi-Fi*, foram desenvolvidos para assegurar a mobilidade e ajudar a gerenciar o tráfego de dados de todos os usuários na rede. O 802.11 possui duas funções coordenadoras, denominadas DCF e PCF, responsáveis pelo controle de acesso ao meio. Essas funções coordenadoras são vulneráveis a ataques que tentam tornar os recursos de um sistema indisponíveis para seus utilizadores, logo, estes serviços são negados às estações. Um recente ataque de negação de serviço estudado pela literatura, denominado ataque de redução da qualidade de serviço, tem como finalidade fazer com que a rede deixe de funcionar completamente. Além das funções coordenadoras, para que a rede possa ter maior economia de energia e um maior reuso espacial, faz-se necessário o uso do controle de potência de transmissão. Nesse controle as estações utilizam somente a energia necessária para que os quadros enviados possam alcançar seus vizinhos sem que o quadro necessite ser repassado. Neste trabalho, é demonstrado como uma rede *Wi-FI* com controle de potência de transmissão pode ter uma taxa de entrega de pacotes similar a ao *Wi-fi* sem controle de potência, porém tendo maior economia de energia. Também é mostrado como os ataques de redução da qualidade de serviço podem degradar em mais de 30% a taxa de entrega de uma rede *Wi-Fi* que utilize, ou não, o controle de potência de transmissão.

Abstract

Wireless networks have been used because they provide mobility to the users and they are in everywhere. Some mechanisms, like IEEE 802.11, also called *Wi-Fi*, have been created to ensure mobility and to help managing the data traffic of all users in the network. 802.11 has two coordinators functions, called DCF and PCF, responsible for media access control. These coordinators functions are vulnerable to attacks that deny the service of stations, such as reduction of quality attacks, that can lead to the whole destruction of the normal behavior of the network. Nevertheless, to ensure that the network may have more power saving and more spatial reuse, it is required to use transmition power control. This control is used when an station wants to send a frame to it's neighbor that is one hop distant. In this work is shown that transmition power control can have frames rate delivery, analogous to the one network that not use transition power control, and it may have more power saving. Also it describes how reduction of quality attacks can degrade the frame rate delivery in more than 30% in one network that uses, or not, transmition power control.

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

INTRODUÇÃO

As redes sem fio *(Wireless Network)* têm sido usadas por proverem ao usuário mobilidade, computação pervasiva e computação ubíqua. Segundo Mark Weiser (1995), a computação ubíqua *(ubiquitous computing)* permite aos usuários a utilização de um sistema de computação, a qualquer momento e em qualquer lugar [44]. Logo, a computação deve ser incorporada às tarefas do dia-a-dia de forma transparente, e, portanto, não pode impor limitações ao comportamento do usuário, como obstruir sua capacidade de deslocamento, garantindo assim sua mobilidade. Outro tipo de computação utilizada em redes sem fio é a computação pervasiva que, segundo Hansmann (2003), prevê que muitos computadores estejam disponíveis em todo o ambiente físico, porém de forma invisível e imperceptível para o usuário [26].

Várias tecnologias de comunicação sem fio foram desenvolvidas com o intuito de adequar-se à computação ubíqua e pervasiva, para com isso assegurar a mobilidade e capacidade de acesso aos dados do usuário. Dentre as inúmeras tecnologias de comunicação já criadas, vale ressaltar as mais atuais, como *Wi-Fi (Wireless Fidelity)* (IEEE 802.11) [20], *Bluetooth* (IEEE 802.15.1) [2], *WiMAX* (IEEE 802.16) [50] e *3G* [58].

Estas tecnologias, como o *Wi-Fi*, possuem mecanismos de controle que ajudam a gerenciar o tráfego de dados de todos os usuários na rede. A tecnologia *Wi-Fi* possui duas funções coordenadoras responsáveis pelo controle de acesso ao meio, o DCF *(Distributed Coordination Function)* e o PCF *(Point Coordination Function)*, sendo o DCF a função principal devido ao PCF atuar sobre o DCF [20]. O DCF possui alguns temporizadores de acesso ao meio, usados para tentar diminuir o número de colisões de quadros devido aos problemas do terminal escondido e do terminal exposto [49], como o DIFS *(Distributed Infer-Frame Space)*, o SIFS *(Shortest Inter-Frame Space)*, o NAV *(Network Allocation Vector)* e um tempo de espera denominado *backoff*.

Assim que uma estação transceptora envia um determinado quadro para o meio são criados dois limiares. O primeiro limiar, denominado área de cobertura ou raio de alcance, caracteriza-se por conter

estações próximas o bastante do transceptor para que o quadro não necessite ser repassado pelo seu vizinho, ou seja, os vizinhos não estão a mais de um salto de distância, por estações que sejam capazes de decodificar o quadro corretamente e por ser menor que o segundo limiar. O segundo limiar, chamado de zona de detecção de portadora, contém estações que estão a uma certa distância do transceptor (mais de dois saltos de distância) e não conseguem decodificar o quadro corretamente, mas conseguem saber que o meio se encontra ocupado. Todas as estações que estejam na zona de detecção de portadora não conseguirão decodificar o quadro corretamente, devido ao sinal recebido por essas estações ser bastante baixo. Para que sejam evitadas colisões, as estações que estejam na zona de detecção de portadora deverão atrasar suas transmissões setando seu NAV com o valor contido no temporizador EIFS *(Extended Inter-Frame Space)*.

As duas funções coordenadoras, DCF e PCF, utilizadas no *Wi-Fi*, necessitam que o comportamento das estações, utilizadas pelos usuários, mantenham-se no padrão estabelecido pela tecnologia. Devido a esta necessidade, nenhum mecanismo de controle foi criado para identificar comportamentos fora do padrão e, por essa razão, ainda são encontradas várias vulnerabilidades nos mecanismos de controle do Wi-Fi. Estas vulnerabilidades podem permitir que uma estação consiga maior tempo de acesso ao meio ou maior banda e também permitem que a comunicação em toda a rede seja totalmente degradada.

Inúmeros ataques foram apresentados contra o DCF devido à sua simplicidade de implementação e a necessidade das estações se comportarem conforme estabelecido pela tecnologia. Segundo Lei Guang (2006), esses ataques podem ser classificados como sendo ataques gulosos e ataques maliciosos [40].

Os ataques gulosos visam o aumento de banda de uma determinada estação, dentre os quais destacam-se, o ataque de redução do tempo de backoff [54], [30], o ataque que permite o uso exagerado do temporizador NAV usando-se valores altos [7], [19] e o ataque de diminuição do período de tempo SIFS [40]. Já os ataques maliciosos, visam destruir o comportamento normal de uma rede por completo, como o ataque de negação de serviço distribuído DDoS *(Distributed Denial-of-Service)*, considerado como um ataque que possui alta taxa de tranferência de dados [35], e o ataque de redução da qualidade de serviço RoQ *(Reduction of Quality)*, considerado como um ataque de negação de serviço com baixa taxa de transferência de dados *(low-rate DoS attack)* [24], [67].

Várias abordagens citadas na literatura, como o DOMINO [55] e o DREAM [21], conseguem diminuir quase que por completo o impacto de vários ataques gulosos. Os ataques maliciosos que possuem alta taxa de transferência foram quase ou completamente mitigados por alguns estudos na litetura, inclusive [17] e [69]. Porém, ataques maliciosos com baixa taxa de transferência de dados possuem poucas abordagens efetivas na literatura [64], devido a sua dificuldade de detecção por explorarem a capacidade dinâmica de adaptação dos mecanismos presentes em todas as camadas [22], [23], como o controle de congestionamento presente no TCP.

1.1 Motivação

O controle de potência de transmissão (CPT) é a forma na qual uma determinada estação utiliza somente a quantidade de energia necessária para que o envio dos quadros possa ser alcançado pelos seus vizinhos a um salto de distância. Além disso, permite maior reuso espacial da rede, na qual as estações conseguem enviar mais dados simultaneamente, e maior economia de energia.

Este trabalho é motivado pelo estudo do CPT em redes *Wi-Fi* como forma de aumentar o reuso espacial da rede bem como diminuir o consumo de energia da estações. Este trabalho também possui como motivação o uso do CPT em redes *Wi-Fi* como forma de diminuir o impacto dos ataques de RoQ. Além disso, na literatura corrente, os ataques de RoQ tem sido pouco estudados devido à sua dificuldade de detecção e por serem bastante recentes.

1.2 Objetivo

Este trabalho possui dois objetivos. O primeiro objetivo é a análise, o estudo e a adaptação para as redes que utilizem tecnologia *Wi-Fi* de duas soluções, propostas por [41], para controle de potência de transmissão. Essas duas soluções propostas foram criadas inicialmente para gerenciamento do CPT em redes de sensores sem fio.

O segundo objetivo consiste na análise da diminuição do impacto dos ataques de RoQ em redes *Wi-Fi* que utilizem CPT. Os ataques de RoQ utilizados e avaliados são *Round-Robin Attack*, *Self-Whisper Attack* e *Flooding Attack*, propostos por [64].

1.3 Solução Proposta

Na tecnologia *Wi-Fi* as estações normalmente utilizam a potência máxima de transmissão para enviar quadros, o que pode acarretar alguns problemas, como grande número de colisões de quadros e alto consumo de energia. Esses problemas podem ser tratados através do uso de CPT, que tem como função diminuir o número de colisões, através do reuso espacial da rede, e o consumo de energia. Porém, o CPT tem como desvantagem o aumento no tempo de entrega dos quadros (latência).

Existem também problemas relacionados aos ataques que visam destruir por completo o comportamento normal de uma rede. Tais ataques negam o serviço das estações e fazem com que a vazão da rede e a taxa de entrega de quadros caia para quase zero, e que o número de colisões de quadros cresça exponencialmente. Ataques, como os de RoQ, são feitos de maneira inteligente para que não sejam descobertos e com isso mitigados, tornando-se complexa sua identificação.

Neste trabalho, os problemas relacionados ao número de colisões de quadros e o alto consumo de

energia foram tratados através do uso do CPT em redes *Wi-Fi*. Para o uso do CPT, foram usados dois protocolos propostos por [41] para redes de sensores sem fio, sendo estes os protocolos de Atenuação e AEWMA *(Atenuation Exponentially Weighted Moving Average)*. Os protocolos de CPT, Atenuação e AEWMA, foram implementados no simulador *network simulator 2 - ns2* [14] e, posteriormente, analisados através de gráficos comparativos, mostrando-se a eficiência do CPT.

Para os ataques de RoQ, foi utilizado o CPT como mecanismos de defesa para tentar diminuir o impacto desses ataques em redes *Wi-Fi*. Os três tipos de ataques de RoQ, descritos anteriormente, foram implementados no simulador ns2 [14] e então analisados.

A solução proposta para uso do CPT em redes *Wi-Fi* e a análise do CPT como mecanismo de defesa contra os ataques de RoQ, foram desenvolvidos e implementados através da ferramenta de simulação de rede ns2 [14]. Para a análise foram usadas as seguintes métricas: a taxa de envio e recebimento das estações alvo, a latência da rede e a potência de transmissão efetiva utilizada pelas estações.

A ferramenta ns2 *(Network Simulator 2)* [14] é um simulador discreto orientado a eventos. É voltada para a pesquisa de redes e bastante conhecida no meio acadêmico. O ns2 utiliza duas linguagens de programação para seus propósitos. A linguagem Tcl é usada para configuração dos *scripts* de simulação e a linguagem C++ é usada para implementar os componentes principais do simulador, como o escalonador de eventos, os protocolos de roteamento, os protocolos na camada de enlace, entre outros.

1.4 Organização do Trabalho

Este trabalho está organizado da seguinte forma, no capítulo 2 é apresentado o Referencial Teórico, que define redes sem fio, apresenta a tecnologia *Wi-Fi* e o controle de potência da transmissão. Além disso, são definidos os ataques gulosos e apresentados três destes ataques estudados na literatura, impacto que cada ataque causa na rede e seu respectivo método de defesa. E por fim são definidos os ataques maliciosos e os quatro ataques de RoQ estudados neste trabalho.

No capítulo 3 é mostrada a Metodologia do Trabalho, que tem como finalidade o enquadramento adequado do trabalho e demonstra como será feita a pesquisa em torno do projeto.

No capítulo 4 são mostrados os Resultados e é feita a análise a respeito dos dois protocolos de controle de potência de transmissão, o de Atenuação e o AEWMA. Após a análise dos protocolos de CPT, será explicada a análise sobre o impacto dos ataques de redução da qualidade de serviço nas redes *Wi-Fi* que possuam, ou não, o CPT.

No capítulo 5 é apresentada a Conclusão a respeito deste trabalho, são citados alguns trabalhos futuros que poderiam ser feitos a partir deste e por último tem-se a Referência Bibliográfica.

Capítulo 2

REFERENCIAL TEÓRICO

Esta seção contextualiza as redes sem fio, explica o funcionamento do protocolo IEEE 802.11, comumente chamado de *Wi-Fi*, e apresenta uma descrição a respeito do controle de potência de transmissão (CPT). O comportamento dos atacantes é descrito e classificado como sendo do tipo guloso ou malicioso, sendo também definidos os tipos de ataques gulosos mais comuns nas redes 802.11. É ainda apresentado o impacto desses ataques na rede e os respectivos métodos de defesa empregados. E por fim, são explicados e definidos os ataques maliciosos, como os ataques de redução da qualidade de serviço *(RoQ attacks)*.

2.1 Redes Sem Fio

O recente aumento das pesquisas na área de redes de computadores está intimamente ligado à capacidade dos usuários poderem conseguir informação de maneira rápida e fácil. Partindo deste princípio, a comunidade acadêmica juntamente com várias empresas começaram a investir em pesquisas que buscassem tecnologias capazes de proporcionar maiores facilidades aos usuários. Estas pesquisas tiveram como resultado a criação de uma nova tecnologia denominada redes sem fio *(Wireless Network)*, que em pouco tempo começaram a ser usadas juntamente com as redes cabeadas.

Em contra partida às redes cabeadas, as redes sem fio estão disponíveis em qualquer lugar, por não necessitarem de cabeamento, além de serem de fácil manutenção. Para proverem acesso por toda parte, de forma transparente e imperceptível para os usuários, as redes sem fio fazem uso da computação ubíqua e da computação pervasiva.

Segundo Mark Weiser (1995), a computação ubíqua *(ubiquitous computing)*, permite aos usuários a utilização de um sistema de computação, a qualquer momento e em qualquer lugar [44]. Logo, a computação deve ser incorporada às tarefas do dia-a-dia de forma transparente, e, portanto, não pode impor limitações ao comportamento do usuário, como obstruir sua capacidade de deslocamento, garan-

tindo assim sua mobilidade. A computação pervasiva, segundo Hansmann (2001), prevê que muitos computadores estejam disponíveis em todo o ambiente físico, porém de forma invisível e imperceptível para o usuário [26].

Inúmeros projetos têm sido criados com o intuito de expandir as redes sem fio e adequar-se à computação ubíqua e pervasiva, para com isso assegurar a mobilidade e capacidade de acesso aos dados do usuário, sendo que vários desses são projetos voltados mais precisamente para as redes WLAN *(Wireless Local Area Network)*. A Figura 2.1 mostra um exemplo de uso das redes sem fio onde as estações que queiram se comunicar com a *Internet* devem passar pelo computador central, que tem como função interligar todas as estações.

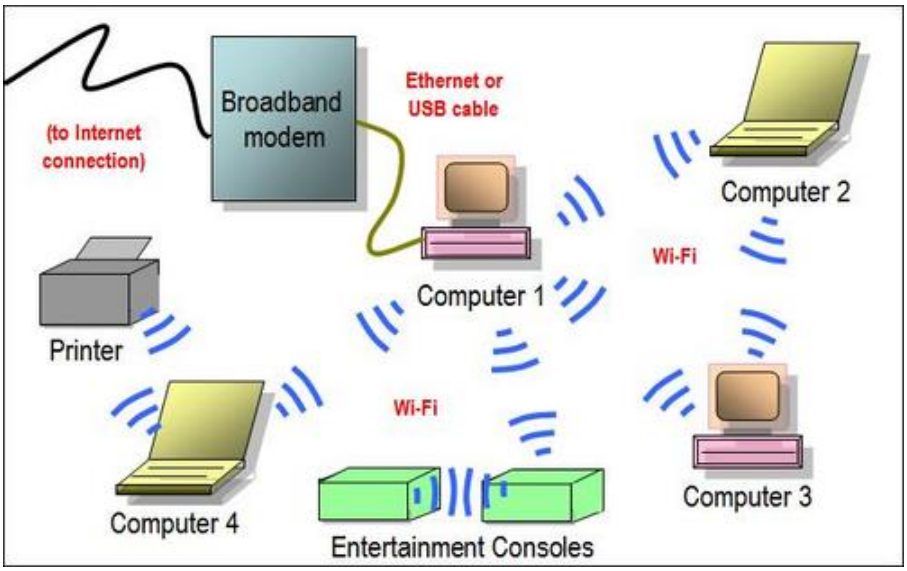

Figura 2.1: Uso das redes sem fio.

As redes sem fio possuem algumas vantagens sobre as redes cabeadas, como mostrado por Matthew Gast em [20]:

- *Mobilidade*: os usuários tendem a se mover enquanto a informação fica armazenada em um lugar centralizado. Possibilitar que os usuários acessem os dados enquanto se movem pode aumentar drasticamente o ganho de produtividade.
- *Instalação*: em diversos locais a instalação de cabos é bastante difícil, como velhos prédios que foram tombados pelo patrimônio histórico e os quais estão submetidos às leis de conservação. Equipamentos que utilizam tecnologia sem fio são de fácil e rápida instalação por não necessitarem de uma infra-estrutura ou tubulação.
- *Flexibilidade*: as redes sem fio permitem aos usuários rápido acesso à internet, sem necessitar que cabos sejam conectados, devido ao acesso ao meio estar sempre disponível.

- *Custo*: em inúmeros casos o uso de redes sem fio pode diminuir bastante o custo. Como um exemplo, tem-se a capacidade de um equipamento que utilize tecnologia sem fio possui de conectar dois prédios.

Devido ao rápido crescimento e grande procura pelas redes sem fio, vários padrões foram criados, como o *Bluetooth* (IEEE 802.15.1) [2], o *WiMAX* (IEEE 802.16) [50], o *3G* [58] e o Wi-Fi (IEEE 802.11) [20] apresentado neste trabalho. Essas tecnologias são os modelos de redes sem fio atualmente encontrados na literatura.

2.2 O Protocolo IEEE 802.11

O protocolo 802.11, também chamado *Wi-Fi*, define duas camadas, a camada física, a qual define as características dos equipamentos de transmissão e recepção, e a camada de enlace, os quais são apresentados os métodos de controle de acesso ao meio *(MAC - Media Access Control)*.

Novos problemas surgiram como consequência da limitação do raio de transmissão e do compartilhamento do meio nas redes *Wi-Fi*. Dois destes problemas são, o **problema do terminal escondido** e o **problema do terminal exposto** [2] e [49].

O **problema do terminal escondido** ocorre da seguinte forma, tomando como base a Figura 2.2, retirada de [2]. Supondo que duas estações, **1** e **3**, necessitem de transmitir dados para a estação **2**, ambos poderão transmitir e terão uma grande probabilidade do envio dos dados ser feito ao mesmo tempo tendo como conseqüência a colisão de dados na estação **2**. Isto ocorre devido ao fato da estação **1** não conseguir detectar a transmissão da estação **3** e nem de **3** detectar a transmissão de **1**.

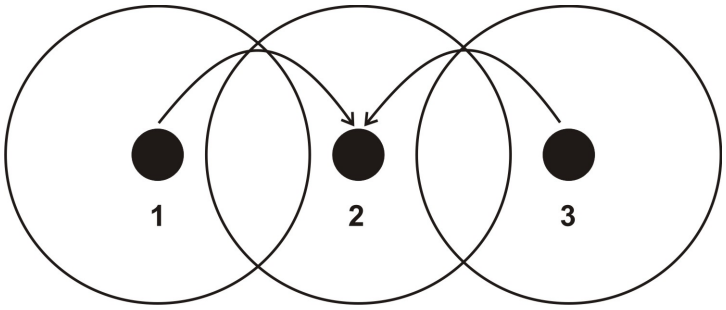

Figura 2.2: O problema do terminal escondido.

O **problema do terminal exposto**, Figura 2.3 retirada de [2], ocorre da seguinte forma, se a estação **1** estiver enviando dados para a estação **2** e a estação **3** necessitar enviar dados para a estação **4**, a transmissão de **3** não poderá acontecer, para que não ocorra colisão de dados em **2**. O problema acontece devido a **3** não saber se **1** está enviado dados para a estação **2**, devido a **3** não escutar a transmissão.

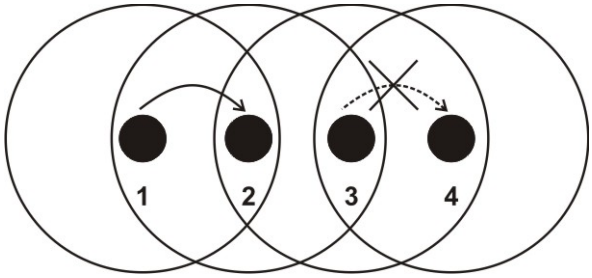

Figura 2.3: O problema do terminal exposto.

Como o padrão *Ethernet*, o 802.11 usa o esquema CSMA *(Carrier Sense Multiple Access)* para controlar o acesso ao meio de transmissão. Os rádios possuem dois modos, o de recepção e o de transmissão. Devido aos rádios não poderem utilizar os dois modos simultaneamente, eles não são capazes de detectar colisão. Para contornar este problema foi criado um esquema denominado CSMA/CA *(Carrier Sense Multiple Access / Collision Avoidance)*. Esse esquema também usa o esquema de distribuição de acesso sem nenhum controlador centralizado [59]. Uma forma de diminuir estes dois problemas citados anteriormente foi demonstrada por Karn (1990) através da utilização do MACA *(Multiple Access with Collision Avoidance)* [49]. O MACA funciona da seguinte maneira, toda vez que uma estação transceptora deseja começar uma transmissão, ela irá enviar um quadro RTS *(Request to Send)* para a estação receptora. Dentro deste quadro será informado o tempo de duração de toda a transmissão. Todas as estações que venham a escutar o RTS que não seja endereçado a elas, irão ajustar seu NAV *(Network Allocation Vector)* com o valor do tempo de duração contido no RTS. O receptor, após receber o RTS, irá responder a estação transceptora com um quadro denominado CTS *Clear to Send*. Dentro do CTS será informado qual o tempo restante de duração da transmissão. Todas as estações que venham a escutar o CTS que não seja endereçado a elas irão ajustar seu NAV com o tempo de duração contido no quadro de CTS. A estação transceptora, após o recebimento do CTS, irá transmitir o quadro de DADOS para o receptor. A troca de quadros RTS e CTS passando-se o tempo de duração de toda a transmissão é denominado de reserva virtual do meio, pois todas as estações que venham a escutar os quadros irão bloquear seus transmissores para que sejam evitadas colisões. A reserva virtual do meio é feita para que os problemas do terminal exposto e do terminal escondido sejam diminuídos.

O 802.11 faz uso de uma extensão do MACA denominada MACAW *(A Media Access Protocol for Wireless LAN's)* [6]. O MACAW, além utilizar os quadros RTS, CTS e de DADOS fazendo uso do mesmo mecanismo de reserva virtual do meio, utiliza também um quadro de resposta ao quadro de DADOS, denominado ACK. O envio de quadros RTS, CTS, de DADOS e ACK é feito pelos modos de acesso ao MAC, que disponibilizam o controle de acesso ao meio.

2.2.1 Modos de Acesso ao Meio

O acesso ao meio sem fio é feito através de funções coordenadoras. O principal modo de acesso é provido pela função coordenadora denominada DCF *(Distributed Coordination Function)*. Caso seja necessário o serviço livre de contenção *(contention-free)*, um ponto de acesso *(Access Point - AP)* pertencente a uma rede que possua infra-estrutura pode provê-lo através de outra função coordenadora denominada PCF *(Point Coordination Function)*.

2.2.2 Acesso ao Meio usando o DCF

Dois limiares são criados assim que uma estação transceptora envia um determinado quadro no meio, como demonstrado na Figura 2.4, retirada de [18]. O primeiro limiar, denominado zona de alcance, zona de recepção ou zona de portadora, caracteriza-se por conter estações próximas o bastante do transceptor que não estejam a mais de um salto de distância. Neste caso as estações são capazes de decodificar o quadro corretamente. O segundo limiar, chamado de zona de detecção de portadora, contem estações que estão a uma certa distância do transceptor (mais de um salto de distância) e não conseguem decodificar o quadro corretamente, mas conseguem saber que o meio se encontra ocupado. Todas as estações que estejam na zona de detecção de portadora deverão usar o temporizador EIFS *(Extended Inter-Frame Space)* para o atraso da transmissão, por não conseguirem decodificar o quadro corretamente e com isso saber qual o tempo total da transmissão. Este temporizador tem como função diminuir o número de colisão de quadros.

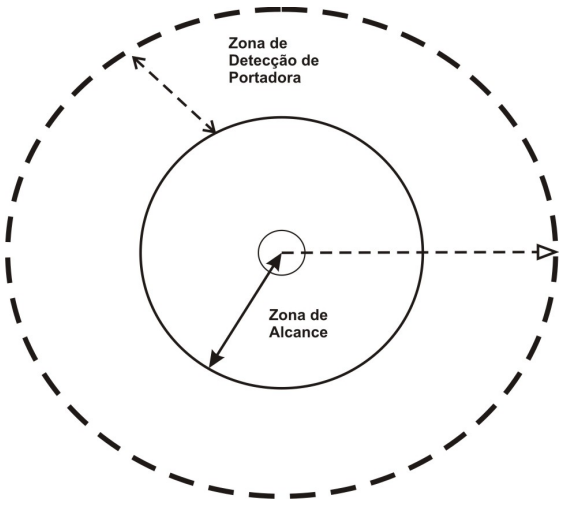

Figura 2.4: Limiares criados ao redor do transmissor.

Assim como todos os esquemas que utilizam o CSMA, o DCF primeiro verifica se o meio de transmissão está livre antes de transmitir seus dados. O DCF se comporta da seguinte forma, tomando

como base a Figura 2.5, retirada de [53], e tendo como exemplos a Figura 2.6 e a Figura 2.7, retiradas de [18], onde as linhas contínuas das figuras mostram a zona de portadora ou zona de recepção e as linhas tracejadas mostram a zona de detecção de portadora:

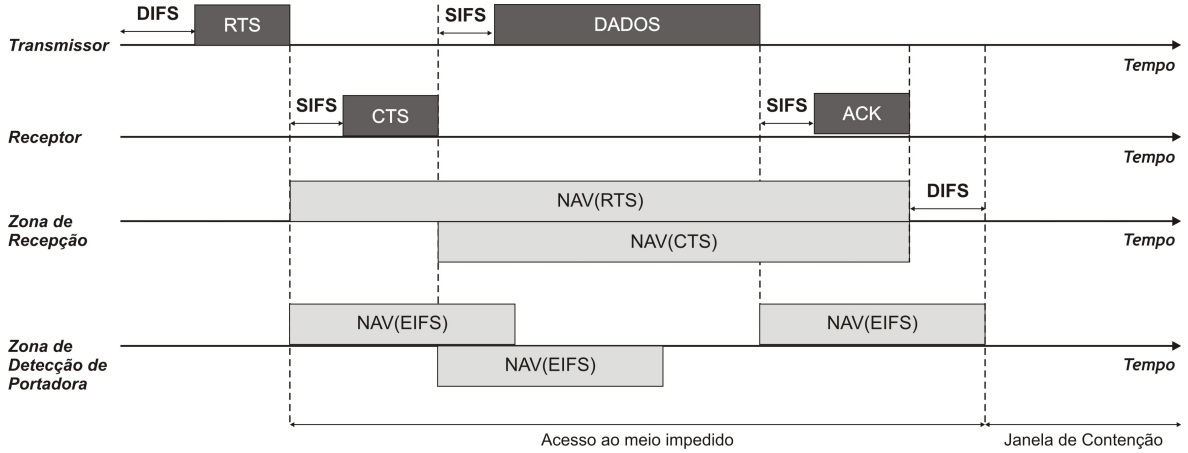

Figura 2.5: Funcionamento do DCF.

1. Antes do início de cada conexão, todas as estações devem esperar por um período de tempo DIFS *(Distributed Inter-Frame Space)*. Após este período, a estação que deseja enviar dados irá verificar se o meio está ocupado. Na Figura 2.5, o meio não estava ocupado, logo a estação poderá transmitir. A estação origem inicia a conexão enviando um quadro RTS para a estação destino requisitando conexão. Como mostrado na Figura 2.6, a estação **1** envia o quadro RTS para a estação de destino **2**. É possível notar também, através da Figura 2.6, a criação dos dois limiares de transferência de quadros, sendo que o limiar com a linha contínua refere-se à zona de alcance e o limiar com a linha tracejada refere-se à zona de detecção de portadora.

2. Sempre que uma estação vizinha escutar um quadro não endereçado a ela e estiver na zona de alcance deve decodificar o quadro, encontrar a informação que diz qual será o tempo total da transmissão, ajustar seu NAV *(Network Allocation Vector)* com este tempo e bloquear suas transmissões com o intuito de evitar colisão de quadros. Na Figura 2.6 é possível notar que, além da estação **2**, as estações **3**, **4**, **5** e **6** estão dentro da zona de alcance, logo poderão decodificar o quadro corretamente e setar seu NAV. Porém, as estações **7** e **9**, pertencentes à zona de detecção de portadora, conseguirão perceber que o meio está ocupado mas não conseguirão decodificar o quadro corretamente. Para que não hajam colisões de quadros, todas as estações que estejam na zona de detecção de portadora deverão setar seu NAV com o valor de EIFS. Vale ressaltar que as estações **8** e **10** poderão transmitir normalmente, por não estarem dentro dos dois limiares.

3. Assim que a estação destino recebe um quadro RTS, ela deve esperar por um período de tempo

SIFS *(Shortest Inter-Frame Space)* para que possa transmitir. Após este período a estação irá checar se o meio está ocupado. Como mostrado na Figura 2.5, o meio não se encontra ocupado, logo a estação destino pode enviar para a estação origem um quadro de resposta ao RTS, denominado CTS. Como mostrado pela Figura 2.7, a estação **2** envia o CTS para a estação **1**. Novamente é possível notar a criação dos dois limiares referentes à transferência de quadros.

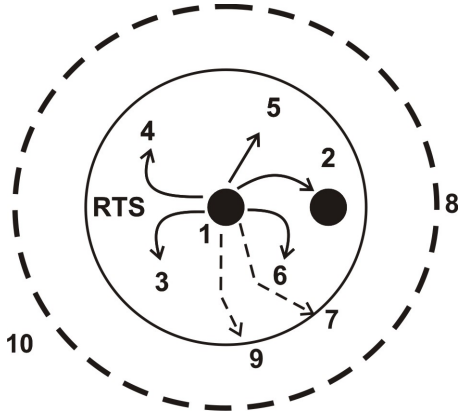

Figura 2.6: Envio do quadro RTS.

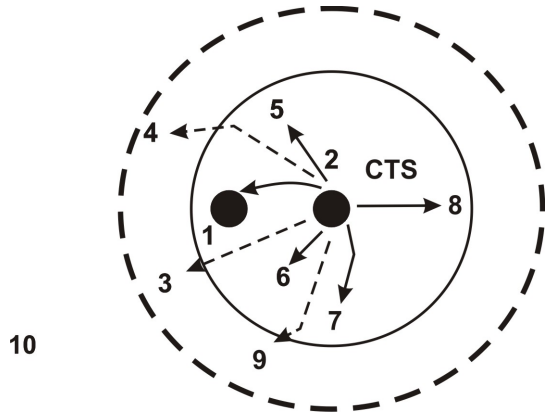

Figura 2.7: Envio do quadro CTS.

4. Todas as estações vizinhas que escutarem o CTS e estiverem na zona de alcance deverão decodificar o quadro, encontrar a informação que diz qual será o tempo total da transmissão, ajustar seu NAV com este tempo, porém, com um decréscimo devido a transferência do quadro RTS já ter ocorrido e bloquear suas transmissões com o intuito de se evitar colisão de quadros. Através da Figura 2.7 é possível notar que, além da estação **1**, as estações **5**, **6**, **7** e **8** fazem parte da zona de alcance, criada pela transmissão do quadro CTS, e poderão decodificar corretamente o quadro CTS e com isso ajustar o NAV. Entretanto, as estações **3**, **4** e **9**, pertencentes à zona de detecção de portadora, conseguirão perceber que o meio se encontra ocupado mas não conseguirão deco-

dificar o quadro corretamente. Com o intuito de se evitar colisões de quadros, todas as estações pertecentes à zona de detecção de portadora deverão ajustar o NAV com o valor de EIFS. Novamente vale ressaltar que estação **10** poderá transmitir normalmente por não estar dentro dos dois limiares.

5. Após o recebimento do quadro CTS, a estação destino deve esperar por um período SIFS para que possa transmitir o quadro de DADOS para a estação destino. Ao final deste período de espera, a estação irá checar novamente se o meio está ocupado para então enviar o quadro de DADOS. No exemplo citado anteriormente, a estação **1** envia o quadro de DADOS para a estação **2**.

6. Após o recebimento do quadro de DADOS, a estação destino espera por um período de tempo SIFS para enviar um quadro ACK para a estação origem. Assim que o período de espera termina, a estação destino irá checa se o meio está ocupado e envia o ACK para a estação origem. No exemplo citado anteriormente, a estação **2** envia o quadro de ACK para a estação **1**.

7. Todas as estações irão aguardar até o final do tempo contido no NAV para poderem transmitir quadros. Se por ventura o NAV de alguma estação que esteja na zona de detecção de portadora terminar antes que alguma transmissão que esteja ocorrendo, a estação irá novamente setar seu NAV com o valor contido em EIFS.

8. Após cada período de tempo, DIFS ou SIFS, para que sejam evitadas colisões, as estações devem checar se o meio encontra-se ocupado ou não. Uma estação somente enviará um determinado quadro caso o meio não esteja ocupado, senão ela terá que esperar por um novo período de tempo escolhido aleatoriamente, denominado período de espera *(backoff)* que está situado no intervalo de zero a **CWmin** *(Contention Window Minimum)*, sendo **CWmin** uma constate do protocolo. Ao final de cada período de *backoff* a estação fará a checagem novamente, porém, se o meio continuar ocupado o valor do *backoff* será dobrado tendendo a um valor máximo **CWmax** *(Contention Window Maximum)*, sendo **CWmax** uma constante do protocolo.

2.3 Consumo de Energia

Ao longo dos últimos anos inúmeras propostas têm sido criadas com o intuito de prolongar o tempo de vida das estações por elas serem alimentadas por baterias. Para que este objetivo seja alcançado, os protocolos MAC reduzem o consumo de energia modificando os parâmetros do transceptor, tais como o estado de operação do rádio (transmissão, repouso, ocioso e escuta), a potência de transmissão [41] e através do gerenciamento de energia *(Power Save)* [18], [3].

No gerenciamento de energia as estações entram em modo de baixo consumo de energia desligando os rádios de suas interfaces quando comandados [25].No controle de potência de transmissão (CPT) as estações são comandadas a enviar quadros diminuindo ou aumentando a potência do sinal para reduzir o consumo de energia das estações e prover maior reuso espacial da rede [41], [63], [32], [12]. Através do reuso espacial várias estações conseguem transmitir mais dados simultaneamente na rede.

Existem também outras linhas de pesquisa que tendem a lidar com estes problemas utilizando protocolos de roteamento que se encarreguem de escolher rotas ótimas visando um menor consumo de energia [29], [31], [62].

2.3.1 Controle de Potência de Transmissão

O controle de potência de transmissão (CPT) é o controle no qual a estação transmissora utiliza somente a quantidade de energia necessária para que o quadro enviado possa ser alcançado e decodificado pelos vizinhos a um salto de distância. Como consequência deste controle, o raio de alcance do quadro transmitido sofre uma diminuição. Porém, apresenta como vantagem o aumento do reuso espacial da rede, significando o aumento de tráfegos na rede, e um menor consumo de energia das estações [41].

Dentre os métodos de controle de potência clássicos, destacam-se os seguintes:

1. Protocolo **MACA** *(Multiple Access with Colision Avoidance)*: desenvolvido por Karn (1990) em [49], foi o primeiro protocolo a propor CPT em redes sem fio. A principal intenção deste protocolo era resolver os problemas do terminal exposto e escondido através da troca de quadros RTS/CTS utilizando o NAV. Entretanto, valendo-se desta idéia, o autor aproveitou a troca destes quadros de controle para propor o CPT. Um dado receptor, ao receber um quadro RTS, após fazer a leitura do nível do sinal recebido (RSSI) insere esta informação dentro do quadro CTS e o envia para o emissor. O emissor, após o recebimento do CTS, atualiza as informações a respeito do nível de sinal no emissor, para auxiliar na estimativa da potência de transmissão dos próximos quadros [41], [52].

2. Protocolo **PCMA** *(Power Controlled Multiple Access)*: desenvolvido por Jung e Vaidya (2002) em [28], permite comunicação entre transmissor e receptor com raio mínimo de propagação, permitindo outros tráfegos na rede sem que hajam colisões. O esquema utiliza dois canais diferentes, sendo um deles utilizado para o envio de quadros de dados e o outro para o envio de quadros de controle. Esses quadros de controle são sinais de ocupado *(busy tone)* que informam às estações próximas que o canal está ocupado. Tais sinais são usados para evitar os problemas do terminal exposto e escondido, ao invés de usar a troca de quadros RTS/CTS [52]. O protocolo PCMA também usa uma técnica que permite variar a potência de transmissão utilizada na transferência

do quadro de DADOS. Esta variação é útil para as estações que estejam na zona de detecção de portadora, devido ao tamanho desta zona ter sido diminuído por causa do CPT. Entretanto, criar este tipo de variação nos rádios atuais é bastante complexo, pois os rádios necessitam variar a potência de transmissão em um curto espaço de tempo utilizando um grande nível de precisão.

3. **Esquema Básico**: é baseado no diálogo de comunição usando quadros RTS-CTS-DADOS-ACK. Neste esquema, os quadros de controle (RTS-CTS) são enviados na máxima potência de transmissão e os quadros de dados (DATA-ACK) são enviados numa potência de transmissão mais baixa. O **Esquema Básico** funciona da seguinte maneira, tomando-se como base uma estação *A* sendo o transmissor e uma estação *B* sendo o receptor: no primeiro momento, a estação *A* envia o quadro RTS utilizando a máxima potência de transmissão; **B**, ao receber o RTS de **A**, compara a potência recebida com sua sensibilidade, calcula a potência mínima de transmissão que **A** deverá usar na próxima transmissão, insere a informação sobre a potência mínima a ser usada no quadro CTS e envia este quadro para **A**; a estação **A**, ao receber o quadro CTS, compara a potência de recebimento do quadro CTS com sua sensibilidade, calcula a potência mínima de transmissão que **B** deverá usar, insere a informação sobre a potência mínima a ser utilizada no quadro de DADOS e envia este quadro para a estação **B** utilizando a potência mínima passada pelo quadro CTS; a estação **B**, ao receber o quadro de DADOS, usa a potência mínima de transmissão contida no quadro para enviar o quadro ACK para a estação **A** [53].

Protocolos que utilizam o **Esquema Básico**, nos quais as estações enviam quadros RTS e CTS utilizando a máxima potência de transmissão e quadros de DADOS e ACK utilizando uma potência de transmissão menor, têm como conseqüência a criação de enlaces assimétricos [28], [53]. O problema do enlace assimétrico ocorre devido à seguinte conjuntura, tomando como base a Figura 2.8 e a Figura 2.9, retiradas de [28].

1. Inicialmente a estação **1** envia um quadro RTS, utilizando a potência de transmissão máxima, ao meio para a estação **2** e assim são criados os dois limiares descritos anteriormente, Figura 2.8 (a). Como a estação **3** se encontra na zona de alcance ou zona de portadora (ZP), ela conseguirá decodificar o quadro corretamente e irá ajustar seu NAV com o tempo da transmissão contido no RTS. As estações **4** e **5**, contidas na zona de detecção de portadora (ZDP) não conseguirã decodificar o quadro corretamente e terão que ajustar o NAV usando o EIFS. A estação **2** após receber o RTS, responde a estação **1** enviando um quadro de CTS, também utilizando a potência de transmissão máxima, e com isso são criados novamente os dois limiares, ZP e ZDP, Figura 2.8 (b). As estações **4** e **5**, presentes na ZDP não conseguirão decodificar o quadro corretamente e irão ajustar o NAV usando o EIFS.

2. Já no envio dos quadros RTS e CTS, feitos na máxima potência de transmissão, os quadros trocaram informações a respeito da potência de transmissão que deverá ser usada para o envio dos quadros de DADOS e ACK. A estação **1**, após receber o CTS da estação **2**, envia o quadro de DADOS com uma potência de transmissão menor previamente calculada e inserida no quadro CTS. Todas as estações que estejam na ZP irão decodificar o quadro corretamente e com isso setar o valor do NAV. As estações presentes na ZDP, estação **3** na Figura 2.9 (c), irão setar o NAV com o valor EIFS. Porém devido ao envio do quadro de DADOS ser feito utilizando-se uma potência de transmissão menor, o raio de alcance do sinal, bem como a zona de detecção de portadora, terão seus tamanhos reduzidos. Esta redução tem como consequência a não percepção de qualquer envio de dados pelas estações **4** e **5**, como mostrado na Figura 2.9 (c). Assim que o tempo contido no NAV das estações **4** e **5** expirar, elas poderão transmitir novamente como mostrado na Figura 2.9 (d). Esta assimetria no enlace pode acarretar em colisões, devido aos quadros de RTS e CTS serem enviados sempre na potência de transmissão máxima, como demonstrado na Figura 2.9 (d).

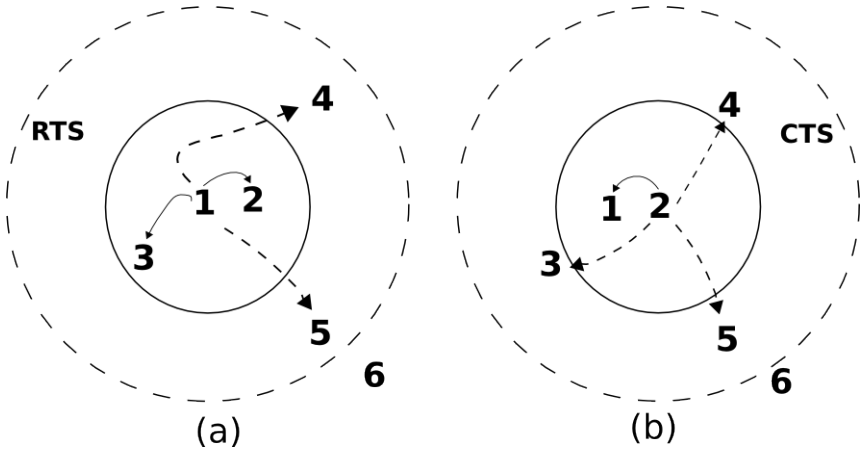

Figura 2.8: O problema de enlaces assimétricos. Envio dos quadros RTS e CTS.

O esquema proposto por [41] impede que existam problemas relacionados ao enlace assimétrico, por não usar os quadros de controle RTS e CTS. Para que as estações consigam atrasar suas transmissões de maneira satisfatória, o campo responsável pelo tempo da transmissão foi inserido diretamente no quadro de DADOS, para que as estações pudessem utilizar tal tempo no NAV. Este esquema também possui uma tabela responsável por guardar a potência de transmissão utilizada por todos os vizinhos de uma determinada estação, de maneira análoga ao Esquema Básico com Memória [52].

Correia (2006) propôs quatro diferentes protocolos para CPT, porém este trabalho terá como estudo os protocolos denominados de Atenuação e AEWMA *(Atenuação com filtro EWMA – Exponentially Weighted Moving Average)*. O primeiro protocolo desenvolvido, denominado de Interação, não foi

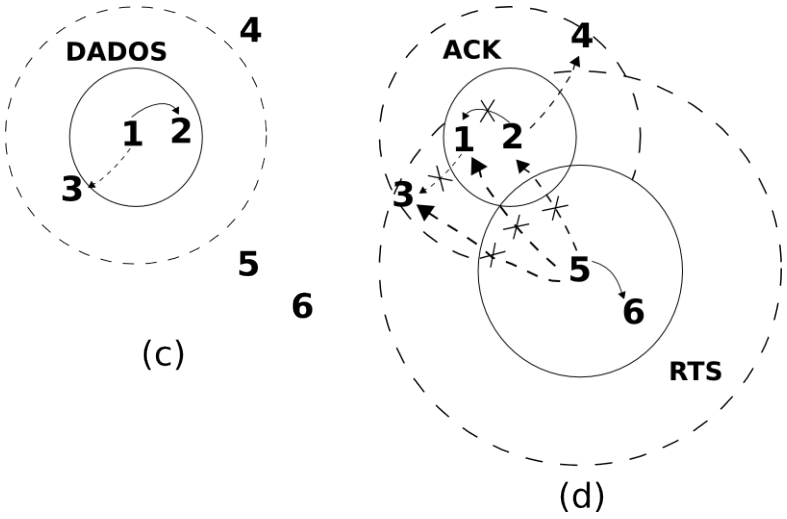

Figura 2.9: O problema de enlaces assimétricos. Envio dos quadros RTS, de DADOS e ACK.

estudado por ter apresentado resultados ruins, conforme demonstrado em [41] e o último protocolo criado, denonimado Híbrido, não foi analisado por ser demasiadamente complexo para este trabalho.

Para todos os protocolos desenvolvidos em [41] existem algumas restrições a serem seguidas:

1. a relação entre o sinal e o ruído deve garantir que o sinal seja decodificado corretamente no receptor (relação sinal ruído desejado ou SNR *(Signal Noise Ratio)* desejado);

2. a potência de transmissão deve compensar a atenuação no meio, de forma que o sinal ainda possa ser decodificado no receptor, denominado *Ganho*, dado por:

$$G = \frac{PRX}{PTX} \tag{2.1}$$

3. o quadro deve ser recebido em um nível de potência, acima de um limite mínimo, denominado *RXdesejado*, que garanta sua decodificação correta:

$$(PRX \geq RXdesejado) \tag{2.2}$$

4. a potência mínima de transmissão deve estar dentro dos limites nominais do rádio:

$$(PTX_{limite\ inferior} \leq PTX_{min} \leq PTX_{limite\ superior}). \tag{2.3}$$

O protocolo de CPT denominado protocolo de Atenuação desenvolvido por [41] funciona da seguinte maneira: de tempos em tempos as estações amostram o nível de ruído do meio quando não

ocorrem transmissões para determinar o ruído base N_B. Uma estação transmissora, ao enviar um quadro para uma estação receptora, informa a potência de transmissão no cabeçalho do quadro. A estação receptora, ao receber o quadro do transmissor, amostra o nível do sinal recebido *(RSS - Received Signal Strength)* e calcula a potência mínima de transmissão (PTX_{min}), dada pela equação:

$$PTX_{min} = \max \left(\frac{Rx_{desejada}}{G_{T \to R}}, \frac{SNR_{desejado} \times N_B}{G_{T \to R}} \right) \tag{2.4}$$

A equação (2.4) garante que as restrições *1* e *4*, descritas anteriormente, sejam atendidas. Por fim, a estação receptora envia o quadro de confirmação ACK de volta para o transmissor com o valor PTX_{min} dentro do quadro, para que seja usado em subsequentes transmissões.

O protocolo de Atenuação sofre da flutuação da potência calculada, o que aumenta a perda de quadros. Esta perda ocorre devido aos parâmetros de entrada como ruído médio, tensão da bateria e potência de recepção estarem sempre mudando por causa das variações do ambiente e da bateria.

O protocolo AEWMA estende o protocolo de Atenuação e soluciona o problema da flutuação da potência de transmissão por usar uma função de amortização EWMA. O EWMA é uma função média móvel ponderada exponencial, onde os valores mais antigos são decrementados exponencialmente. O valor de saída da função EWMA é dado por: $O_i = O_{i-1} \times (1 - \alpha) + v_i \times \alpha$, onde O_{i-1} é a potência armazenada na lista de potência usada para o envio de quadros para os vizinhos, v_i é dado pela equação (2.4) e α é um fator de ponderação, onde $0 \leq \alpha \leq 1$.

O protocolo AEWMA possui o seguinte comportamento: uma estação transmissora, ao enviar um quadro para o receptor, insere no cabeçalho do quadro a potência de transmissão utilizada no envio. A estação receptora amostra o nível de sinal do quadro recebido (RSSI) e do ruído local, calcula a potência mínima de transmissão através da equação (2.4), utiliza o resultado da equação (2.4) na função de amortização EWMA e envia o resultado da função dentro do cabeçalho do quadro de resposta ACK utilizando a mesma potência que o transmissor usou para enviar o quadro de DADOS.

Segundo [41], as técnicas para CPT que utilizam os protocolos Interativo, de Atenuação, AEWMA e o Híbrido, mostraram-se capazes de reduzir o consumo de energia em até 57% e uma melhoria da taxa de entrega em 10% em relação aos protocolos de CPT existentes.

2.4 Ataques em Redes Sem Fio

Inúmeros ataques são encontrados em redes sem fio na literatura corrente. Enquanto alguns ataques são específicos de uma determinada camada da pilha TCP/IP [33], [59], outros ataques afetam todas as camadas simultaneamente.

Estudos que mostram o estado da arte dos ataques e defesas que influenciam as camadas da pilha

TCP/IP em redes sem fio foram demonstrados em [5], [27]. A Tabela 2.1, retirada de [5], mostra alguns ataques que afetam as camadas do TCP/IP.

Tabela 2.1: *Camadas x Ataques*

Camadas	**Ataques**
Camada de Aplicação	repudiation, data corruption
Camada de Transporte	session hijacking, syn flooding
Camada de Rede	wormhole, blackhole, byzantine, flooding, resource consumption, location disclosure attacks
Camada de Enlace	traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Camada Física	jamming, interceptions, eavesdropping
Multi-Camada	DoS, impersonation, replay

Em [43] é demonstrado o estado da arte dos ataques e defesas referentes à camada de rede do TCP/IP. Alguns estudos definiram o estado da arte acerca dos ataques e defesas referentes ao protocolo 802.11, dentre eles pode-se citar [8] e [47].

Existem também outras linhas de estudo que tendem a tratar da tolerância da rede devido aos esquemas preventivos e reativos não serem capazes de contornar os ataques que venham a sofrer. Esta tolerância deve garantir a sobrevivência da rede mesmo estando sob condições adversas. Este novo conceito, chamado de sobrevivência *(Survivability)*, foi definido em [45].

Diversos tipos de ataques que desvirtuam o comportamento normal do 802.11 são apresentados na literatura. Segundo Lei Guang (2006), o mau comportamento das estações pode ser classificado de duas formas, (1) comportamento guloso e (2) comportamento malicioso [40].

Os atacantes que possuem comportamento guloso geralmente tendem a obter o meio para uso próprio para que seu desempenho possa ser aumentado. Devido às estações em uma rede sem fio, que utilizem tecnologia *Wi-Fi*, terem que utilizar multi-salto [9] para repassar quadros para seus vizinhos, uma estação maliciosa, para aumentar seu desempenho poderia não repassar quadros conservando a energia de sua bateria por meio das vulnerabilidades encontradas no 802.11. Tal estação maliciosa poderia utilizar ataques como, o ataque de redução do tempo de *backoff*, denominado *backoff attack* [54], [30], o ataque que permite o uso exagerado do temporizador NAV usando-se valores altos, denominado *nav attack* [7], [19], e o ataque de diminuição do período de tempo SIFS, denominado *timeout attack* [40].

Os ataques maliciosos tendem a desvirtuar o completo funcionamento da rede ao negar completa-

mente o serviço das estações e fazer com que o vazão da rede caia para quase zero, na maioria dos casos. Kuzmanovic (2006), em [35], classificou os ataques maliciosos de duas formas, em ataques de negação de serviço com alta taxa de transferência de dados *(high-rate DoS attacks)*, como o ataque de negação de serviço distribuído *(DDoS)* [17], e em ataques de negação de serviço com baixa taxa de transferência de dados *(low-rate DoS attacks)*, como o ataque de redução da qualidade serviço *RoQ attack* [24], [67].

Inúmeras abordagens de tratamento para os ataques gulosos e maliciosos têm sido abordadas na literatura. Existem alguns mecanismos de defesa bastante eficazes contra ataques gulosos, como o DOMINO [55] e o DREAM [21]. Ataque de negação de serviço com alta taxa de transferência de dados também possuem alguns dispositivos de defesa, como demonstrado por [17] e [69]. Porém, ataques de negação de serviço com baixa taxa de transferência de dados possuem poucas abordagens efetivas, devido à sua complexidade de tratamento e detecção, como demonstrado por [22] e [23].

Nas próximas subseções serão contextualizados os ataques gulosos mencionados anteriormente, por serem ataques mais clássicos citados na litetura. Será também demonstrado o impacto que tais ataques ocasionam na rede e os seus respectivos mecanismos de defesa encontrados na literatura.

2.4.1 Ataque de Diminuição do Backoff

A função coordenadora padrão do 802.11, DCF, utiliza um algoritmo randômico para seleção do período de *backoff*. Este período de tempo, como mencionado na Seção 2.2.2, é usado quando alguma estação encontrar o meio ocupado.

Como demonstrado por Pradeep Kyasanur em [54] e [30], uma estação maliciosa, explorando a incapacidade de outras estações preverem se uma determinada estação maliciosa utilizou o tempo de backoff adequadamente ou não, poderia diminuir seu backoff e com isso ganhar prioridade de acesso ao canal. Este comportamento tem como conseqüência a diminuição da vazão de dados das outras estações da rede por encontrarem o canal sempre ocupado e com isso aumentar seu tempo de *backoff* exponencialmente.

Impacto causado pelo ataque de diminuição do backoff

Em [38] os autores demonstraram o impacto do ataque de diminuição de *backoff* em uma rede, através do simulador NS2 [14]. Foram usados na simulação dois tipos de protocolos de roteamento diferentes, o DSR *(Dynamic Source Routing)* [15] e o AODV *(Ad hoc On-Demand Distance Vector)* [51]. Foi usada também uma topologia com um cenário estático com 50 estações, sendo uma estação maliciosa, em uma área de 1500m X 300m, com tamanho de pacote fixado em 512 bytes e tráfego CBR *(Constant Bit Rate)* com dois tipos de taxas de envio variando o número de estações origem: 10 origens

com uma taxa de 4 pacotes por segundo e 30 origens com 10 pacotes por segundo.

Foram feitas três comparações entre os dois protocolos de roteamento DSR e AODV sofrendo o ataque de diminuição do *backoff*. A primeira comparação feita teve como foco medir a taxa de pacotes entregues por cada um dos protocolos. Segundo os autores, não existe muita diferença entre os dois protocolos nesta primeira comparação.

A segunda comparação feita teve como foco o atraso médio de ambos os protocolos de roteamento. Para o caso com 10 origens os dois protocolos têm o mesmo comportamento. Porém, quando o número de origens aumenta para 30, o protocolo DSR passa a ter o atraso maior que o AODV. A explicação para o DSR ter maior atraso médio que o AODV é que, devido à ocorrência de maior congestionamento e colisões na rede, o AODV consegue ter uma resposta mais rápida por descobrir novas rotas menos congestionadas que o DSR.

A terceira comparação teve como função medir a carga de roteamento entres os dois protocolos de roteamento. Em ambos os casos, para 10 e 30 origens, o AODV teve uma carga de roteamento maior que o DSR. Isto ocorre devido ao fato de ser mais difícil para o protocolo AODV encontrar um novo caminho por depender do descobrimento de rotas e por este descobrimento ser feito enquanto a rede está sendo atacada, enquanto o DSR depende do armazenamento de rota, criado no início da transmissão, para encontrar um novo caminho.

Defesas contra o ataque de diminuição do backoff

Existem algumas abordagens de defesa estudadas na literatura para conter este ataque, porém as abordagens de [55] e [54] tem maior destaque.

A abordagem de defesa criada por Pradeep Kyasanur em [54] usa as regras do 802.11, porém modifica o mecanismo de backoff em alguns pontos, ao incluir um campo chamado *attemptNumber* no quadro RTS e ao incluir um campo chamado *nextBackoff* no quadro CTS.

O seguinte algoritmo é seguido quando uma estação transmissora **S** deseja enviar dados para uma estação receptora **R**:

1. Quando **S** deseja enviar um quadro para **R** pela primeira vez, como citado na Seção 2.2.2, a estação deve esperar por um período de tempo DIFS para enviar o quadro. Assim que o DIFS termina, caso o meio não esteja ocupado, a estação **S** enviará um quadro RTS para **R** após ajustar o valor de *attemptNumber* para 1. Se o meio estiver ocupado, a estação **S** irá gerar um valor randômico do *backoff* entre 0 e CW_{min} e esperar até que o *backoff* termine.

2. Assim que **R** recebe o RTS de **S**, a estação **R** gera um *backoff* randômico X entre 0 e CW_{min} e envia um quadro CTS de volta para **R** após ajustar o valor do campo *nextBackoff* com o valor

de X. A estação **R** então armazena este valor X como o *backoff* esperado para as próximas transmissões de **S**.

3. Após **S** receber o CTS, a estação armazena o valor do campo *nextBackoff* como sendo o valor de *backoff* para suas próximas transmissões. Logo, quando **S** necessitar de enviar um quadro para **R**, após ter feito uma primeira transmissão, **S** usará o valor contido em *nextBackoff* para escutar o meio e enviar o quadro ao final deste tempo.

4. Após enviar um quadro RTS para **R**, se nenhum quadro CTS for recebido até o fim do temporizador, o valor de *attemptNumber* é incrementado e CW é dobrado, limitado a um máximo de CW_{max}. Um novo valor *Y* para o *backoff* é então computado através de uma função determinística f dada por: $Y = f(nextBackoff, nodeID, attemptNum) \times CW$, na qual *nextBackoff* é o valor armazenado do backoff, *nodeID* é um valor de identificador único (endereço MAC por exemplo) e *attemptNum* é o número de tentativas anteriores sem sucesso. O RTS é então transmitido após o tempo de *Y* expirar e caso o meio não esteja ocupado.

Além de um algoritmo para o envio de quadros, os autores também demonstraram alguns procedimentos para a detecção do mau comportamento de uma suposta estação atacante.

Designou-se **M** como sendo a estação receptora e monitora, na qual é responsável por observar a transmissão da estação transmissora **S** para detectar um possível mau comportamento. A estação **M** possui um contador *IdleCounter*, responsável por contar os slots de tempo que não estão ocupados, além de monitorar todas as transmissões armazenando os valores de *nextBackoff* enviados pelas estações transmissoras para as estações receptoras.

Quando **M** envia um quadro ACK reconhecendo o dado recebido de **S**, **M** armazena o valor *IdleCounter* na hora como sendo o tempo $eTime_S$, quando **S** começará a decrementar o valor de *backoff*. Quando **M** recebe um quadro RTS da estação **S** (exceto quando eles estão se comunicando pela primeira vez), **M** pode verificar se a estação **S** esperou pelo número requerido de slots não ocupados. O número de slots B_{exp} na qual é suposto que **S** espere é dado por: $B_{exp} = nextBackoff_S + Y$, na qual *Y* é computado como $\sum_{i=2}^{attemptNum} f(nextBackoff_S, nodeID, i) * CW_i$, onde *attemptNum* é o número da tentativa de transmissão enviada no quadro RTS, $nextBackoff_S$ é o *backoff* gerado por **M** para a estação **S**, *nodeID* é o identificador único de **S** e CW_i é o valor da janela de contenção *(Contention Window)* para a i-ésima tentativa de transmissão e é dado por $CW_i = \min\left(CW_{min} \times 2^{i-1}, CW_{max}\right)$.

A estação **S** é dita como estando conforme a especificação do protocolo se o atual número de slots não ocupados ultrapassar a função B_{obsr}, sendo esta função computada como a diferença do valor atual de *IdleCounter* e $eTime_S$, que satisfaz a condição $B_{obsr} \geq \alpha \times B_{exp}$, $0 < \alpha \leq 1$, onde α é uma constante do protocolo. Se a condição acima não for satisfeita, então a estação **S** é designada como

sendo um provável atacante.

Quando a estação monitora **M** identifica mais que um determinado patamar *THRESH* de desvios feitos por **S** nos últimos *K* quadros (*THRESH* e *K* são constantes do protocolo), **M** designa a estação **S** como sendo mau comportada e toma uma ação adequada, como informar as camadas acima ou tomar alguma ação corretiva na camada MAC.

Uma ação corretiva poderia ser uma esquema que penaliza a estação atacante por estar tendo um mau comportamento.

Quando um quadro RTS é recebido pelo estação **M**, ela é capaz de comparar o valor esperado do *backoff* com o atual valor do *backoff*, para identificar desvios. A diferença *D*, computada de acordo com a função $\max\left(\alpha \times B_{exp} - B_{obsr}, 0\right)$, é adicionada ao *nextBackoff* gerado randomicamente na qual foi mandado no CTS.

O esquema de correção penaliza as estações maliciosas pelo benefício ganho por terem menos colisões por transmissões efetuadas com sucesso. O número de *slots* de tempo adicionados é dado através da função $AS = \sum_{i=aNum_{MB}+1}^{aNum_{MB}+E_{diff}} f(nextBackoff_{MB}, nodeID, i) \times CW_i$, onde $aNum_{MB}$ é o atual número de colisões sofridas pela estação atacante *MB*, CW_i é a Janela de Contenção *(Contention Window)* para a i-ésima tentativa de transmissão, *nodeID* o identificador único de **MB** e E_{diff} um valor encontrado através da análise teórica desenvolvida em [10].

Logo a penalidade *PENALTY* é dada por: $PENALTY = (\alpha \times B_{exp} - B_{obsr}) + AS$, sendo que B_{exp} e B_{obsr} foram apresentados anteriormente.

Esta abordagem de defesa criada por [54] é dispendiosa, devido à necessidade de mudança no protocolo 802.11. Uma abordagem alternativa, que não necessita de mudanças no protocolo, foi proposta por [55].

O mecanismo de defesa proposto por [55], denominado DOMINO, utiliza três testes para o *backoff* para determinar se uma determinada estação é maliciosa, o *backoff* máximo *(Maximum Backoff)*, o *backoff* real *(Actual Backoff)* e o *backoff* consecutivo *(Consecutive Backoff)*:

1. **Backoff Máximo** *(Maximum Backoff)*: o teste se baseia na idéia de que o *backoff* tende a $CW_{min} - 1$. A partir desta propriedade, as estações suspeitas tendem a ter o valor de *backoff* menor que um determinado patamar *threshold(maxbkf)*. Segundo os autores, na simulação feita esse valor de patamar é igual a $\frac{CW_{min}}{2}$. Porém, esse teste falha contra estação maliciosa mais inteligente que envia ao menos um quadro com o *backoff* menor ou igual ao patamar.

2. **Backoff Real** *(Actual Backoff)*: neste teste é feita a média do *backoff* a partir dos quadros enviados por uma estação e a média do *backoff* de todos os quadros recebidos pelo AP. Se o *backoff* médio da estação for menor que o *backoff* médio medido pelo AP, a estação é suspeita de ser ma-

liciosa. Porém, esse teste falha na detecção quando a estação atacante utiliza *interframe delays*, como o controle de congestionamento do TCP, devido a este teste utilizar os *delays* ao invés do *backoff*, adicionando o período de ausência entre as transmissões da mesma origem.

3. **Backoff Consecutivo** *(Consecutive Backoff)*: este teste é usado principalmente em casos onde existe tráfego TCP, na qual representa cerca de 91% do tráfego real na rede. Ele é feito da seguinte maneira, se o AP observa dois quadros não consecutivos de uma determinada estação **S**, o AP pode considerar que o tempo de ausência entre os dois quadros se deve ao *backoff* juntamente com o período de DIFS. Logo, o sistema pode coletar diversos *backoffs* de **S** e realizar o teste como no **Backoff Atual**.

Para que sejam diminuídos o número de falsos positivos, uma estação somente será considerada suspeita após exceder um patamar de K vezes, sendo K uma constante definida pelo mecanismo de defesa. Após a verificação de que a estação é maliciosa, cabe ao AP definir a penalidade que será dada a esta estação.

Através de simulações feitas usando-se o ns2 [14], os autores demonstraram a eficácia do DOMINO. Foi usada uma topologia em círculo com 8 estações enviando dados para o AP, que se encontra no centro do círculo. A distância das estações até o AP é de 50 metros e consegue enviar quadros umas as outras sem necessitar de utilizar multi-salto.

Foram utilizados dois tipos de tráfegos para demonstrar os testes explicados anteriormente, um tráfego UDP, no qual além do atacante, 7 estações enviam tráfego CBR *(Constant Bit Rate)* para o AP a uma taxa de 200 pacotes por segundo, sendo que o atacante também utiliza tráfego CBR e um tráfego TCP, no qual cada uma das oito estações executa uma aplicação FTP, sendo uma estação maliciosa.

Através de gráficos os autores demonstraram a eficácia do DOMINO para os dois tipos de tráfegos mencionados acima, tendo uma eficácia alta para encontrar as estações maliciosas e por demonstrar ter baixo número de falsos positivos. Além de demonstrar a eficácia do DOMINO no simulador ns2, os autores fizeram também simulações em um ambiente real demonstrando novamente a sua eficácia.

2.4.2 Ataque de Timeout

A principal função coordenadora do 802.11, DCF, utiliza três janelas de tempo para o acesso ao canal, o SIFS, o DIFS e o EIFS, sendo as duas primeiras as mais importantes. Como mostrado anteriormente, o DIFS é usado no início de qualquer transmissão, ou seja, sempre que uma estação desejar enviar qualquer dado deve esperar por este período de tempo. O SIFS é usado pelas estações após o quadro RTS ter sido enviado e antes do envio de qualquer outro quadro. Segundo [39], que propôs este novo ataque, um atacante qualquer poderia ter total controle sobre o meio mandando quadros sempre

antes do término do SIFS e sempre depois do término do DIFS, quando o canal não estiver ocupado.

O ataque de *timeout* geralmente tem efeito em dois casos. O primeiro caso acontece quando a estação destino da transmissão é a estação atacante e deliberadamente seleciona valores maiores para o SIFS e o segundo caso quando a estação origem da transmissão é a estação atacante e seleciona valores menores para o SIFS.

No primeiro caso, quando a estação destino seleciona valores maiores para o SIFS, quadros RTS ou de DADOS enviados pela estação origem são forçados a terem seu temporizador para cada quadro esgotado *(timeout)*. Após sucessivas retransmissões sem sucesso a estação origem será obrigada a descartar o quadro e reportar a quebra de enlace à camada de roteamento. Este ataque tem como consequência o rompimento do processo de descobrimento de rota feito pelo protocolo de roteamento forçando os pacotes das estações a passarem por rotas que não sejam ótimas. Logo, uma estação atacante com este comportamento iria conservar sua bateria por não repassar pacotes, que não sejam interessantes, para outras estações, além de poder acessar o meio com maior facilidade e ter sua vazão de dados aumentada sem ter que realizar qualquer outro tipo de ataque.

No segundo caso, a estação origem que seleciona valores menores para o SIFS iria ter seus temporizadores esgotados antes da chegada dos quadros CTS e de ACK. O objetivo desta ataque é o rompimento do descobrimento de rota e a interrupção do fluxo de dados forçando os quadros a serem re-roteados em torno dos atacantes.

Impacto causado pelo ataque de timeout

Em [39] os autores mostram o impacto do ataque de *timeout* usando o simulador ns2 [14]. Foi usada uma topologia que gera aleatoriamente a posição de 50 estações, sendo que cada estação é estática e possui raio de transmissão de 250m.

Na rede existem 10 fluxos de dados, todos os fluxos usando tráfego CBR a uma taxa de 8 pacotes por segundo. Foi usado o protocolo de roteamento AODV [51], uma fila de espera de 50 pacotes, taxa de bits de canal de 2Mbps e tempo de simulação de 200 segundos. Inicialmente todas as estações possuem comportamento padrão, porém, após todos fluxos serem estabilizados, depois de 50 segundos, uma porcentagem das estações passa a ter mau comportamento.

Primeiramente foi escolhido um valor para o SIFS de 13 μs, sendo o valor padrão de 10 μs. Assim que o ataque se inicia, é possível notar que todos os fluxos que passam pelas estações maliciosas são rompidos fazendo com que estes fluxos sejam obrigados a encontrar outra rota. É mostrado que, quando a porcentagem de estações maliciosas da rede é de 20% do número total de estações, o número de pacotes repassados pelos nós é de quase 9.000 pacotes a menos que o normal, sendo o comportamento normal da rede o de repassar 20.000 pacotes sem a existência de atacantes. Neste primeiro experimento

é mostrado também que as estações maliciosas são responsáveis pelo descarte de quase 50% de pacotes entregues quando a porcentagem de estações maliciosas passa de 20%.

Em um segundo caso, foi usado o mesmo cenário anterior com 20% de estações maliciosas e considerado o número de pacotes repassados por estas estações. Como resultado, o número de pacotes repassados pelos atacantes foi em torno de 1.500 pacotes, ou seja, 3.500 pacotes a menos que o caso normal.

Por último, os autores demonstraram o impacto de um ataque híbrido, na qual um único atacante usa um valor maior para o SIFS para o tráfego cruzado, o valor normal do SIFS para o tráfego local e seleciona um menor valor de *backoff* para seu próprio tráfego. A simulação foi feita em uma rede que possui topologia em grade de 4x4 estações, com 8 fluxos CBR a uma taxa de dados de 0,4 Mbps cada um. O atacante foi inserido no centro da grade e sempre selecionava o valor do SIFS para 13 μs. Para o ataque de *backoff* a estação maliciosa selecionava CW_{min} igual a 3 e CW_{max} igual a 127, para seu próprio tráfego. Comportando-se normalmente, a estação maliciosa consegue atingir uma vazão de 125 kbps, porém a estação consegue obter a vazão de quase 200 kbps somente mudando o valor do SIFS e de 350 kbps ao executar o ataque híbrido.

Defesa para o ataque de timeout

Em [40] os autores estudaram um mecanismo de defesa para o ataque de *timeout*. Como mostrado na descrição do ataque, é possível notar que tanto a estação transmissora quanto a estação receptora podem ser estações atacantes, logo, o esquema de detecção deve ser implementado para ambos os casos.

No primeiro caso (primeiro esquema de reação), quando a estação transmissora é maliciosa **(M)**, a estação receptora **(R)** deve seguir três etapas:

1. **Identificação do suspeito**: a estação **R** guarda a seqüência de quadros RTS enviadas a ela devido a necessidade de saber quando quadros RTS repetidos são enviados novamente. Se **R** recebe um quadro RTS pela primeira vez de **M**, **R** inicializa um parâmetro denominado $RTS_{seq(M)}$ em 1, espera pelo período de tempo SIFS, envia um quadro CTS para **M** e inicia o temporizador de tempo *(timeout)* esperando por um quadro de DADOS de **M**. Quando a estação **R** recebe algum quadro RTS repetido ela não consegue concluir o que aconteceu com seu quadro CTS enviado anteriormente devido a: **(a)** a estação transmissora é maliciosa, **(b)** a estação transmissora é vítima de um ataque de uma terceira estação que intencionalmente enviou um quadro ao mesmo tempo que o CTS e **(c)** a estação transmissora está sob um ataque que ocorre em sua vizinhança. Através de todas estas alternativas é possível prever que a estação transmissora não é confiável. **R** consegue avaliar o nível de confiança de uma determinada estação transmissora através de

um parâmetro denominado *badCredit*. Quando o segundo RTS chega a **R** durante o *timeout*, a estação **M** provavelmente é uma estação maliciosa e seu *badCredit* é aumentado de forma brusca (aumentando-o com o auxílio de uma constante ou dobrando seu valor). Se o segundo RTS chegar depois do *timeout*, provavelmente a estação **M** seja vítima de um ataque e seu *badCredit* é incrementado em 1. Uma vez que *badCredit* alcance um determinado patamar, **M** torna-se uma estação suspeita e **R** chama pelo esquema de ajustamento.

2. **Ajustamento do timeout**: este esquema é utilizado para certificar o correto diagnóstico da estação **M**. Uma vez que **M** é designada como suspeita, **R** irá ajustar seu SIFS para um menor valor **SIFS'**, ou seja, se SIFS equivale a 10 μs, **SIFS'** irá valer 2 μs. É possível notar que, usando-se um valor menor para o SIFS, o valor do *timeout* é aumentado e nenhum ataque irá acontecer. Após o envio do CTS, **R** irá ver qual a reação de **M**.

3. **Manipulando o atacante**: uma vez enviado o CTS para **M** com um menor valor para o SIFS, se **R** receber o quadro de DADOS de **M** irá significar que: (1) **M** não está mais sob ataque, (2) **M** não está ciente do sistema de detecção implementado e (3) **M** está ciente porém não quer que seu nível de confiança seja diminuído. Se por ventura **R** não venha a receber o quadro de DADOS de **M**, significa que **M** detectou a reação de **R** e ajustou seu SIFS para intencionalmente descartar o CTS ou ainda está sob ataque. Em todos os casos, **M** não é mais confiável para qualquer tipo de transmissão e tem seu nível de confiança diminuído por **R**. Este monitoramento continua por mais algum tempo até que o nível de confiança de **M** fique abaixo de determinado patamar de confiança, determinado pelo mecanismo de defesa, fazendo com que **R** chame o segundo esquema de reação [21].

No segundo caso, quando a estação receptora é maliciosa **(M)**, a estação transmissora **(T)** deve seguir 3 etapas:

1. **Identificação do suspeito**: quando **T** deseja transmitir dados ele envia primeiramente o quadro RTS para **M**, incrementa o valor de $RTS_{seq(M)}$ afim de saber o número de quadros RTS enviados com mesmo número de seqüência e inicia seu *timeout* esperando pelo envio do CTS correspondente. Se **M** não for um atacante, ele enviará o quadro CTS assim que o meio não estiver ocupado, senão, ele irá atrasar a transmissão do CTS por ter aumentado seu valor do SIFS. A estação **T** irá esperar pelo quadro CTS até que o *timeout* expire. Depois que o *timeout* expirar, **T** irá enviar novamente o RTS para **M**. Existem dois tipos de cenários distintos para este caso: (1) **M** atrasou o envio do CTS para **T** por ter aumentado ligeiramente o valor de SIFS e (2) **M** seleciona um valor muito grande para o SIFS ou **M** tem seu NAV indicando que o meio está ocupado. No primeiro cenário, **T** irá incrementar um contador denominado $CTS_{seq(M)}$ para indicar o número

de quadros CTS que **M** atrasou e o punirá incrementando em 1 o valor do *badCredit* para a estação **M**. No segundo cenário **T** somente irá incrementar o valor de *badCredit* da estação **M** em um. Uma vez que o parâmetro *badCredit* da estação **M** venha a atingir um determinado patamar, sendo este parâmetro uma constante do protocolo, **M** se tornará um suspeito e **T** irá chamar o primeiro esquema de reação.

2. **Ajustamento do timeout**: Uma vez que a estação **M** seja considerada suspeita, **T** irá incrementar o valor do seu SIFS para **SIFS'** fazendo que o valor do *timeout* para o quadro CTS também aumente.

3. **Manipulando o atacante**: Após **T** transmitir o RTS novamente com o valor do SIFS aumentado, se **T** receber o CTS de **M** dentro do *timeout* ajustado indicará que: (1) a estação **M** não é mais maliciosa, ou (2) **M** não sabe sobre o esquema de reação de **T** ou (3) **M** silenciosamente segue o ajustamento para evitar a diminuição do seu nível de confiança. Como resultado **T** irá enviar de volta o quadro de DADOS. Se **M** continuar atrasando o envio do CTS, indicará que **T** não escolheu um valor alto o suficiente para o SIFS e terá que sofrer um reajustamento até um valor de SIFS, sendo este valor uma constante do mecanismo de defesa. Toda vez que **T** reage aumentando o valor do SIFS e do *timeout*, ele decrementa o parâmetro *badCredit* da estação **M**. Como mencionado no primeiro caso, após o nível de confiança de **M** alcançar um determinado patamar, a estação **T** irá chamar o segundo esquema de reação [21].

Os autores, através de simulações feitas usando-se o simulador ns2 [14], demonstraram a eficácia deste mecanismo de defesa. Para a simulação foi usado um cenário com uma topologia em grade com 48 estações com comportamento normal e uma estação maliciosa, separadas a uma distância de 100 metros. São gerados 8 fluxos de transmissão de dados CBR. Devido à função de detecção para transmissão ser similar à função de detecção para recepção, os autores simularam os ataques tendo como base o transmissor bem comportado e um receptor malicioso. O SIFS da estação maliciosa foi ajustado em 7 μs, enquanto as outras estações tiverem o SIFS ajustado em 10 μs. Na presença de uma estação suspeita, uma estação comportada invocaria o primeiro sistema de reação reduzindo seu SIFS para 2 μs. Porém, é considerado que a estação obedeça ao primeiro esquema de reação, sendo que o segundo esquema de reação, onde as estações negligenciariam a primeira reação, foi apresentado somente em [21]. Este mecanismo de defesa proposto consegue encontrar 100% das estações maliciosas, porém, a taxa de detecção na qual estações comportadas são erroneamente diagnosticadas como suspeitas está compreendida entre 10 a 20% e varia conforme o patamar *creditThreshold*.

2.4.3 Ataque de Abuso do NAV

O 802.11 usa o CSMA/CA para evitar os problemas do terminal escondido e terminal exposto através da troca de quadros RTS e CTS. As estações que desejam transmitir quadros necessitam indicar a duração da transmissão através do NAV, logo uma determinada estação irá reservar o meio por um período de tempo NAV. Todas as estações vizinhas que ouvirem a transmissão irão esperar pelo fim da transmissão usando o NAV como temporizador.

Um atacante que deseja obter maior acesso ao canal poderia explorar a reserva do meio setando o NAV com valores altos sempre que for enviar um quadro RTS. Como dito anteriormente, todas as estações vizinhas que ouvirem o RTS (ou o correspondente CTS) irão setar o NAV e esperar por todo este período.

Sendo o valor máximo para o NAV de 32767, aproximadamente 32 ms, o atacante poderia enviar 30 quadros por segundo setando o NAV para este valor máximo. Como consequência deste envio de quadros o atacante irá tomar o meio completamente para si, além de gerar um DoS em toda a rede e diminuir a vazão das outras estações para zero, pois as outras estações encontrarão o meio ocupado constantemente.

Impacto causado pelo ataque de abuso do NAV

Em [19] os autores demonstraram o impacto deste ataque através de simulações usando o simulador ns2 [14]. O ataque é simulado usando-se o valor máximo do NAV na troca de quadros RTS e CTS em uma rede com topologia de oito estações ao redor de um ponto de acesso (AP). Para melhor estudar o efeito do ataque na rede, os autores consideraram diferentes tempos de início do ataque quando comparado às outras estações. O início do tráfego em *early start* indica que o ataque é iniciado um segundo antes do tráfego dos outros nós, em *same start* o ataque é iniciado ao mesmo tempo e em *late start* o ataque começa 10 segundos depois que o tráfego dos outros nós é iniciado. Para todas os cenários o tamanho do pacote é setado em 1.000 bytes e o tempo de simulação é de 200 segundos.

Foram usados dois tipos de fluxos de pacotes, taxa de bits constante *(Constant Bit Rate – CBR)*, onde as estações atacantes enviam pacotes para o AP a uma taxa constante e o fluxo TCP, onde as estações recebem pacotes ACK do AP a cada pacote de dados enviado:

- **Fluxo CBR**: fluxos CBR foram estabilizados entres todas as estações e o AP. A Figura 2.10, retirada de [19], contém o gráfico que mostra o impacto de um atacante, estação **4**, na rede mandando pacotes a uma taxa de 20 pacotes por segundo para o AP. A Figura 2.11, retirada de [19], contém o gráfico onde dois atacantes, estações **4** e **5**, enviam pacotes a uma taxa de 30 pacotes por segundo cada uma para o AP. Como é possível verificar, em ambos os gráficos o ataque é

realizado com sucesso tendo como resultado o controle do meio e a negação do serviço (DoS) para as demais estações, não importando o tempo de início dos ataques. Os autores também demonstraram o mesmo ataque com as estações quatro e oito sendo os atacantes, porém o resultado foi praticamente o mesmo, como mostrado na Figura 2.11. Para investigar se este ataque requer que o meio seja completamente controlado perante os pacotes ACK do AP, os autores também fizeram simulações usando-se o fluxo TCP.

- **Fluxo TCP**: fluxos TCP foram estabilizados entre todos os nós e o AP. A Figura 2.12, retirada de [19], mostra a vazão quando somente a estação **4** é maliciosa. É possível perceber que, quando a estação **4** inicia a transmissão de dados antes que as outras estações, ela é capaz de tomar o meio completamente para si além de criar um DoS em toda a rede. Porém, em *same start* e *late start* o atacante não consegue ter controle sobre o meio acarretando a falta de sucesso do ataque. Isto ocorre devido a transmissão dos pacotes ACK feitas pelo AP. Logo, uma vez que o AP torna o canal ausente para o atacante para que ele possa transmitir pacotes ACK, o AP também transmite pacotes para estações que tenham o comportamento normal. Devido a esta característica, o atacante não consegue tomar o controle do meio e como resultado o impacto do ataque não é tão forte quanto em *early start* onde o AP sempre transmite pacotes ACK para o atacante, permitindo que ele tome o controle do meio. Foram feitas também duas simulações usando-se dois atacantes na rede. Na Figura 2.13, retirada de [19], ambos os atacantes, estações **4** e **5**, encontram-se distantes uma da outra, enquanto na Figura 2.14, os atacantes, estações **4** e **8**, encontram-se próximas uma da outra, ou seja, são adjacentes. Como pode ser verificado em ambos os gráficos, em *early start* os atacantes conseguem causar um DoS na rede, porém em *same start* e *late start* isto não acontece devido aos pacotes ACK, como explicado anteriormente. Também pode ser verificado que, devido ao efeito da combinação do ACK juntamente com a seleção randômica da janela de congestionamento das estações a vazão da estação atacante **5**, em *late start*, caiu para aproximadamente zero e a vazão da estação estações **4** permaneceu mais alto que a vazão das outras estações. Na Figura 2.13 o ataque foi melhor sucedido devido à localização de ambos os atacantes.

Defesas para o ataque de abuso do NAV

Algumas abordagens de defesa para o ataque de abuso do NAV são encontradas na literatura, sendo duas delas citadas a seguir [19] e [55].

Em [19] os autores demonstraram que, se o TCP é usado nas camadas acima, ele irá reconhecer os pacotes enviados pela estação maliciosa, enviando pacotes ACK de volta, fazendo com que o atacante

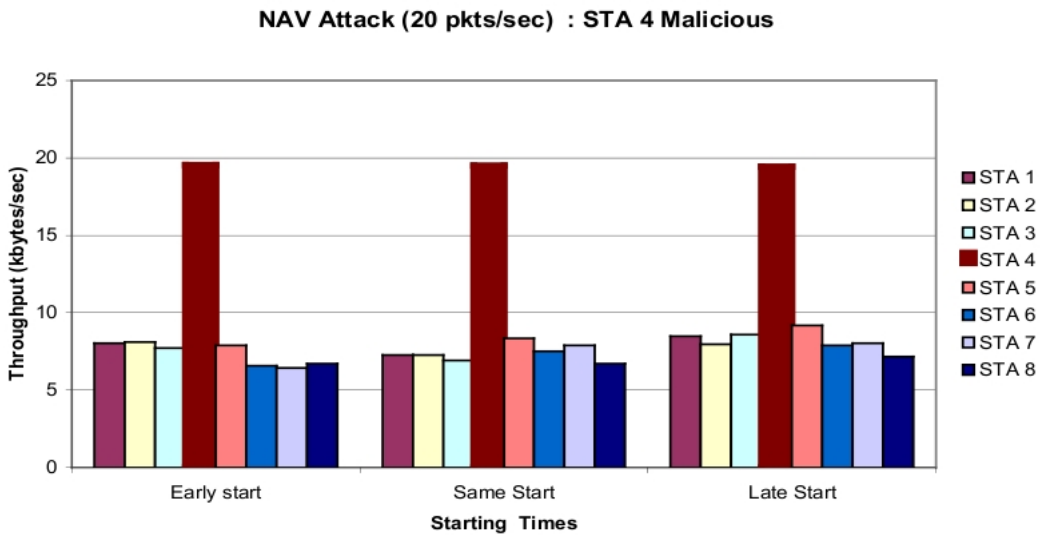

Figura 2.10: Impacto do ataque gerado pela estação **4** utilizando fluxo de dados CBR.

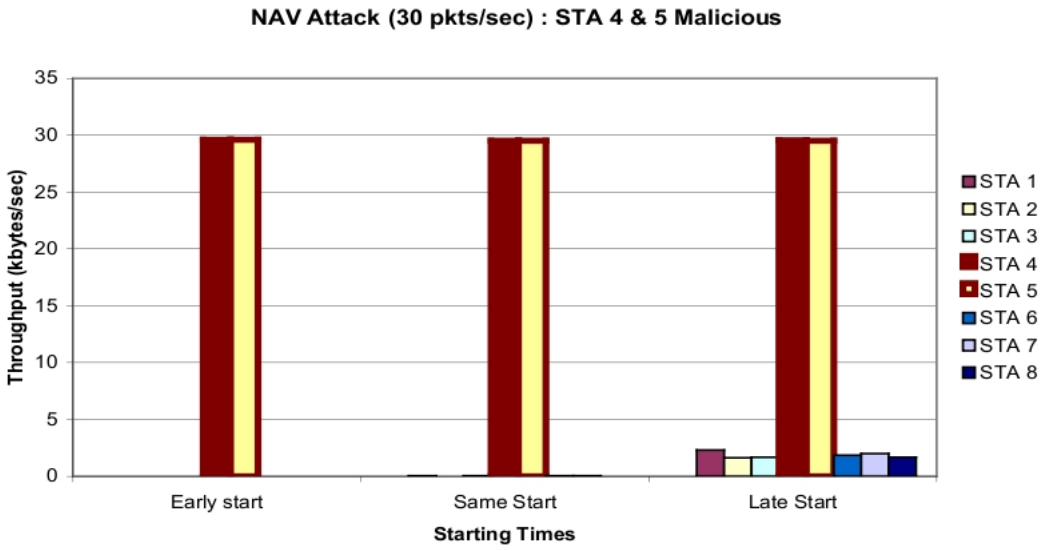

Figura 2.11: Impacto do ataque gerado pelas estações **4** e **5** usando fluxo de dados CBR.

tenha que abandonar o canal. Se por ventura o atacante venha a entregar o canal, ele terá que competir com todas estações vizinhas para tê-lo de volta. Uma vez que o atacante tenha o controle do canal novamente, o TCP irá fazer com que este controle seja por pouco tempo. Como consequência, o ataque da estação maliciosa será anulado. Os resultados mostrados pelos autores também indicaram que os protocolos do MAC poderiam prover uma forma de controle do fluxo e de igualdade, acoplando estes mecanismos com os protocolos da camada de transporte garantindo uma operação livre de ataques.

Em [55], o mecanismo de defesa utilizado pelo DOMINO utiliza a duração atual de uma trans-

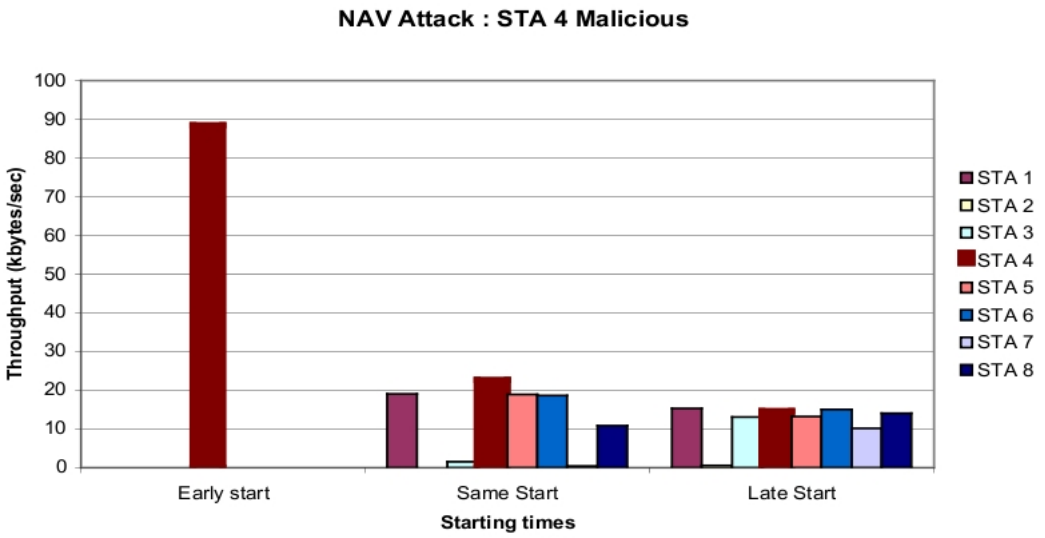

Figura 2.12: Impacto do ataque gerado pela estação **4** utilizando fluxo de dados TCP.

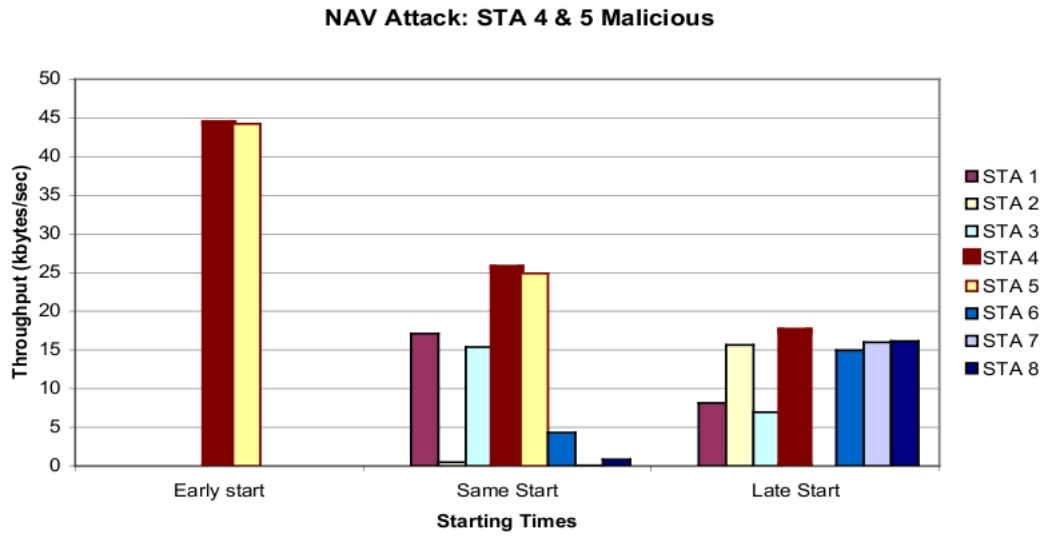

Figura 2.13: Impacto do ataque gerado pelas estações **4** e **5** usando fluxo de dados TCP.

missão, incluindo a transferência dos quadros RTS, CTS, de DADOS e ACK, e compara esta duração com o valor do NAV contidos nos cabeçalhos dos quadros RTS e CTS. Se o valor do NAV contido no cabeçalho dos quadros RTS e CTS for maior, a estação que enviou estes quadros pode ser um possível atacante.

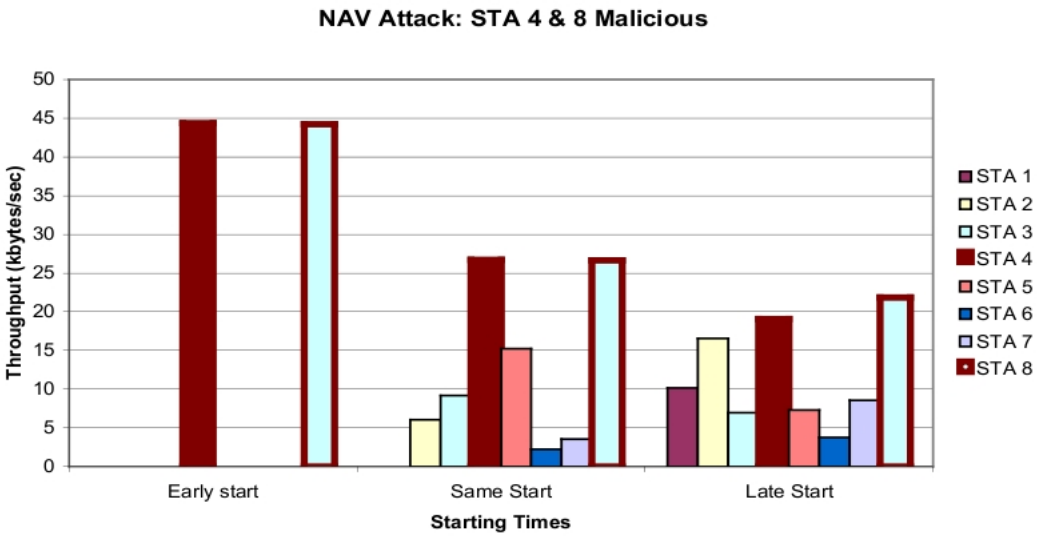

Figura 2.14: Impacto do ataque gerado pelas estações **4** e **8** usando fluxo de dados TCP.

2.5 Os Ataques de DoS

Os ataques de negação de serviço *(Denial of Service - DoS)* [7], também denominados de ataques maliciosos [40], são usados para impedir os usuários de utilizarem os recursos disponíveis no sistema. As redes sem fio que utilizam *Wi-Fi* são mais suceptíveis a ataques de DoS devido ao DCF ter sido criado para maximizar a vazão da rede utilizando pequenos quadros de controle.

Dois tipos de ataques de negação de serviço podem ser citados, os ataques de negação com alta taxa de transferência de dados *(high-rate DoS attacks)* [34], como o ataque de *Jamming* [4], [16], [48] e o ataque de negação de serviço distribuído *DDoS* [37], [46] e o os ataques de negação de serviço com baixa taxa de transferência de dados *(low-rate DoS attacks)* [22], [67], como o ataque de redução da qualidade de serviço *(RoQ attacks)* [23], [24] e o ataque *shrew (Shrew Attack)* [34].

Algumas abordagens na literatura corrente, como [11], [17] e [69], conseguiram reduzir o impacto dos ataques de negação com alta taxa de transferência de dados com bastante eficiência. Porém, ataques maliciosos com baixa taxa de transferência de dados possuem poucas abordagens efetivas na literatura [64], devido a sua dificuldade de detecção por explorarem a capacidade dinâmica de adaptação dos mecanismos presentes em todas as camadas camadas [22], [23], como o controle de congestionamento do TCP, balanceamento de carga, etc.

2.5.1 Os Ataques de RoQ

Segundo [22], o ataque de redução da qualidade de serviço *(Reduction of Quality - RoQ)* é um ataque que explora o comportamento adaptativo da rede. Podem-se citar alguns mecanismos de adaptação

que são vulneráveis aos ataques de RoQ como o TCP, que confia em mecanismos de *feedback* para adaptar suas taxas de transferência de dados procurando a justiça ou igualdade *(fairness)* na rede, os esquemas de gerenciamento de *buffer*, que possuem grande importância na efetividade nos mecanismos de controle de transmissão por constituírem o sinal de *feedback* (marcando ou descartando pacotes) para vários mecanismos de adaptação, as técnicas de gerenciamento ativo de fila que têm sido desenvolvidas para tentar manter o tamanho da fila em um determinado padrão ótimo e realizar descarte de pacote probabilítisco, entre outros.

Vários estudos na literatura corrente demonstraram o impacto dos ataques de RoQ na rede. Em [23], através de simulações feitas usando-se servidores de *Web* na Internet, os autores demonstraram o impacto dos ataques de RoQ nos controladores de admissão. Os controladores de admissão são usados para proteger a rede contra condições de sobrecarregamento rejeitando (adiando) requisições que fariam com o que sistema saísse de um estado quiescente (latente). Em [24], os autores analisaram o impacto dos ataques *Shrew* e RoQ no sistema de controle de congestionamento do TCP. O controle de congestionamento funciona da seguinte forma, quando uma estação está congestionada ele começa a descartar pacotes. Estes descartes são considerados pelo TCP como um sinal de congestionamento e como reação o TCP diminui a taxa de transferência pela metade. Caso nenhum pacote seja perdido, o TCP aumenta sua janela de congestionamento em um pacote a cada *Round Trip Time - RTT*. Neste trabalho também é mencionado uma forma de defesa para os ataques de negação de serviço com baixa taxa de transferência de dados que tem como alvo o TCP, proposto por [34] e estudado por [66].

Em [64], são propostos quatro tipos de ataques RoQ, também estudados neste trabalho. O primeiro ataque, chamado de *pulsing* Figura 2.15, uma estação atacante envia quadros para uma estação vítima vizinha escolhida aleatoriamente. O segundo ataque, chamado de *round-robind* Figura 2.15, múltiplas estações maliciosas enviam quadros para múltiplas vítimas vizinhas escolhidas aleatoriamente, pode-se dizer que o *round-robin attack* é o agrupamento de vários *pulsing*. O terceiro ataque, denonimado *self-whisper* Figura 2.16, uma estação maliciosa escolhe aleatoriamente uma estação vizinha que também seja maliciosa para enviarem quadros uma para a outra. O quarto ataque, denonminado *flooding* Figura 2.16, estações maliciosas escolhem aleatoriamente uma única estação vizinha e enviam quadros para esta estação. É importante salientar que os ataques de RoQ devem ser totalmente aleatórios para continuarem sendo complexos evitando assim serem descobertos.

A seguir é definida a Metodologia em torno do trabalho.

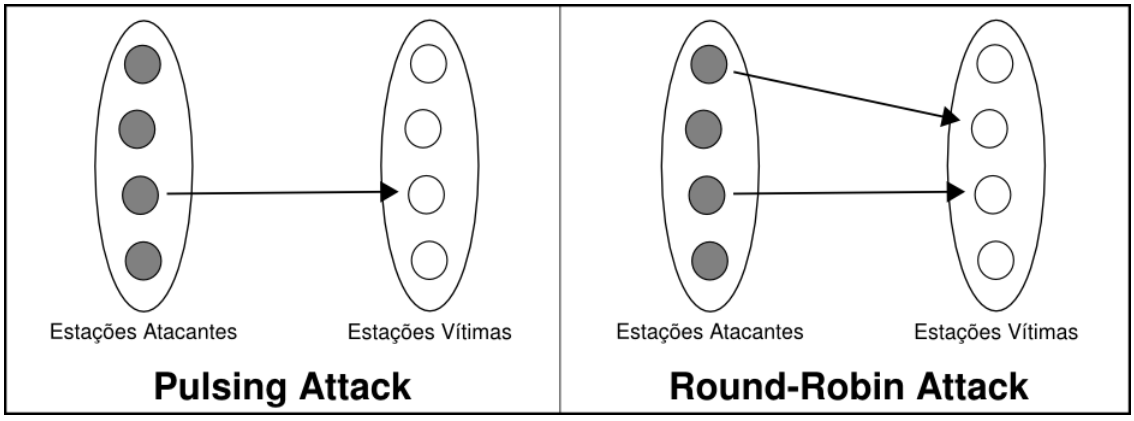

Figura 2.15: Ataques *pulsing* e *round-robin*.

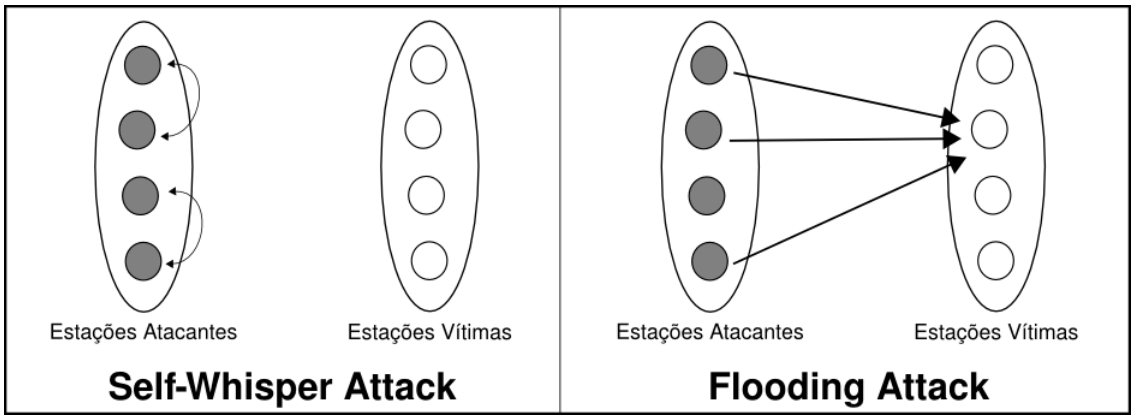

Figura 2.16: Ataques *self-whisper* e *flooding*.

Capítulo 3

METODOLOGIA

A pesquisa feita neste trabalho está situada da seguinte forma, como proposto por [68]: **Quanto à natureza** é uma pesquisa básica que tem como objetivo entender ou descobrir novos fenômenos. Neste trabalho, estes fenômenos estão ligados diretamente aos protocolos de controle de potência de transmissão (CPT), bem como a análise feita sobre o uso do CPT como mecanismo de defesa contra os ataques de RoQ *(Reduction of Quality attacks)* em redes *Wi-Fi*. **Quanto aos objetivos** é uma pesquisa descritiva ou explicativa pois tem como finalidade a observação, registro e análise dos fenômenos simulados na ferramenta ns2 *(Network Simulator 2)* [14]. **Quanto aos procedimentos** é uma pesquisa experimental pois busca a descoberta de novos métodos através de ensaios e estudos em laboratório, visando o controle de algumas variáveis que possam intervir no experimento. Entende-se como pesquisa em laboratório aquela onde ocorre a possibilidade de se controlar as variáveis que possam intervir no experimento.

3.1 Procedimentos Metodológicos

As atividades serão realizadas em duas fases distintas, uma durante a qual tem-se a obtenção dos requisitos básicos necessários ao desenvolvimento do trabalho e outra que consistirá da implementação e avaliação do projeto proposto.

O objetivo da primeira fase foi determinar o tema do trabalho, fazer o levantamento bibliográfico, conseguir os conhecimentos básicos sobre o protocolo IEEE 802.11 e sobre CPT, e estudar a documentação de toda a bibliografia encontrada. Também na primeira fase foram estudados os ataques existentes em redes sem fio, de maneira geral, e depois foram estudados os ataques gulosos que venham a desvirtuar o comportamento normal do *Wi-Fi* e por estudou-se os ataques maliciosos, mais precisamente os ataques de redução da qualidade de serviço *(RoQ)*.

Em paralelo à primeira fase, foi estudada a linguagem TCL, usada para a criação de scripts de

simulação, a ferramenta de criação de gráficos *GNUPlot* e a ferramenta de simulação de rede ns2, que foi usada no desenvolvimento da segunda fase.

A segunda fase teve como função a adaptação e implementação, para redes *Wi-Fi*, dos protocolos de Atenuação e AEWMA *(Atenuação com filtro EWMA – Exponentially Weighted Moving Average)*, anteriormente criados para trabalhar em redes de sensores sem fio [41]. Concomitantemente, foi feita a análise do CPT sendo usado como mecanismo de defesa contra ataques *RoQ* em redes *Wi-Fi*. Nesta fase foram gerados e analisados inúmeros gráficos seguindo algumas métricas, que serão descritas nas próximas subseções.

3.1.1 Primeira Fase

A primeira fase iniciou-se com o estudo da tecnologia *Wi-Fi* buscando-se principalmente o entendimento a respeito do funcionamento da função coordenadora DCF [20]. Após o estudo do protocolo IEEE 802.11, iniciou-se a aprendizagem a respeito do controle de potência de transmissão. Nesta parte foram estudados alguns métodos clássicos de CPT, como o **MACA** desenvolvido por Karn (1990) em [49], o MACAW desenvolvido por Bharghavan (1994) em [6], o **PCMA** desenvolvido por Jung e Vaidya [28], e o **Esquema Básico**, juntamente com o problema de enlaces assimétricos contextualizado em [28] e [53]. Os protocolos desenvolvidos por Correia (2006) em [41] foram também estudados, por serem menos complexos e terem apresentado ótimo desempenho em comparação aos outros protocolos até então criados para redes de sensores sem fio.

Após a base estar consolidada, partiu-se para um estudo geral referente aos ataques existentes em redes sem fio, e teve como foco o estudo a respeito dos ataques existentes em todas as camadas. Artigos como [1], [5], [27] e [43] mostram os principais ataques existentes e propõem algumas medidas de segurança para a prevenção de ataques ou a minimização dos seus impactos.

Posteriormente, foram feitos estudos sobre os ataques que afetam diretamente o protocolo IEEE 802.11. Tais ataques na camada MAC foram classificados conforme seu comportamento. O primeiro comportamento estudado refere-se a ataques gulosos que tem como objetivo obter maior acesso ao meio. Inúmeros estudos na literatura corrente foram examinados, entre eles [19], [21], [38], [54] e [55]. Dentre estes artigos estudados, alguns mostraram o impacto dos ataques gulosos em uma rede e outros mostraram mecanismos de defesa capazes de contornar o efeito de tais ataques por completo.

O segundo comportamento pode ser denominado de ataques maliciosos. Estes ataques são divididos em ataques de negação de serviço com alta taxa de transferência de dados e ataques de negação de serviço com baixa taxa de transferência de dados. Os trabalhos, [13], [61] e [65], referentes aos ataques de negação de serviço com alta taxa de transferência de dados foram estudados. Algumas propostas, como [17] e [69], conseguem reduzir quase que por completo estes ataques. Outros trabalhos na lite-

ratura corrente, como [22], [23], [24], [34], [35], [37], [42] e recentemente [57], estudaram o impacto dos ataques de negação de serviço com baixa taxa de transferência.

O estudo sobre a ferramenta ns2 iniciou-se após a consolidação do conhecimento básico sobre Redes de Computadores e Redes Sem Fio. A ferramenta ns2 [14] é um software *open-source* distruibuída para o Sistema Operacional **GNU/Linux**, podendo ser usada no **Windows** através da ferramenta **Cygwin** [36].

3.1.2 Segunda Fase

A segunda fase da Metodologia está compreendida em duas partes. Na primeira parte os protocolos de CPT foram adaptados para a tecnologia *Wi-Fi* e posteriormente analisados. Na segunda parte foram desenvolvidos os ataques de RoQ nas redes *Wi-Fi*, que utilizem ou não CPT, e então examinados através de gráficos.

Adaptação dos protocolos de CPT para redes *Wi-Fi*

A segunda fase iniciou-se com a adaptação, para redes *Wi-Fi*, dos protocolos de Atenuação e AEWMA desenvolvido por [41]. A Figura 3.1, adaptada de [53], mostra como foi feito o desenvolvimento do CPT no simulador ns2. Juntamente ao módulo que faz o controle de acesso ao meio (**MAC**) foi implementado e adicionado um módulo responsável pelo CPT, marcado com a cor cinza. A este módulo do CPT, existem dois outros módulos responsáveis pelo controle dos protocolos de Atenuação e AEWMA, marcados pela cor cinza. A classe responsável por seguir o comportamento do *Wi-Fi* no MAC teve de ser modificada para que as estações pudessem transmitir os quadros utilizando uma potência de transmissão menor. Como mencionado anteriormente, a potência de transmissão menor é determinada através do quadro ACK por uma estação destino, após receber o quadro de DADOS.

Nos módulo responsável pelo controle de potência de transmissão, foi criada uma classe responsável por cuidar para que uma estação destino pudesse calcular a potência de transmissão que uma determinada estação origem teria que usar em posteriores transmissões. Dentro desta classe, além de conter os protocolos de Atenuação e AEWMA explicados anteriormente, existe também uma tabela de vizinhos que tem como função guardar a última potência de transmissão utilizada para enviar um quadro para uma determinada estação alvo. Esta tabela de vizinhos foi utilizada anteriormente por Pires (2004) no Esquema Básico com Memória em [52] e por Correia (2006) em [41].

Os rádios reais devem, por obrigação, utilizar níveis discretos de potência para o envio de quadros, porém, nas simulações as estações não utilizaram níveis de potência para efetuarem transmissões. Assim que a próxima potência de transmissão é calculada pela estação destino e enviada para a estação origem, a estação origem irá adicionar esta potência à sua lista de transmissões dos vizinhos. Portanto,

neste caso, não são usados níveis discretos de potência. Se por ventura, um quadro RTS ou de DADOS necessite ser retransmitido, a estação que deseja enviar tal quadro o fará utilizando a potência máxima de transmissão. A máxima potência de transmissão utilizada neste trabalho é de 200 mW.

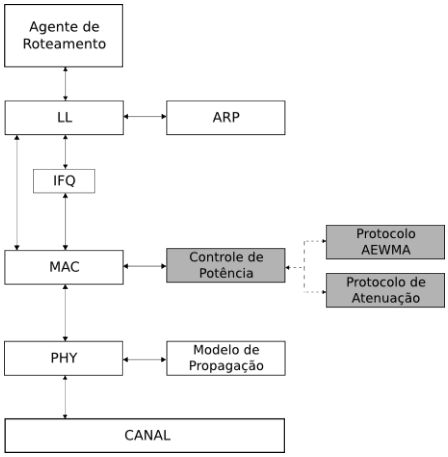

Figura 3.1: Implementação do CPT no simulador.

Desenvolvimento dos ataques de RoQ

A classe responsável pelo *W-Fi*, após ter o CPT inserido, foi modificada para que a análise sobre o impacto dos ataques de RoQ pudesse ser feita. Um módulo responsável pelo comportamento dos ataques, marcado com a cor preta como mostrado na Figura 3.2, foi adicionado para que pudesse se comunicar com o MAC e com o CPT. Os atacantes ao executarem um ataque, irão escolher aleatoriamente um determinado nível de potência de transmissão e enviar o quadro para a estação vítima.

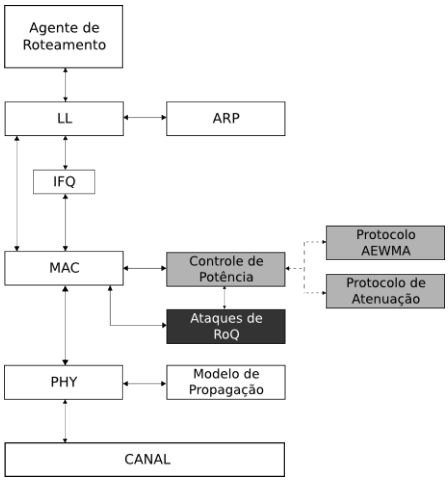

Figura 3.2: Implementação dos ataques de RoQ.

No módulo dos atacantes foram inseridos nove níveis discretos de potência: 1, 25, 50, 75, 100, 125,

150, 175 e 200 mW, sendo 200 mW a máxima potência de transmissão. Porém, as estações atacantes somente irão escolher os níveis acima de 100 mW, para assegurarem de que o quadro conseguirá alcançar a vítima. Sempre que uma retransmissão necessitar ser feita, as estações atacantes utilizarão a máxima potência de transmissão .

Cenário de Simulação

Para a análise dos protocolos de CPT, foi usada uma topologia em *grade*, Figura 3.3, com 36 estações, sendo que as estações estão afastadas umas das outras a uma distância de 75 metros. Esse tipo de topologia em *grade* foi utilizado por [64] para a análise do impacto dos ataques de RoQ. Foram analisados dois tráfegos principais, sendo que em uma simulação os tráfegos principais iniciam ao mesmo tempo após 2 segundos e em outra simulação os tráfegos principais iniciam em tempo diferentes, o primeiro tráfego é iniciado após 2 segundos e o segundo tráfego é iniciado após 30 segundos. Os dois tráfegos principais escolhidos são sempre executados pelas mesmas estações, o primeiro tráfego tem como origem a estação **14** e como destino a estação **17** e o segundo tráfego tem como origem a estação **8** e como destino a estação **11**. Além dos dois tráfegos principais, foram realizadas simulações com 5 e 15 tráfegos secundários, escolhidos aleatoriamente. Os tráfegos principais e secundários utilizam tráfego exponencial a uma taxa de 0,3 Mb sendo que são os dados são enviados durante 0,01 s e durante 0,04 s os tráfegos ficam latentes.

Para a análise dos ataques de RoQ, foi utilizada uma topologia em *grade*, Figura 3.3 com 36 estações afastadas umas das outras a uma distância de 75 metros. Foi criado um tráfego na rede e através deste tráfego mediu-se o impacto que os ataques de RoQ podem causar sobre a rede. Este único tráfego criado tem como origem a estação **14** e como destino a estação **17** e utiliza uma taxa de transferência de 0,3 megabytes sendo o envio de dados feito em 0,01 s e permanecendo latente durante 0,04 s.

Para o ataque *pulsing* foi executada somente uma simulação com um atacante na rede. Para os ataques *round-robin*, *self-whisper* e *flooding* foram executadas simulações com 30%, e 50% de atacantes na rede. Os ataques de RoQ foram simulados em uma rede *Wi-Fi* que use os protocolos de Atenuação e AEWMA e também em uma rede onde não exista CPT.

Os resultados a respeito da análise dos gráficos são mostrados na Seção **Avaliação e Resultados**.

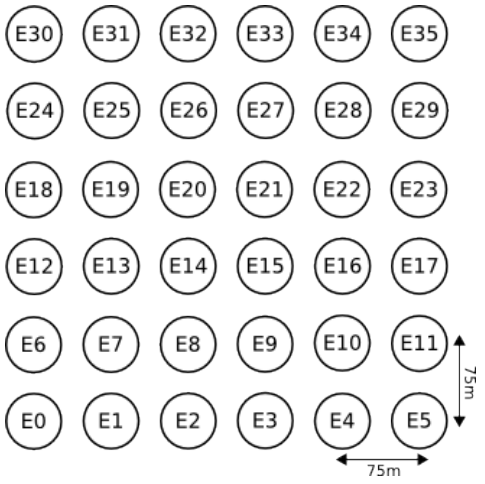

Figura 3.3: Topologia em grade contendo 36 estações - 75m x 75m.

Capítulo 4

AVALIAÇÃO e RESULTADOS

Este capítulo apresenta a análise de dois protocolos de controle de potência de transmissão (CPT), um denominado Atenuação e o outro AEWMA *(Atenuação com filtro EWMA – Exponentially Weighted Moving Average)*. Após a análise dos protocolos de CPT, é mostrada a análise sobre o uso do CPT como mecanismo de defesa contra os ataques de redução da qualidade de serviço *(Reduction of Quality - RoQ)* nas redes *Wi-Fi*. A ferramenta ns2 *(Network Simulator 2)* [14] foi utilizada na simulação dos protocolos e dos ataques.

4.1 Análise dos Protocolos de CPT

A análise do CPT foi feita comparando-se o rendimento dos protocolos de Atenuação e AEWMA juntamente com uma rede *Wi-Fi* que não utilize CPT. Para a comparação foram utilizados dois tráfegos primários (principais), o primeiro partindo da estação **14** tendo como destino a estação **17** e o segundo partindo da estação **8** tendo como destino a estação **11**. Através do uso de tráfegos principais é possível verificar se o CPT está sendo útil para os dois tráfegos. Estes dois tráfegos foram analisados começando ao mesmo tempo, após 2 segundos de simulação, e começando em tempos distintos, no qual o primeiro tráfego primário inicia após 2 segundos de simulação e o segundo tráfego primário começa após 30 segundos de simulação. Ao fazer os dois tráfegos principais iniciar em tempos iguais, estaria-se fazendo o pior caso, pois as estações origens dos tráfegos iriam concorrer pelo meio ao mesmo tempo. Fazendo com que as estações comecem em tempo diferentes, após 30 segundos por exemplo, não haveria concorrência pelo meio no início da transmissão de cada origem dos tráfegos principais.

Além dos dois tráfegos primários, também foram feitas simulações utilizando 5 e 15 tráfegos secundários, sendo que estes tráfegos são escolhidos aleatoriamente. Cada tráfego secundário é iniciado de 15 em 15 segundos de simulação. A simulação e todos os tráfegos da rede, inclusive os primários e secundários, terminam após 280 segundos. Os tráfegos secundários foram utilizados para que

o meio fosse ocupado por mais tempo, de forma a verificar se os tráfegos primários estão efetuando transmissões ao mesmo tempo que os tráfegos secundários.

4.1.1 Simulação com 5 Tráfegos Secundários

Foram feitas duas simulações com 5 tráfegos secundários, uma na qual os tráfegos primários começam ao mesmo tempo e uma outra na qual os tráfegos primários começam em tempos diferentes. Primeiramente foi contextualizada a análise a respeito dos tráfegos primários começando ao mesmpo tempo e depois foi mostrada a análise sobre os dois tráfegos primários começando em tempos diferentes.

Tráfegos primários iniciando ao mesmo tempo

Ambos os tráfegos primários iniciam após 2 segundos de simulação. A Figura 4.1 e a Figura 4.2 mostram o atraso referente a entrega dos quadros no primeiro e segundo tráfego primário respectivamente. É possível notar que a rede sem CPT e a rede que utiliza o protocolo AEWMA possuem um atraso em torno de 2 μs. Porém, em ambos os gráficos, o protocolo de Atenuação possui um atraso médio em torno de 15 μs. Isto ocorre devido ao protocolo de Atenuação ter o comportamento de variar constantemente a potência de transmissão, o que acarreta em demasiada perda de quadros. Entretanto, o protocolo AEWMA, por utilizar o EWMA, torna-se mais conservador e como consequencia tem um comportamento parecido com uma rede que não utilize CPT.

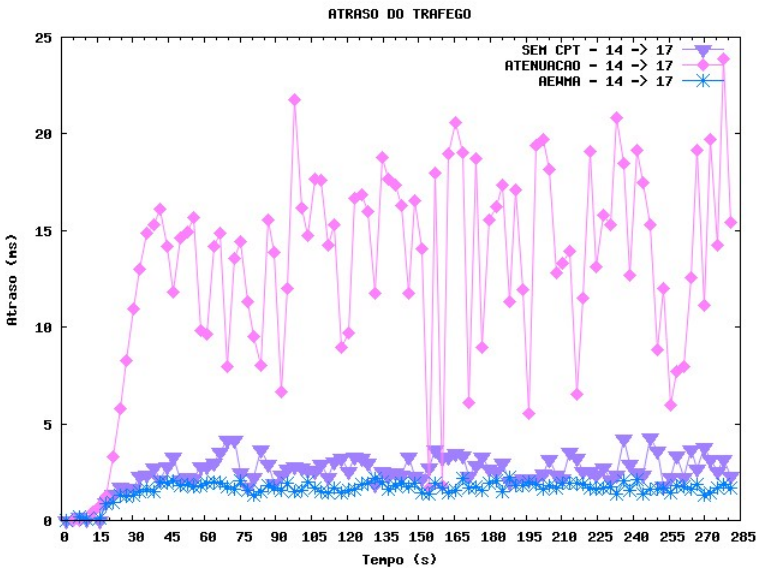

Figura 4.1: Atraso do primeiro tráfego primário com 5 tráfegos secundários.

A Figura 4.3 mostra a taxa de entrega dos protocolos com relação ao primeiro tráfego primário

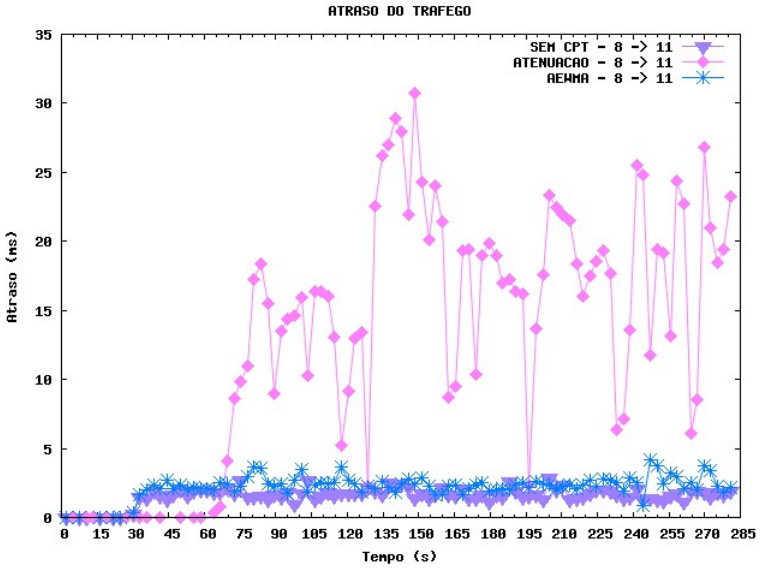

Figura 4.2: Atraso do segundo tráfego primário com 5 tráfegos secundários.

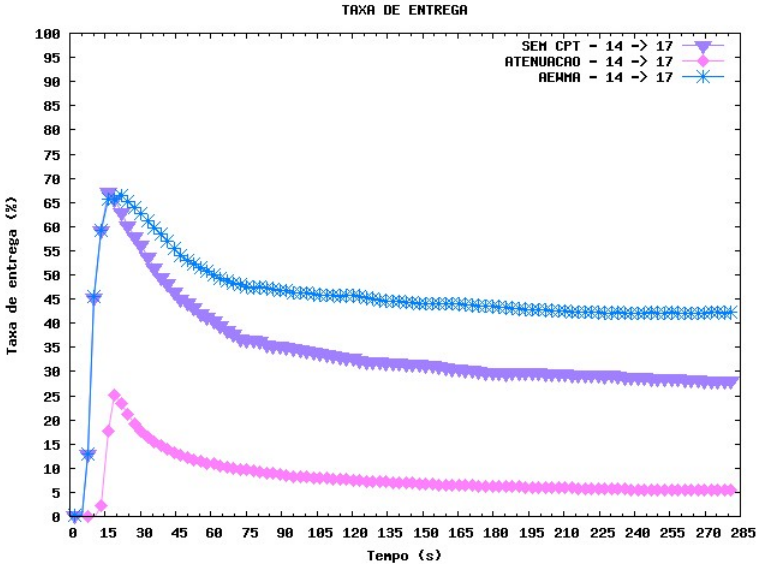

Figura 4.3: Taxa de entrega do primeiro tráfego primário com 5 tráfegos secundários.

(partindo da estação origem **14** tendo como destino a estação **17**) e a Figura 4.4 mostra a taxa de entrega dos protocolos com relação ao segundo tráfego primário (partindo da estação origem **8** tendo como destino a estação **11**). A taxa de entrega em ambos os casos está intimamente ligada ao atraso na entrega dos quadros, explicado anteriormente. É possível notar que devido ao grande atraso, o protocolo de Atenuação possui uma taxa de entrega bastante inferior em comparação ao protocolo AEWMA. O AEWMA, por outro lado, possui 15% a mais de taxa de entrega na Figura 4.3, porém na Figura 4.4 a rede sem CPT tem quase 10% a mais de taxa de entrega de quaros.

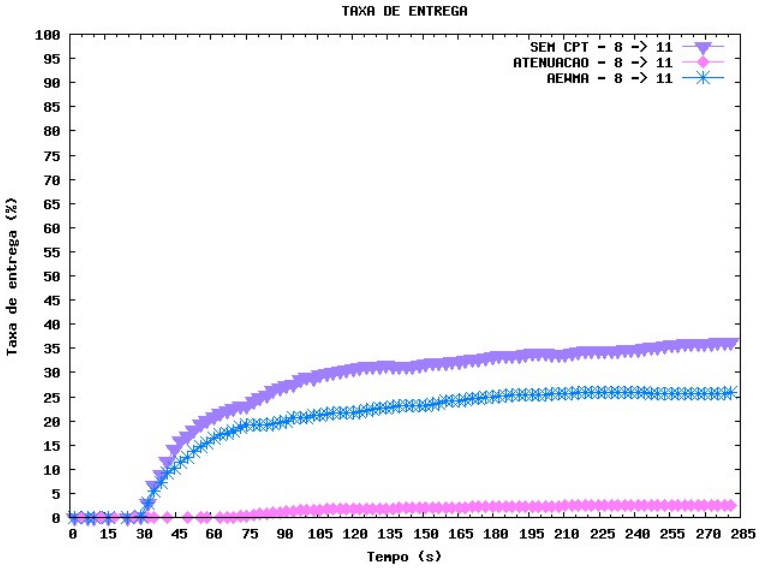

Figura 4.4: Taxa de entrega do segundo tráfego primário com 5 tráfegos secundários.

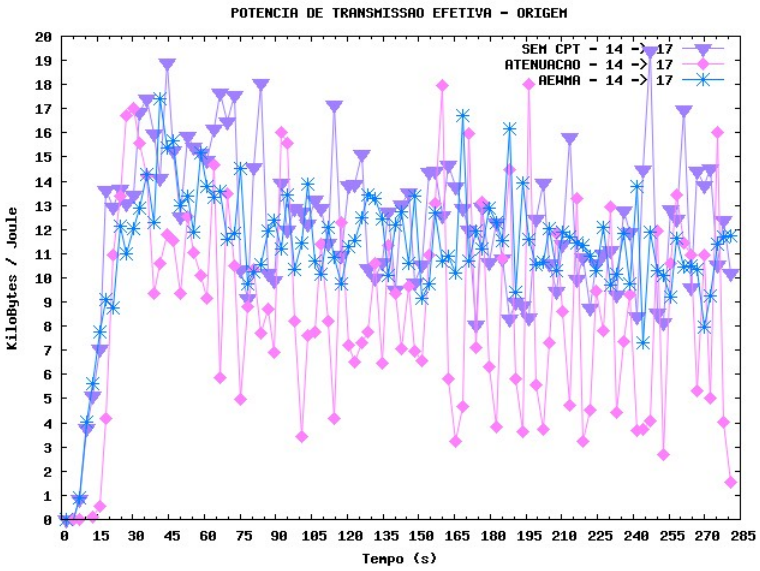

Figura 4.5: Potência de transmissão efetiva da estação **14**

A Figura 4.5 e a Figura 4.6 mostram respectivamente, a potência de transmissão efetiva da origem do primeiro tráfego primário e da origem do segundo tráfego primário. A potência de transmissão efetiva mostra a quantidade de bytes que chegou no destino usando-se uma menor quantidade de energia. A rede com o protocolo AEWMA e a rede que não utiliza CPT, na figuras 4.5 e 4.6, tiveram o comportamento parecido, enviando, respectivamente, em torno de 13 KiloBytes e 8 KiloBytes, a cada Joule utilizado. Entretanto, por variar constantemente a potência de transmissão, o protocolo de Atenuação ficou com o rendimento abaixo do AEWMA e da rede que não utiliza CPT.

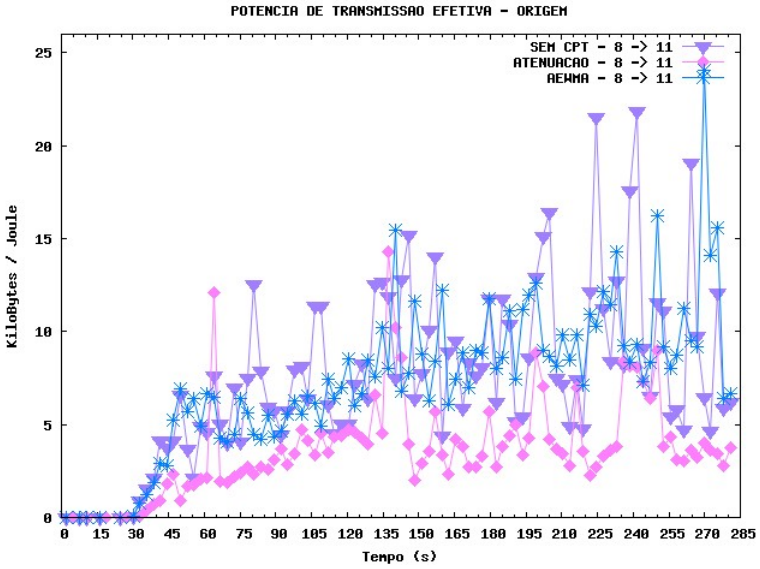

Figura 4.6: Potência de transmissão efetiva da estação **8**

Tráfegos primários iniciando em tempos diferentes

Nesta simulação o primeiro tráfego primário é iniciado após 2 segundos e o segundo tráfego secundário é iniciado após 30 segundos. Devido aos tráfegos principais começarem em tempos distintos, o atraso do protocolo de Atenuação que era em torno de 15 μs, nos dois tráfegos principais, passou para algo entre 4 e 5 μs. A sua taxa de entrega aumentou em mais de 10% nos dois tráfegos principais, como mostrado na Figura 4.7 e na Figura 4.8.

É possível notar que a taxa de entrega do protocolo AEWMA foi 15% superior em comparação à rede sem CPT, no primeiro tráfego primário, como mostrado na Figura 4.7. Entretanto, na Figura 4.8, referente ao segundo tráfego primário, a rede sem CPT conseguiu ter uma taxa de entrega 30% superior à rede que utiliza o AEWMA. O principal motivo da taxa de entrega referente à rede que não utiliza CPT ter sido bem maior do que o AEWMA, no segundo tráfego primário, é que o atraso referente ao AEWMA foi maior do que o sem CPT, como mostrado na Figura 4.9.

4.1.2 Simulação com 15 Tráfegos Secundários

Foram feitas duas simulações com 15 tráfegos secundários, uma na qual os tráfegos primários começam ao mesmo tempo e uma outra na qual os tráfegos primários começam em tempos diferentes. Primeiramente será contextualizada a análise a respeito dos tráfegos primários começando ao mesmpo tempo para depois ser mostrada a análise sobre os dois tráfegos primários começando em tempos diferentes.

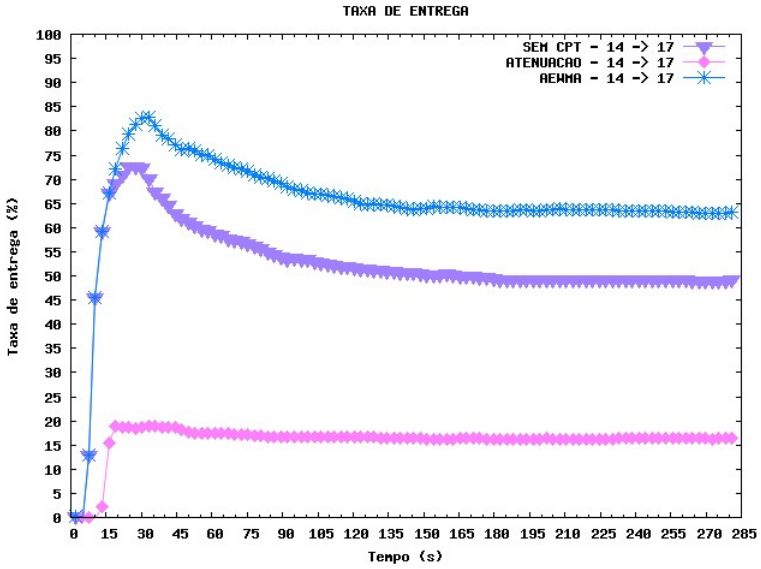

Figura 4.7: Taxa de entrega do primeiro tráfego primário com 5 tráfegos secundários.Tráfegos primários começando em tempos diferentes.

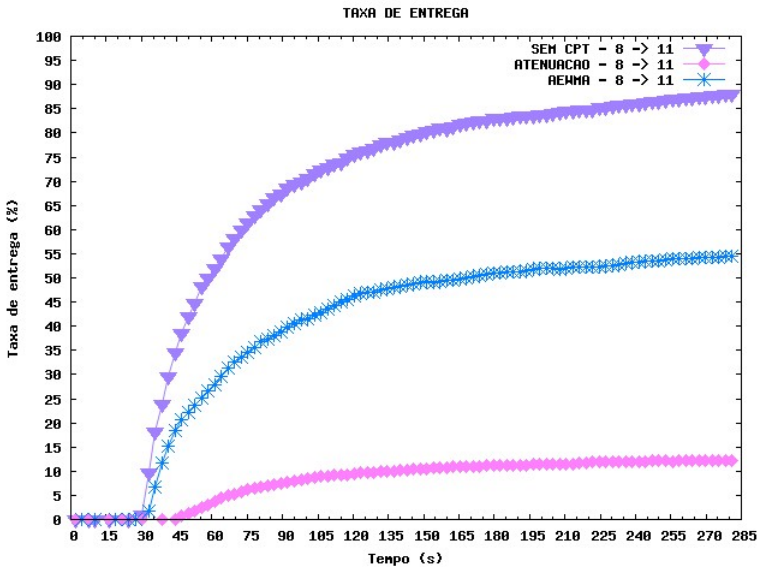

Figura 4.8: Taxa de entrega do segundo tráfego primário com 5 tráfegos secundários. Tráfegos primários começando em tempos diferentes.

Tráfegos primários iniciando ao mesmo tempo

Após 2 segundos de simulação são iniciados os dois tráfegos primários. As figuras 4.10 e 4.11 mostram o atraso da entrega de pacotes. Novamente é possível notar que o protocolo de Atenuação possui um atraso bem maior quando comparado ao protocolo AEWMA e à rede sem CPT. Entretanto, o atraso na rede sem CPT ficou um pouco acima do que o protocolo AEWMA, nas duas figuras, o que

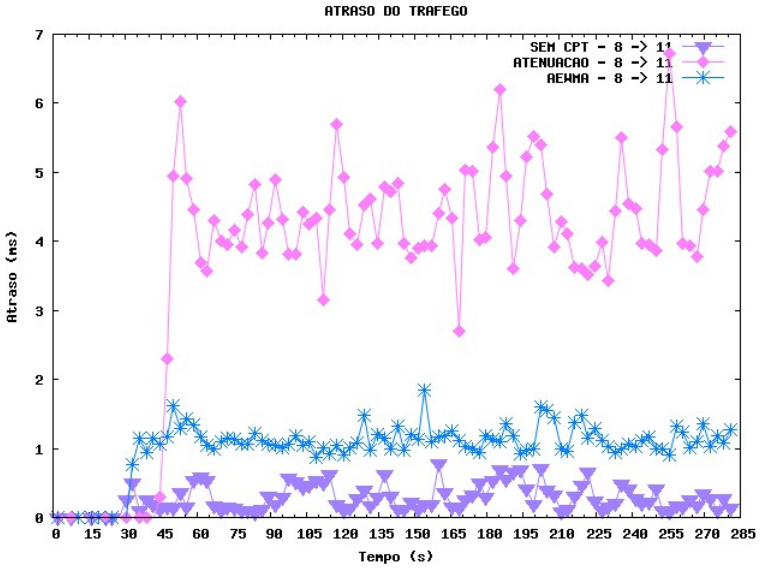

Figura 4.9: Atraso do segundo tráfego primário com 5 tráfegos secundários na rede. Tráfegos primários começando em tempos diferentes

acarretou em uma taxa de entrega superior do AEWMA nos dois tráfegos principais, como mostrados na Figura 4.12 e na Figura 4.13.

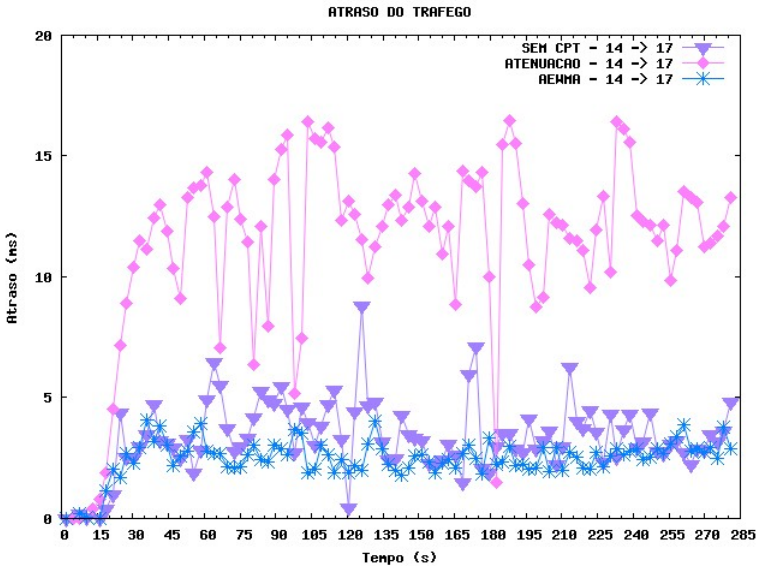

Figura 4.10: Atraso do primeiro tráfego primário com 15 tráfegos secundários na rede. Tráfegos primários começando ao mesmo tempo.

A Figura 4.14 e a Figura 4.15 mostram a potência efetiva utilizada pelos tráfegos primários. Nas duas figuras o comportamento do AEWMA e da rede sem CPT é bastante similar, porém, o protocolo de Atenuação possui um rendimento inferior.

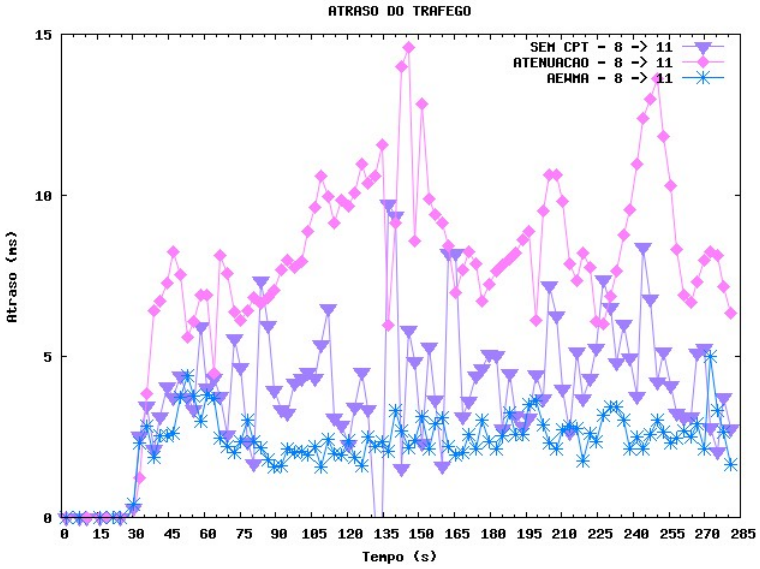

Figura 4.11: Atraso do segundo tráfego primário com 15 tráfegos secundários na rede. Tráfegos primários começando ao mesmo tempo.

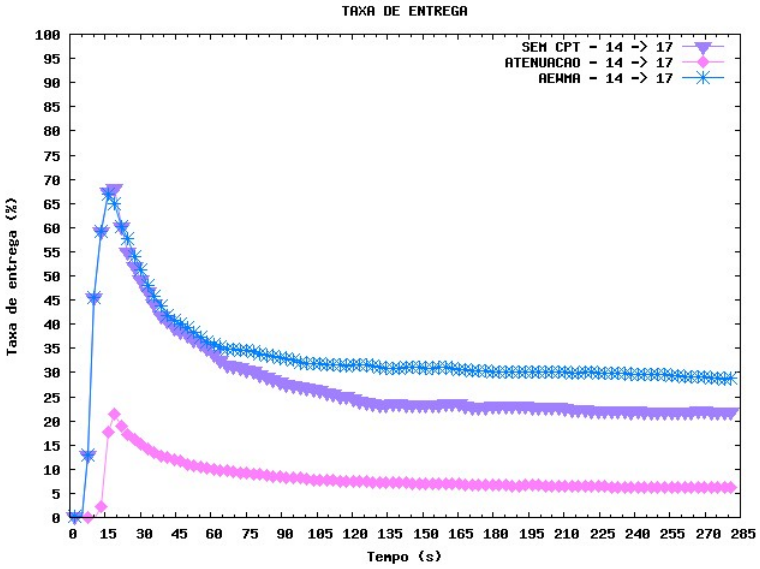

Figura 4.12: Taxa de entrega do primeiro tráfego primário com 15 tráfegos secundários na rede. Tráfegos primários começando ao mesmo tempo.

Tráfegos primários iniciando em tempos diferentes

A Figura 4.16 mostra o atraso da entrega de quadros referente ao primeiro tráfego primário. Novamente o atraso do protocolo de Atenuação é maior comparando-se ao protocolo AEWMA e a rede sem CPT. Também é possível notar na Figura 4.18 que a taxa de entrega do protocolo AEWMA consegue ser a mais alta, ficando em torno de 30% e da rede sem CPT em torno de 25%. Esta taxa de

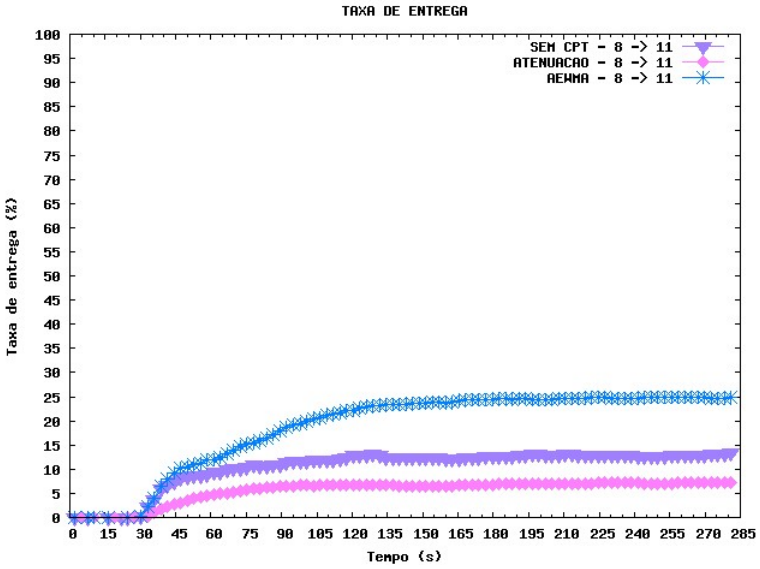

Figura 4.13: Taxa de entrega do segundo tráfego primário com 15 tráfegos secundários na rede. Tráfegos primários começando ao mesmo tempo.

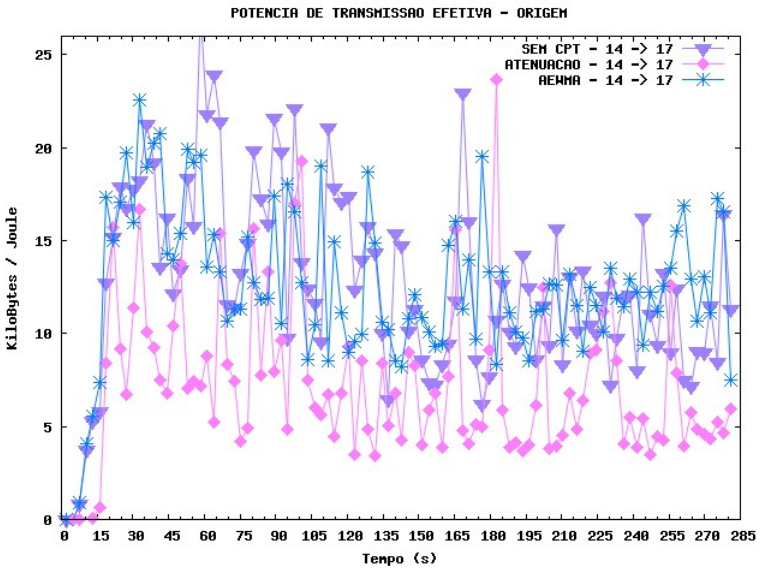

Figura 4.14: Potência de transmissão efetiva da estação **14**. 15 tráfegos secundários na rede. Tráfegos primários começando ao mesmo tempo.

entrega baixa ocorreu devido ao número de tráfegos secundários na rede. A queda em torno de 15 e 20 segundos ocorreu devido ao começo do primeiro tráfego secundário, sendo que cada tráfego secundário inicializa sua transmissão de quadros após 15 segundos de simulação. Tanto o AEWMA quando o Atenuação, mesmo após 10 tráfegos secundários terem sido inicializados (após 150 segundos de simulação), conseguiram manter um comportamento padrão, em contra-partida a rede sem CPT que até

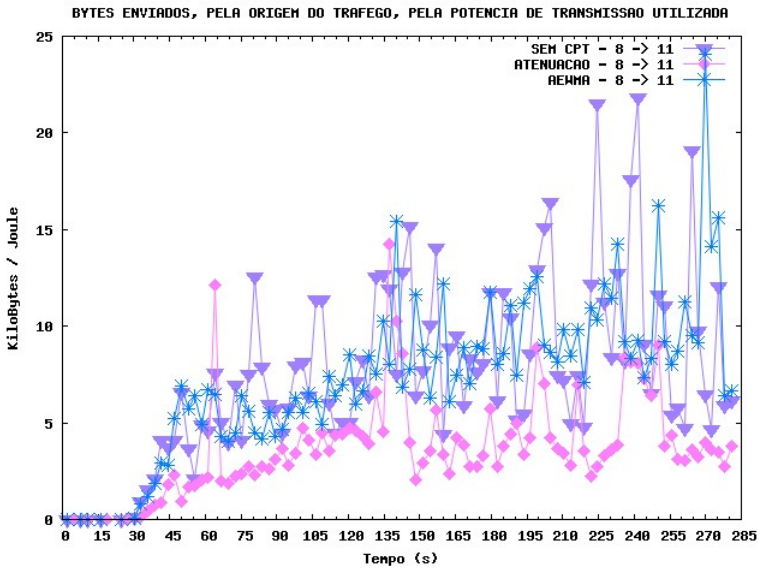

Figura 4.15: Potência de transmissão efetiva da estação **8**. 15 tráfegos secundários na rede. Tráfegos primários começando ao mesmo tempo.

o final da simulação estava diminuindo sua taxa de entrega. Devido ao atraso do protocolo AEWMA ser mais baixo, foi possível o envio de um maior número de Bytes por Joule gasto, como mostrado na Figura 4.20.

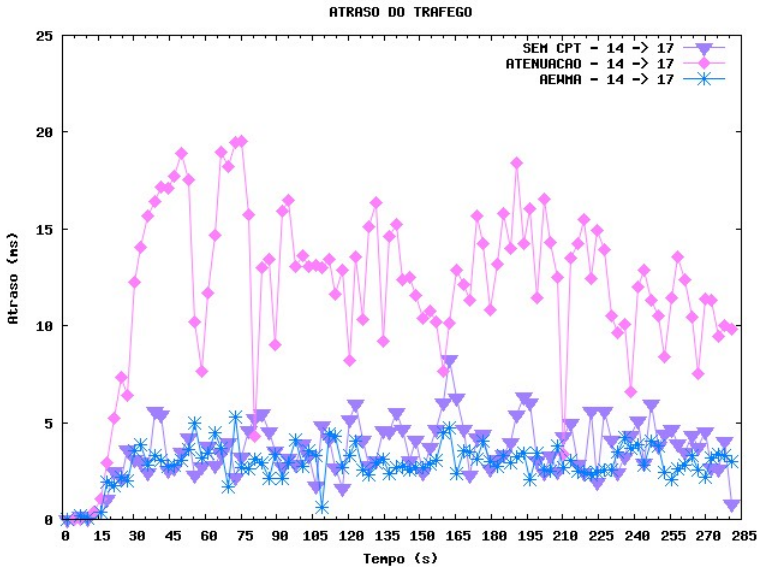

Figura 4.16: Atraso do primeiro tráfego primário com 15 tráfegos secundários na rede. Tráfegos primários começando em tempos diferentes.

Na Figura 4.17 que mostra o atraso relacionado ao segundo tráfego primário, o atraso do protocolo AEWMA teve grande influência na taxa de entrega dos quadros Figura 4.19, onde a taxa de entrega

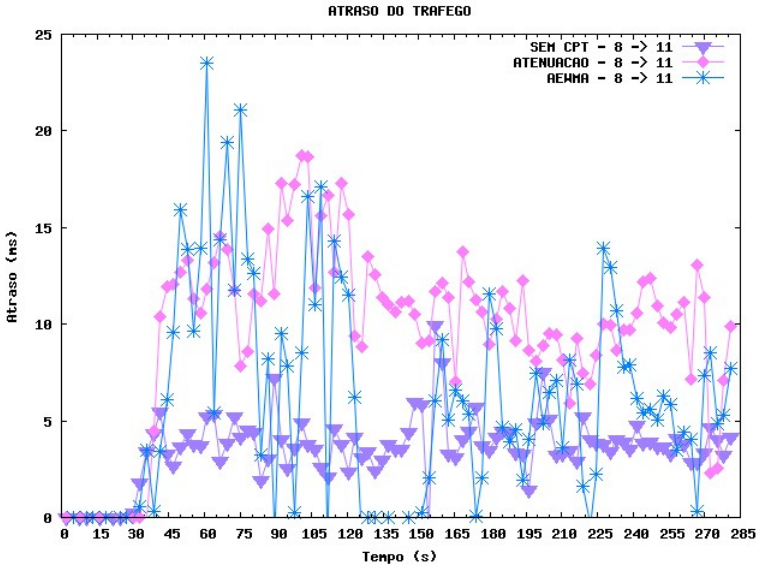

Figura 4.17: Atraso do segundo tráfego primário com 15 tráfegos secundários na rede. Tráfegos primários começando em tempos diferentes.

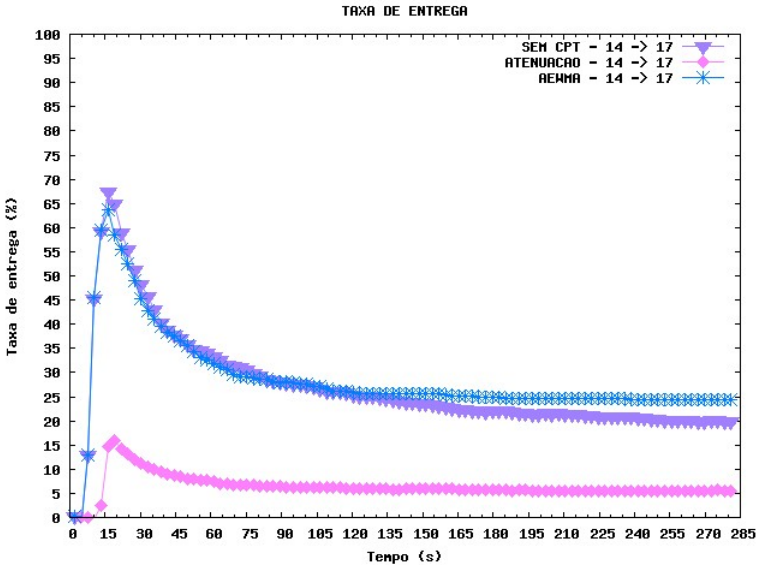

Figura 4.18: Taxa de entrega do primeiro tráfego primário com 15 tráfegos secundários na rede. Tráfegos primários começando em tempos diferentes.

chegou a somente 5%. Esta taxa de entrega na rede é ocasionada pela pouca quantidade de Bytes enviados por Joule gasto, como mostrado na Figura 4.21.

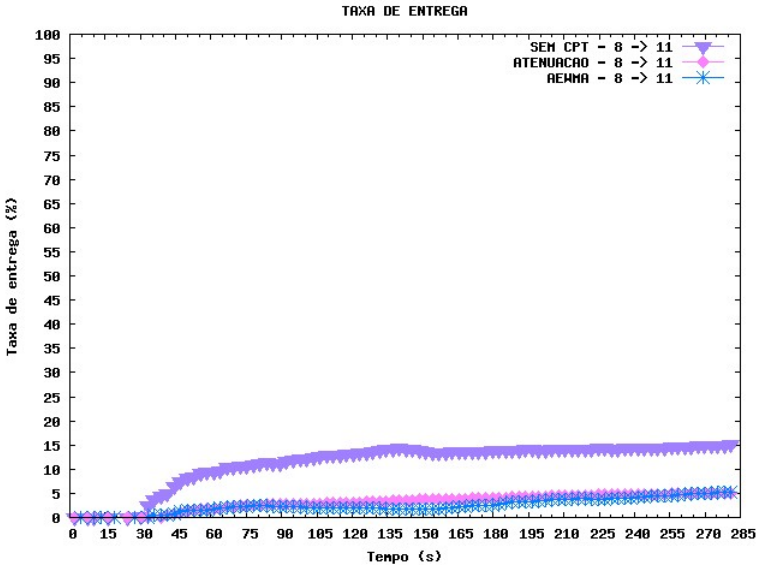

Figura 4.19: Taxa de entrega do segundo tráfego primário com 15 tráfegos secundários na rede. Tráfegos primários começando em tempos diferentes.

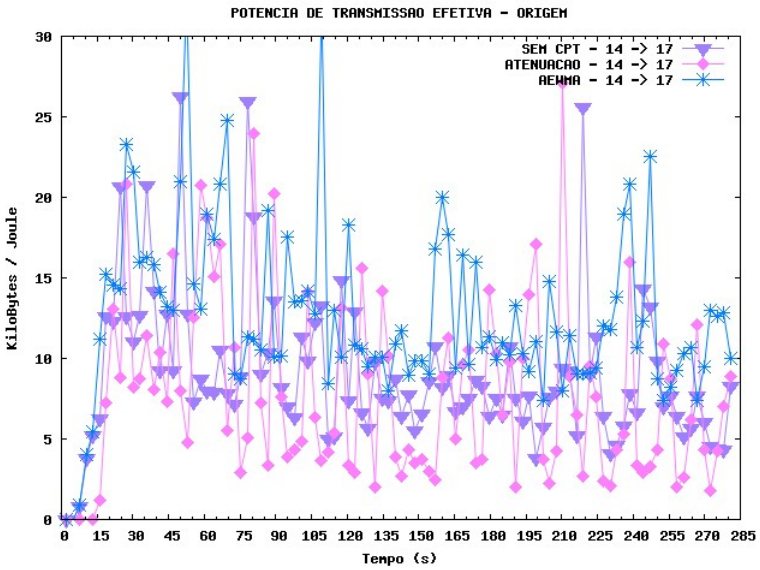

Figura 4.20: Potência de transmissão efetiva da estação **14**. 15 tráfegos secundários na rede. Tráfegos primários começando em tempos diferentes.

4.2 Análise dos Ataques de RoQ

A análise do CPT como mecanismo de defesa para os ataques de RoQ foi feita comparando-se os protocolos de Atenuação e AEWMA juntamente com uma rede *Wi-Fi* que não utilize CPT. Para a comparação foi utilizado um tráfego principal, partindo da estação **14** e tendo como destino a estação

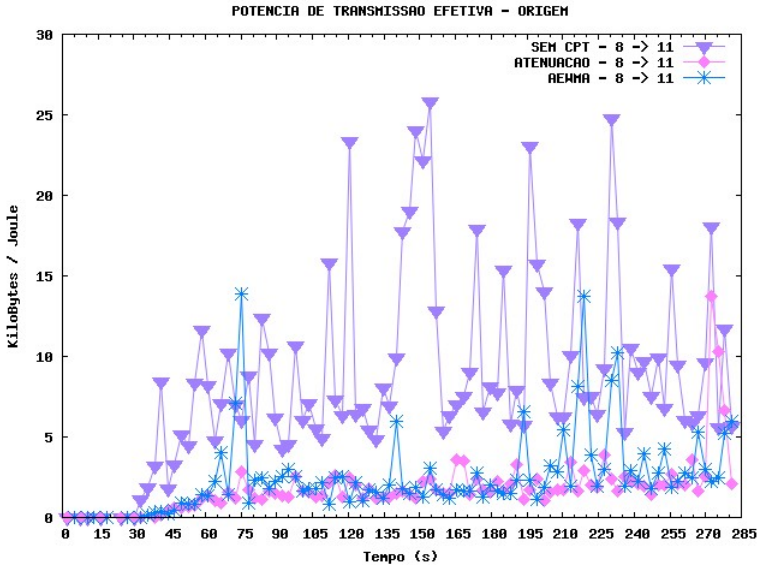

Figura 4.21: Potência de transmissão efetiva da estação **8**. 15 tráfegos secundários na rede. Tráfegos primários começando em tempos diferentes.

17, como feito em [64]. Este tráfego principal é inicializado após 2 segundos de simulação e termina quando a simulação chega a 280 segundos.

Para cada protocolo, inclusive a rede sem CPT, foram analisados os ataques *round-robin*, *self-whisper* e *flooding* em uma topologia em grade com 36 estações. Esses ataques foram escolhidos por serem demasiadamente complexos de se detectar. O ataque *pulsing*, por ser feito utilizando-se um só atacante, não teve nenhum impacto na rede. Foram feitas simulações utilizando-se 30% e 50% de atacantes na rede, sendo que o tráfego do primeiro atacante foi inicializado após 50 segundos de simulação e cada tráfego dos atacantes posteriores foi inicializado após 10 segundos do início do atacante anterior.

4.2.1 Ataque Round-Robin

Como explicado nos capítulos anteriores, no ataque *round-robin* os atacantes enviam quadros para as vítimas, escolhidas aleatoriamente, que estejam a um salto de distância. Primeiramente será analisado o impacto do ataque *round-robin* com 30% de atacantes na rede para, posteriormente, ser analisado com 50% de atacantes na rede.

Ataque com 30% de atacantes na rede

A Figura 4.22 mostra o atraso da rede perante o ataque *round-robin*. Na figura o protocolo de Atenuação após ter um atraso bastante acentuado, entre 60 e 100 segundos, diminuiu seu atraso para algo em torno de um segundo, ficando abaixo da rede sem CPT e do protocolo AEWMA. A rede sem

CPT teve um atraso em torno de 2 μs, o que acarretou em uma taxa de entrega 10% menor do que o AEWMA e 15% menor que o protocolo de Atenuação, com mostrado na Figura 4.23. Na Figura 4.24, apesar do comportamento dos protocolos de CPT e da rede sem CPT serem bastante semelhantes, após 255 segundos de simulação os protocolos de Atenuação e AEWMA enviaram aproximadamente 3 KiloBytes a mais de dados por Joule do que a rede sem CPT.

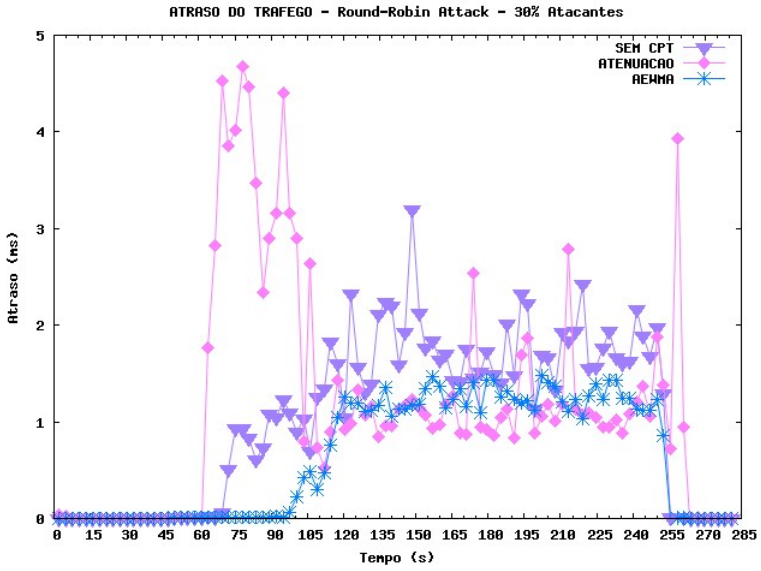

Figura 4.22: Atraso provocado pelo ataque *round-robin* com 30% de atacantes na rede.

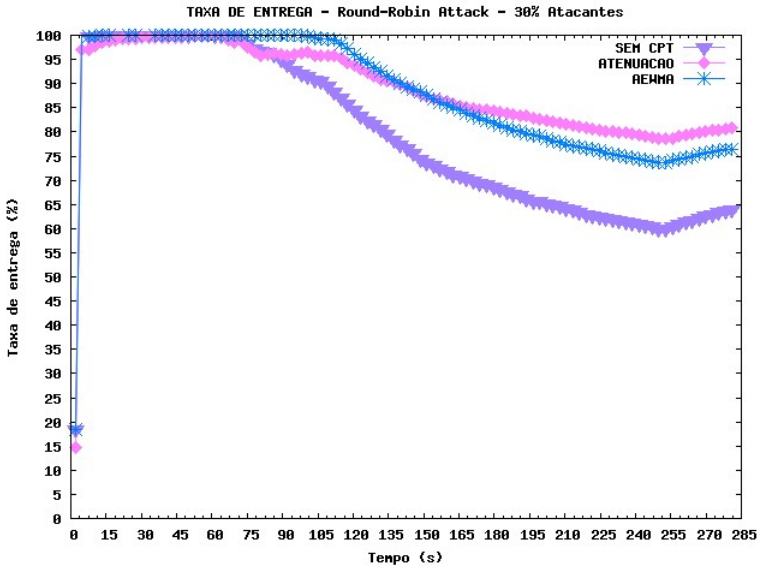

Figura 4.23: Taxa de entrega da rede sob o ataque *round-robin* com 30% de atacantes na rede.

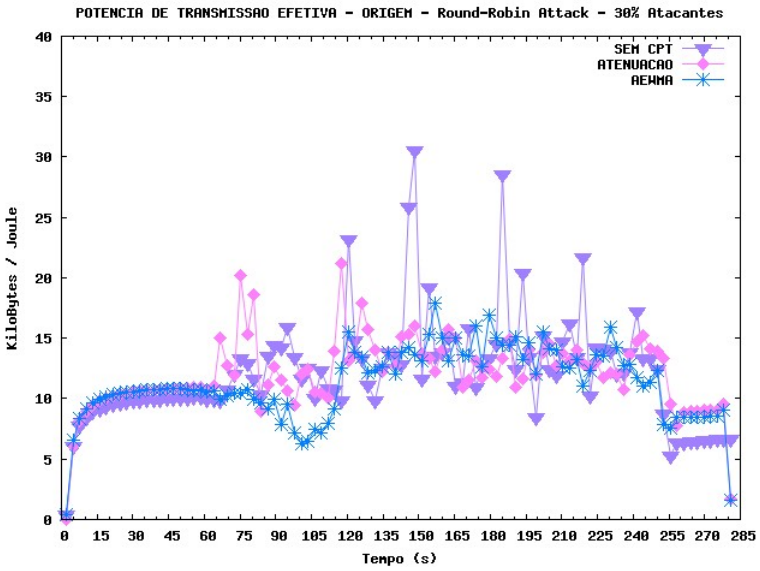

Figura 4.24: Potência efetiva da estação **14** sob o ataque *round-robin* com 30% de atacantes na rede.

Ataque com 50% de atacantes na rede

O ataque *round-robin* com 50% de atacantes na rede teve maior impacto no atraso dos quadros no protocolo de Atenuação, como mostrado na Figura 4.25. O atraso para o protocolo AEWMA e para a rede sem CPT foi praticamente o mesmo, entre 1 e 2 μs. Apesar do protocolo de Atenuação ter tido o maior atraso, ele teve praticamente a mesma taxa de entrega, em torno de 75% ao final da simulação, com relação a rede sem CPT. A taxa de entrega do protocolo AEWMA, ao final da simulação, ficou em torno de 70%, porém, o protocolo conseguiu enviar mais de 5 KiloBytes por Joule que o protocolo de Atenuação e a rede sem CPT, na média. Mesmo com a taxa de entrega estando um pouco mais baixa, o protocolo AEWMA conseguiu ter uma economia de energia mais acentuada que os outros dois.

4.2.2 Ataque Flooding

No ataque de *flooding*, as estações atacantes enviam dados para uma determinada vítima a um salto de distância. Para a análise do ataque, inicialmente será mostrado o impacto com 30% de atacantes na rede e logo depois será mostrado o impacto com 50% de atacantes na rede.

Ataque com 30% de atacantes na rede

O ataque de *flooding* com 30% de atacantes não teve muito impacto na rede sem CPT, pois diminuiu a taxa de entrega dos quadros em somente 10%, como mostrado na Figura 4.29. O protocolo de Atenuação teve uma taxa de entrega 5% superior que o protocolo AEWMA, porém o AEWMA conseguiu enviar quase o dobro de KiloBytes por Joule do que a rede sem CPT, Figura 4.30, mostrando ser

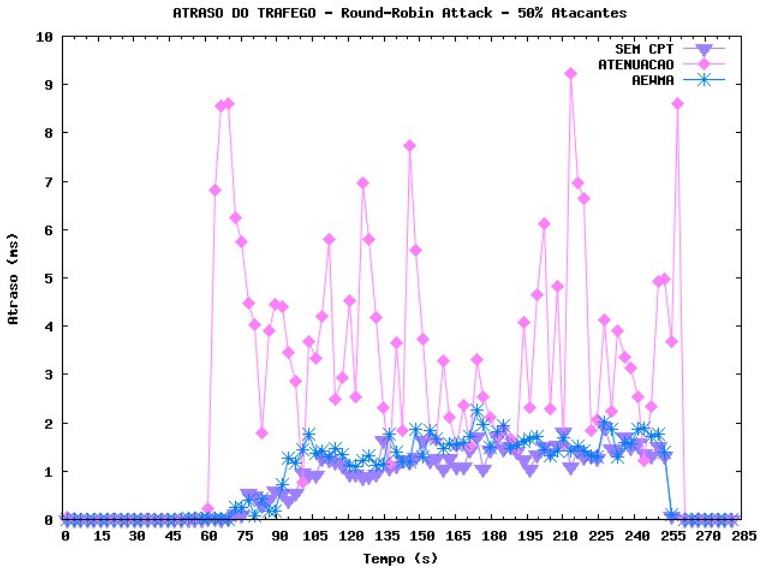

Figura 4.25: Atraso provocado pelo ataque *round-robin* com 50% de atacantes na rede.

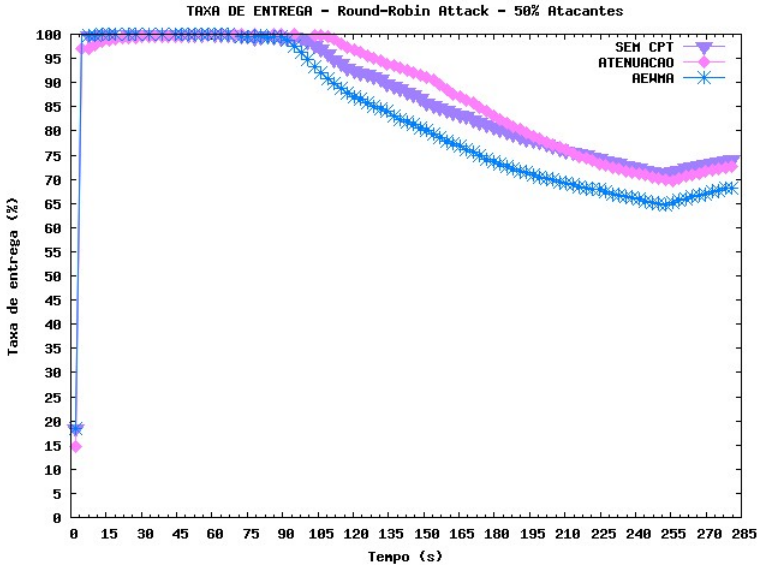

Figura 4.26: Taxa de entrega da rede sob o ataque *round-robin* com 50% de atacantes na rede.

o protocolo mais econônimo perante este ataque. Também é possível notar que o ataque de *flooding* influenciou no atraso da entrega de quadros do protocolo AEWMA.

Ataque com 50% de atacantes na rede

A taxa de entrega de quadros sofreu com o impacto do ataque de *flooding* com 50% de atacantes, Figura 4.31. Apesar dos protocolos de CPT terem sido criados para aumentarem o reuso espacial da rede, a rede sem CPT obteve uma taxa de entrega final de quase 75%, enquanto o AEWMA teve uma

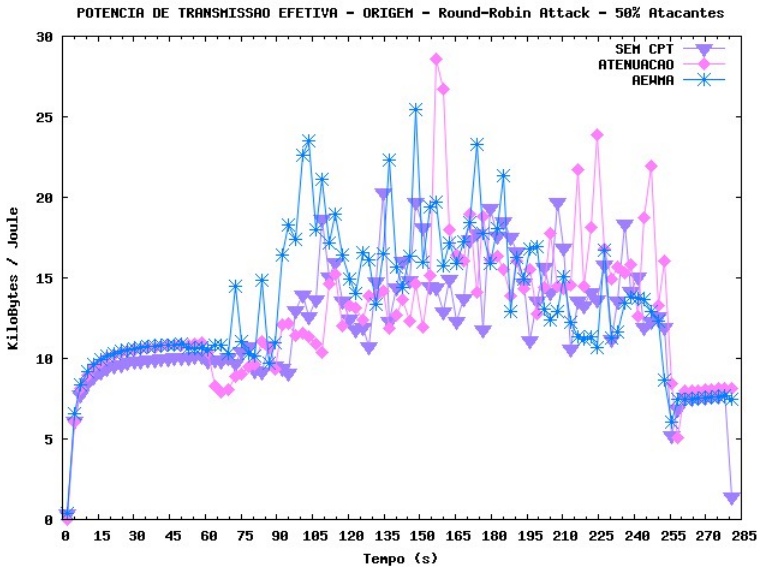

Figura 4.27: Potência efetiva da estação **14** sob o ataque *round-robin* com 50% de atacantes na rede.

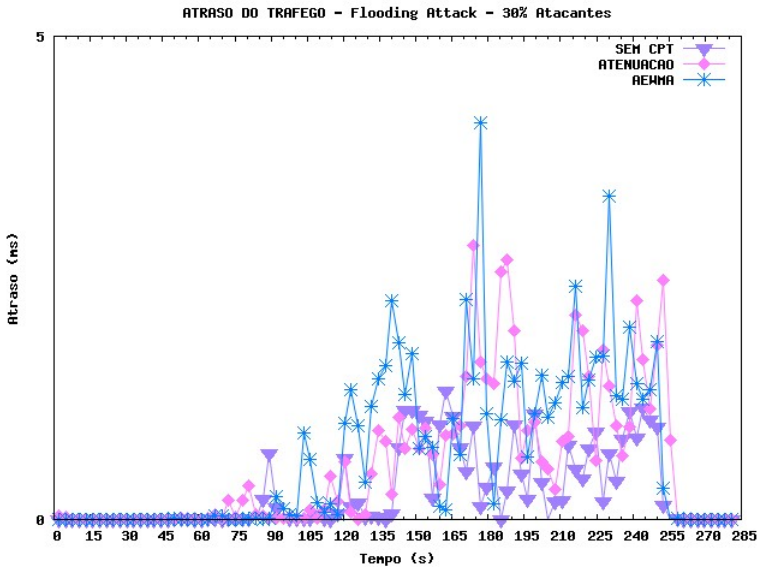

Figura 4.28: Atraso provocado pelo ataque *flooding* com 30% de atacantes na rede.

taxa de entrega de quase 70% e o protocolo de Atenuação uma taxa de 65%. Ambos os protocolos de CPT conseguiram conservar mais energia que a rede sem CPT, como mostrado na Figura 4.32.

4.2.3 Ataque Self-Whisper

No ataque *self-whisper* as duas estações responsáveis pelo tráfego, tanto a origem quanto o destino, são consideradas como atacantes. Para a análise do ataque, inicialmente será mostrado o impacto com 30% de atacantes na rede e logo depois será mostrado o impacto com 50% de atacantes na rede.

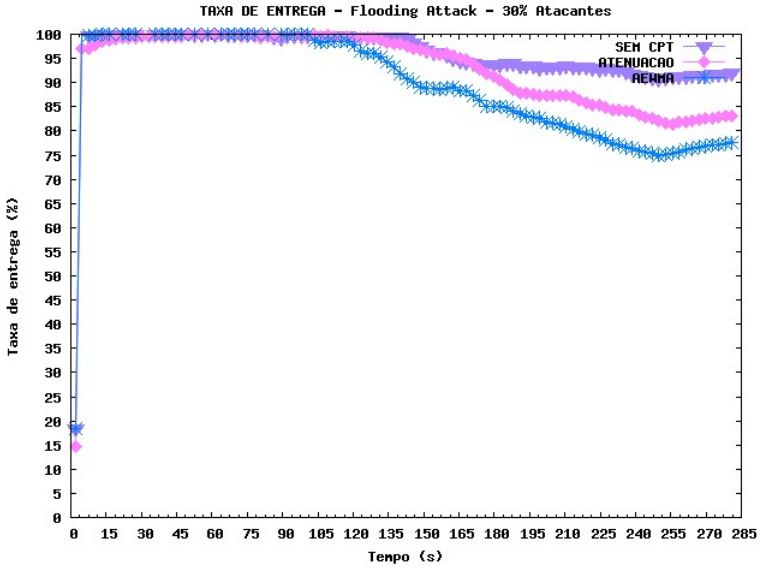

Figura 4.29: Taxa de entrega da rede sob o ataque *flooding* com 30% de atacantes na rede.

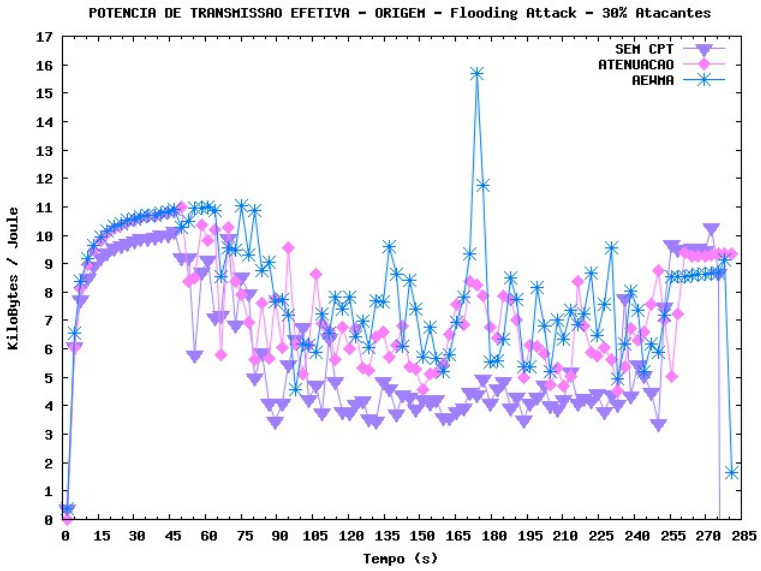

Figura 4.30: Potência efetiva da estação **14** sob o ataque *flooding* com 30% de atacantes na rede.

Ataque com 30% de atacantes na rede

O protocolo de Atenuação teve o maior atraso entre 90 e 135 ms, como mostrado na Figura 4.33. É também neste intervalo de tempo que a taxa de entrega teve uma queda mais acentuada ao cair mais de 30%, Figura 4.34. Apesar do protocolo AEWMA ter tido um atraso de quase 1 μs, sua taxa de entrega ficou somente 5% maior que a taxa do protocolo de Atenuação, tendo a rede sem CPT o mesmo comportamento que o AEWMA.

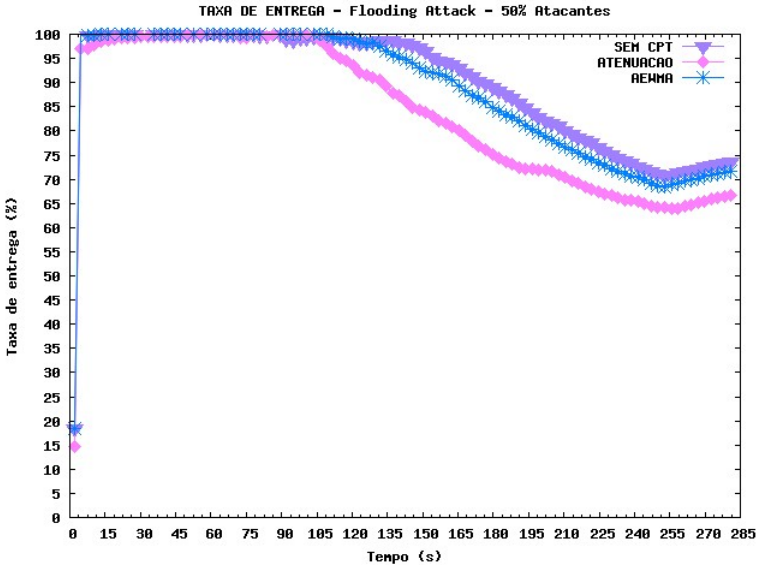

Figura 4.31: Taxa de entrega da rede sob o ataque *flooding* com 50% de atacantes na rede.

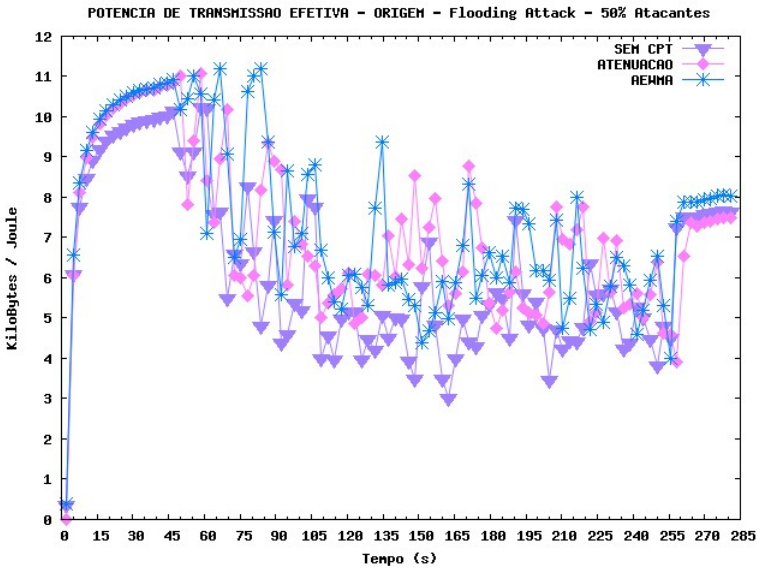

Figura 4.32: Potência efetiva da estação **14** sob o ataque *flooding* com 50% de atacantes na rede.

Ataque com 50% de atacantes na rede

O ataque *self-whisper* com 50% de atacantes na rede teve maior impacto no protocolo AEWMA e na rede sem CPT, como mostrado na Figura 4.36. Mesmo o protocolo de Atenuação possuir uma taxa de entrega de mais de 15% ao final da simulação do que o AEWMA, este protocolo conseguiu novamente ter um menor consumo de energia, logo, mais KiloBytes foram enviados utilizando menos Joules, como mostrado na Figura 4.37.

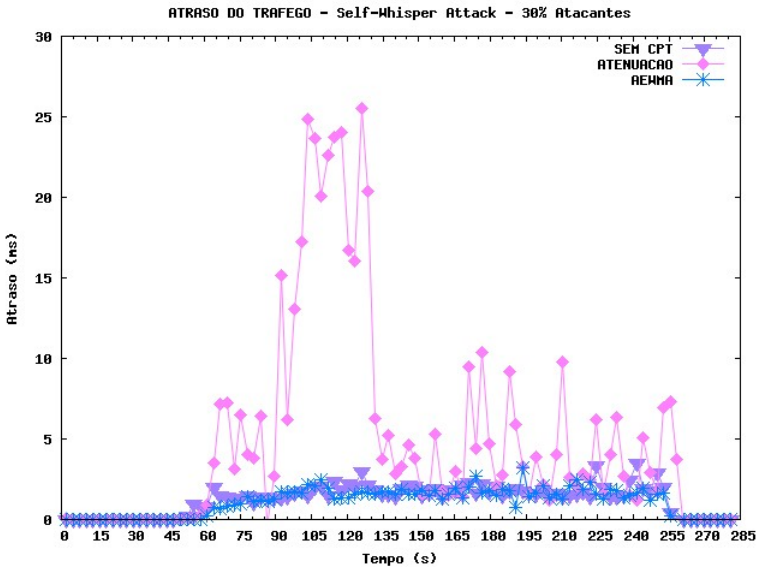

Figura 4.33: Atraso provocado pelo ataque *self-whisper* com 30% de atacantes na rede.

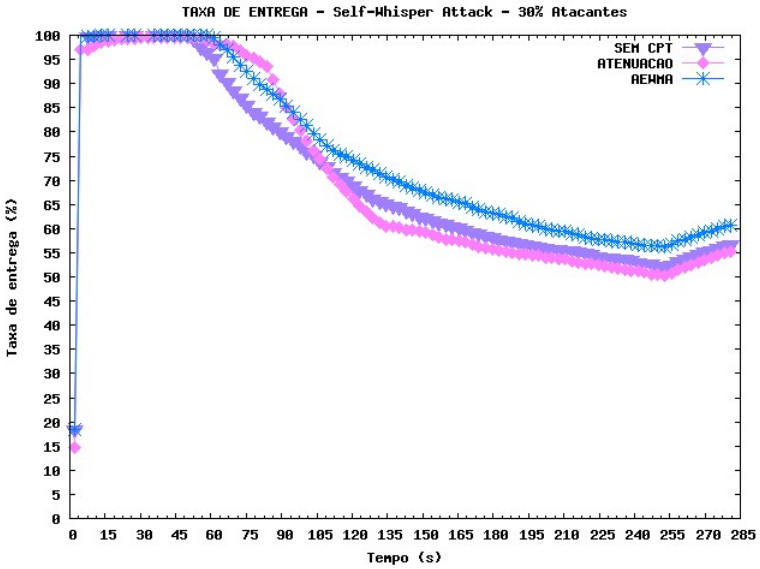

Figura 4.34: Taxa de entrega da rede sob o ataque *self-whisper* com 30% de atacantes na rede.

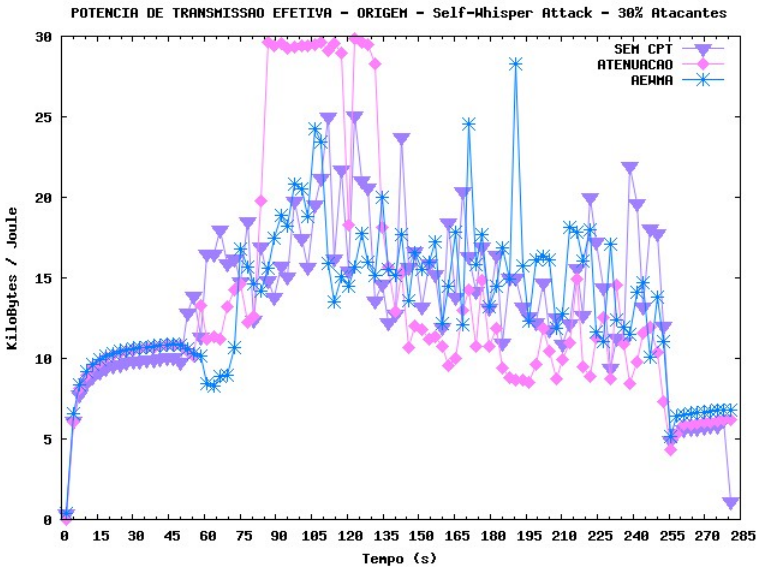

Figura 4.35: Potência efetiva da estação **14** sob o ataque *self-whisper* com 30% de atacantes na rede.

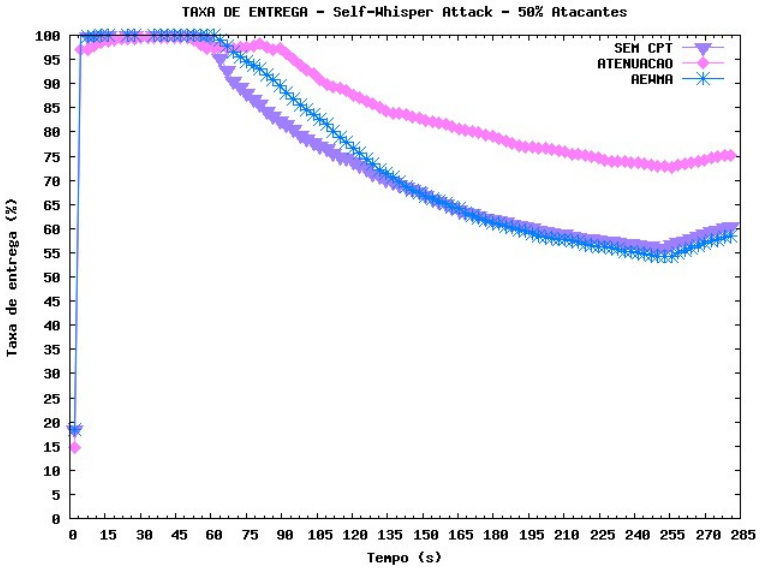

Figura 4.36: Taxa de entrega da rede sob o ataque *self-whisper* com 50% de atacantes na rede.

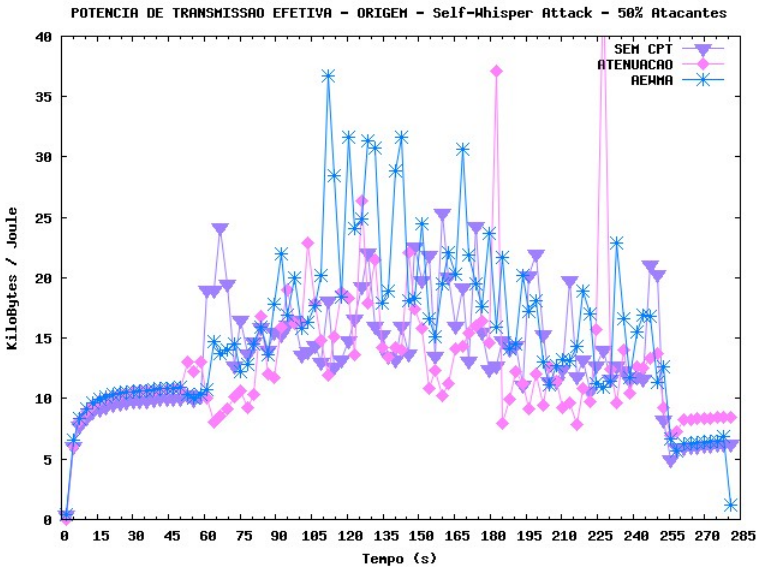

Figura 4.37: Potência efetiva da estação **14** sob o ataque *self-whisper* com 50% de atacantes na rede.

Capítulo 5

CONCLUSÕES e TRABALHOS FUTUROS

Este capítulo apresenta as conclusões dos estudos sobre o uso dos protocolos de controle de potência de transmissão (CPT), denominados de Atenuação e AEWMA *(Atenuação com filtro EWMA – Exponentially Weighted Moving Average)*, adaptados para redes *Wi-Fi*. Apresenta também uma conclusão a respeito do uso do CPT como mecanismo de defesa contra ataques de redução da qualidade de serviço *(Reduction of Quality - RoQ)* nas redes *Wi-Fi*.

5.1 Protocolos de CPT

Nas simulações realizadas, o protocolo AEWMA *(Atenuação com filtro EWMA – Exponentially Weighted Moving Average)*, nas simulações utilizando 5 e 15 tráfegos secundários teve um comportamento análogo a uma rede sem CPT, com relação à taxa de entrega de quadros e ao atraso na entrega. Todavia, o AEWMA conseguiu mostrar maior economia de energia, ao transmitir um maior número de Bytes por Joule. Por outro lado, o protocolo de Atenuação teve um comportamento bastante ineficiente, ao promover taxas de entrega de no máximo 20%.

A ineficiência do protocolo de Atenuação neste estudo se deve por causa do seu comportamento de aumentar e diminuir a potência de transmissão constantemente, fato que não ocorre no AEWMA devido ao uso da função EWMA. Outro fato que acarretou na baixa eficiência do protocolo de Atenuação se deve ao fato do problema dos enlaces assimétricos. Este problema é comum a todos os protocolos de CPT que utilizem o Esquema Básico (EB), como demonstrado por [18].

Para a avaliação dos protocolos de Atenuação e AEWMA, foi adicionado ao simulador ns2 um módulo responsável pelo CPT, que implementa os esquemas propostos.

5.2 Ataques de RoQ

Após a realização das simulações, foi possível constatar que o protocolo de Atenuação teve uma taxa de entrega de quadros melhor que o protocolo AEWMA e a rede sem CPT. Isto se deve ao fato dos ataques serem feitos na vizinhança das estações alvo. Entretanto, apesar de possuir uma taxa de entrega menor, o AEWMA conseguiu promover uma maior economia de energia, ao enviar um maior número de Bytes por Joule do que os outros dois esquemas propostos.

Vale ressaltar que, o ataque *self-whisper* foi o que teve mais impacto na rede, por ter diminuído a taxa de entrega da rede em mais de 40% nas três abordagens propostas. No ataque *self-whisper* são criados dois tráfegos entre duas estações, para que o meio possa ficar mais tempo ocupado e com isso diminuir a vazão da rede. O ataque *flooding*, apesar de ter como alvo uma das duas estações do tráfego principal analisado, teve o impacto suavizado pelos protocolos de CPT. O ataque *round-robin* teve um impacto mediano, sendo que com 30% de atacantes na rede conseguiu diminuir a taxa de entrega de quadros da rede sem CPT para somente 60%.

Aplicações de vídeo e multimídia, seriam afetadas no ataque *round-robin*, com 30% e 50% de atacantes na rede nos dois protocolos de CPT e na rede sem CPT. O ataque *flooding* com 30% de atacantes afetaria os protocolos de Atenuação e AEWMA e com 50% de atacantes afetearia as três abordagens. O ataque *self-whisper* com 30% e 50% de atacantes afetaria os protocolos AEWMA e de Atenuação e também a rede sem CPT. Por fim, após o estudo e análise dos gráficos contidos na Seção **Avaliação e Resultados**, foi possível constatar que o CPT não pode ser usado como mecanismo de defesa contra os ataques de RoQ, por ter apresentado taxas de entrega semelhantes às obtidas pela rede Wi-Fi sem CPT em todos os ataques.

5.3 Trabalhos Futuros

Os trabalhos futuros compreendem fazer maiores simulações para o CPT utilizando outras métricas, como número de quadros enviados no meio por segundo e a taxa de entrega de quadros utilizando-se quadros ACK; fazer simulações utilizando topologia aleatória que possua movimentação; e fazer simulações utilizando algum patch que crie ruído na rede, como o proposto em [56]. Além disso, será verificado se não estão ocorrendo muitos problemas com enlaces assimétricos.

Também serão feitas comparações dos métodos propostos por [41], adaptado para o *Wi-Fi*, com outros métodos já criados para estas redes. Serão feitas comparações utilizando os métodos propostos por [41], adaptados para o *Wi-Fi*, usando-se algum protocolo de roteamento com outras técnicas mostradas na literatura, como o proposto por [60].

Será também proposto o salto de freqüência para tentar lidar com ataques de RoQ e um estudo que

faça uma revisão bibliográfica sobre os ataques gulosos e maliciosos (estudo da arte - *survey*).

Referências Bibliográficas

[1] Aad, I., Hubaux, J., and Knightly, E. W. **Denial of service resilience in ad hoc networks**. In Proceedings of the 10th Annual international Conference on Mobile Computing and Networking (Philadelphia, PA, USA, September 26 - October 01, 2004). MobiCom '04. ACM, New York, NY, pp. 202-215.

[2] ALBINI, Luiz Carlos Pessoa; BANNACK, Angelo. **Redes Sem Fio**. 2006.

[3] Anastasi, G., Conti, M., Gregori, E., and Passarella, A. **802.11 power-saving mode for mobile computing in Wi-Fi hotspots: limitations, enhancements and open issues**. Wirel. Netw. 14, 6 (Dec. 2008), pp. 745-768.

[4] Awerbuch, B., Richa, A., and Scheideler, C. **A jamming-resistant MAC protocol for single-hop wireless networks**. In Proceedings of the Twenty-Seventh ACM Symposium on Principles of Distributed Computing (Toronto, Canada, August 18 - 21, 2008). PODC '08. ACM, New York, NY, pp. 45-54.

[5] B. Wu, J. Chen, J. Wu, and M. Cardei. **A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks**. Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D. -Z. Du (eds.), Springer, 2008.

[6] Bharghavan, V., Demers, A., Shenker, S., and Zhang, L. **MACAW: a media access protocol for wireless LAN's**. In Proceedings of the Conference on Communications Architectures, Protocols and Applications (London, United Kingdom, August 31 - September 02, 1994). SIGCOMM '94. ACM, New York, NY, pp. 212-225.

[7] Bellardo, J. and Savage, S. **802.11 denial-of-service attacks: real vulnerabilities and practical solutions**. Proceedings of the 12th Conference on USENIX Security Symposium - Volume 12 (Washington, DC, August 04 - 08, 2003). USENIX Security Symposium. USENIX Association, Berkeley, CA, 2-2.

[8] Boland, H. Mousavi, H. **Security issues of the IEEE 802.11b wireless LAN**. Electrical and Computer Engineering, 2004. Canadian Conference on (Carleton Univ., Ottawa, Ont., Canada; May 2 - 5, 2004), Volume 1, pp. 333 -336.

[9] Broch, J., Maltz, D. A., Johnson, D. B., Hu, Y., and Jetcheva, J. **A performance comparison of multi-hop wireless ad hoc network routing protocols.** In Proceedings of the 4th Annual ACM/IEEE international Conference on Mobile Computing and Networking (Dallas, Texas, United States, October 25 - 30, 1998). W. P. Osborne and D. Moghe, Eds. MobiCom '98. ACM, New York, NY, pp. 85-97.

[10] Cali, F. Conti, M. Gregori, E. **IEEE 802.11 protocol: design and performance evaluation of anadaptive backoff mechanism**. Selected Areas in Communications, IEEE Journal on, Volume 18, Issue 9, pp. 1774-1786.

[11] Chae, C., Lee, S., Lee, J., and Lee, J. **A Study of Defense DDoS Attacks Using IP Traceback**. In Proceedings of the the 2007 international Conference on intelligent Pervasive Computing (October 11 - 13, 2007). IPC. IEEE Computer Society, Washington, DC, 402-408.

[12] Chang, C. and Chang, H. **Power control and fairness MAC mechanisms for 802.11 WLANs**. Comput. Commun. 30, 7 (May. 2007), pp. 1527-1537.

[13] D. Chen, J. Deng, and P. K. Varshney. **Protecting Wireless Networks against a Denial of Service Attack Based on Virtual Jamming**. ACM MobiCom '03, Poster, San Diego, CA, USA, September 14-19, 2003.

[14] DARPA with SAMAN and NSF with CONSER and ACIRI. **Network Simulator 2**. *http://www.isi.edu/nsnam/ns/ns-build.html*. Acesso em: Outubro, 2008.

[15] D.B. Johnson and D.A. Maltz. **Dynamic source routing in ad hoc wireless networks**. In: Mobile Computing,eds.T.Imielinskiand H. Korth (Kluwer Academic, 1996) pp. 153-181.

[16] David Thuente and Mithun Acharya. **Intelligent Jamming in Wireless Networks with Applications to 802.11b and Other Networks**. Proceedings of the 25th IEEE Communications Society Military Communications Conference (MILCOM), Washington DC, USA, 2006.

[17] Estan, C. and Varghese, G. **New directions in traffic measurement and accounting: Focusing on the elephants, ignoring the mice**. ACM Trans. Comput. Syst. 21, 3 (Aug. 2003), pp. 270-313.

[18] E.-S. Jung and N.H. Vaidya. **A power saving MAC protocol for wireless networks**. Tech. Rep. University of Illinois at Urbana Champaign, 2002.

[19] G. Khanna, A. Masood, and C. N. Rotaru. **Channel Access and Synchronization Attacks Against MAC Protocols in Wireless Networks**. Addressing MAC based attacks in Wireless Networks, May, 2005.

[20] Gast, Matthew. **802.11 Wireless Networks: the Definitive Guide**. 1st. O'Reilly & Associates, Inc, 2002.

[21] Guang, L., Assi, C., and Ye, Y. **DREAM: A system for detection and reaction against MAC layer misbehavior in ad hoc networks**. Comput. Commun. 30, 8 (Jun. 2007), pp. 1841-1853.

[22] Guirguis, M., Bestavros, A., and Matta, I. **Exploiting the Transients of Adaptation for RoQ Attacks on Internet Resources**. In Proceedings of the 12th IEEE international Conference on Network Protocols (October 05 - 08, 2004). ICNP. IEEE Computer Society, Washington, DC, pp. 184-195.

[23] Guirguis, M. Bestavros, A. Matta, I. Zhang, Y. **Reduction of quality (RoQ) attacks on Internet end-systems**. INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, Volume 2, pp. 1362-1372.

[24] Guirguis, M. Bestavros, A. Matta, I. **On the Impact of Low-Rate Attacks**. Communications, 2006. ICC '06. IEEE International Conference on Volume 5, pp. 2316-2321.

[25] Halkes, G. P., van Dam, T., and Langendoen, K. G. **Comparing energy-saving MAC protocols for wireless sensor networks**. Mob. Netw. Appl. 10, 5 (Oct. 2005), pp. 783-791.

[26] Hansmann, U., Nicklous, M. S., and Stober, T. **Pervasive Computing Handbook**. Springer-Verlag New York, Inc, 2001.

[27] Hu, Y. and Perrig, A. **A Survey of Secure Wireless Ad Hoc Routing**. IEEE Security and Privacy 2, 3 (May. 2004), pp. 28-39.

[28] Jung, E. and Vaidya, N. H. 2002. **A power control MAC protocol for ad hoc networks**. In Proceedings of the 8th Annual international Conference on Mobile Computing and Networking (Atlanta, Georgia, USA, September 23 - 28, 2002). MobiCom '02. ACM, New York, NY, pp. 36-47.

[29] Kawadia, V.; Kumar, P.R. **"Principles and protocols for power control in wireless ad hoc networks"**. Selected Areas in Communications, IEEE Journal on , vol.23, no.1, pp. 76-88.

[30] Kyasanur, P. **Selfish MAC Layer Misbehavior in Wireless Networks**. IEEE Transactions on Mobile Computing 4, 5 (Sep. 2005), pp. 502-516.

[31] Kim, K. and Koo, H. **Optimizing Power-Aware Routing using Zone Routing Protocol in MANET**. In Proceedings of the 2007 IFIP international Conference on Network and Parallel Computing Workshops (September 18 - 21, 2007). NPC. IEEE Computer Society, Washington, DC, pp. 670-675.

[32] Kim, T., Lim, H., and Hou, J. C. **Improving spatial reuse through tuning transmit power, carrier sense threshold, and data rate in multihop wireless networks**. In Proceedings of the 12th Annual international Conference on Mobile Computing and Networking (Los Angeles, CA, USA, September 23 - 29, 2006). MobiCom '06. ACM, New York, NY, pp. 366-377.

[33] KUROSE, James F ; ROSS, Keith W ; ZUCCHI, W. L. **Redes de Computadores e a Internet: Uma Nova Abordagem**. São Paulo: Addison Wesley, 2003. 548 p.

[34] Kuzmanovic, A. and Knightly, E. W. **Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants**. In Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols For Computer Communications (Karlsruhe, Germany, August 25 - 29, 2003). SIGCOMM '03. ACM, New York, NY, pp. 75-86.

[35] Kuzmanovic, A. and Knightly, E. W. **Low-rate TCP-targeted denial of service attacks and counter strategies**. IEEE/ACM Trans. Netw. 14, 4 (Aug. 2006), pp. 683-696.

[36] GJ Noer. **Cygwin: A free win32 porting layer for unix applications**. In 2d USENIX NT Symposium, 1998.

[37] Gu, Q., Liu, P., and Chu, C. **Analysis of area-congestion-based DDoS attacks in ad hoc networks**. Ad Hoc Netw. 5, 5 (Jul. 2007), 613-625.

[38] Lei Guang; Assi, C. **MAC layer misbehavior in ad hoc networks**. Electrical and Computer Engineering, 2005. Canadian Conference on, 1-4 May, 2005, pp. 1103-1106.

[39] Guang, L. and Assi, C. **On the resiliency of mobile ad hoc networks to MAC layer misbehavior**. In Proceedings of the 2nd ACM international Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (Montreal, Quebec, Canada, October 10 - 13, 2005). PE-WASUN '05. ACM, New York, NY, pp. 160-167.

[40] Lei Guang; Assi, C. **A Self-Adaptive Detection System for MAC Misbehavior in Ad Hoc Networks**. Communications, 2006. ICC. IEEE International Conference on Volume 8, Issue, pp. 3682-3687.

[41] Luiz H. A. Correia, Daniel F. Macedo, Aldri Luiz dos Santos, Antonio A. Loureiro and José M. Nogueira. **Ajustando a Potência de Transmissão em Protocolos MAC**. 24º Simpósio Brasileiro de Redes de Computadores, pp. 589-604.

[42] M. Guirguis, A. Bestavros, I. Matta. **Bandwidth stealing via link targeted RoQ attacks**. In: CCN'04, 2004.

[43] M. O. Pervaiz, M. Cardei, and J. Wu. **Routing Security in Ad Hoc Wireless Networks**. In Network Security, S. Huang, D. MacCallum, and D. -Z. Du (eds.), Springer, 2008.

[44] Mark Weiser. **The computer for the 21st century**. In Human-Computer interaction: Toward the Year 2000, R. M. Baecker, J. Grudin, W. A. Buxton, and S. Greenberg, Eds. Morgan Kaufmann Publishers, San Francisco, CA, pp. 933-940.

[45] Michele N. Lima, Aldri L. Santos, Guy Pujolle. **A Survey of Survivability in Mobile Ad Hoc Networks**. IEEE Communications Surveys and Tutorials, 2009 (to appear).

[46] Mirkovic, J. and Reiher, P. **A taxonomy of DDoS attack and DDoS defense mechanisms**. SIGCOMM Comput. Commun. Rev. 34, 2 (Apr. 2004), pp. 39-53.

[47] Mishra, A., Petroni, N. L., Arbaugh, W. A., and Fraser, T. **Security issues in IEEE 802.11 wireless local area networks: a survey: Research Articles**. Wirel. Commun. Mob. Comput. 4, 8 (Dec. 2004), pp. 821-833.

[48] Negi, R.; Rajeswaran, A. **DoS analysis of reservation based MAC protocols**. Communications, 2005. ICC 2005. 2005 IEEE International Conference on , Vol.5, pp. 3632-3636, 16-20 May 2005.

[49] P. Karn. **MACA - a new channel access method for packet radio**. In ARRL/CRRL Amateur Radio 9th Computer Networking Conference, pp. 134-40, ARRL, 1990.

[50] Paschoalini, Fabio Manuel. **WiMAX: Uma Recente Tecnologia Sem Fio**. Monografia, Departamento de Ciência da Computação, Universidade Federal de Lavras, 2006.

[51] Perkins, C. E.; Belding-Royer, E. M. **Ad hoc On-Demand Distance Vector Routing**. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp. 90-100.

[52] Pires, A. A., Fontes, M. F. e Rezende, J. F. **Proposta e Avaliação de um Esquema de Controle de Potência com Memória em Redes Ad Hoc 802.11**. XXII Simpósio Brasileiro de Redes de Computadores - SBRC'2004, pp. 351-364, Gramado, RS, 2004.

[53] PIRES, A. A. ; REZENDE, José Ferreira de. **FN-ALCA: Esquema de Controle de Potência para Economia de Energia e Aumento da Capacidade de Redes Ad Hoc 802.11**. SBRC 2005, Fortaleza.

[54] P. Kyasanur and N. Vaidya. **Detection and handling of mac layer misbehavior in wireless networks**. In Proceedings of the International Conference on Dependable Systems and Networks, June 2003.

[55] Raya, M., Hubaux, J., and Aad, I. **DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots**. In Proceedings of the 2nd international Conference on Mobile Systems, Applications, and Services (Boston, MA, USA, June 06 - 09, 2004). MobiSys '04. ACM, New York, NY, 84-97.

[56] RJ Punnoose, PV Nikitin, DD Stancil. **Efficient simulation of Ricean fading within a packet simulator**. Vehicular Technology Conference, 2000. IEEE VTS-Fall VTC 2000. 52nd, Vol. 2 (2000), pp. 764-767 vol.2.

[57] Shevtekar, A. and Ansari, N. **A router-based technique to mitigate reduction of quality (RoQ) attacks**. Comput. Netw. 52, 5 (Apr. 2008), pp. 957-970.

[58] Smith, C. and Collins, D. **3G Wireless Networks**. McGraw-Hill, Inc, 2001.

[59] Tanenbaum, A. S. **Redes de Computadores**. 4a Ed. Rio de Janeiro: Campus, 2003.

[60] V. Kawadia and P. Kumar. **Principles and protocols for power control in wireless ad hoc networks**. In wireless ad hoc networks. IEEE Journal on Selected Areas in Communications, pp. 76-88.

[61] V. Navda, A. Bohra, S. Ganguly, R. Izmailov, and D. Rubenstein. **Using channel hopping to increase 802.11 resilience to jamming attacks**. In IEEE Infocom Minisymposium.

[62] Wang, N., Chen, J., Huang, Y., and Su, Y. December, 2007. **A Power-Aware Multicast Routing Protocol for Mobile Ad Hoc Networks With Mobility Prediction**. Wirel. Pers. Commun. 43, 4 (Dec. 2007), pp. 1479-1497.

[63] Wang-Hei Ho, I. and Chang Liew, S. **Impact of Power Control on Performance of IEEE 802.11 Wireless Networks**. IEEE Transactions on Mobile Computing 6, 11 (Nov. 2007), pp. 1245-1258.

[64] Wei Ren, Dit-Yan Yeung, Hai Jin, and Mei Yang. **Pulsing RoQ DDoS Attack and Defense Scheme in Mobile Ad Hoc Networks**. International Journal of Network Security, Vol.4, No.2, March 2007, pp. 227-234.

[65] Y. Zhou, D. Wu, and S. Nettles. **Analyzing and preventing mac-layer denial of service attacks for stock 802.11 systems**. In Workshop on Broadband Wireless Services and Applications, BROADNETS.

[66] Yang, G., Gerla, M., and Sanadidi, M. Y. **Defense against low-rate TCP-targeted denial-of-service attacks**. In Proceedings of the Ninth international Symposium on Computers and Communications 2004 Volume 2 (Iscc"04) - Volume 02 (June 28 - July 01, 2004). ISCC. IEEE Computer Society, Washington, DC, 345-350.

[67] Yu Chen; Kai Hwang. **Spectral Analysis of TCP Flows for Defense Against Reduction-of-Quality Attacks**. Communications, 2007. ICC apos;07. IEEE International Conference on, pp. 1203-1210.

[68] Zambalde, A. L.; Silva E Padua, C. I. P. **O documento cientifico em Ciência da Computação - suas partes e sua redação: estudo e análise em uma Instituição Federal de Ensino (IFES)**. Belo Horizonte/MG: DCC-UFMG, 2005 (anotações de aula).

[69] **Controlling High-Bandwidth Flows at the Congested Router**. In Proceedings of the Ninth international Conference on Network Protocols (November 11 - 14, 2001). ICNP. IEEE Computer Society, Washington, DC, 192.