O impacto de ataques RoQ em redes 802.11 com controle de potência de transmissão

Urlan S. de Barros[1]*, Tiago de C. Freire[2], Michele N. Lima[3], Luiz H. A. Correia[2], Aldri L. dos Santos[1]

Dep. de Informática[1]
Univ. Federal do Paraná
Curitiba-PR, Brasil
{urlan,aldri}@inf.ufpr.br

Dep. de Ciência da Comp.[2]
Univ. Federal de Lavras
Lavras-MG, Brasil
{lcorreia,tiagocf}@ufla.br

Lab. D'Informatique[3]
UPMC, Paris 6
Paris, França
michele.nogueira@lip6.fr

Abstract. *IEEE 802.11 has two coordinator functions, called DCF and PCF, which are responsible for media access control. Transmition power control (TPC) has been employed to save power of devices and improve spatial reuse of the network. However, both 802.11 and TPC techniques are vulnerable to attacks that deny services, such as reduction of quality (RoQ) attacks, since they need that stations keep default transmission behavior. RoQ attacks intend to optimize the attack traffic to reach the maximum damage and avoid prevention or detection mechanisms. This work analyzes how RoQ attacks affect 802.11 and TPC techniques in relation to saving power and spatial reuse. We evaluate by simulation the impact of attacks considering three different TPC techniques: AEWMA, Atenuation and Basic Scheme. Results show higher saving power when using AEWMA technique, and that spatial reuse has been affected only in presence of 30% or more of misbehaving self-whiper RoQ attackers.*

Resumo. *O IEEE 802.11 possui duas funções coordenadoras, denominadas DCF e PCF, responsáveis pelo controle de acesso ao meio. Além disso, técnicas de controle de potência de transmissão (CPT) têm sido utilizadas para assegurar que a rede tenha uma maior economia de energia e uma maior vazão de dados através do reuso espacial. Contudo, tanto o 802.11 quanto as técnicas de CPT são vulneráveis a ataques de redução da qualidade de serviço (RoQ), devido à necessidade das estações manterem um comportamento de transmissão padrão. Os ataques RoQ têm a finalidade de aumentar a vazão do tráfego dos atacantes com o intuito de produzir um dano máximo na rede e evitar mecanismos de detecção ou prevenção. Este trabalho analisa como os ataques RoQ, self-whiper, flooding e round-robin afetam o protocolo IEEE 802.11 padrão e as técnicas de CPT. Resultados mostram que a técnica AEWMA apresentou a maior economia de energia na presença de qualquer ataque. Além disso, o reuso espacial não foi afetado, exceto diante do ataque self-whisper com 30% e 50% de atacantes.*

1. Introdução

O protocolo IEEE 802.11 foi criado com o intuito de promover o desenvolvimento de redes sem fio em direção à computação ubíqüa [Weiser 1999] e pervasiva

*Bolsista CNPq número 551867/2009-4. Trabalho apoiado pelo CNPq - processo: 303770/2008-2

[Hansmann et al. 2001]. Este protocolo é empregado na construção de diversos tipos de redes sem fio, como as MANETs *(Mobile Ad Hoc Networks)*, por garantir a comunicação entre dispositivos mesmo diante de mobilidade. Com o intuito de prover o acesso ao meio às estações, O IEEE 802.11 utiliza duas funções coordenadoras, a função DCF *(Distributed Coordination Function)* e a PCF *(Point Coordination Function)* [Gast 2005], sendo que o acesso ao meio ocorre de maneira distribuída na DCF e de forma centralizada na PCF. Na função DCF, as estações transmissoras enviam os dados considerando alguns temporizadores, tais como, o DIFS *(Distributed Inter-Frame Space)*, o SIFS *(Shortest Inter-Frame Space)*, o EIFS *(Extended Inter-Frame Space)* e o NAV *(Network Allocation Vector)*, além de quadros de controle para a reserva virtual do meio, como o RTS *(Request-to-Send)* e o CTS *(Clear-To-Send)*.

O controle de potência de transmissão (CPT) [Monks 2001] possibilita à estação transmissora empregar a quantidade de energia necessária para que as estações vizinhas a um salto de distância decodifiquem corretamente o quadro transmitido. A utilização do CPT em MANETs tem como vantagens o aumento da vazão da rede por reuso espacial do meio de comunicação, na qual várias estações transmitem dados ao mesmo tempo, e o aumento do tempo médio de vida das estações, ao reduzir o consumo de energia [Correia et al. 2006]. A primeira técnica de CPT proposta para MANETs, denominada MACA ou Esquema Básico [Karn 1990], realiza a reserva virtual do meio empregando o maior nível de potência do rádio no envio dos quadros RTS/CTS, e transmite os quadros de dados e ACK usando níveis menores. Contudo, as estações ao transmitirem quadros empregando diferentes níveis de potência criam o problema de enlaces assimétricos [Jung and Vaidya 2002]. Esse problema aumenta o número de colisões nas estações e reduz o reuso espacial da rede, devido à condição de assimetria no meio. Diversas técnicas de CPT tentam solucionar o problema de enlaces assimétricos. No entanto, tais soluções são parciais [Pires et al. 2004], inviáveis na prática [Jung and Vaidya 2002] ou possuem efeitos colaterais como os problemas do terminal exposto e escondido existentes nas técnicas Atenuação e AEWMA [Correia et al. 2006].

Ataques gulosos e maliciosos exploram as vulnerabilidades da função DCF em consequência da sua simplicidade de implementação [Awerbuch et al. 2008]. Nos ataques gulosos, um atacante tem o intuito de aumentar a vazão do seu tráfego, mas sem destruir o comportamento normal da rede. Por outro lado, atacantes maliciosos possuem o objetivo de consumir o maior número de recursos e negar os serviços das estações em uma rede. Os ataques maliciosos são classificados em ataques de negação de serviço *(Denial of Service - DoS)* com alta taxa de transmissão de dados e ataques de DoS com baixa taxa de transmissão de dados, como os ataques de redução da qualidade de serviço *(Reduction of Quality - RoQ)*. Os ataques RoQ possuem poucas abordagens efetivas de defesa [Ren et al. 2008], por explorarem a capacidade dinâmica de adaptação de mecanismos presentes nas camadas de comunicação da rede [Guirguis et al. 2004, Guirguis et al. 2005]. Como consequência, os atacantes tornam complexa sua detecção e prevenção [Guirguis et al. 2007].

As técnicas de CPT baseadas em [Karn 1990], assim como a função DCF do IEEE 802.11, são vulneráveis aos ataques RoQ por possuírem mecanismos que realizam dinamicamente a reserva virtual do meio. Os ataques RoQ exploram a reserva virtual do meio criando enlaces assimétricos na rede, deteriorando assim a taxa de entrega e aumentando o consumo de energia das estações. Este trabalho analisa a influência dos ataques RoQ

- *flooding*, *round-robin* e *self-whisper* [Ren et al. 2008] - sob o protocolo 802.11 padrão e o 802.11 utilizando as técnicas de CPT: Esquema Básico [Karn 1990], Atenuação e AEWMA [Correia et al. 2006]. Resultados simulados mostram que a técnica AEWMA apresentou um menor consumo de energia e uma taxa de entrega próxima ao 802.11 padrão. Porém, a taxa de entrega de quadros da técnica AEWMA é ainda susceptível ao ataque *self-whisper*.

O artigo está organizado da seguinte forma. A Seção 2 apresenta os trabalhos relacionados. A Seção 3 apresenta as técnicas de CPT consideradas neste trabalho. A Seção 4 define os tipos de ataques RoQ utilizados para a avaliação das técnicas. A Seção 5 apresenta e analisa os resultados tendo como métricas o reuso espacial da rede e a economia de energia das estações. A Seção 6 apresenta a conclusão e os trabalhos futuros.

2. Trabalhos Relacionados

Baseado em MACA [Karn 1990], outras técnicas de CPT para a camada de enlace foram desenvolvidas, tais como PCMA *(Power Controlled Multiple Access)* [Jung and Vaidya 2002] e Esquema Básico com Memória (EBM) [Pires et al. 2004]. Essas técnicas têm como objetivo o aumento da economia de energia e do reuso espacial da rede, além da redução dos enlaces assimétricos inicialmente criados pela MACA.

Na técnica PCMA, as estações enviam os quadros de controle considerando a máxima potência de transmissão, enquanto o quadro de dados é transmitido empregando-se uma elevação periódica da potência de transmissão, com o intuito de mitigar o problema de enlaces assimétricos. Contudo, esta técnica é inviável, por necessitar que os rádios atuais modifiquem a potência de transmissão rapidamente e com bastante precisão. Na técnica EBM, as estações possuem uma tabela de vizinhos que guarda as potências recentemente usadas para enviar um quadro [Pires et al. 2004]. Para transmitir os quadros de controle, as estações buscam na tabela a última potência empregada, com o objetivo de diminuir a área na qual a reserva virtual do meio é feita. Esse esquema reduz o consumo de energia e aumenta o reuso espacial da rede, mas sofre do problema da flutuação da potência calculada, por modificar com grande intensidade os níveis de potência.

[Correia et al. 2006] propuseram para as redes de sensores sem fio quatro técnicas de CPT, denominadas Iteração, Atenuação, AEWMA e Híbrida, que não permitem a criação de enlaces assimétricos. Tais técnicas, no lugar de quadros de controle, incluem um campo no quadro de dados para a reserva virtual do meio. Contudo, devido à ausência dos quadros RTS/CTS, os problemas do terminal escondido e exposto, que antes eram parcialmente solucionados pelo protocolo 802.11, voltam a ocorrer com maior frequência.

Os ataques de DoS com baixa taxa de transferência de dados nas camadas de rede têm sido estudados em [Guirguis et al. 2004, Guirguis et al. 2005, Guirguis et al. 2006, Chen and Hwang 2007]. [Guirguis et al. 2005] demonstraram o impacto dos ataques RoQ em controladores de admissão. Esses mecanismos protegem a rede contra condições de sobrecarga, rejeitando requisições que fazem que o sistema saia do seu comportamento normal. [Guirguis et al. 2006] analisaram o impacto dos ataques *Shrew* e RoQ no sistema de controle de congestionamento do TCP.

Este trabalho analisa o impacto dos ataques RoQ no comportamento das estações que se utilizam das técnicas AEWMA, Atenuação e Esquema Básico. Os ataques estudados, *flooding*, *round-robin* e *self-whisper* [Ren et al. 2008], criam enlaces assimétricos

ao explorarem a reserva virtual do meio. Além disso, com o objetivo de minimizar os problemas de terminal escondido e exposto, as estações que usam as técnicas AEWMA e Atenuação transmitem os quadros de controle RTS/CTS empregando níveis de potência menores, de maneira similiar ao EBM.

3. Técnicas de CPT

Os protocolos empregam técnicas de CPT para diminuir o consumo de energia das estações e aumentar a vazão da rede através do reuso espacial. As técnicas de CPT analisadas são Esquema Básico [Karn 1990], Atenuação e AEWMA [Correia et al. 2006].

3.1. Esquema Básico

A técnica MACA [Karn 1990], também conhecida como Esquema Básico [Jung and Vaidya 2002], foi a primeira técnica a propor o CPT em redes sem fio. A idéia principal desta técnica é usar a máxima potência de transmissão para enviar os quadros de controle RTS/CTS e transmitir os quadros de dados e ACK com a menor potência de transmissão possível. Os protocolos que empregam esta técnica trabalham da seguinte maneira [Chen et al. 2006]:

1. O transmissor envia um quadro RTS utilizando a máxima potência de transmissão $P_{TX_{max}}$.
2. O receptor, ao receber o quadro RTS com uma dada potência de recepção P_{RX}, calcula a potência de transmissão mínima $P_{TX_{min}}$ que o transmissor empregará para enviar o quadro de dados através da equação:

$$P_{TX_{min}} = \frac{P_{TX_{max}}}{P_{RX}} \times RX_{desejado} \quad (1)$$

   onde $RX_{desejado}$ é a menor potência de recepção para que a estação decodifique o quadro corretamente. Após calcular a potência de transmissão mínima, o emissor insere a potência calculada no quadro CTS e envia o quadro como resposta ao RTS do transmissor, usando a máxima potência de transmissão.
3. Ao receber o CTS, o transmissor empregará a potência de transmissão $P_{TX_{min}}$ para enviar o quadro de dados para o emissor. O transmissor também insere a mesma potência de transmissão considerada para o envio do quadro de dados. Isto é feito para que o emissor possa utilizar a mesma potência de transmissão $P_{TX_{min}}$ para enviar o ACK.
4. Ao receber o quadro de dados o emissor enviará o ACK empregando a potência de transmissão $P_{TX_{min}}$ retirada do quadro de dados.

Todos os protocolos que empregam a técnica de Esquema Básico são afetados pelo problema do enlace assimétrico [Pires et al. 2004]. Ao fazer a reserva virtual do meio enviando os quadros RTS e CTS com a máxima potência de transmissão, todos as estações localizadas na zona de portadora (zona de alcance) fixarão seu NAV com o tempo contido nos quadros de controle para evitar colisões. Todas as estações que estejam na zona de detecção de portadora fixarão seu NAV com o tempo EIFS. Entretanto, as estações localizadas na zona de detecção de portadora terão acesso ao meio antes que a transmissão do quadro de dados termine. Como o quadro de dados é enviado em uma potência de transmissão menor, as estações que estão dentro da zona de detecção de portadora não

saberão que uma transmissão ainda ocorre e enviarão os quadros de controle na máxima potência de transmissão para reservar o meio, acarretando uma colisão.

Outro problema inerente ao Esquema Básico é o baixo reuso espacial da rede. Este problema ocorre devido à reserva do meio ser feita usando-se a máxima potência de transmissão. Ao utilizar esta técnica, as estações vizinhas que eventualmente transmitiriam dados terão que esperar até o fim de uma determinada transmissão.

3.2. Atenuação

As técnicas de CPT propostas por [Correia et al. 2006], devem seguir restrições impostas pelo meio de transmissão e pelos limites nominais do rádio, sendo elas:

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)*);
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:

$$G = \frac{P_{RX}}{P_{TX}} \tag{2}$$

3. o quadro deve ser recebido em um nível de potência, acima de um limite mínimo, denominado $RX_{desejado}$, que garanta sua decodificação correta:

$$(P_{RX} \geq RX_{desejado}) \tag{3}$$

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

$$(P_{TX_{limite\ inf.}} \leq P_{TX_{min}} \leq P_{TX_{limite\ sup.}}) \tag{4}$$

Tanto a técnica Atenuação, quanto a técnica AEWMA, foram inicialmente implementadas para redes de sensores sem fios [Correia et al. 2006]. Nessas implementações, uma tabela guarda a potência de transmissão empregada para o envio de quadros para o vizinho, similar ao esquema proposto por [Pires et al. 2004]. Ao serem adaptadas para o protocolo IEEE 802.11, habilitou-se o envio de quadros RTS/CTS para realizar a reserva virtual do meio. Uma estação origem antes de transmitir um quadro ao meio verifica na sua tabela de vizinhos a potência de transmissão referente à estação de destino. Na ausência de um valor na tabela, a estação considera a máxima potência na transmissão.

A técnica de Atenuação funciona da seguinte maneira: na ausência de transmissões, as estações amostram o nível de ruído do meio (N_B) de tempos em tempos. 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 *(RSSI - Received Signal Strength Indication)* e calcula a potência mínima de transmissão ($P_{TX_{min}}$), através da equação:

$$P_{TX_{min}} = \max\left(\frac{RX_{desejado}}{G_{T\rightarrow R}}, \frac{SNR_{desejado} \times N_B}{G_{T\rightarrow R}}\right) \tag{5}$$

A equação 5 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 $P_{TX_{min}}$ dentro do quadro. Ao receber o ACK, o transmissor insere $P_{TX_{min}}$ na posição relativa à origem na tabela de vizinhos, sendo usado em subsequentes transmissões.

A técnica de Atenuação sofre da oscilação da potência calculada, o que aumenta a perda de quadros. Tal 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.

3.3. AEWMA

A técnica AEWMA *(Atenuação com filtro EWMA – Exponentially Weighted Moving Average)* estende a técnica de Atenuação e soluciona o problema da oscilação da potência de transmissão por usar uma função de amortização [Correia et al. 2006]. O EWMA é uma função média móvel ponderada exponencial na qual os valores mais antigos são decrementados exponencialmente. O valor de saída da função EWMA é dado por:

$$P_{TX_{AEWMA}} = P_{TX_{antigo}} \times \Big(1 \; - \; \alpha\Big) + \Big(P_{TX_{min}} \times \alpha\Big) \tag{6}$$

nas quais $P_{TX_{antigo}}$ é a potência armazenada na lista de potência usada para o envio de quadros para os vizinhos, $P_{TX_{min}}$ é a potência de transmissão mínima dada pela equação 5 e α é um fator responsável por decrementar a potência, onde $0 \leq \alpha \leq 1$.

Essa técnica possui o seguinte comportamento: uma estação transmissora, ao enviar um quadro para o receptor insere no cabeçalho do quadro a potência de transmissão empregada no envio. A estação receptora amostra o nível de sinal do quadro recebido (RSSI) e do ruído local, e calcula a potência mínima de transmissão através da equação 5. Posteriormente, a estação considera o resultado da equação 5 na função 6 e envia o resultado da função dentro do cabeçalho do quadro ACK, utilizando a mesma potência que o transmissor usou para enviar o quadro de dados, afim de evitar enlaces assimétricos.

4. Ataques de Redução da Qualidade de Serviço

Esta seção descreve padrões de ataques RoQ baseando-se nas características dos protocolos que seguem o comportamento de transmissão do IEEE 802.11. Tais ataques se aproveitam da reserva virtual do meio que é feita dinamicamente. Um atacante RoQ envia um quadro de controle RTS/CTS empregando um nível de potência menor *(X - 1)*, para efetuar a reserva virtual do meio, e envia um quadro de dados ou ACK considerando um nível maior *(X)*.

Os atacantes criam um caos na rede ao reservar virtualmente o meio de maneira arbitrária. Para não serem descobertos, eles escolhem aleatoriamente os níveis de potência para o envio dos quadros. No entanto, um atacante sempre escolhe um nível de potência maior para o envio dos quadros de dados e ACK com o intuito de criar enlaces assimétricos na rede. Um atacante, após transmitir um quadro de controle utilizando uma potência de transmissão menor, enviará o quadro de dados empregando uma potência de transmissão maior. Assim, todas as estações vizinhas que não receberam os quadros de controle, receberão o quadro de dados. Se por ventura uma transmissão estiver ocorrendo, acontecerá uma colisão de quadro no receptor por causa do quadro do atacante.

A seguir são explicados três tipos de ataques RoQ propostos por [Ren et al. 2008], denominados *round-robin*, *flooding* e *self-whisper*. Na abordagem proposta os atacantes criam enlaces assimétricos tendo como alvo um determinado tráfego na rede.

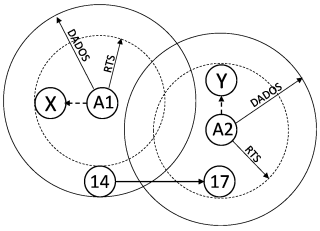

Figura 1. *Ataque round-robin*.

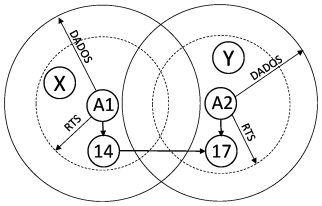

Figura 2. *Ataque flooding*.

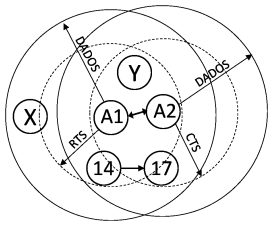

Figura 3. *Ataque self-whisper*.

Round-Robin - Nesse ataque, os atacantes vizinhos de um determinado tráfego escolhem vítimas aleatoriamente que não façam parte deste tráfego. Com o intuito de criar colisões na estação receptora do tráfego, o atacante realiza a reserva virtual do meio de maneira maliciosa. No exemplo ilustrado na Figura 1, os atacantes *A1* e *A2*, vizinhos das estações *14* e *17*, escolhem as vítimas *X* e *Y* para executar o ataque.

Ao escolher uma vítima, o atacante envia um quadro de controle RTS utilizando uma potência de transmissão menor para reservar o meio. Se por ventura as estações do tráfego escolhido não detectarem o quadro RTS, elas continuarão a transmissão normalmente. No entanto, após a vítima enviar um quadro CTS, o atacante enviará o quadro de dados usando uma potência de transmissão maior; criando assim enlaces assimétricos próximos a um determinado tráfego.

Flooding - Nesse ataque, múltiplos atacantes escolhem a origem ou o destino de um determinado tráfego aleatoriamente. Após esta escolha, o atacante inicia a reserva do meio de maneira arbitrária enviando um quadro RTS. Posteriormente, ele enviará quadros de dados para a vítima. No exemplo ilustrado na Figura 2, os atacantes *A1* e *A2*, vizinhos das estações *14* e *17*, executam o ataque enviando quadros de dados para as estações *14* e *17*, respectivamente.

O ataque *flooding* difere do ataque *round-robin* por criar enlaces assimétricos na rede e em alguns casos gerar o problema do terminal escondido em um determinado tráfego da rede. Além de causar colisões em vários receptores, os atacantes reduzem a vazão do tráfego.

Self-Whisper - Nesse ataque, múltiplas estações maliciosas, vizinhas de um tráfego, se comunicam com outras estações atacantes, afim de criar um tráfego malicioso na rede. Após fazer a reserva virtual do meio de maneira arbitrária utilizando uma potência de transmissão menor, as duas estações atacantes enviam quadros de dados e ACK usando uma potência de transmissão maior. No exemplo ilustrado na Figura 3, os atacantes *A1* e *A2*, vizinhos das estações *14* e *17*, fazem o ataque enviando quadros entre si.

Este ataque tem como consequência a criação de enlaces assimétricos focados em um determinado tráfego. Como os atacantes enviam quadros empregando potências de transmissão diferentes, as estações do tráfego não conseguem enviar quadros uma para a outra. Além da ocorrência de colisões na estação receptora, o transmissor consome mais energia devido ao aumento do número de retransmissões.

5. Avaliação e Resultados

O impacto dos ataques RoQ no protocolo 802.11 empregando as técnicas AEWMA, Atenuação e Esquema Básico, foi avaliado utilizando-se o simulador NS-2.31. Um módulo que melhora a camada MAC e física do simulador NS2, denominado dei80211mr [Baldo et al. 2007], foi adicionado para modelar a taxa de erro de pacote *(Packet Error Rate - PER)*. Este modelo verifica se um quadro foi recebido corretamente calculando o SNIR *(Signal Noise Interference Ratio)* definido através da força do sinal recebido, do ruído e da interferência gerada no meio. A interferência é calculada segundo um modelo gaussiano que verifica as transmissões recebidas simultaneamente nas estações receptoras e o ruído empregado no módulo é estático por padrão.

No módulo dei80211mr, adicionou-se um modelo de ruído que possibilita a aproximação do comportamento de um ambiente real, no qual o ruído é um parâmetro dinâmico. A geração do ruído é feita a cada 100 milisegundos usando-se o modelo estatístico GEV *(Generalized Extreme Value)* [Bali 2003]. Os parâmetros *location*, *scale* e *shape*, mostrados na Tabela 1, são utilizados pela GEV para o cálculo do ruído e foram obtidos através de análises feitas por [Su and Boppana 2007].

A Tabela 1 apresenta os principais parâmetros considerados na simulação. O cenário simulado para as duas análises, com e sem atacantes, consiste em uma rede estacionária com 36 estações em uma topologia em grade, como utilizado em [Ren et al. 2008], com as estações separadas em 10 metros. Para a análise utilizou-se um único tráfego exponencial na rede tendo como origem a estação *14* e como destino a estação *17*. Todas as estações possuem uma *interface* da série CISCO Aironet 1250 com um rádio que provê nove níveis diferentes de potência, sendo utilizado os valores padrões do NS2 para o modelo de energia.

Tabela 1. Parâmetros de simulação.

Número de estações	36
Tempo total	250 segundos
Área	500 metros x 500 metros
Tráfego analisado	$14 \rightarrow 17$ - 300 Kbps (Exp/UDP)
Taxa de dados do enlace	6 Mbps
MAC	dei80211mr
Rádio	Cisco Aironet 1250
Protocolo de roteamento	AODV
Parâmetro α da função EWMA	0.325
Tempo de mudança do ruído	100 ms
Modelo de ruído	*Generalized Extreme Value (GEV)*
Parâmetros da GEV: *location* *scale* *shape*	 -93.768 dBm 1.579 0.179

A análise do impacto dos ataques RoQ está dividida em duas partes. Primeiramente, verificou-se o comportamento dos protocolos sem nenhum atacante na rede. Posteriormente, analisou-se o impacto dos ataques *flooding*, *round-robin* e *self-whisper* com base no comportamento das técnicas. As análises foram feitas considerando-se 10%, 30%

e 50% de atacantes na rede escolhidos aleatoriamente. Todos os valores apresentados foram obtidos pela média de 35 simulações, gerando um intervalo de confiança de 95%.

5.1. Avaliação dos Protocolos sem Atacantes na Rede - Cenário 1

Este cenário, sem atacantes, avalia o protocolo 802.11 ao empregar as técnicas AEWMA, Atenuação e Esquema Básico, considerando as métricas taxa de entrega de quadros (Figura 4) e potência consumida pelas estações nas transmissões de quadros (Figura 5). A Figura 4 mostra que a técnica AEWMA e o protocolo 802.11 padrão obtiveram uma taxa de entrega superior a 90%, sendo que o 802.11 obteve a maior taxa. Os intervalos de confiança nestas figuras foram desconsiderados por apresentarem pouca relevância.

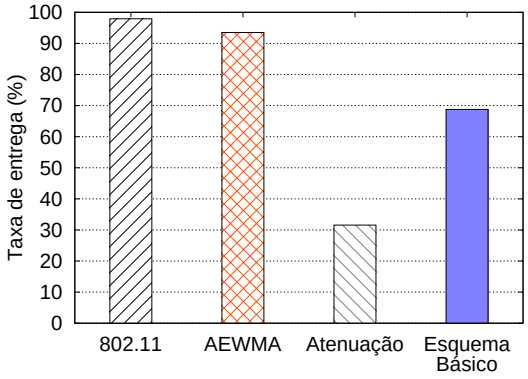

Figura 4. Taxa de entrega obtida pelo tráfego $14 \rightarrow 17$.

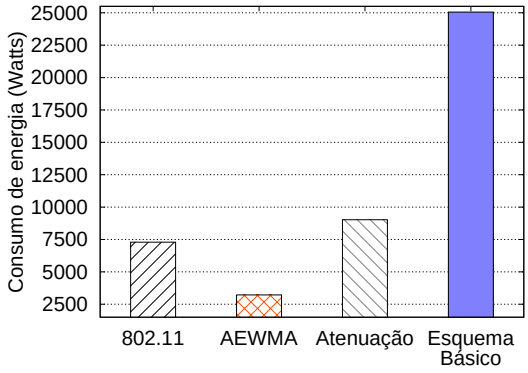

Figura 5. Potência de transmissão utilizada pelo tráfego $14 \rightarrow 17$.

A técnica AEWMA conseguiu uma alta taxa de entrega de quadros por usar a função EWMA juntamente com o parâmetro α para a escolha de um novo nível de potência. Ao utilizar α com o valor 0.325, a técnica se torna mais conservadora a ponto de modificar com menor intensidade os níveis de potência, além de aumentar seu consumo de energia. Todavia, a técnica gera uma maior taxa de entrega ao trabalhar de maneira eficiente com a atenuação do ruído no meio. Apesar do aumento do consumo de energia, a técnica AEWMA apresentou a maior economia em comparação às outras técnicas, consumindo aproximadamente 3.000 Watts. Quando comparada ao protocolo 802.11 padrão, o qual consumiu aproximadamente 7.280 Watts, a técnica demonstrou uma economia de 59%.

O protocolo 802.11 com a técnica de Esquema Básico conseguiu obter uma taxa de entrega de aproximadamente 70%. Entretanto, a potência de transmissão empregada pelas estações no Esquema Básico passou de 24.000 Watts. Este alto consumo de energia ocorre devido ao problema de enlaces assimétricos ser intríseco ao Esquema Básico. Na ocorrência de colisões desencadeadas pelos enlaces assimétricos, as estações que utilizam essa técnica consideram o emprego da máxima potência na retransmissão do quadro para que ele chegue corretamente ao destino.

A técnica Atenuação obteve o menor desempenho por ser uma técnica menos conservadora, ao modificar constantemente o nível de transmissão, e por não conseguir trabalhar de maneira ótima com a atenuação do ruído e a interferência gerada no meio.

5.2. Avaliação dos Protocolos sob o Ataque Flooding - Cenário 2

Este cenário avalia o ataque *flooding*, no qual os atacantes enviam quadros para uma vítima, sendo esta a estação *14* ou a estação *17*. Na Figura 6, verifica-se que o ataque teve pouco impacto na taxa de entrega dos protocolos 802.11 padrão e 802.11 utilizando a técnica AEWMA, sendo que nas técnicas Esquema Básico e Atenuação a taxa de entrega aumentou com 50% de atacantes na rede. A Figura 7 mostra o impacto do ataque no consumo de energia das estações *14* e *17*.

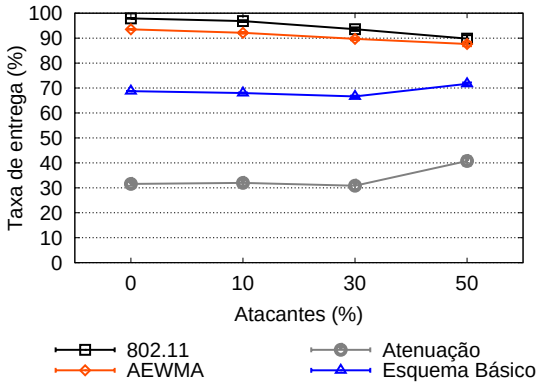

Figura 6. Taxa de entrega X ataque Flooding.

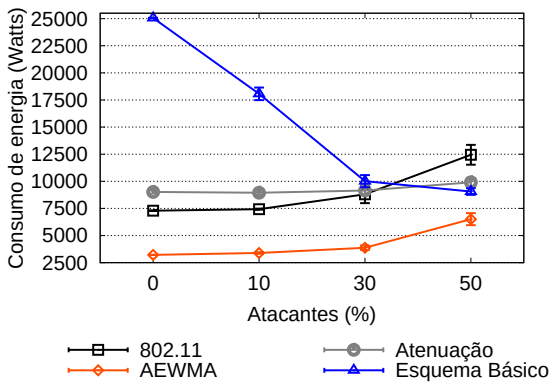

Figura 7. Potência de transmissão X ataque Flooding.

O protocolo 802.11 padrão sob a influência de 10% de atacantes na rede conseguiu o mesmo desempenho apresentado no Cenário 1, tanto na taxa de entrega de quadros quanto na energia consumida. Sob a influência de 30% de atacantes, esta técnica apresentou uma taxa de entrega 4% menor e um consumo de energia 20% maior que o apresentado no Cenário 1. Com 50% de atacantes na rede, o número de retransmissões do protocolo 802.11 padrão aumentou por causa dos enlaces assimétricos. Como consequência, sua taxa de entrega ficou em torno de 8% menor e o consumo de energia aumentou 71%, do que o apresentado no Cenário 1.

O protocolo 802.11 ao empregar a técnica AEWMA sob a influência de 10% de atacantes na rede, obteve praticamente o mesmo desempenho apresentado no Cenário 1. Sob a influência de 30% de atacantes, a técnica conseguiu uma taxa de entrega em torno de 4% menor e um consumo de energia 20% maior que o apresentado no Cenário 1. Sob a influência de 50% de atacantes, a técnica AEWMA apresentou uma taxa de entrega 6% menor e um consumo de energia 102% maior. Devido às colisões criadas pelos enlaces assimétricos, o número de retransmissões aumentou, acarretando em um maior consumo de energia e uma redução na taxa de entrega de quadros.

O protocolo 802.11 ao usar a técnica Atenuação, alcançou praticamente o mesmo desempenho apresentado no Cenário 1 sob a influência de 10% e 30% de atacantes na rede. Com 50% de atacantes, esta técnica teve um consumo de energia 9% maior ao obter uma taxa de entrega 9% maior. Em virtude do aumento da ocupação do meio, houve uma diminuição da flutuação da potência calculada. Como consequência, a técnica Atenuação conseguiu transmitir mais quadros.

Ao utilizar a técnica de Esquema básico, o protocolo 802.11 conseguiu maior economia de energia sob a influência dos atacantes. Com 50% de atacantes na rede, consumiu

63% a menos de energia do que o apresentado no Cenário 1. Devido ao número de atacantes na rede, o meio se tornou mais ocupado fazendo com que as estações variassem com menos intensidade a potência de transmissão. Logo, o consumo de energia das estações reduziu e a taxa de entrega aumentou.

5.3. Avaliação dos Protocolos sob o Ataque Round-Robin - Cenário 3

Este cenário avalia o ataque *round-robin* no qual os atacantes escolhem uma vítima aleatoriamente e criam enlaces assimétricos próximos ao tráfego que tem como origem a estação *14* e como destino a estação *17*. As Figuras 8 e 9 mostram que esse ataque teve pouco impacto nas técnicas de CPT, sendo que na técnica de Esquema Básico o consumo de energia reduziu.

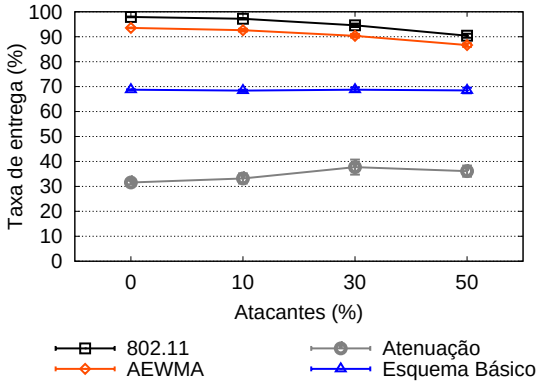

Figura 8. Taxa de entrega X ataque Round-Robin.

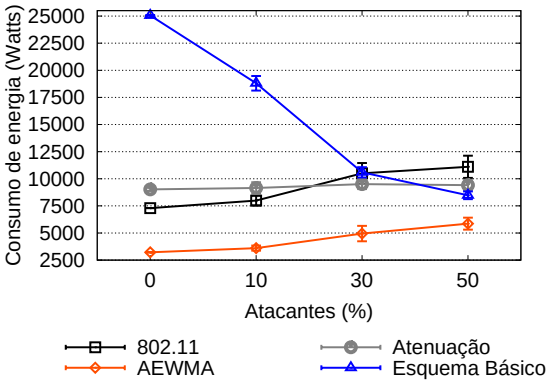

Figura 9. Potência de transmissão X ataque Round-Robin.

O protocolo 802.11 padrão, em comparação ao desempenho apresentado no Cenário 1, obteve a mesma taxa de entrega com 10% de atacantes, uma taxa 3% menor com 30% de atacantes e uma taxa de entrega 7% menor com 50% de atacantes na rede. O consumo de energia alcançado nas transmissões foi 43% maior sob a influência de 30% de atacantes e 53% maior sob a influência de 50% de atacantes na rede. Apesar do ataque *round-robin* ter afetado em pequena escala a taxa de entrega, o consumo de energia das estações aumentou em mais de 50%. Como consequência dos enlaces assimétricos, inúmeras colisões ocorreram na rede acarretando em um aumento no número de retransmissões e no consumo de energia.

Ao empregar a técnica AEWMA, o protocolo 802.11 sofreu um impacto relevante do ataque sob a influência de 30% e 50% de atacantes na rede, consumindo 53% e 82% a mais de energia, respectivamente, do que o apresentado no Cenário 1. Assim como no protocolo 802.11 padrão, os enlaces assimétricos criados na rede tiveram pouco impacto na taxa de entrega dos quadros. No entanto, como a potência de transmissão varia com menor intensidade nesta técnica, o número de retransmissões fez com que o consumo de energia aumentasse.

O protocolo 802.11 utilizando a técnica Atenuação obteve um pequeno aumento na taxa de entrega e a mesma economia de energia em todas as abordagens. Em consequência da ocupação do meio devido aos tráfegos criados pelos atacantes, a potência de transmissão teve uma menor flutuação. Logo, o número de quadros perdidos reduziu, acarretando uma maior taxa de entrega.

Ao usar a técnica de Esquema Básico, o protocolo 802.11 obteve a mesma taxa de entrega e um menor consumo de energia em todos os casos, em comparação ao apresentado no Cenário 1. Com 10% de atacantes a técnica gastou 21% a menos de energia, com 30% economizou 39% de energia e com 50% de atacantes teve um consumo de energia 63% menor. Devido a menor flutuação da potência de transmissão, a taxa de entrega das estações que utilizam esta técnica não sofreu impacto com o ataque *round-robin*.

5.4. Avaliação dos Protocolos sob o Ataque Self-Whisper - Cenário 4

Este cenário avalia o ataque *self-whisper* no qual dois atacantes estabelecem um tráfego malicioso afim de criar colisões nas estações *14* e *17*. As Figuras 10 e 11 mostram que esse ataque teve impacto no protocolo 802.11 padrão e ao empregar a técnica AEWMA.

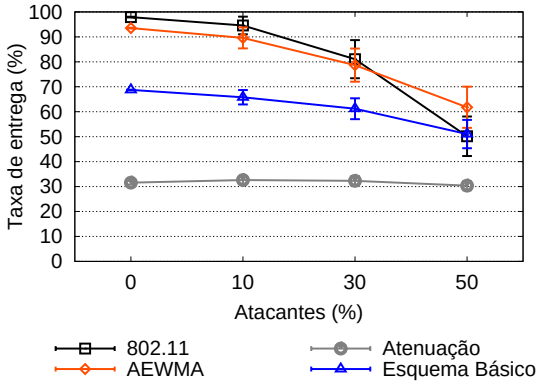

Figura 10. Taxa de entrega X ataque Self-Whisper.

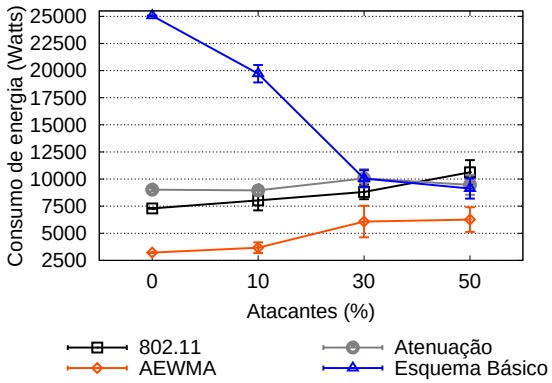

Figura 11. Potência de transmissão X ataque Self-Whisper.

O protocolo 802.11 padrão obteve uma taxa de entrega 15% menor com 30% de atacantes e 50% menor com 50% de atacantes na rede, em comparação ao Cenário 1, sendo que o consumo de energia aumentou gradativamente conforme o aumento do número de atacantes. Como os enlaces assimétricos do ataque são focados no tráfego, as estações *14* e *17* além de sofrerem um maior número de colisões, não conseguem transmitir com tanta eficiência como apresentado no Cenário 1.

Ao empregar a técnica AEWMA, o protocolo 802.11 teve uma diminuição da taxa de entrega maior que 10% com 30% de atacantes e de aproximadamente 31% com 50% de atacantes na rede, em comparação ao Cenário 1. O consumo de energia com 30% de atacantes aumentou em 89% e com 50% de atacantes aumentou aproximadamente 95%. Através dos enlaces assimétricos, os ataques aumentaram o número de colisões das estações consideravelmente, reduzindo a taxa de entrega (Figura 10). Por sua vez, as estações empregaram mais energia devido a um maior número de retransmissões.

O ataque *self-whisper* não conseguiu diminuir o rendimento do protocolo 802.11 ao empregar a técnica Atenuação, comparando-se ao Cenário 1. Como o meio se tornou mais ocupado, a potência de transmissão oscilou com menos intensidade. Logo, esta técnica conseguiu enviar mais quadros ao meio, aumentando o consumo de energia. Todavia, a técnica Atenuação não conseguiu apresentar uma taxa de entrega significativa quando comparado à técnica AEWMA.

O protocolo 802.11 usando a técnica de Esquema Básico obteve uma taxa de entrega 10% menor com 30% de atacantes, e 20% menor com 50% de atacantes na rede. Apesar da diminuição do consumo de energia ocasionado pela redução da flutuação da potência de transmissão, os enlaces assimétricos causaram colisões nas estações *14* e *17*, afetando a taxa de entrega.

6. Conclusão

Este trabalhou analisou o impacto dos ataques RoQ que criam enlaces assimétricos no protocolo IEEE 802.11 padrão e no IEEE 802.11 empregando técnicas de CPT. As técnicas de CPT adaptadas e avaliadas foram AEWMA, Atenuação e Esquema Básico diante dos ataques *flooding*, *round-robin* e *self-whisper*.

Resultados de simulação mostraram que a técnica AEWMA obteve a maior economia de energia em todos os ataques. O protocolo 802.11 padrão obteve a menor economia de energia em todos os ataques com 50% de atacantes. Nos ataques *flooding* e *round-robin* com 50%, a técnica AEWMA obteve praticamente a mesma taxa de entrega que o 802.11 padrão, no entanto, este último consumiu duas vezes mais energia que a técnica AEWMA. No ataque *self-whisper* com 30% de atacantes, o protocolo 802.11 padrão obteve a mesma taxa de entrega que AEWMA. Desta maneira, é necessário o desenvolvimento de uma técnica que apresente características similares ao desempenho alcançado pela técnica AEWMA, porém que seja eficiente diante de ataques com comportamento semelhante ao *self-whisper*.

Como trabalhos futuros, avaliaremos o impacto dos ataques RoQ levando em conta a mobilidade das estações. Desenvolveremos um método de defesa baseado no salto de frequência [Khattab et al. 2008] contra estes ataques. Além de verificar ataques nos quais a estação destino envia maliciosamente a potência mínima de transmissão a ser utilizada pelo emissor.

Referências

Awerbuch, B., Richa, A., and Scheideler, C. (2008). A jamming-resistant mac protocol for single-hop wireless networks. In *Proceedings of the 27th ACM symposium on Principles of distributed computing (PODC '08)*, pages 45–54, New York, NY, USA. ACM.

Baldo, N., Maguolo, F., Miozzo, M., Rossi, M., and Zorzi, M. (2007). ns2-miracle: a modular framework for multi-technology and cross-layer support in network simulator 2. In *Proceedings of the 2nd international conference on Performance evaluation methodologies and tools (ValueTools '07)*, pages 1–8, ICST, Brussels, Belgium, Belgium.

Bali, T. G. (2003). The generalized extreme value distribution. *Economics Letters*, 79(3):423–427.

Chen, H.-H., Fan, Z., and Li, J. (2006). Autonomous power control mac protocol for mobile ad hoc networks. *EURASIP Journal on Wireless Communication and Networking*, 2006(2).

Chen, Y. and Hwang, K. (2007). Spectral analysis of tcp flows for defense against reduction-of-quality attacks. In *Proceedings of the 2007 IEEE International Conference on Communications (ICC '07)*, pages 1203–1210.

Correia, L. H. A., Macedo, D. F., dos Santos, A. L., Loureiro, A. A., and Nogueira, J. M. (2006). Ajustando a potência de transmissão em protocolos mac. In *24ºSimpósio Brasileiro de Redes de Computadores*, pages 589–604.

Gast, M. (2005). *802.11 Wireless Networks: The Definitive Guide, Second Edition (Definitive Guide)*. O'Reilly Media, Inc.

Guirguis, M., Bestavros, A., and Matta, I. (2004). Exploiting the transients of adaptation for roq attacks on internet resources. In *Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP'04)*, pages 184–195, Washington, DC, USA. IEEE Computer Society.

Guirguis, M., Bestavros, A., and Matta, I. (2006). On the impact of low-rate attacks. Technical report, CS Department, Boston University.

Guirguis, M., Bestavros, A., Matta, I., and Zhang, Y. (2005). Reduction of quality (roq) attacks on internet end-systems. In *Proceedings of the 24 th IEEE International Conference on Computer Communication (Infocom'05)*, pages 1362–1372.

Guirguis, M., Bestavros, A., Matta, I., and Zhang, Y. (2007). Reduction of quality (roq) attacks on dynamic load balancers: Vulnerability assessment and design tradeoffs. In *Proceedings of the 26th IEEE International Conference on Computer Communication (Infocom'07)*.

Hansmann, U., Nicklous, M. S., and Stober, T. (2001). *Pervasive computing handbook*. Springer-Verlag New York, Inc., New York, NY, USA.

Jung, E.-S. 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 (MobiCom '02)*, pages 36–47, New York, NY, USA. ACM.

Karn, P. (1990). Maca — a new channel access method for packet radio. In *Proceedings of the ARRL/CRRL Amateur Radio 9th Computer Networking Conference*, pages 134–140.

Khattab, S., Mosse, D., and Melhem, R. (2008). Jamming mitigation in multi-radio wireless networks: reactive or proactive? In *Proceedings of the 4th international conference on Security and privacy in communication netowrks (SecureComm '08)*, pages 1–10, New York, NY, USA. ACM.

Monks, J. P. (2001). Transmission power control for enhancing the performance of wireless packet data networks. Technical report.

Pires, A. A., Fontes, M. F., and de Rezende, J. F. (2004). Proposta e avaliação de um esquema de controle de potência com memória em redes ad hoc 802.11. In *22ºSimpósio Brasileiro de Redes de Computadores*.

Ren, W., yan Yeung, D., Jin, H., and Yang, M. (2008). Pulsing roq ddos attack and defense scheme in mobile ad hoc networks.

Su, X. and Boppana, R. V. (2007). On the impact of noise on mobile ad hoc networks. In *Proceedings of the 2007 international conference on Wireless communications and mobile computing (IWCMC '07)*, pages 208–213, New York, NY, USA. ACM.

Weiser, M. (1999). The computer for the 21st century. *ACM SIGMOBILE Mobile Computing and Communications Review*, 3(3):3–11.