Um modelo para mitigação de ataques de negação de serviço em redes 802.11

Adriano Cesar Ribeiro[1,2], Alex Roschildt Pinto[1], Kalinka Castelo Branco[3], Adriano Mauro Cansian[1,2]

[1]Universidade Estadual Paulista – Júlio de Mesquita Filho (UNESP)
São José do Rio Preto – SP – Brasil

[2]Laboratório ACME! de Pesquisa em Segurança

[3]Universidade de São Paulo – Instituto de Ciências Matemáticas e de Computação (ICMC) – São Carlos – SP – Brasil

adrianoribeiro@acmesecurity.org, arpinto@ibilce.unesp.br, kalinka@icmc.usp.br, adriano@acmesecurity.org

Abstract. *Wireless networks are widely deployed and have many uses, for example in critical embedded systems. The applications of this kind of network meets the common needs of most embedded systems and addressing the particularities of each scenario, such as limitations of computing resources and energy supply. Problems such as denial of service attacks are common place and cause great inconvenience. Thus, this paper presents simulations of denial of service attacks on 802.11 wireless networks using the network simulator OMNeT++. Furthermore, we present an approach to mitigate such attack, obtaining significant results for improving wireless networks.*

Resumo. *As redes sem fio são largamente utilizadas e possuem diversas utilidades, por exemplo, em sistemas embarcados críticos. A aplicação deste tipo de rede atende as necessidades comuns da maioria dos sistemas embarcados e visa atender as particularidades de cada cenário, tais como as limitações dos recursos de computação e de fornecimento de energia, comuns nesse tipo de sistema. Problemas como ataques de negação de serviço são corriqueiros e causam grande transtorno. Sendo assim, este artigo apresenta simulações de ataques de negação de serviço em redes sem fio 802.11 utilizando o simulador de redes OMNeT++. Além disso, é apresentada uma abordagem para mitigação de um ataque desse tipo, obtendo resultados expressivos para a melhoria das redes sem fio.*

1. Introdução

Um sistema embarcado é um sistema que possui seu processamento dedicado e customizado entre *software* e *hardware,* geralmente voltado para um objetivo específico, melhorando assim, o custo, espaço, desempenho e consumo de energia [Yu et al 2010]. Diferentemente de computadores de propósito geral, um sistema embarcado realiza um conjunto de tarefas predefinidas, geralmente com requisitos específicos. Já que o sistema é dedicado a tarefas específicas, por meio de engenharia pode-se otimizar o projeto reduzindo tamanho, recursos computacionais e custo do produto. O espaço dos

embarcados está crescendo constantemente com o tempo [Yaghmour et al. 2008], de modo que eles têm desempenhado as mais diferentes tarefas que vão desde fotografar uma região até tarefas mais complexas como processor de uma missão de reconhecimento.

A comunicação entre sistemas embarcados mostra a importância inegável que têm as redes de computadores nos dias atuais, e devido a sua ampla disseminação e utilização em diferentes lugares, a comunicação sem fio tem se destacado. Dentre os padrões existentes de protocolos de comunicação sem fio, se destaca o padrão IEEE 802.11 (Wi-Fi) [IEEE 802.11 2007]. É o padrão mais utilizado atualmente e possui grande crescimento nas aplicações e infraestruturas do cotidiano [FENG 2012].

As ações maliciosas as quais esses sistemas estão suscetíveis vão desde roubo de informações até interferência na comunicação e no uso ilegítimo desses sistemas. Para que exista um nível de segurança razoável, é necessário que existam maneiras de se detectar e sanar problemas relacionados a ataques direcionados aos sistemas em questão. Dentre os diversos ataques a que estão sujeitos, um dos ataques mais utilizados e que merece destaque é o ataque de negação de serviço – *Denial of Service* (DoS), que consiste na tentativa de tornar o serviço fornecido pela rede indisponível [SANDSTRÖM 2001].

Esse trabalho tem como objetivo apresentar o estudo e análise de um ataque sendo proferido a uma rede sem fio e os meios de mitigar esse tipo de ataque de forma efetiva. Para isso utilizou-se como base para a confecção da rede o simulador OMNeT++ [OMNET++ 2012], que provê toda a estrutura necessária para o projeto e estruturação da rede, bem como provê meios de se averiguar a efetividade do ataque e das contramedidas utilizadas.

O restante deste artigo está organizado como segue: na seção 2 são apresentados os trabalhos relacionados. A seção 3 aborda o problema, assim como o ataque estudado e a mitigação proposta, além dos parâmetros utilizados nas simulações. Na seção 4 são apresentados os estudos de caso e resultados obtidos. Por fim, na seção 5 é apresentada uma conclusão e os trabalhos futuros.

2. Trabalhos Relacionados

Os problemas relacionados à segurança de redes sem fio, principalmente em relação a ataques de negação de serviço, são de grande interesse da comunidade acadêmica. Em [MALEKZADEH et al. 2011] é mostrado por meio de simulações feitas no simulador OMNeT++ a consequência de um ataque de negação de serviço em uma rede sem fio. Além disso, é feita uma comparação entre a simulação e um ataque real com a intenção de validar o simulador mostrando que os dados obtidos são aceitáveis. Nos cenários de simulação, os autores realizaram testes verificando o *throughput* e o *delay* da rede com tráfego gerado a partir de segmentos TCP (*Transmission Control Protocol*) e UDP (*User Datagram Protocol*). Os resultados obtidos apresentam uma queda brusca para 0 Bps no *throughput* e um aumento considerável no *delay*, de 0 segundos para aproximadamente 6 segundos, dentro do período em que o ataque é realizado. A quantidade de pacotes perdidos nas simulações foi de 37,90% quando o

ataque foi realizado. A partir da viabilidade de comparação do modelo simulado com o real pode-se comprovar que os resultados obtidos na mitigação do ataque, caso explorado nesse artigo, também pode ser considerado viável e condizente com o que acontece em um ataque real.

Em [SINGH; SHARMA 2011] é proposta uma técnica para detecção e redução de ataques de negação de serviço, que é dividida em três fases: inicialização, requisição e autenticação. Na fase de inicialização, o servidor de autenticação escolhe uma chave privada para a estação e calcula sua respectiva chave pública. Essa etapa é realizada antes de qualquer outra e é necessária apenas uma vez. Na fase de requisição, acontece a requisição da estação ao Access Point (AP) para obter acesso à rede desejada. O AP envia então à estação um conjunto de números aleatórios juntamente com a chave pública que será usada na sua troca de informações. Já na fase de autenticação, a estação envia uma mensagem contendo um *hash* do número aleatório recebido do AP utilizando sua chave pública, entre outras informações, como a senha. Os números aleatórios previnem ataques de negação de serviço dos tipos *flood*, *deauthentication* e *disassociation*.

Para prevenir ataques de negação de serviço do tipo *deauthentication* e *disassociation*, é proposto em [NGUYEN; NGUYEN e TRAN 2008] um protocolo baseado em fatoração de números primos muito grande. Inicialmente a estação gera dois números primos (p1 e n1) que são multiplicados. O mesmo faz o AP (p2 e n2), porém com seus próprios números primos. Na fase de autenticação, ocorre a troca desses números entre a estação e o AP. Caso algumas das partes envolvidas enviem pacotes *deauthentication*, ela também envia juntamente seu número p1 ou p2 para a verificação de autenticidade do pacote *deauthetication*. Os testes realizados possuíam diferentes tamanhos de números primos (p e q), sendo de 64, 128, 256 e 512 bits. Em todos os casos, a defesa contra esse tipo de ataque foi satisfatória, ou seja, mesmo com o *spoofing* de pacotes *deauthentication*, o AP foi capaz de ignorar o pedido falso.

Para o caso de ataque de negação de serviço que utiliza *frame control*, é proposto em [NEGI e RAJESWARAN 2005] um método que revoga a reserva do canal feita por um atacante. Enviando um pacote com um *Request to Send* (RTS) muito alto, o AP admite essa reserva e envia em *broadcast* um pacote *Clear to Send* (CTS) avisando da reserva do canal por aquele tempo requisitado. Entretanto, se o AP não receber em seguida qualquer pacote, ele então revoga aquela reserva, caracterizando um ataque de negação de serviço. Como resultados, foi obtido um aumento no *throughput* durante o ataque, que era de 0,3 para 0,6 pacotes por intervalo de tempo.

O trabalho apresentado em [LEE; CHIEN e TSAI 2009] é baseado em *bits* não utilizados nos *frames* do protocolo 802.11i. Assim, são inseridos *bits* aleatórios nos *frames* de *authentication/deauthentication* e *association/disassociation*, que são gerados pela comunicação entre os *hosts* por algum algoritmo qualquer. Todos os *frames* do processo são enviados com esse valor e caso algum não confira com o verdadeiro, aquele *frame* é rejeitado. Os testes realizados envolveram máquinas reais que realizavam a troca de dados via FTP (*File Transfer Protocol*). O ataque obtém sucesso para algumas configurações dos *bits* utilizados na verificação, porém, em outras, não, mitigando os ataques analisados.

Em [SORYAL e SAADAWI 2012], é proposto um método de detecção que se baseia no número de pacotes enviados com sucesso por uma estação, com o número de CTS que essa mesma estação recebeu. Cada estação sonda o canal, e faz uso de um método chamado de cadeia de Markov, que, é utilizado para medir o *throughput* da rede. Sendo assim, é verificado o *throughput* obtido no cálculo de Markov e a quantidade de *frames* CTS recebidos. Se essa quantidade de *frames* CTS for maior do que o *throughput*, então aquele nó é identificado como um atacante pelo seu endereço MAC.

A proposta de defesa contra ataques do tipo *frame control* proposto por [MYNEMI e HUANG 2010], é utilizar um método de geração e distribuição de chaves, apresentado no 802.11f. Em seguida, é gerada uma mensagem de código de autenticação usando a chave gerada. Inicialmente o AP busca por outros APs no canal, se não encontrar nenhum, é gerado um número K, que será enviado via conexão TCP a outras estações. Além desse número K, é gerado um número de sequência S, que toma por base a duração da reserva do canal contido nos *frames* RTS/CTS. Os resultados foram obtidos por meio de simulações que permitiram observar que os ataques não tiveram êxito. O valor de *throughput* antes do ataque foi de 28.4 Mbps utilizando UDP, e após o ataque com a mitigação, o *throughput* foi de 27.6 Mbps.

A Tabela 1 mostra de maneira resumida a abordagem e os resultados dos trabalhos relacionados desta seção.

Tabela 1. Abordagem dos trabalhos relacionados.

Artigo	Abordagem	Resultados
MALEKZADEH et al.	Avaliar ataque de negação de serviço RTS/CTS tanto em simulações quanto em cenário real.	Queda brusca no *throughput*, aumento no *delay* dos pacotes de 0 para 6 segundos e taxa perda de pacotes de 37,9%
SINGH; SHARMA	Dividir em fases, que consistem na geração, troca e autenticação por meio de chaves pública.	Detecta ataques DoS na autenticação e reduz o *flood* de DoS durante a autenticação e a fase de *probe request*.
NGUYEN; NGUYEN; TRAN	Realizar fatoração de números primos muito grande.	Mesmo para números primos com variação de *bits*, o modelo obteve sucesso, ignorando ataques *deauthentication*.
NEGI; RAJESWARAN	Revoga o pedido de reserva do canal, caso não seja enviado nenhum pacote útil dentro de um intervalo de tempo.	Obteve resultados em que o *throughput* da rede em um dos cenários de testes subisse de 0,3 para 0,6 pacotes por intervalo de tempo.
LEE; CHIEN; TSAI	Faz uso de *bits* não utilizados no cabeçalho para gerar números aleatórios.	Para um uso de 5 *bits* ou mais para os números aleatórios, a mitigação ocorre conforme esperada.

SORYAL; SAADAWI	Utiliza cadeia de Markov para obter um *throughput* mais preciso. Com isso, é feita uma verificação da quantidade e *frames* CTS recebido pelo *host*. Se essa proporção CTS for maior do que o resultado da cadeia de Markov, o ataque DoS é detectado.	Os testes obtidos mostram que o modelo obteve sucesso detectando o atacante pelo seu endereço MAC.
MYNEMI; HUANG	É utilizada uma abordagem de geração e distribuição de chaves. Para complementar, é gerado um número de sequência baseado no tempo requisitado no *frame* RTS.	Testes observando o *throughput* da rede mostraram que com um tráfego UDP o valor foi de 28,4 Mbps e com o modelo de mitigação, o valor do *throughput* foi de 27,6 Mbps.

Devido ao fato de ataques de negação de serviço ser muito popular e ter uma eficácia satisfatória, existem muitas maneiras de se realizar um ataque desse tipo. Dessa forma, são necessárias diversas formas de prevenção de atividades maliciosas, conforme apresentado nos trabalhos discutidos anteriormente. A proposta deste trabalho é mitigar um tipo de ataque de negação de serviço que possui a característica de inundar um *host* com requisições de transmissão de informações.

3. Descrição da Abordagem

3.1 Descrição do problema

Em se tratando de redes sem fio, é provável que existam situações em que as estações tenham problemas em sondar o canal para o início de sua transmissão. Um problema apontado se refere ao problema do terminal oculto, que, devido ao desvanecimento, os *hosts* não conseguem detectar a transmissão dos demais, causando colisões [KUROSE e ROSS 2007].

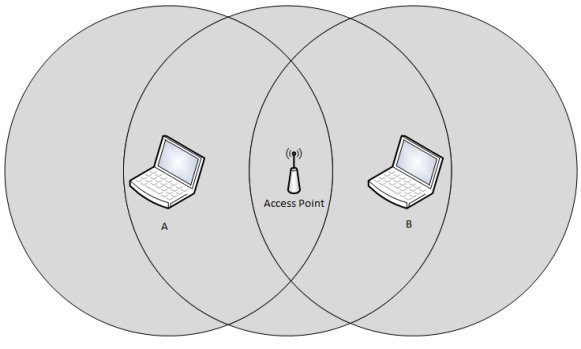

Figura 1. O problema do terminal oculto.

Para problemas como esse, existe um esquema no protocolo IEEE 802.11 que inclui uma reserva do canal a ser utilizado um quadro de controle, chamado *Request to Send* (RTS). Quando uma estação deseja enviar uma informação, ela escutará o canal para verificar se o mesmo está ocioso. Devido ao problema do terminal oculto, pode ser que alguma outra estação tenha iniciado uma transmissão e não tenha sido possível

identificar esse uso do canal. Dessa forma, ao identificar que o canal está ocioso, a estação espera um tempo DIFS (*Distributed Inter Frame Spacing*) antes de enviar um *frame* RTS. Esse *frame* RTS contém a duração estimada em microssegundos do tempo que a estação precisará do canal para transmitir sua informação. Assim que o AP receber esse *frame*, ele enviará outro *frame* chamado CTS em *broadcast* a todas as estações vizinhas, avisando que o canal estará ocupado pelo tempo requisitado.

3.2 Descrição do ataque e mitigação

O modelo de ataque realizado no presente trabalho faz uso da "inundação" ou *flood*, de envio de informações fazendo uso do *frame* RTS. Essa técnica envia uma quantidade grande de *frames* RTS em curto espaço de tempo a um servidor, por exemplo, e causa o congestionamento do mesmo. Neste caso, acontece o congestionamento de reservas do canal sem fio usando o *frame* RTS. Dessa forma, o ataque terá domínio completo do canal, negando serviço aos demais *hosts* na rede sem fio.

O algoritmo modelado para o ataque utilizado neste trabalho consiste em iniciar em um tempo estipulado nas configurações do simulador. Em seguida, o atacante observa se o canal está ocioso e se estiver, começa um *loop* de envio de pacotes ICMP (*Internet Control Message Protocol*) ao seu destino, de acordo com o intervalo de tempo entre esses pacotes, até que atinja o limite estipulado para o término do ataque. O algoritmo ilustrado na Figura 2 detalha como o ataque de negação de serviço foi proferido nas simulações deste trabalho.

```
se canal está ocioso, faça
        espera um intervalo SIFS (Short Interframe Space)
        envia um frame RTS com duração alterada
        obtém um frame CTS do AP liberando o canal
        envia um pacote ICMP ao destinatário
se fim do ataque for verdadeiro, pare.
```

Figura 2. Modelo de ataque de negação de serviço utilizado.

De acordo com o tipo de ataque realizado, foi desenvolvido um modelo como mitigação. Esse modelo consiste em receber um frame RTS com a duração alterada para um valor muito alto e enviar o frame CTS reservando o canal ao atacante. Em seguida, ao receber o pacote de fato com a informação, no caso o ICMP, é feita uma verificação do tempo requisitado fazendo uso do tamanho do pacote enviado. Se o tempo de transmissão obtido for muito menor do que o requisitado, a conexão é cancelada. O algoritmo ilustrado na Figura 3 detalha como é feita a mitigação.

```
recebe frame RTS
envia CTS com tempo_reservado
calcular tempo_correto
se tempo_reservado >> tempo_calculado
        cancela conexão
```

Figura 3. Modelo de mitigação proposto.

3.3 Topologia e parâmetros

O protocolo utilizado nas simulações é o 802.11b e em uma rede sem fio do tipo infraestrutura. A topologia proposta é ilustrada na Figura 4.

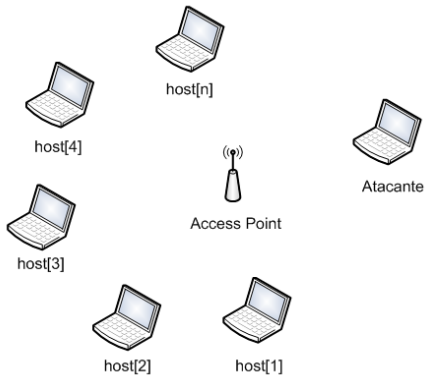

Figura 4. Topologia utilizada nos estudos de casos.

A topologia ilustrada na Figura 4 é genérica e pode ser estendida para o número desejado de *hosts*, APs e inclusive de atacantes. Entretanto, o modelo proposto neste trabalho é de apenas um atacante, caracterizando assim, um ataque de DoS.

Para a realização das simulações faz-se necessário que alguns parâmetros sejam configurados. Esses parâmetros foram obtidos através da experiência com testes e simulações prévios. Na Tabela 2 são apresentados os parâmetros utilizados nas simulações.

Tabela 2. Parâmetros utilizados para as simulações.

Padrão utilizado	802.11b
Tempo de simulação	10 segundos
Tamanho dos pacotes ICMP	56 bytes
Intervalo de envio dos pacotes ICMP	100 milissegundos para os cenários com 2, 4 e 8 *hosts*
Intervalo de envio dos pacotes ICMP	1 segundo para os cenários com 16, 32, 64 e 128 hosts
Início do ataque	2 segundos
Término do ataque	2,3 segundos
Intervalo de envio dos pacotes ICMP do atacante	5 milissegundos

4. Resultados

A coleta dos resultados se baseia na utilização de funções que os módulos do simulador implementa, tendo como meta obter a hora do envio dos pacotes por cada um dos hosts e o tempo que levou para os pacotes chegarem até seu destino. Além disso, é apresentada uma porcentagem de *drop* dos pacotes que, conforme será possível observar, aumenta com o ataque DoS e, por fim, volta ao normal quando utiliza-se o modelo de mitigação proposto.

As simulações realizadas foram baseadas em cenários, os quais consistem nos seguintes dados para avaliação dos testes: tráfego normal, ou seja, compostos com *hosts* lícitos, comportamento da rede sob ataque de negação de serviço e comportamento da rede utilizando o modelo de mitigação. Cada um desses conjuntos de testes representa um cenário específico, e, além disso, existem variações desses cenários com 2, 4, 8, 16, 32, 64 e 128 *hosts* lícitos, respectivamente.

A métrica utilizada como base para analisar o comportamento da rede foi o *throughput*. Essa métrica é muito utilizada quando se deseja obter uma avaliação da utilização da rede. O valor dessa medida pode ser obtido por meio da equação ilustrada na Figura 5.

$$throughput = size/time\_to\_arrive$$

Figura 5. Cálculo do *throughput*.

No caso da Figura 5, *size* significa o tamanho do pacote, nesse caso em bytes, que foi enviado e *time_to_arrive* é o tempo em segundos que esse pacote demorou a chegar até seu destino.

Os gráficos obtidos das simulações de tráfego normal e tráfego sob ataque DoS são apresentados nas Figuras de 6 até 12.

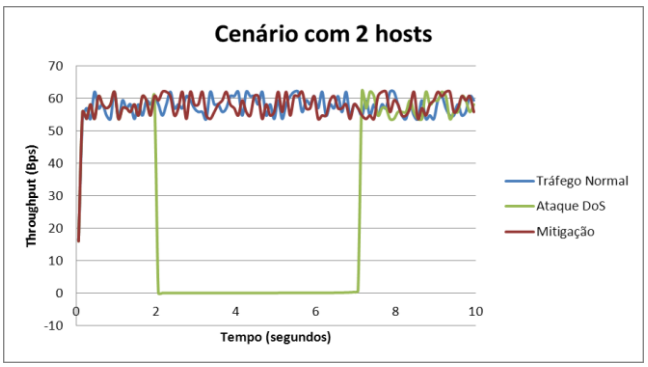

Figura 6. Simulações com 2 *hosts* lícitos.

A variação do *throughput* apresentado na Figura 6 é pequena, isso se deve ao número reduzido de *hosts* simulados na rede sem fio. A variação média dessa simulação sem a atuação de um atacante foi de 57,28 Bps. Entretanto, observa-se que a variação do *throughput* sob ataque DoS varia a partir do início do ataque, onde o *throughput* chega a praticamente zero Bps por aproximadamente 5 segundos. Nessa simulação o

throughput médio fica em 27,78 Bps. Utilizando o modelo de mitigação elaborado, observa-se que o *throughput* se mantém parecido com o que era na simulação normal, mantendo uma média de 57,45 Bps.

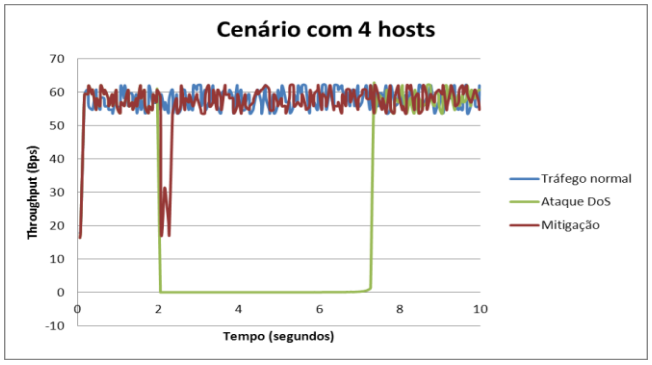

Figura 7. Simulações com 4 *hosts* lícitos.

A variação do *throughput* ilustrada na Figura 7 para o tráfego normal é similar em relação à simulação com 2 *hosts* da Figura 6, mantendo uma média de *throughput* de 57,53 Bps. Ao início do ataque, o meio fica ocupado por aproximadamente 5 segundos até que a rede consiga se reestabelecer novamente. A média do *throughput* foi de 26,84 Bps. Na simulação utilizando a mitigação, ocorre uma queda significativa, porém, ela não chega a zero e não se mantém por muito tempo. A média do *throughput* é de 56,64 Bps, sendo bem próxima do que seria em uma simulação de tráfego normal.

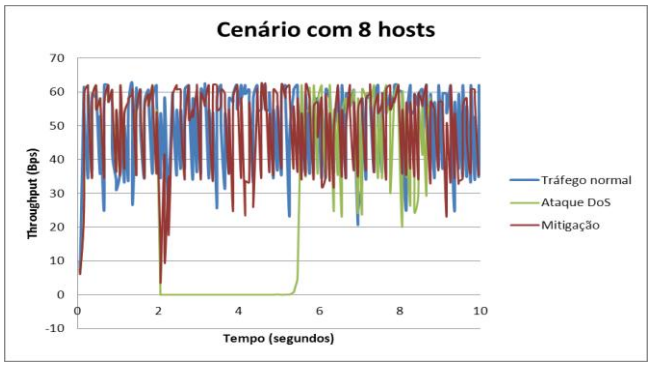

Figura 8. Simulações com 8 *hosts* lícitos.

Na Figura 8 é apresenta uma variação maior em relação ao *throughput* devido ao aumento de número de *hosts* participantes na rede sem fio. Com isso, ocorre um congestionamento na rede, contudo, o *throughput* médio é de 50,03 Bps. Com o início do ataque de negação de serviço o *throughput* cai a praticamente zero por aproximadamente 4 segundos, obtendo um *throughput* médio de 29,67 Bps. Ao realizar o teste com a mitigação, ocorre uma breve queda no *throughput*, mas sem chegar a zero. A média do *throughput* para a simulação de ataque com mitigação é de 49,38 Bps.

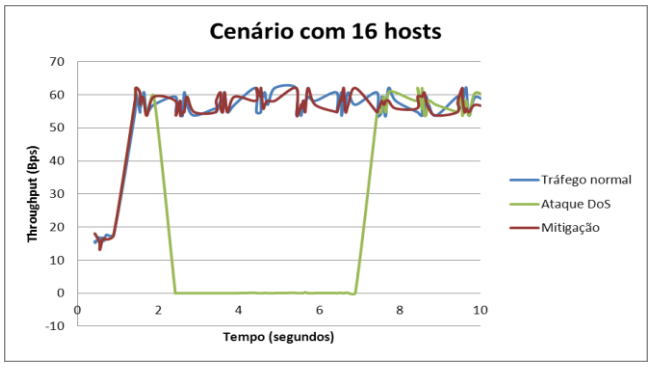

Figura 9. Simulações com 16 *hosts* lícitos.

Na Figura 9, é possível observar que o *throughput* da rede sem fio volta a ter menos variação. Isso acontece pelo fato de que a partir de redes com 16 *hosts*, as simulações possuem o intervalo de envio dos pacotes ICMP aumentados para 1 segundo, ao invés de 100 milissegundos como acontecia nas simulações anteriores. Por isso, o *throughput* da rede se mantém com poucas oscilações e com uma média de 54,49 Bps. Na simulação de ataque, o *throughput* da rede sofre novamente com o impacto do ataque de negação de serviço, chegando a zero por alguns segundos, com média de *throughput* igual a 35,61 Bps. Essa média é maior do que a das simulações anteriores, mesmo possuindo mais *hosts* na rede, pelo fato do intervalo de tráfego ser maior do que nas simulações anteriores. A simulação com a atuação da mitigação apresenta um gráfico que se mantém praticamente sem uma queda no *throughput*. Isso se deve ao fato, novamente, de que o intervalo entre o envio de pacotes é aumentado para um valor muito maior do que nas simulações anteriores. A média do *throughput* é de 54,61 Bps.

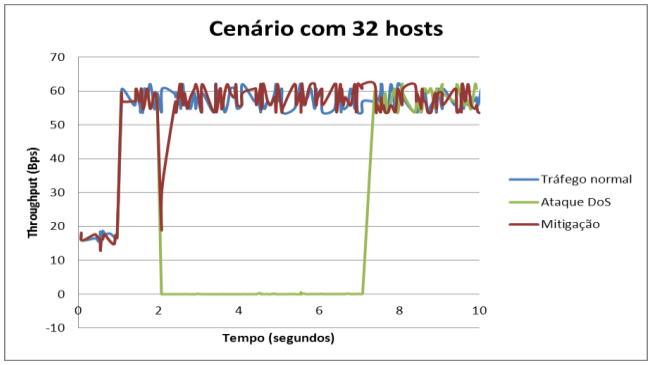

Figura 10. Simulações com 32 *hosts* lícitos.

Na figura 10 é apresentado o tráfego normal em uma simulação com 32 *hosts* em uma rede sem fio. A variação se mantém dentro de um intervalo pequeno, possuindo assim, uma média de *throughput* igual a 55,51 Bps. A variação do *throughput* na simulação de ataque é mantida no início como deveria ser, de acordo com o tráfego normal, e é alterada bruscamente quando o ataque de negação de serviço é iniciado. Assim, a média do *throughput* cai para 41,06 Bps. Conforme o intervalo adotado para troca de pacotes é aumentado, a quantidade de medidas diminui e, portanto, apesar do gráfico ser muito parecido com os das simulações com 2 e 4 *hosts*, a quantidade de medidas é bem menor, causando uma variação na média do *throughput*. Quando a

mitigação é simulada para esse conjunto de *hosts*, ocorre uma breve queda no *throughput* e, novamente, não chega a ser zero, obtendo uma média de *throughput* igual a 54,23 Bps. O modelo de mitigação apresenta dados satisfatórios, pois a média do *throughput* está muito próxima da que foi obtida com a simulação sem ação de um atacante.

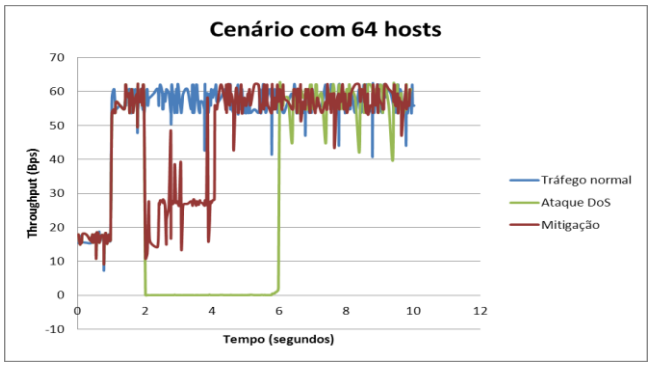

Figura 11. Simulações com 64 *hosts* lícitos.

Na Figura 11 é apresentado o tráfego normal de uma simulação com 64 *hosts*. A variação do *throughput* aumenta um pouco e a quantidade de medidas também é maior, apresentando uma média do *throughput* igual a 55,99 Bps. A simulação de ataque apresenta a queda do *throughput* a praticamente zero devido ao ataque de negação de serviço, causando uma queda na média do *throughput* para 47,93 Bps. Na simulação de mitigação, o *throughput* cai um pouco e se mantém em uma medida inferior do normal por alguns segundos. Isso se deve ao fato da rede possuir muitos nós. Entretanto, o *throughput* não chega a zero e mantém uma média de 54,05 Bps, ou seja, próxima da média obtida na simulação sem a ação de um atacante.

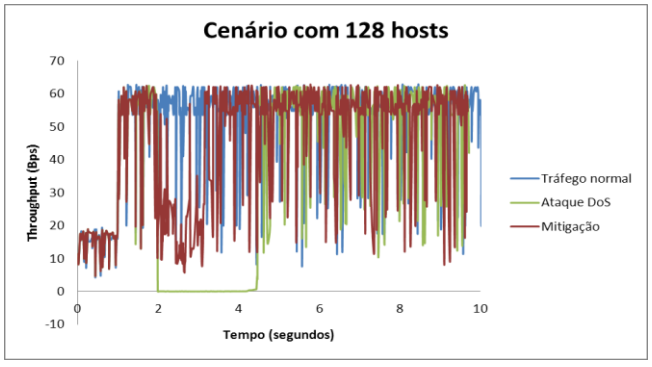

Figura 12. Simulações com 128 *hosts* lícitos.

A Figura 12 mostra que a variação do *throughput* para a simulação com 128 *hosts* oscila bastante em relação às anteriores. A média do *throughput* para essa simulação sem atacante é de 51,22 Bps. Ao iniciar o ataque, a rede sofre uma queda devido ao ataque realizado. A média do *throughput* para essa simulação é de 45,93 Bps. Assim como na Figura 11, a Figura 12 também sobre uma leve queda no *throughput* por

alguns segundos, mas nunca chegando a zero. A média do *throughput* é 50,20, também muito próxima do que foi obtida na simulação sem atacante.

De acordo com os gráficos apresentados, fica evidente que os ataques de negação de serviço são preocupantes. O *throughput* da rede cai a praticamente zero quando o ataque é realizado e a rede só se reestabelece após algum tempo do final do ataque. Além disso, é possível observar que com a mitigação proposta, existe uma melhora bastante expressiva. Em alguns gráficos obtidos, o *throughput* da rede, dentro do intervalo em que o ataque ocorre, apresenta uma queda devido ao volume de pacotes que são trafegados na rede e ao intervalo que esses pacotes são enviados. Além disso, a quantidade de *hosts* na rede também afetam tanto o *throughput* sob tráfego normal e sob ataque quanto para o tráfego obtido com a mitigação em ação.

Para melhor visualização do *throughput* da rede dos cenários testados, na Figura 13 é ilustrado um gráfico dos valores médio do *throughput* de cada cenário tanto do tráfego normal, quanto do tráfego sob ataque e do tráfego com a mitigação sendo utilizada.

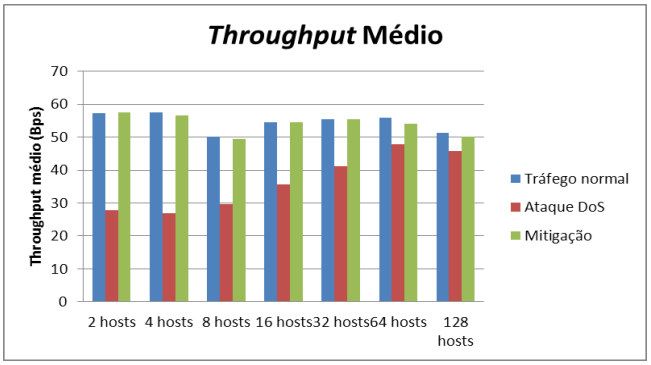

Figura 13. *Throughput* médio dos cenários de teste.

Os valores utilizados para gerar o *throughput* médio são os mesmos utilizados nas simulações ilustradas nos gráficos resultantes dos cenários. Dessa forma, o *throughput* possui uma média maior à medida que o número de *hosts* aumenta, pois o intervalo de tráfego entre os *hosts* é maior do que nos cenários com menos *hosts*.

De acordo com a Figura 13, é visível o impacto que uma rede sem fio sofre com ataques de negação de serviço. Ao longo do tempo simulado, a vazão da rede cai consideravelmente mesmo com um tempo de ataque bastante curto, apenas 0,3 segundos. Normalmente, ataques de negação de serviço podem durar vários minutos ou até mesmo horas.

Outra forma de se avaliar o impacto de uma rede é a contagem de pacotes descartados (*drops*). Na Tabela 3 são exibidas as porcentagens de *drop* nos cenários testados.

Tabela 3. Porcentagem de *drop* dos cenários de teste.

	***Drop* (%)**		
Cenário	Tráfego normal	Ataque DoS	Mitigação

2 *hosts*	0	26,65	0
4 *hosts*	0	31	0
8 *hosts*	0	25,64	0
16 *hosts*	0	20,67	0
32 *hosts*	0	27	0
64 *hosts*	0	6,89	0
128 *hosts*	0	12,59	0

Para os testes com tráfego normal, não houve *drop* de nenhum pacote. Ao realizar o ataque de negação de serviço, a rede sofre, dependendo do fluxo de pacotes trafegados na rede, uma quantidade alta de *drop*. Ao realizar os testes de ataque com a atuação do modelo de mitigação, é observado que o *drop* volta a ser 0%, assim como era antes de se proferir o ataque DoS.

5. Conclusão

Em sistemas embarcados críticos é imprescindível que exista uma boa comunicação entre os nós. A sensibilidade da rede, por utilizar normalmente tecnologias sem fio, permite que atividades mal intencionadas causem danos aos sistemas e os impeçam de realizar suas tarefas.

O problema aqui apresentado mostra claramente o prejuízo que um ataque de negação de serviço causa em uma rede. Com o modelo de mitigação proposto foi possível encontrar uma forma para minimizar os danos que esse ataque possa causar. Ainda, as simulações se mostraram expressivas em questões de quantidades de nós em uma rede, variando desde poucos *hosts* até grandes quantidades onde o tráfego é mais disputado e congestionado.

Diante dos trabalhos relacionados com o tema, é possível observar que existem diversas maneiras de mitigar ataques de negação de serviço. Devido ao fato dos pacotes e *frames* não serem autenticados, é possível que os atacantes realizem com maior facilidade seus ataques DoS. Diversos trabalhos apresentam formas de autenticarem esses pacotes e frames, apresentando grande melhora na rede.

O trabalho aqui apresentado, diferentemente dos encontrados na literatura aberta, propõe uma abordagem simples. Os resultados são diversos e mostram que o método utilizado é eficaz e que pode ser bastante útil na segurança de redes sem fio, e consequentemente, em sistemas embarcados críticos.

Como trabalhos futuros, poderão ser realizadas novas simulações envolvendo outros cenários e coletas de dados. Além disso, a utilização de outra técnica de ataque bem como a elaboração de sua forma de detecção e mitigação servirá para incrementar a segurança em ambientes de rede sem fio.

6. Referências

FENG, P. Wireless LAN security issues and solutions. 2012 IEEE Symposium on Robotics and Applications (ISRA), p. 921-924, jun. 2012.

IEEE 802.11. IEEE Standard 802.11. Local na Metropolitan Area Networks – Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 12 jun. 2007. 1232 p.

KUROSE, J. F.; ROSS, K. W. Redes de computadores e a Internet: uma abordagem top-down. 5ª Edição. Pearson, 2009. 614p.

LEE, Y.; CHIEN, H.; TSAI, W. Using Random Bit Authentication to Defend IEEE 802.11 DoS Attacks. Journal of Information Science and Engineering 25, p. 1485-1500, 2009.

MALEKZADEH, M; GHANI, A. A. A.; SUBRAMANIAM, S.; DESA, J. Validating Reliability of OMNeT++ in Wireless Networks DoS Attacks: Simulation vs Testbed. International Journal of Network Security, v. 13, n.1, p. 13-21, jul. 2011.

MYNEMI, S.; HUANG, D. IEEE 802.11 Wireless LAN Control Frame Protection. 7th IEEE Consumer Communications and Networking Conference, p. 9-12 jan. 2010.

NEGI, R.; RAJESWARAN, A. DoS Analysis of Reservation Based MAC Protocols. Communications, 2005, v. 00, p. 3632-3636, 2005.

NGUYEN, T. D.; NGUYEN, D. H. M.; TRAN, B. N.; VU, H; MITTAL, N. A Lightweight Solution for Defending Against Deauthentication/Disassociation Attacks on 802.11 Networks. … and Networks, 2008. p. 1-6, 2008.

OMNET++. OMNET++ Manual. 2012. Disponível em: < http://www.omnetpp.org/doc/omnetpp/manual/usman.html>. Acesso em: 14 fev. 2013.

PING, W. Research on the Embedded System Teaching. 2008 International Workshop on Education Technology and Training & 2008 International Workshop on Geoscience and Remote Sensing, p. 19-21, dez. 2008.

SANDSTRÖM, H. A Survey of the Denial of Service Problem. 2001.

SINGH, R.; SHARMA, T. P. Detecting and Reducing the Denial of Service attacks in WLANs. 2011 World Congress on Information and Communication Technologies, p. 968-973, dez. 2011.

SORYAL, J.; SAADAWI, T. IEEE 802.11 Denial of Service Attack Detection in MANET. Telecommunications Symposium (WTS), 2012.

YAGHMOUR, K.; MASTERS, J.; BEN-YOSSEF, G.; GERUM P. Building Embedded Linux Systems, 2ed. Sebastopol, CA 95472, USA: O´Reilly Media, 442 p., 2008. Disponível em: http://shop.oreilly.com/product/9780596002220.do

YU, Y. et al. The Practice and exploration on the education mode for embedded systems major. 2010 International Conference on Education and Management Technology, p. 367-370, nov. 2010.