DOI: 10.5102/un.gti.v1i2.1452

Correlação dos modelos de ataques em diversas camadas de protocolos de redes ad hoc*

Edna Dias Canedo[1]
Luigi Silva Mota[2]

Resumo

As redes sem fio possuem vulnerabilidades específicas, associadas, principalmente, à transmissão pelo ar, à ausência de infraestrutura e ao encaminhamento colaborativo das mensagens. Nas redes sem fio, além dos ataques convencionais, o roteamento colaborativo apresenta novas vulnerabilidades e a ausência de infraestrutura dificulta a criação de mecanismos de defesas simples e eficientes. Este trabalho apresenta os principais mecanismos de segurança utilizados para a proteção aos ataques, assim como uma simulação do ataque *jamming* na camada física utilizando o NS2. Um ataque *jamming* pode facilmente ser efetuad o por um adversário emitindo sinais de rádio frequência que não seguem um protocolo MAC subjacente e pode interferir severamente com as operações normais de redes sem fio, afetando os serviços em múltiplas camadas de protocolos e, consequentemente, são necessários mecanismos que possam lidar com tais ataques. Neste artigo, examinaremos ataques de interferência de rádio e estudaremos o problema da condução deles sobre redes sem fio.

Palavras-chave: Redes ad hoc. Modelos de ataques. Mecanismos de seguranças e impactos. Rede 802.15.4. Ataques *jamming.*

* Recebido em: dia/05/2011
Aprovado em: dia/09/2011

[1] Doutoranda em Engenharia Elétrica pela Universidade de Brasília (UNB). Mestre pela Universidade Federal da Paraíba UFPB. Área de concentração: Sistemas de Software. Área Especifica: Engenharia de Software, título concedido em 29.08.2002. Graduada em Análise de Sistemas pela Universidade Salgado de Oliveira..

[2] Possui graduação em Licenciatura em Computação (2003), Mestrado em Tecnologia da Informação pela Universidade Federal do Ceará (2008) e pela Universidade do Norte do Paraná.

1 Introdução

Redes *Mobile Ad hoc Networks* (MANET) não dependem de qualquer administração centralizada ou infraestrutura de rede fixa e os seus nós estabelecem uma estrutura de roteamento de forma auto-organizada. Assim, são autônomas e devem ser capazes de autoconfiguração, organização e manutenção devido às falhas de comunicação e chegada e saída de nós. Além disso, a topologia da rede pode mudar dinamicamente devido à mobilidade dos nós. As redes ad hoc são constituídas por dispositivos móveis que utilizam comunicação sem fio e qualquer um dos nós dentro de um determinado perímetro de alcance das transmissões pode se comunicar diretamente com outros. A comunicação entre os nós que estão fora do alcance de transmissão é feita em múltiplos saltos por meio da colaboração de nós intermediários com base em roteamento do tipo reativo ou proativo.

As redes MANET têm grande flexibilidade e rapidez na sua implantação, sendo adequadas para muitas aplicações, como a comunicação em ambientes heterogêneos. As redes MANET possuem como grande vantagem o baixo custo de instalação e a facilidade de configuração. Por outro lado, o meio de comunicação sem fio, a ausência de infraestrutura e o roteamento colaborativo em múltiplos saltos as tornam alvos potenciais de diversos tipos de ataques. Assim, a segurança é um ponto crucial a ser analisado nas redes ad hoc.

Os ataques podem vir de várias direções e visar qualquer nó da rede, bastando que o nó atacado esteja no alcance de transmissão do nó atacante (FERNANDES et al, 2006). Dessa maneira, sendo possível que um nó malicioso tenha acesso às informações transmitidas, ele pode criar, modificar e destruir mensagens em trânsito ou ainda tentar se passar por outros nós da rede. Assim, cada nó da rede deve estar preparado para lidar direta ou indiretamente com ações maliciosas de outros nós.

Devido à ausência de infraestrutura, as redes ad hoc exigem a colaboração distribuída dos nós da rede para o encaminhamento das mensagens. Todos os nós participam do protocolo de roteamento, devendo estar aptos a desempenhar a função de roteador. Além disso, esses nós roteadores estão sob o controle dos

usuários da rede, e não de administradores. Isso possibilita a criação de novos ataques que visam às vulnerabilidades dos algoritmos cooperativos. Os protocolos de roteamento devem ser robustos a ataques conhecidos e a novos tipos de ataques.

As redes ad hoc introduzem outros obstáculos importantes à implementação de mecanismos de segurança devido às constantes alterações na topologia da rede. Essa dinamicidade implica em novos nós que se tornam vizinhos e antigos nós que deixam de ser vizinhos e podem até causar o particionamento da rede. Assim, os mecanismos de segurança devem se adaptar dinamicamente às mudanças na topologia da rede e ao movimento dos nós entrando e saindo da rede. Além disso, as redes ad hoc são em geral compostas por dispositivos portáteis, portanto com restrições de energia, processamento e memória. Com isso, estão sujeitas a diferentes ataques de negação de serviço que visam esgotar os recursos dos nós a fim de prejudicar o funcionamento da rede. Dessa forma, as redes ad hoc possuem vulnerabilidades específicas ligadas principalmente ao meio de comunicação sem fio, à ausência de infraestrutura e ao roteamento colaborativo.

A maior parte dos ataques concentra-se na camada de redes e, consequentemente, também a maioria dos mecanismos de defesa específicos das redes ad hoc. Entretanto, há diversos ataques em outras camadas e, em particular nas camadas física e de enlace, onde, por exemplo, ataques de *jamming* podem ser realizados de modo a interferir severamente nas operações normais de redes sem fio afetando os serviços em múltiplas camadas de protocolos. Consequentemente, são necessários mecanismos que possam lidar com tais ataques.

O artigo está assim organizado: na primeira seção, é apresentada uma descrição do padrão IEEE 802.15.4; na seção 2, são apresentadas as pesquisas e trabalhos relacionados; na seção 3, apresentamos os tipos de ataques em redes MANET; na seção 4, é apresentada a correlação entre os modelos de ataques em diversas camadas de protocolos de redes ad hoc; na seção 5, apresentamos uma simulação do *jamming* em um ambiente de rede sem fio utilizando a ferramenta NS2. Por último, são discutidos os resultados obtidos e apresentadas as conclusões.

2 Uma descrição do padrão IEEE 802.15.4

O padrão IEEE 802.15.4 define as especificações da camada física (PHY) e da subcamada de controle de acesso ao meio (MAC) para redes sem fio de baixa taxa de dados entre dispositivos relativamente simples que consomem pouca energia e tipicamente operam no *Personal Operating Space* (POS) de 10 metros ou menos. Uma rede 802.15.4 pode simplesmente ter forma de uma estrela com apenas um salto (*one-hop*) ou, quando as distâncias de comunicação excedem 10 metros, pode ser uma rede *multi-hop* autoconfigurável. Um dispositivo em uma rede 802.15.4 pode usar um endereço IEEE de 64-bits ou um endereço curto de 16-bits atribuído durante o processo de associação. Os enlaces 802.15.4 podem operar em três licenças de bandas de frequências livres da *Industrial Scientific Medical* (ISM), com taxas de dados de 250 kb/sec (ou expressado em símbolos, 62.5 ksym/sec) na banda 2.4 GHz, 40 kb/sec (40 ksym/sec) na banda 915 MHz, e 20 kb/sec (ksym/sec) na banda 868 MHz. No total, 27 canais são alocados no 802.15.4, com 16 canais na banda 2.4 GHz, 10 canais na banda 915 MHz, e 1 canal na banda 868 MHz.

As redes 802.15.4 são inerentemente suscetíveis à interceptação e à interferência, e diversas pesquisas em segurança foram realizadas acerca desses problemas (ZHENG; LEE, 2006), mas a questão de segurança nesse contexto permanece uma questão desafiadora. Vale notar que o padrão 802.15.4 emprega um protocolo de *handshake* completo para transferências de dados confiáveis e engloba o padrão de criptografia AES para transferência de dados segura. Nas seções seguintes, é apresentada uma breve descrição da camada física, da camada MAC e algumas funções gerais do 802.15.4, podendo ser obtidas informações detalhadas (IEEE, 2003).

2.1 A camada PHY

A camada PHY fornece dois serviços acessados através de dois pontos de acesso ao serviço (SAPs). Eles são os serviços de dados PHY e o serviço de gerenciamento PHY. A camada PHY é responsável pelas seguintes tarefas:

- **Ativação e desativação do transceptor de rádio:** ligar, de acordo com o pedido da subcamada MAC, o transceptor de rádio em um dos três

estados: transmitindo, recebendo, ou desligado (*sleeping*). O tempo de transmissão ou recebimento de um pacote de transmitir e receber, ou vice-versa, deve ser maior do que 12 símbolos por período.

- **Detecção de energia (ED) no canal atual:** consiste em fornecer uma estimativa da energia do sinal recebido dentro da largura de banda de um canal IEEE 802.15.4. Nenhuma tentativa é feita para identificar ou decodificar sinais sobre o canal nesse processo. O tempo de detecção de energia deve ser igual a 8 símbolos por período. O resultado da detecção de energia pode ser usado por uma entidade da camada de rede como parte de um algoritmo de seleção do canal, ou para a finalidade de avaliação de canal disponível (CCA) - sozinho ou combinado com a portadora.
- **Indicação de qualidade de enlace (LQI) para pacotes recebidos:** fornece uma medida de indicação de qualidade de enlace que é realizada para cada pacote recebido. A camada PHY usa a detecção de energia recebida (ED) ou uma razão sinal-ruído, ou uma combinação delas para medir a intensidade e/ou qualidade do enlace pelo qual um pacote é recebido. Contudo, o uso de LQI pelas camadas de rede ou aplicações não é especificado no padrão.
- **Avaliação de canal disponível (CCA) para portadora de acesso múltiplo com detecção de colisão (CSMA-CA):** a camada PHY realiza a CCA usando detecção de energia ou de portadora ou uma combinação das duas. No modo de detecção de energia, o meio é considerado ocupado se alguma energia acima de um limiar predefinido é detectada. No modo de detecção de portadora, o meio é considerado ocupado se um sinal com as características de modulação e espalhamento do IEEE 802.15.4 é detectado. E no modo combinado, ambas as condições mencionadas precisam ser observadas a fim de concluir que o meio está ocupado.
- **Seleção de canal de frequência:** como os enlaces podem operar em 27 canais diferentes (mas uma rede específica pode escolher uma parte dos canais), a camada PHY deve ser capaz de sintonizar seu transceptor em certo canal ao receber um pedido da subcamada MAC.

- **Transmissão e recepção de dados:** para realizar a tarefa essencial da camada PHY, são usadas técnicas de modulação e espalhamento. A PHY a 2.4 GHz emprega uma técnica de modulação 16-ária quase ortogonal, na qual cada informação de 4 bits é mapeada em uma sequência de ruído pseudo-aleatória chip-32 (PN). As sequências PN para sucessivos símbolos de dados são então concatenadas e moduladas para a portadora usando *offset quadrature phase shift keiyng* (O-QPSK). A PHY a 868/915 MHz emprega *direct sequence spread spectrum* (DSSS) com *binary phase shift keying* (BPSK) usada para modulação chip e codificação diferencial usada para codificação de símbolos de dados. Cada símbolo de dados é mapeado em uma sequência PN 15-chip e as sequências PN concatenadas são, então, moduladas para a portadora usando BPSK com forma de pulso cosseno levantada.

2.2 A subcamada MAC

A subcamada MAC fornece uma interface entre a subcamada de convergência específica de serviço (SSCS) e a camada PHY. Como a camada física, a subcamada MAC também fornece dois serviços, ou seja, o serviço de dados MAC e o serviço de gerenciamento MAC. A camada MAC é responsável pelas seguintes tarefas:

- **Geração de *beacons* de rede se o dispositivo é um coordenador:** um coordenador pode determinar se ele trabalha em um modo *beacon* habilitado, no qual um *superframe* é utilizado. O *superframe* é delimitado por *beacons* de rede e dividido em *aNumSuperframeSlots* (valor padrão é 16) slots de tamanhos idênticos. Um coordenador envia *beacons* periodicamente para sincronizar os dispositivos conectados e para outras finalidades.
- **Sincronização com *beacons*:** um dispositivo conectado ao coordenador operando em modo *beacon* pode monitorar os *beacons* para sincronizar com o coordenador. Essa sincronização é importante para *data polling*, economia de energia, e detecção de órfãos.

- **Suporte a área de rede pessoal (PAN) para efeito de associação e dissociação:** para suporte a autoconfiguração, o 802.15.4 foi especificado com funções de associação e dissociação em sua camada MAC. Isso não somente habilita uma topologia estrela a se configurar automaticamente, mas também permite a criação de uma rede *peer-to-peer* autoconfigurável.
- **Mecanismo de portadora de acesso múltiplo com anticolisão (CSMA-CA) para acesso ao canal:** Como muitos outros protocolos projetados para redes sem fio, o 802.15.4 usa o mecanismo CSMA-CA para acesso ao canal. Contudo, o padrão não inclui o mecanismo *request-to-send* (RTS) e *clear-to-send* (CTS), em consideração à baixa taxa de dados usada em LR-WPANs.
- **Mecanismo de manuseio e manutenção de garantia de *time slot* (GTS):** Quando trabalhando no modo *beacon*, um coordenador pode alocar porções de um *superframe* ativo para um dispositivo. Essas porções são chamadas de GTS, e compreendem o período livre de contenção (CFP) do *superframe*.
- **Fornecer um link confiável entre duas entidades MAC pares (*peers*):** a subcamada MAC emprega vários mecanismos para atingir a confiabilidade do enlace entre dois *peers*; entre eles estão a verificação de dados usando um CRC 16-bit, os *frames* de reconhecimento, a capacidade de retransmissão, bem como o método CSMA-CA.

2.3 Funções gerais

O padrão 802.15.4 fornece especificações detalhadas dos seguintes itens descritos na presente seção: tipo de dispositivo, estrutura de *frame*, estrutura de *superframe*, modelo de transferência de dados, robustez e considerações de consumo de energia.

Dois diferentes tipos de dispositivos são definidos em uma rede 802.15.4; um dispositivo de função completa (FFD) e um dispositivo de função reduzida (RFD). Um FFD pode conversar com RFDs e outros FFDs, e opera em três modos

de serviço, quer como um coordenador PAN, um coordenador ou um dispositivo. Um RFD pode somente conversar com um FFD e é utilizado para aplicações extremamente simples.

O padrão permite o uso opcional de uma estrutura *superframe*. O formato do *superframe* é definido pelo coordenador. Como é apresentado na figura 1, o *superframe* compreende uma parte ativa e uma parte inativa opcional, e é delimitado por *beacons* de rede. O comprimento do *superframe* (também denominado intervalo entre *beacon*, BI) e o comprimento de sua parte ativa (também denominada duração do *superframe*, SD) são definidos como:

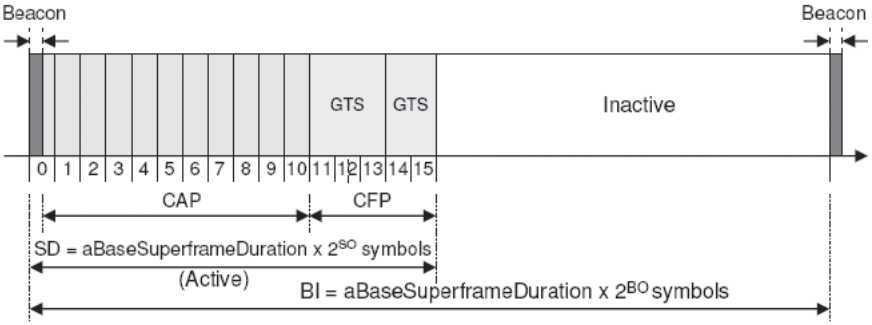
$$BI = aBaseSuperframeDuration * 2^{BO}$$
$$SD = aBaseSuperframeDuration 2^{SO}$$

Onde,

ABaseSuperframeDuration = 960 símbolos
BO = beacon order
SO = superframe order

Os valores de BO e SO são determinados pelo coordenador. A parte ativa do *superframe* é dividida em *aNumSuperframeSlots* (o valor padrão é 16) slots de tamanhos idênticos e o *beacon frame* é transmitido no primeiro slot de cada *superframe*. A parte ativa pode ser subdividida em dois períodos: um período de acesso de contenção (CAP) e um (opcional) período livre de contenção (CFP). O CFP opcional pode acomodar até 7 intervalos chamados de *slots* de garantia de tempo (GTSs), e um GTS pode ocupar mais do que um período de *slot*. Contudo, uma porção suficiente do CAP deve permanecer para permitir o acesso baseado em contenção de outros dispositivos de rede ou novos dispositivos que desejam aderir à rede. Um mecanismo *slotted* CSMA-CA é usado para acesso ao canal durante o CAP. Todas as transações baseadas em contenção devem estar completas antes de o CFP começar. Também todas as transações usando GTSs devem ser finalizadas antes do tempo do próximo GTS ou do fim do CFP.

Figura 1 – Exemplo de uma Estrutura Superframe



Fonte: do autor.

As transferências de dados podem ocorrer de três diferentes formas: (1) de um dispositivo para o coordenador; (2) de um coordenador para um dispositivo; e (3) de um *peer* para outro em uma rede multi-hop *peer-to-peer*. Usando outro ponto de vista, neste estudo, classificou-se a transferência de dados nos seguintes três tipos:

- **Transmissão de dados direta:** aplica-se a toda transferência de dados, seja de um dispositivo para um coordenador, de um coordenador para um dispositivo, ou entre dois *peers*. Os métodos CSMA-CA *unslotted* ou CSMA-CA *slotted* são usados para transmissão de dados, dependendo se o modo não *beacon* ou o modo *beacon* é utilizado.
- **Transmissão de dados indireta:** somente se aplica à transferência de dados de um coordenador para seus dispositivos. Nesse modo, um *frame* de dados é mantido em uma lista de transações pelo coordenador, esperando para extração pelo correspondente dispositivo. Um dispositivo pode localizar se ele tem um pacote pendente na lista de transações checando os frames *beacon* recebidos de seu coordenador. Ocasionalmente, transmissões de dados indiretas podem acontecer no modo não *beacon*. Por exemplo, durante um processo de associação, o coordenador mantém o *frame* de resposta de associação em sua lista de transações e o dispositivo de pesquisa (*poll*) e extrai o frame de

resposta de associação. O CSMA-CA *unslotted* ou o CSMA-CA *slotted* é utilizado nos procedimentos de extração de dados.

- **Transmissão de dados GTS:** somente se aplica à transferência de dados entre um dispositivo e seu coordenador, seja do dispositivo para o coordenador ou do coordenador para o dispositivo. Nenhum dos dois métodos CSMA-CA é necessário nas transmissões de dados GTS.

3 Trabalhos relacionados

A fim de lidar com a ameaça dos ataques *jamming*, é importante entender os diferentes modelos de ataque que podem ser empregados pelos adversários, os métodos que são necessários para diagnosticar essas ameaças, e as contramedidas que podem ser empregadas para se defender contra os ataques *jamming*.

A literatura tradicional sobre *jamming* primeiramente foca sobre o projeto das tecnologias de camada física, tal como espalhamento espectral, que são resistentes a *jamming* (PROAKIS, 2000 ; SCHLEHER, 1999). Deve-se perceber que as tecnologias de camada física que precisam resistir ao *jamming* não têm encontrado implantação generalizada para os dispositivos sem fio, tal como LANs sem fio e rede de sensores. Muitos trabalhos têm a perspectiva que ao invés de substituir sistemas existentes com plataformas de rádio mais complicadas, é desejável entender os modos de ataques que podem ser lançados contra as plataformas existentes, e ser capaz de detectá-los. Após a detecção, contramedidas apropriadas devem ser empregadas.

A questão de detecção de *jamming* foi brevemente estudada por Wood e Stankovic (2003) no contexto das redes de sensores. Esse estudo colocou a questão da detecção do *jamming* no contexto avulso de utilidade dos canais de comunicação, e apresentou vários fatores que pode afetar a utilidade dos canais. O trabalho de (XU et al., 2004) focou esse assunto sobre a questão de mapear a região afetada pelo *jamming* e o uso de métricas estatísticas não serem suficientes para decidir se a rede está sofrendo um ataque do tipo *jamming.* Este trabalho propõe dois algoritmos de decisão para a detecção de um ataque *jamming:* um empregando a

intensidade do sinal e outro empregando as informações de localização do nó para a checagem de consistência.

Embora não seja precisamente um ataque *jamming*, pode-se explorar a camada MAC para encontrar um aumento nos recursos de rede (BELLARDO; SAVAGE, 2003; KYASANUR; VAIDYA, 2003). A questão da complacência de não detecção MAC foi estudada por (RAYA; HUBAUX; AAD, 2004), trabalho que mostrou que um usuário ganancioso pode aumentar a sua quota de largura de banda modificando o *driver* de seu adaptador de rede. O usuário ganancioso pode tentar corromper o RTS e CTS dos outros usuários para evitar a transmissão de pacote, ou pode corromper ACKs para causar um aumento da contenção de janela ACK, levando a um grande *backoff*. Foi proposto o DOMINO, um sistema de detecção de tal comportamento ganancioso na camada MAC das redes do padrão IEEE 802.11.

Contramedidas para lidar com regiões afetadas por *jamming* em redes sem fio foram estudadas por (NOUBIR; LIN, 2003; XU; TRAPPE; ZHANG, 2004). Segundo (NOUBIR; LIN, 2003), o uso do código LDPC (*Low Density Parity Check*) é proposto para lidar com o *jamming*. Além disso, uma técnica *anti-jamming* foi proposta para 802.11b que envolve o uso do código Reed-Solomon. Em Xu, Trappe e Zhang, (2004), duas contramedidas são apresentadas para lidar com *jamming*. O primeiro método, *canal surfing*, envolve uma forma de salto de frequência sob demanda na camada de enlace, onde participantes válidos trocam o canal que estão se comunicando quando ocorre um ataque de negação de serviço. O segundo método, retiro espacial, envolve dispositivos de rede legítimos se movendo ao redor do adversário para restabelecer as conexões.

O trabalho realizado por Chen e Leneutre, (2011) investigou o ataque *jamming* em redes sem fio utilizando uma abordagem de teoria de jogos. Baseado nas análises dos jogos *jamming*, foi proposta uma estratégia de defesa consistindo de uma luta ativa com o *jammer* face a face drenando sua energia. Foi demonstrado que a estratégia de defesa pode eliminar o equilíbrio indesejável e aumentar o consumo de energia do *jammer* sem degradar a performance da rede. Um trabalho interessante é combinar essa solução com a abordagem de salto de canal. O trabalho em Chen e Leneutre, (2011) pode ser estendido na forma que o *anti-jammer*

transmite uma isca no canal para diminuir a probabilidade de que o canal com a transmissão legítima seja atacado pelo *jammer*. Nessas considerações, drenar a energia do *jammer* e limitar danos do *jamming* pode ser conseguido simultaneamente, o que abre uma nova dimensão para a estratégia de defesa *jamming*.

4 Ataques *jamming*

Nesta seção, introduziremos os ataques de interferência de rádio que podem ser lançados contra redes sem fio. O adversário (dispositivo sem fio malicioso) que lançar um ataque é referido como *jammer* neste artigo. Primeiro, definiremos as características de um comportamento do *jammer* e em seguida enumeraremos métricas que podem ser usadas para medir a eficácia de um ataque *jamming*. Essas métricas são estreitamente relacionadas à capacidade de um dispositivo de rádio para enviar ou receber pacotes. Apresentaremos quatro modelos típicos de ataques *jammer*, os quais representam grande quantidade das estratégicas de ataques, o que servirá de base para discussão ao longo do artigo.

4.1 Características e métricas do *jamming*

Apesar de vários estudos de Noubir e Lin (2003), Xu et al. (2004) terem classificado ataques de estilo *jamming*, a definição desse tipo de ataque permanece incerta. Um ponto de concordância é que um *jammer* emite continuamente sinais de interferência de rádio (RF) para ocupar um canal sem fio, bloqueando totalmente o tráfego legítimo (WOOD; STANKOVIC ; SON, 2004; XU et al., 2004). Um *jammer* é definido como sendo uma entidade que está propositadamente tentando interferir com a transmissão e recepção física das comunicações sem fio (XU et al., 2005). Mas, adicionalmente, uma grande quantidade de comportamentos pode ser adotada por um *jammer*. Por exemplo, um *jammer* pode permanecer quieto quando não existir atividade no canal, e iniciar a interferência quando ele detecta uma transmissão. Uma característica comum dos ataques *jamming* é que suas comunicações não são compatíveis com os protocolos da camada MAC. O objetivo de um *jammer* é interferir com a legítima comunicação sem fio. Um *jammer* pode

alcançar esse objetivo evitando uma fonte de tráfego legítimo de enviar um pacote, ou evitar a recepção de pacotes legítimos. Vamos assumir que *A* e *B* representam dois participantes legítimos que podem estar incapazes de enviar pacotes por várias razões. Por exemplo, um *jammer X* pode emitir continuamente um sinal sobre o canal, tal que *A* nunca sentirá o canal livre, ou *X* pode permanecer enviando pacotes de dados regulares e forçar a receber pacotes sem valor o tempo todo. Por outro lado, mesmo se *A* enviar pacotes com sucesso para *B*, é possível que *X* interrompa uma transmissão de rádio, corrompendo a mensagem recebida por *B*. São definidas duas métricas para medir a eficácia de um *jammer* ((XU et al., 2005):

- **Taxa de Envio de Pacote (PSR):** taxa de pacotes que são enviados com sucesso por uma fonte de tráfego *A* legítima comparada com o número de pacotes que ela pretendia enviar na camada MAC. Muitas redes sem fio empregam algumas formas de controle de acesso múltiplo com detecção de portadora antes que a transmissão possa ser efetuada. Supondo que *A* tenha um pacote para enviar, o canal deve ser observado como estando no estado livre pelo menos durante alguma quantidade de tempo aleatória antes que *A* possa enviar o pacote. Além disso, diferentes protocolos MAC têm definição diferente sobre o que é um canal livre. Alguns comparam simplesmente o sinal medido com um limiar fixado, enquanto outros podem adaptar o limiar baseados no nível de ruído sobre o canal. Um ataque de interferência de rádio pode levar o canal a ser sentido como ocupado, causando um atraso na transmissão de *A*. Se muitos pacotes também são armazenados na camada MAC, os pacotes que chegam são descartados. É possível também que um pacote fique na camada MAC por um longo tempo, resultando em um *timeout* e o pacote acaba sendo descartado. Se *A* pretende enviar *n* mensagens, mas somente *m* são enviadas, o PSR é *m*/*n*. O PSR pode ser facilmente medido por um dispositivo que mantém um controle do número de pacotes que pretende enviar e o número de pacotes que são enviados com sucesso.
- **Taxa de Pacotes Entregues (PDR):** taxa de pacotes que são entregues com sucesso a um destino *B* comparada com o número de

pacotes enviados pelo emissor *A*. Mesmo após o pacote ser enviado por *A*, *B* pode não ser capaz de decodificá-lo corretamente, devido à interferência introduzida por *X*. Tal cenário é uma entrega sem sucesso. O PDR pode ser medido no receptor *B* calculando a taxa de número de pacotes que passa na verificação CRC em relação ao número de pacotes recebidos. O PDR pode também ser calculado pelo emissor *A* tendo *B* retornado um pacote de reconhecimento (ACK). Em ambos os casos, se nenhum pacote é recebido, o PDR é definido como zero (0).

4.2 Modelos de ataques *jamming*

Existem diferentes estratégias de ataques que um *jammer* pode empregar para interferir com outras comunicações sem fio. Como consequência, os modelos de ataques terão diferentes níveis de sucesso e podem também exigir diferentes estratégias de detecção. É impraticável descrever todos os possíveis modelos de ataques que podem existir, segundo Xu et al. (2005), propõe os seguintes tipos de *jammers*: **1) *Constant jammer***: este emite continuamente um sinal de rádio, enviando bits aleatórios para o canal sem seguir algum padrão da camada MAC. O *constant jammer* não espera que o canal se torne ocioso para começar a transmitir. Se o protocolo MAC subjacente detecta se um canal está ocioso ou não comparando a medida de intensidade do sinal com um limiar fixado, o qual é usualmente menor do que a intensidade do sinal gerada pelo *constant jammer*, este pode efetivamente impedir que fontes de tráfego legítimo obtenham o canal e enviem pacotes. **2) *Deceptive jammer*:** ao invés de enviar bits aleatórios, o *deceptive jammer* injeta constantemente pacotes regulares no canal sem algum intervalo entre as transmissões de pacotes subjacentes. Como resultado, um comunicador normal será induzido a acreditar que há um pacote legítimo e permanecerá no estado de espera. Por exemplo, se uma transmissão é detectada, um nó permanecerá no modo de espera, independente do fato se o nó tem um pacote para transmitir ou não. Por isso, mesmo se um nó tem pacotes para enviar, ele não pode mudar o estado para enviar porque um fluxo constante de pacotes de entrada será detectado. **3) *Random jammer*:** ao invés de enviar continuamente um sinal de rádio, um *random jammer* alterna entre os estados *sleeping* e *jamming*. Especificamente, após fazer

jamming por t_i unidades de tempo, ele desliga sua transmissão e entra em modo *sleeping*. Ele retomará o *jamming* após ficar em *sleeping* por t_s unidades de tempo. T_j e t_s podem ser valores fixos ou aleatórios. Durante sua fase de *jamming*, o atacante pode se comportar com um *constant jammer* ou um *deceptive jammer.* A distinção entre o *random jammer* e o *constant jammer* e o *deceptive jammer* reside no fato que o *random jammer* tenta levar em consideração a conservação de energia, especialmente para os *jammers* que não têm fonte de energia ilimitada. Ao ajustar os valores que regem a distribuição t_j e t_s podemos alcançar vários níveis de *tradeoff* entre eficiência energética e eficácia de *jamming*. **4) *Reactive jammer*:** os três modelos discutidos acima são *jammers* ativos no sentido de que eles tentam bloquear o canal independente do padrão de tráfego sobre o canal. *Jammers* ativos são usualmente eficazes porque mantém o canal ocupado o tempo todo. Mas, esses métodos são relativamente fáceis de detectar. Uma abordagem alternativa para *jamming* em comunicações sem fio é a de empregar a estratégica reativa. No *jammer* reativo, não é necessário interferir no canal quando ninguém está se comunicando. Ao invés disso, o *jammer* fica quieto quando o canal está ocioso, mas inicia a transmissão de sinal tão logo ele sinta atividade sobre o canal. Como resultado, um *jammer* reativo objetiva primeiro a recepção de uma mensagem. A principal especificidade de um *jammer* reativo é que ele pode ser difícil de detectar.

5 Correlação dos modelos de ataques

Existem alguns ataques que não estão ligados a uma camada específica, mas que podem afetar diversas camadas.

1) Exaustão de bateria: neste ataque, o nó malicioso tem como objetivo consumir a bateria do nó atacado, até que ele fique inativo. De fato, esse ataque pode se aplicar tendo como alvo entidades pertencentes a várias camadas de protocolos. No caso de fazer essa atividade por meio de interferências, trata-se de um problema de camada física. Já se a interferência for gerada com o objetivo de causar retransmissões, trata-se de um problema da camada enlace. O ataque pode também retransmitir mensagens reais de controle da rede, como as de roteamento, dificultando sua detecção e perturbando a visão que as entidades de rede possuem

da topologia, o que as leva a recalcular rotas. A existência de várias versões para o mesmo ataque se justifica pela importância da vida útil da bateria para dispositivos móveis, e, pela mesma razão, várias metodologias para poupar bateria já foram desenvolvidas. Por essa razão também, aplicativos de segurança que exigem do nó a escuta em modo promíscuo são muito criticados, pois a ação de escutar a rede continuamente gasta muita energia do nó, sendo mais recomendado que o nó permaneça em repouso sempre que possível.

2) *Negação de serviço*: o conceito de negação de serviço (DoS) é muito amplo. O ataque de negação de serviço pode ser definido como qualquer ação que reduza ou elimine a capacidade da rede de realizar uma de suas funções esperadas. Assim sendo, a negação de serviço não seria causada apenas por ataques, mas por qualquer evento que prejudicasse a rede, como falhas de hardware, defeitos de programas, exaustão de recursos intencional ou não, condições ambientais não favoráveis ou qualquer interação entre esses fatores. Dessa forma, todos os ataques ativos poderiam gerar uma negação de serviço na rede, o que permite a esses ataques a classificação de multicamadas. Uma forma mais elaborada do ataque é a negação de serviço distribuída. Nesse caso, vários atacantes estão espalhados pela rede fazendo um conluio para impedir que usuários legítimos tenham acesso aos serviços. Esse ataque tem um efeito muito mais rápido sobre a rede, podendo impedir totalmente o seu funcionamento sem grandes dificuldades.

O ataque de negação de serviço pode ser realizado em qualquer camada. Neste artigo abordamos o DoS na camada física e na camada MAC.

a) DoS na camada física: todos os ataques físicos que impedem a rede de exercer as suas funções normalmente são considerados ataques de negação de serviço. Um ataque DoS na camada física é chamado de *jamming*, conforme discutido acima. Um dispositivo malicioso pode efetuar um bloqueio através da transmissão de um sinal de frequência. O sinal *jamming* contribui para o ruído na rede e sua energia é suficiente para reduzir a relação sinal-ruído abaixo do nível necessário que os nodos utilizam no canal para receber os dados corretamente. O *jamming* pode ser realizado em uma

região, impedindo todos os nós dessa região de se comunicarem. O *jamming* pode ser feito temporariamente com intervalos de tempo aleatórios, dificultando a detecção.

b) DoS na camada de Enlace: os algoritmos da camada de enlace apresentam vulnerabilidades aos ataques de DoS: **a) Exaustão de bateria por colisão:** neste ataque, o nó malicioso tem como objetivo consumir a bateria do nó atacado gerando retransmissões continuamente. As retransmissões são geradas por operações de ataque como, por exemplo, ao ouvir o início de uma transmissão, o atacante gerar uma colisão tardia no fim do quadro. Se a colisão intencional for provocada com um pacote de ACK, poderá acarretar em um aumento exponencial do *back-off* em alguns protocolos MAC. O uso repetido causará a exaustão da bateria do nó atacado, pois a transmissão é uma operação onerosa, e que só deve ser feita quando necessário. Uma variação deste ataque é conhecida como o ataque da interrogação. O nó atacante explora características da interação de protocolos da subcamada MAC que utilizam o *Request To Send* (RTS), *Clear To Send* (CTS) e mensagens de dados e ACK. O nó malicioso faz pedidos de alocação do canal com RTS repetidos, forçando inúmeras respostas CTS do nó atacado, levando ambos ao consumo total da bateria. A exaustão de bateria é de difícil tratamento, pois necessariamente a camada de enlace conta com certa confiança entre os nós participantes. Mas também, um nó malicioso tem a possibilidade de negar acesso ao canal repetidamente, impedindo o funcionamento da rede sem ter um grande gasto de energia. Soluções para essa variação de ataque são obtidas pela reformulação dos protocolos, tornando-os mais robustos a comportamentos inadequados. **b) Alteração de ACK:** a maioria dos algoritmos de roteamento confia nos ACKs da camada de enlace. Um atacante pode forjar um ACK com a finalidade de enganar o receptor a respeito de observações como a qualidade do canal, ou ainda dizer que um nó desativado ainda está ativo. Isso implicaria na escolha de rotas por enlaces inapropriados ou passando por nós que não participam mais da rede.

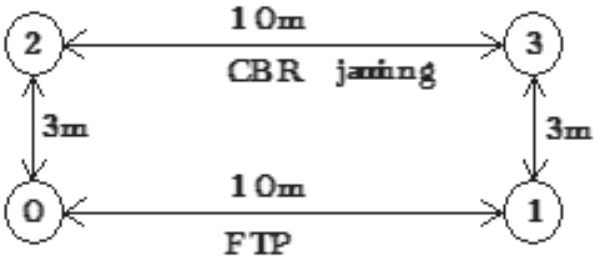
6 Simulação de um ataque *jamming* usando o pacote WPAN do NS2

Neste trabalho, utilizamos os códigos do 802.15.4 (WPAN) do *Network Simulator* NS2 para gerar um *jamming* na camada MAC (ZHENG; LEE, 2006). Para adaptar ao nosso cenário de *jamming,* alteramos os códigos do WPAN desabilitando o sensor de canal e derrubamos as operações da camada MAC de modo que os pacotes possam ser transmitidos e recebidos independente de outras atividades que estejam ocorrendo.

Como o NS só funciona à base de eventos discretos, ou seja, é necessário ter uma conexão para gerar os eventos, utilizamos um cenário com quatro nós para a nossa simulação. Dois desses nós foram configurados para realizar uma transmissão FTP, simulando uma comunicação de dados, e os outros dois nós são usados para aplicar uma taxa CBR variante com o objetivo de interferir na comunicação FTP (*jamming*), já que estará usando o mesmo canal de transmissão.

O objetivo é de analisar a performance da comunicação FTP com a variação do cenário desde o estado não *jamming* até o estado de *jamming* quando a taxa CBR ocupa todos os *time-slots* disponíveis no canal, o que equivale a um comportamento do modelo *deceptive jammer* já descrito anteriormente. Os nós que estão se comunicando estão distantes entre si de 10 metros e entre eles deixamos uma distância de 03 metros para que ocorra a interferência *jamming* nas transmissões, conforme mostra a figura 2 abaixo:

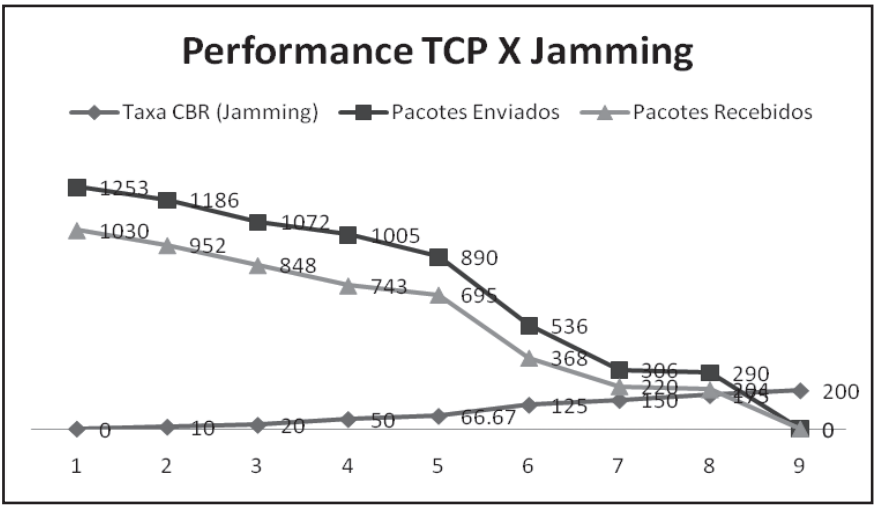
Figura 2 – Diagrama posicional dos nós na simulação



Fonte: do autor.

Com esse arranjo, aplicamos uma simulação de 10 segundos e observamos a evolução da performance com a variação da taxa CBR do *jamming*, conforme Figura 3.

Figura 3 – Relação da Taxa de Pacotes TCP com a variação do *jamming*.



Fonte: do autor.

Observa-se que à medida que o tráfego CBR vai aumentando entre os nós 2 e 3, os pacotes enviados e recebidos vão ligeiramente caindo, afetando a comunicação FTP. Isso porque o tráfego CBR começa a ocupar mais o canal disponível fazendo com que o tráfego FTP comece a encontrar o canal ocupado em alguns tempos de transmissão. Esse processo vai ocorrendo até que a taxa CBR chegue a 200 pacotes por segundo, o que preenche totalmente o canal de transmissão e o FTP acaba não conseguindo mais enviar nenhum pacote.

7 Conclusões

Redes sem fio estão sendo implantadas em uma variedade de formas, especificamente como redes locais *ad hoc* e redes de sensores. A natureza compartilhada do meio sem fio permite a adversários ameaçar a segurança efetuando ataques

de interferência de rádio. O combate aos ataques de *jamming* é essencial para garantir a operação de redes sem fio.

No presente artigo, é explorada a correlação dos modelos de ataques em diversas camadas de protocolos de redes *ad hoc*, em particular com a correlação do *jamming* na camada física com a perda de pacotes em comunicações de dados da camada de aplicação.

O ataque de *jamming* foi implementado por simulação no NS2, na qual alteramos o protocolo 802.15.4 para se adaptar ao estudo de interferência simulado. Esse assunto ainda é de extrema importância para as redes de baixa taxa de transmissão, relacionadas ao protocolo 802.15.4, que explora o baixo custo e economia de energia. Pesquisas que procuram mapear todos os processos de *jamming* tanto em simuladores quanto em dispositivos sensores de testes são de grande importância para o futuro dessas redes.

Este trabalho é uma experiência inicial no sentido de adaptar/melhorar simuladores de redes sem fio de baixa taxa de transmissão para ajudar e facilitar estudos de comportamentos futuros dessas redes. Além disso, constitui uma primeira etapa na criação de mecanismos de defesa que possam lidar com ataques afetando os serviços em múltiplas camadas de protocolos, posto que, como trabalho futuro, será examinada a questão crítica de diagnosticar a presença de ataques *jamming*, no intuito de obter medidas que sirvam como base para detectar um ataque *jamming*, mas também explorar cenários onde cada medida não é suficiente para classificar a presença de um ataque *jamming*, como nos casos em que o congestionamento normal se confunde com o *jamming* em redes de baixo consumo e baixa taxa de transmissão como as redes WPAN. Nesses casos, a correlação com o modelo de ataque em outra camada parece promissora para o diagnóstico correto da situação.

Correlation models of attacks in several layers of protocols for ad hoc networks

Abstract

The wireless has specific vulnerabilities, mainly associated to transmission by air, to the lack of infrastructure and the collaborative routing of messages. In wireless, besides mentioning the conventional attacks, collaborative routing introduces new vulnerabilities and the lack of infrastructure hinders the establishment of simple and efficient defense mechanisms. This article introduces the mainly mechanisms of security used to the protection of attacks, as well as the simulation of a jamming attack in the physical layer using NS2. A jamming attack can be easily made by an adversary sending radio frequency signals that do not follow an underlying MAC protocol. Jamming attacks can be severely interfered with the normal operations of wireless affecting the services in multiple layers of protocols and, therefore, being necessary mechanisms that can deal with these attacks. In this paper, we will examinate these attacks of radio interference and we will study the conduction of attacks from radio interference on these wireless.

Keywords: Ad hoc networks. Models of attacks. Security mechanisms and impacts. Network 802.15.4. Jamming attacks.

Referências

ADNAME, A. et al.. Integrating trust reasonings into node behavior in OLSR, In: ACM INTERNATIONAL WORKSHOP ON QOS AND SECURITY FOR WIRELESS AND MOBILE NETWORKS (Q2WINIT 2007), 3., 2007, Chania. Chania – Grécia, 2007.

ADNAME, A. BIDAN, C. SOUSA JUNIOR, R. T. de. Validation of the OLSR routing table based on trust reasoning. In: INTERNATIONAL WORKSHOP ON TRUST IN MOBILE ENVIRONMENTS (TIME 08): collocated with iTrust/PST, 8., 2008, Trondheim, Norway. *Proceedings…* Trondheim, Norway, 2008.

BELLARDO, J.; SAVAGE, S. 802.11 denial-of-service attacks: real vulnerabilities and practical solutions. In: USENIX SECURITY SYMPOSIUM, 2003, Washington, DC. *Proceedings…* Washington, DC, 2003, p. 15-28.

BUCHEGGER, S.; BOUDEC, J. L. Performance analysis of the confidant protocol: Cooperation of nodes - fairness in dynamic ad-hoc networks. In: IEEE/ACM SYMPOSIUM ON MOBILE AD HOC NETWORKING AND COMPUTING (MobiHOC), 2002, Lausanne, CH. *Proceedings…* Lausanne, CH, 2002.

ERDAL, C.; CHUNMING, R. *Security in wireless ad hoc and sensor networks*. Norway: Hardcover, 2009. ISBN: 0470027487.

CONTI, M.; GREGORI, E.; MASELLI, G. Cooperation issues in mobile ad hoc networks. In: INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS WORKSHOPS., 24., 2004, Tokyo, Japan. *Proceedings*… Tokyo, Japan, 2004. p. 803-808.

CHEN, L.; LENEUTRE, J. *Fight jam with jam*: a game theoretic analysis of jamming attack in wireless networks and defense strategy: technical report, available at: <http://perso.enst.fr/˜lchen/jamming.pdf>. Access on: 08 mar. 2010.

FERNANDES, N. C. et al. Ataques e mecanismos de segurança em redes ad hoc. In: SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS – SBSEG, 2006, Santos, SP. *Minicursos*. Santos, SP, 2006. p. 49-102.

GUANG, L.; ASSI, C. Cross-layer cooperation to handle MAC misbehavior in ad hoc networks. In: 06. CANADIAN CONFERENCE ON ELECTRICAL AND COMPUTER ENGINEERING (CCECE), 6., 2006, Ottawa, Canada. *Proceedings*… Ottawa, Canada , 2006. p. 219-222.

HU, Y. C.; PERRIG, A.; JOHNSON, D. B**.** Ariadne: a secure on-demand routing protocol for ad hoc networks. *Wireless Networks*, Heidelberg, Germany, v. 11, n. 1-2, p. 21-38, nov. 2005.

IEEE. *P802.15.4/D18:* Draft Standard: Low Rate Wireless Personal Area Networks**,** Feb. 2003.

KARGL, F.; KLENK, A.; EBER, S. S. M. *Advanced detection of selfish or malicious nodes in ad hoc networks*: technical report. Ulm, Germany: University of Ulm. Dep. of Multimedia Computing, 2004.

KYASANUR, P.; VAIDYA, N. Detection and handling of mac layer misbehavior in wireless networks. In: IEEE INTERNATIONAL CONFERENCE ON DEPENDABLE SYSTEMS AND NETWORKS, 2003, San Francisco, USA. *Proceedings*… San Francisco, USA, 2003. p. 173-182.

NOUBIR, G.; LIN, G. Low-power DoS attacks in data wireless lans and countermeasures: SIGMOBILE Mob. *Comput. Commun. Rev.*, New York, USA. v. 7, n. 3, p. 29-30, jul. 2003.

PAPADIMITRATOS, P.; HAAS, Z. Secure routing for mobile ad hoc networks. In: SCS COMMUNICATION NETWORKS AND DISTRIBUTED SYSTEMS MODELING AND SIMULATION CONFERENCE, 2002, San Antonio, USA. *Proceedings…* San Antonio, USA, 2002.

PROAKIS, J. G. *Digital communications*. 4. ed. New York, USA:McGraw-Hill, 2000.

RAYA, M.; HUBAUX, J.; AAD, I. Domino: a system to detect greedy behavior in ieee 802.11 hotspots. In: MOBISYS INTERNATIONAL CONFERENCE ON MOBILE SYSTEMS, APPLICATIONS, AND SERVICES, 4., Boston, USA. 2004. Boston, USA: ACM Press, 2004.

SANZGIRI, K. et al. A secure routing protocol for ad hoc networks: In: INTERNATIONAL CONFERENCE ON NETWORK PROTOCOLS (IEEE), 10., 2002, Paris, France.? *Proceedings…* Paris, France, 2002. p. 78-87.

SCHLEHER, C. *Electronic warfare in the information age.* Guernsey: MArtech House, 1999.

SERVICES, 2., 2004, New York, USA . *Proceedings*… New York, USA. ACM Press, 2004. p. 84-97.

WOOD, A.; STANKOVIC, J.; SON, S**.** JAM: a jammed-area mapping service for sensor networks. In: IEEE REAL-TIME SYSTEMS SYMPOSIUM, 24., 2003, Cancun, Mexico: *Proceedings*… Cancun, Mexico, 2003. p. 286-297.

XU, W. et al. *The feasibility of launching and detecting jamming attacks in wireless networks:* ACM MobiHoc. Urbana-Champaign, USA. May 2005.

XU, W.; TRAPPE, W.; ZHANG,Y**.** Channel surfing and spatial retreats: defenses against wireless denial of service. In: ACM WORKSHOP ON WIRELESS SECURITY, 2004, Philadelphia, USA. *Proceedings*… Philadelphia, USA, 2004. p. 80-89.

ZHENG, J.; LEE, M. J. A comprehensive performance study of IEEE 802.15.4: sensor network operations. In: *Wiley Interscience*. Malden, USA. IEEE Press, 2006. p. 218-237. ISBN 0-471-71976-5.

Para publicar na revista Universitas Gestão e TI, entre no endereço eletrônico www.publicacoesacademicas.uniceub.br. Observe as normas de publicação, facilitando e agilizando o trabalho de edição.