Detecção de nós maliciosos em redes de sensores sem fio

Waldir Ribeiro Pires Júnior[1] , **Thiago H. de Paula Figueiredo**[1] *,
Hao Chi Wong[1], **Antonio A.F. Loureiro**[1]

[1]Departamento de Ciência da Computação
Universidade Federal de Minas Gerais
Belo Horizonte, MG

{wpjr,thiagohp,hcwong,loureiro}@dcc.ufmg.br

Abstract. *This work provides a solution to identify malicious nodes in wireless sensor networks through detection of malicious message transmissions in a network. A message transmission is considered suspicious if its signal strength is incompatible with its originator's geographical position. We provide protocols for detecting suspicious transmissions – and the consequent identification of malicious nodes – and for disseminating this information in the network. We evaluate the detection rate and the efficiency of our solution along a number of parameters.*

Resumo. *Este trabalho apresenta uma solução para identificar nós maliciosos em redes de sensores sem fio via detecção de transmissões de mensagens maliciosas em uma rede. Uma transmissão de mensagem é considerada suspeita se sua potência de sinal é incompatível com a posição geográfica de seu originador. São providos protocolos para detectar transmissões maliciosas – e a consequente identificação de nodos maliciosos – e para disseminar esta informação na rede. A taxa de detecção e a eficiência de nossa solução são avaliadas levando-se em conta múltiplos parâmetros.*

1. Introdução

Uma rede de sensores sem fio (RSSF) consiste em um conjunto de dispositivos compactos e automatizados chamados de nós sensores. Um nó sensor é um dispositivo computacional que tem memória, bateria, processador, transceptor e pelo menos um dispositivo sensor. O Berkeley MICA Mote [Hill and Culler, 2001] é um exemplo de nó sensor. Eles são distribuídos em uma área e trocam mensagens entre si, formando uma rede ad-hoc (*Mobile Ad-hoc Network*, MANET). Redes de sensores contêm nós especiais, chamados de sorvedouros (*sinks*), que processam e armazenam as informações coletadas na rede. A comunicação entre dois nós é feita em múltiplos saltos (*hops*) caso eles não estejam um dentro do alcance de transmissão do outro.

RSSFs coletam dados do ambiente no qual elas estão embutidas. Os dados são muitas vezes processados pelos nós sensores e enviados através de canais não seguros para o sorvedoro para processamento posterior. Algumas das aplicações previstas para

*Este trabalho foi realizado com apoio do CNPq.

RSSFs são monitoração ambiental, gerenciamento de infraestrutura e segurança pública. Devido ao seu aspecto crítico, estas aplicações têm uma grande probabilidade de serem atacadas.

Há um grande número de ataques possíveis contra uma RSSF. Um nó malicioso, por exemplo, pode alterar campos de uma mensagem enquanto ela está em trânsito, de forma que o destinatário recebe uma cópia alterada da mensagem original. Pode-se também interferir no *software* ou *hardware* de um nó de modo a alterar seu comportamento. Diferentes tipos de ataques requerem diferentes tipos de medidas de defesa.

Neste trabalho, dois tipos de ataques são focados: ataques de enchente de mensagens HELLO (daqui em diante chamados de ataques de enchente) e de canalização (*wormholes*) [Karlof and Wagner, 2003]. Mensagens HELLO são usadas em muitos protocolos por nós que desejam anunciar sua presença e proximidade a seus vizinhos. A maioria destes protocolos se baseia na premissa de que um nó A está dentro do alcance de transmissão de um outro nó B se A consegue receber mensagens de B. Num ataque de enchente, um nó malicioso pode tentar transmitir uma mensagem com uma potência muito maior de modo que todos ou muitos deles acreditem que ele é seu vizinho.

Ataques de canalização podem ser descritos como a seguir. Um adversário A tunela uma mensagem recebida para um outro nó malicioso B, que está em uma parte distante da rede, utilizando um canal de baixa latência e largura de banda maior. B então retransmite a mensagem exatamente como recebida para os nós em sua vizinhança. Um resultado imediato de um ataque deste tipo é que todos os nós que escutam a transmissão de B são enganados, passando a acreditar que eles são vizinhos do remetente original da mensagem, sendo que este está provavelmente em uma parte distante da rede.

O ataque de enchente e o de canalização podem comprometer o estabelecimento de rotas em uma rede. Por exemplo, quando um nó malicioso envia uma mensagem de roteamento com uma potência muito alta, ele pode fazer com que um grande número de nós tentem utilizá-lo como o próximo salto para o sorvedouro. Mas estes nós estão suficientemente distantes do sorvedouro para que as mensagens nunca cheguem a seu destino. Um cenário similar resulta de um ataque de canalização. Um nó malicioso pode convencer nós que estão a múltiplos saltos do sorvedouro de que eles estão a apenas um salto. Estes nós tentariam enviar suas mensagens diretamente para o sorvedouro, que por sua vez não conseguiria recebê-las.

Neste trabalho, é proposto um mecanismo baseado em potência de sinal e informações geográficas para detectar nós maliciosos que estejam realizando ataques de enchente e de canalização. A idéia é comparar a potência do sinal recebido com o seu valor esperado, calculado utilizando-se de informações geográficas e a configuração do transceptor. Um protocolo para disseminar informações sobre nós maliciosos também é proposto. A taxa de detecção desta solução depende de alguns parâmetros. A correlação entre eles é avaliada através de simulações.

2. Trabalhos relacionados

O nosso trabalho se encaixa na grande área de detecção de intrusos (*Intrusion Detection*, ID). Existe um grande número de soluções de ID em redes fixas (exemplos [Lippmann et al., 2000] e [Debar et al., 1999]). Elas geralmente são baseadas em *logs*

de acesso. Esta característica não permite que ID tradicional seja utilizada em RSSFs, já que a memória de nós sensores é muito limitada para armazenar *logs*.

Em [Zhang and Lee, 2000] é proposto um sistema de detecção para MANETs onde cada nó da rede se comporta como um IDS e os nós cooperam entre si para detectar intrusos. As diferenças entre as RSSF e as MANETs impedem que essa solução seja aplicada diretamente em RSSF já que o nó sensor não será capaz de comportar um IDS completo.

[Marti et al., 2000] propõe, entre outras coisas, uma estratégia para detectar nós que não repassam os pacotes que deveriam em MANETs. Ela funciona da seguinte forma: o nós A é vizinho de B, que por sua vez é vizinho de C. Quando A envia ou encaminha uma mensagem para C através de B, A pode verificar se B realmente repassou a mensagem para C. Se isto não ocorreu, B não está se comportando como deveria, o que pode ser uma indicação de nó malicioso.

O trabalho relacionado mais próximo ao nosso é o de [Hu et al., 2003]. Ele propõe uma medida de prevenção contra ataques de canalização em MANETs. É introduzido o conceito de coleiras de pacote (*packet leashes*), uma espécie de informação adicional adicionada a pacotes normais para restringir sua distância máxima de viagem. Dois tipos de coleiras foram propostos: geográficas e temporais. O primeiro faz com que o receptor de uma mensagem esteja sempre dentro de uma certa distância do nó remetente. O segundo limita o tempo de vida de um pacote. Ambos os tipos dependem de um certo grau de sincronização de relógio entre nós. Como isto requer um grande consumo de recursos, coleiras de pacotes têm uma aplicabilidade muito restrita em RSSFs.

Quanto ao uso de potência de sinal para prover segurança, podemos citar dois trabalhos. [Banerjee and Mishra, 2002] provê um serviço de determinação de localização e autenticação baseado em potência de sinal, permitindo que um grupo determinado de nós móveis possa trocar informações entre si de forma segura. Já [Tao et al., 2003] propõe um sistema de determinação de localização de nós em ambientes fechados. É necessário um treinamento prévio de uma rede de Markov através da medição da potência de sinal em pontos fixos do ambiente.

3. Detecção de nós maliciosos via potência de sinal

Nesta seção é descrito o esquema de detecção de mensagens e nós maliciosos via potência de sinal (*Malicious Node Detection by Signal Strength*, MNDSS)

3.1. O modelo

Neste trabalho supõe-se RSSFs homogêneas (todos os nós da rede têm a mesma configuração de *hardware* e *software*) e simétricas (o nó A só consegue se comunicar com o nó B se B pode se comunicar com A). Também é suposto que os nós sempre têm sua posição geográfica atualizada antes de enviar uma mensagem, tornando assim o esquema aqui proposto também utilizável em redes nas quais os nós não têm posição geográfica fixa. Em particular, os transceptores de todos os nós da rede operam com a mesma configuração por todo o tempo de vida da rede (potência de transmissão, altura da antena e ganho de antena).

Todos os nós têm um identificador único e conhecem sua posição geográfica. Ela pode ser obtida através de um sistema de posicionamento tal como o GPS. A posição geográfica de um nó e seu identificador são incluídos em todas as mensagens enviadas por ele. É suposto que o envio de mensagens da rede é protegido contra a alteração de seus dados, utilizando um mecanismo criptográfico, por exemplo. (Note que apenas mecanismos de chave simétrica podem ser utilizados, dado que os de chave pública são excessivamente caros para o tipo de plataforma considerado.)

Também é suposto que a propagação de rádio segue um modelo definido, tal como o modelo de espaço aberto (*free space model*) ou o modelo Two-Ray Ground [Rappaport, 2002], que especifica como os valores da potência de transmissão, de potência do sinal recebido e da distância entre transmissor e receptor se relacionam entre si. Por exemplo, o modelo de propagação Two-Ray Ground (equação 1) assume que um sinal enviado não é recebido através de um caminho único (uma linha reta), mas também eventualmente através de uma reflexão no solo.

$$P_r = \frac{P_t \times G_t \times G_r \times h_t^2 \times h_r^2}{d^4 \times L} \tag{1}$$

Na equação 1, P_r é a potência do sinal recebido em Watts, P_t é a potência de transmissão, também em Watts, G_t é o ganho de antena do transmissor, G_r é o ganho de antena do receptor, h_t é a altura da antena de transmissão em metros, h_r é a altura da antena de recepção em metros, d é a distância entre o receptor e o transmissor em metros e L é a perda do sistema (uma constante). Um sinal só é detectado por um nó receptor se a potência de sinal recebido P_r é igual ou maior que o limite mínimo de potência de sinal recebido P_m.

É suposto que a potência de um sinal recebido pode ser facilmente obtida do transceptor. O transceptor Chipcon SmartRF CC1000 [Chipcon, 2003], usado na série mais recente dos MICA Motes [Mica2 Radio Stack for TinyOS, 2003], por examplo, tem um pino RSSI (*Received Signal Strength Indicator*, Indicador de Potência de Sinal Recebido) que produz um sinal analógico. Quando a função RSSI está habilitada, a voltagem de saída do pino RSSI é inversamente proporcional à potência do sinal recebido. As fórmulas 2 e 3 especificam a potência do sinal recebido P_r, em dBm, quando o transceptor está operando em 433 MHz e 868 MHz, respectivamente. V_{RSSI} é a voltagem medida no pino RSSI.

$$P_r = -51.3 \times V_{RSSI} - 49.2 \tag{2}$$

$$P_r = -50.0 \times V_{RSSI} - 45.5 \tag{3}$$

Finalmente, é suposto que os nodos maliciosos são capazes de realizar somente ataques de enchente e de canalização.

No que segue, uma transmissão é maliciosa se a posição geográfica incluída na mensagem correspondente foi forjada ou se foi transmitida com uma potência que difere daquela escolhida para todos os nós da rede. Um nó é malicioso se ele envia uma transmissão maliciosa.

Ao receber uma mensagem, um nó pode classificá-la como suspeita ou não suspeita, dependendo se o nó acha que a transmissão é maliciosa ou não. Considerando-se

que esta classificação (suspeita ou não suspeita) é feita localmente, transmissões maliciosas podem não ser classificadas como suspeitas (falsos negativos) e transmissões não maliciosas podem ser classificadas como suspeitas (falsos positivos).

3.2. Detecção de mensagens maliciosas via potência de sinal

No modelo descrito acima, qualquer nó pode obter dois valores em toda transmissão que ele escuta. O primeiro valor é o valor esperado da potência do sinal recebido, que pode ser computado usando-se a potência de transmissão padrão da rede e a distância entre o nó receptor e o nó transmissor. O segundo valor é o valor da potência do sinal recebido detectado no transceptor do receptor.

Num sistema no qual tudo está correndo bem, estes dois valores devem ser bem próximos. Isto não acontecerá caso a rede esteja sob um ataque de enchente ou um ataque de canalização. Este fato é usado para identificar mensagens suspeitas na rede.

No esquema aqui proposto, todas as tranmissões na rede estão sujeitas a verificação: todos os nós monitoram todas as transmissões que eles escutam (ou uma porcentagem definida delas, dependendo da configuração do esquema). O protocolo a seguir é rodado localmente em cada nó sensor. Para cada transmissão que ele escuta, independentemente de ele ser o destinatário da mensagem, o nó compara a potência do sinal recebido com a potência esperada. Quando a diferença entre estes dois valores é maior que um dado limite, a mensagem é considerada suspeita.

Cada nó também mantém uma tabela local contendo a "reputação" de seus vizinhos. Cada entrada contém o identificador do nó, o número de votos dizendo que ele é suspeito e o número de votos dizendo que ele não é suspeito.

Depois de verificar se uma mensagem recebida é suspeita ou não, o nó atualiza sua tabela: se a mensagem é suspeita, ele incrementa o contador de votos dizendo que o nó originador da mensagem é suspeito; se não, tudo continua como está. Note que o originador da mensagem pode ser determinado, já que seu identificador está incluído na mensagem.

Se a mensagem é suspeita, o nó dissemina esta informação entre seus vizinhos. Este protocolo de disseminação é descrito na seção 3.3. Toda mensagem suspeita ou originada de um nó suspeito não é processada.

3.3. Protocolo de disseminação de informações sobre nós suspeitos

Um nó A, rodando o protocolo SNIDP (*Suspicious Node Information Dissemination Protocol*, Protocolo de Disseminação de Informações sobre Nodos Suspeitos), quando detecta uma mensagem suspeita, transmite uma mensagem para todos os seus vizinhos informando-os que o nó S, originador da mensagem suspeita, é suspeito. Esta mensagem também é uma consulta: aqueles que escutam a consulta (por exemplo, o nó B) devem responder dizendo sua opinião sobre S (ele é suspeito ou não?). B determina sua opiniao (e resposta) desta maneira:

- Se B não tem S como seu vizinho, isto é, se B nunca ouviu uma mensagem vinda de S, B responde que S não é suspeito;
- Se B tem S como vizinho, então ele responde dizendo que S é um nó suspeito se o seu número de votos dizendo que S é suspeito é maior que o número de votos dizendo o contrário; caso contrário, responde que S não é suspeito.

O nó A coleciona todas as respostas e atualiza sua tabela de suspeitos: para cada voto dizendo que S é suspeito, ele incrementa o número de votos dizendo que S é suspeito. O mesmo acontece com votos dizendo que S não é suspeito.

Note que a resposta de B, tal como todas as mensagens deste protocolo, será escutada por todos os seus vizinhos, incluindo aqueles que não têm S como vizinho e aqueles que não têm A como vizinho (em outras palavras, nós que não escutaram a transmissão suspeita de S ou não escutaram a mensagem de A dizendo que S é suspeito). Todos eles atualizam suas tabelas de acordo com as mensagens recebidas.

Um ponto importante sobre o protocolo SNIDP é o fato de ele ser executado somente quando uma mensagem suspeita é detectada. A premissa aqui é que, em cirscunstâncias normais (sendo otimista), todas as transmissões não serão suspeitas e assim os nós da rede não precisam trocar mensagens entre si por causa do protocolo. Esta troca é o único custo adicional do SNIDP.

4. Avaliação

Nosso esquema depende de um número de parâmetros. Nesta seção é investigado como variações deles afetam as taxas de detecção. Quatro parâmetros são avaliados neste trabalho: densidade da rede, multiplicador de potência, probabilidade de verificação de mensagem e diferença máxima de quociente.

A densidade da rede determina diretamente o número de vizinhos que um nó pode ter. Dado que a detecção de nó malicioso depende em uma troca de informações entre vizinhos, este parâmetro terá um grande peso na taxa de detecção de nós maliciosos.

O nó malicioso, na maioria das vezes, não tem as limitações de recursos que um nó regular tem. Desta forma, ele poderia enviar mensagens com potência acima da usada por nós regulares, incluindo-se aí a possibilidade de se realizar ataques de enchente. A relação entre o multiplicador de potência M, a potência de transmissão de nodo malicioso P_{tm} e a potência de transmissão de nós regulares P_{tr} é descrita na fórmula 4:

$$M = \frac{P_{tm}}{P_{tr}} \tag{4}$$

Nodos sensores são muito limitados em recursos, existindo um custo para cada mensagem que um nó recebe e verifica. Diminuir o número de mensagens verificadas diminuiria o consumo total de recursos. A probabilidade de verificação de mensagem C determina a probabilidade de uma mensagem recebida ser verificada por quem a escutou. Para cada transmissão, um número c entre 0 e 1, dado por uma variável aleatória uniforme, determinará se o nó verificará a mensagem. Ela será verificada somente se $c < C$.

A diferença máxima de quociente determina o quanto a potência do sinal recebido P_r pode diferir da potência esperada sem que a transmissão seja considedrada suspeita. Este parâmetro é utilizado no tratamento de imprecisões na medida da potência do sinal e no protocolo de localização. Dado um sinal, sua diferença de quociente r é definida pela equação 5:

$$r = 1 - \frac{min(P_r, P_e)}{max(P_r, P_e)} \tag{5}$$

onde $min(a, b) = a$ se $b > a$, caso contrário, $min(a, b) = b$; $max(a, b) = b$ se $b > a$, caso contrário, $max(a, b) = a$. Para cada mensagem que um nó recebe, ela será classificada como suspeita se $r > R$. Este parâmetro é utilizado para se lidar com imprecisões na medida da potência de sinal e no protocolo de localização.

O modelo de propagação de rádio Two-Ray Ground, descrito na seção 3.1, foi o utilizado neste trabalho até agora. A tabela 1 mostra os valores assumidos para parâmetros dos transceptores dos nós regulares [Chipcon, 2003]. Os transceptores de nós maliciosos são aqui simulados como tendo as mesmas configurações excluindo-se a potência de transmissão, que é um dos parâmetros do esquema aqui avaliados.

Potência de transmissão P_t	$3.16e^{-4}$ W
Ganho de antena de transmissão G_t	1.0
Ganho de antena de recepção G_r	1.0
Altura da antena de transmissão h_t	0.05 m
Altura da antena de recepção h_r	0.05 m
Limite mínimo de potência de sinal recebido P_m	$3.98e^{-14}$ W
Perda de sistema L	1.0

Tabela 1: Parâmetros de nós regulares

São considerados dois tipos de cenários nesta avaliação: focado e não focado. No cenário não focado, todos os nós, incluindo-se o malicioso, são ligados ao mesmo tempo e enviam uma mensagem HELLO cada. Nodos maliciosos enviam suas mensagens com uma potência diferente daquela utilizada em nós regulares, porém sem regulá-la para enganar algum nó em particular (razão pela qual este cenário é chamado de não focado). A potência de transmissão do nó malicioso é igual à potência de transmissão de nós regulares multiplicado pelo multiplicador de potência. Este cenário modela casos em que o nó malicioso consegue estar presente durante a instalação e inicialização da rede.

No cenário focado, o nó malicioso inicia suas atividades depois que a rede foi instalada e iniciada. Isto é, o nó malicioso só transmite alguma mensagem depois que todos os membros da rede já foram ligados e já enviaram mensagens HELLO. Neste caso, o nó malicioso escolhe uma vítima (razão pela qual este cenário é chamado de focado), escolhe uma posição dentro do alcance de rádio da vítima e regula sua potência de transmissão de modo que ela não consiga detectar que a transmissão é maliciosa. O valor que deve ser utilizado pelo nó malicioso para poder enganar sua vítima pode ser facilmente calculado a partir da fórmula 1.

O esquema é avaliado através de simulação.

5. Simulação e resultados

5.1. Modelo de simulação

Foi desenvolvido um simulador de RSSFs sem fio para avaliar este trabalho. É um simulador de eventos discretos escrito em Java.

Também foi construído um gerador de RSSFs. Para este trabalho, elas são compostas de n nós mais um nó malicioso, todos localizados em um campo quadrado de di-

mensões $L \times L$. Cada nó tem coordenadas x e y escolhidas aleatoriamente. Em nenhum caso dois nós compartilham as mesmas coordenadas. Redes com $50, 100, 150, \ldots, 500$ nós em campos de 179 m $\times$ 179 m foram geradas e utilizadas como entrada para o simulador. Para cada rede com um dado número de nós, 200 diferentes topologias foram criadas. Como cada rede utilizada aqui está num campo de 179 m $\times$ 179 m, a densidade da rede pode ser medida em número de nós. O número médio v de vizinhos por nó pode ser obtido com uma boa aproximação através da fórmula $v = 0,02 \times n$, onde n é o número de nós.

Cada arquivo de entrada gerado foi executado em ambos os cenários (focado e não focado) com diferentes combinações de valores para cada um dos parâmetros. Cada parâmetro tem um intervalo de valores que ele pode assumir (vide tabela 3), um dos dos quais é o valor padrão (vide tabela 2). Em cada execução da simulação o valor de um parâmetro é variado enquanto é utilizado o valor padrão dos outros três parâmetros.

Parâmetro	**Valor padrão**
Densidade da rede	200 nós num campo de 179 m $\times$ 179 m
Multiplicador do nó malicioso	2
Diferença máxima de quociente	0.3
Probabilidade de verificação de mensagem	1.0

Tabela 2: Valores padrão de parâmetros

Parâmetro	**Valores utilizados**
Densidade da rede	50, 100, . . ., 500 nós
Multiplicador do nó malicioso	1.1, 1.2, . . ., 2.0
Máxima diferença de quociente	0.1, 0.2, . . ., 1.0
Probabilidade de verificação de mensagem	0.1, 0.2, . . ., 1.0

Tabela 3: Valores utilizados para os parâmetros

No cenário não focado, foram executadas 200 diferentes simulações para cada combinação de parâmetros, uma para cada topologia de rede gerada. No cenário focado, foram executadas cinco simulações para cada topologia de rede. Em cada simulação, o nó malicioso utiliza um diferente nó como vítima.

5.2. Resultados

Nesta seção são apresentados e discutidos os resultados obtidos até agora. Todos os valores nos gráficos são o valor médio coletado em múltiplas execuções para um dado conjunto de valores utilizados nos parâmetros. Em cada caso, é investigada a taxa de detecção de mensagens maliciosas (razão entre o número de mensagens recebidas consideradas maliciosas e o número total de recepções de mensagens maliciosas) e também a taxa de detecção de nós maliciosos (razão entre o número de nós que detectaram o nó malicioso e o número de nós que poderiam detectá-lo). Nos gráficos, a sigla TD significa taxa de detecção.

Como esperado, nenhuma transmissão não maliciosa foi considerada suspeita.

5.2.1. Taxa de detecção vs. densidade da rede

Na figura 1 é mostrado como a taxa de detecção de mensagens maliciosas se correlaciona com a densidade da rede. Nossas simulações mostram que os resultados são praticamente similares para os dois cenários. No caso não focado, todas as mensagens maliciosas recebidas são consideradas suspeitas. No cenário não focado, uma pequena fração de recepções de mensagens maliciosas não é classificada como suspeita. Isto acontece porque em cada transmissão o nó vítima é realmente enganado.

Raramente algum outro nó também é enganado. Isto acontece apenas quando o nó vítima e o outro nó enganado têm praticamente a mesma distância para a posição falsa na qual o nó malicioso diz que está e praticamente a mesma distância para a posição real do nó malicioso.

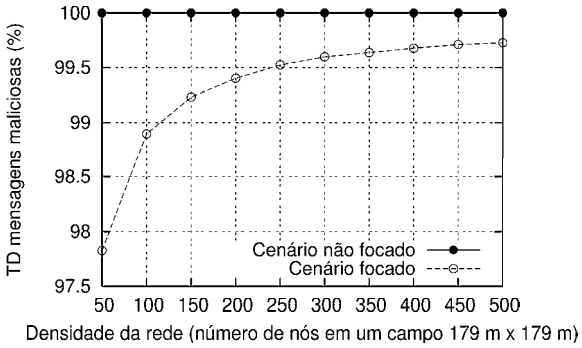

Figura 1: Porcentagem de recepções de mensagens maliciosas detectadas vs. densidade da rede

Em ambos os cenários, todos os nós que estão no alcance de rádio do nó malicioso escutam suas transmissões e, utilizando o protocolo SNIDP, conseguem concluir que ele é suspeito. Este resultado é válido para todas as densidades de rede consideradas. Dada a uniformidade deste resultado, o gráfico correspondente é omitido aqui.

5.2.2. Taxa de detecção vs. multiplicador de potência

A taxa de detecção de mensagens maliciosas e o multiplicador de potência (somente utilizado no cenário não focado) têm uma correlação simples entre si: se o multiplicador é acima de aproximadamente 1.43, todas as recepções de mensagens maliciosas são consideradas suspeitas; caso contrário, nenhuma delas é detectada.

5.2.3. Taxa de detecção vs. diferença máxima de quociente

Os resultados sobre a diferença máxima de quociente estão nas figuras 2 e 3. O impacto deste parâmetro nos dois cenários é praticamente igual. No cenário focado, a taxa de detecção de mensagens e de nós suspeitos é 100% quando a diferença máxima de quociente é igual ou menor que 0.4. Para o cenário focado, a taxa é um pouco menor que 100% para as mesmas condições. Para valores deste parâmetro acima de 0.4, transmissões maliciosas não são mais detectadas como suspeitas.

Este esquema de detecção de nós maliciosos não apresenta grandes requisitos no *hardware* sendo utilizado. O protocolo trabalha bem mesmo quando a diferença máxima de quociente é utilizada com valores até 0.4, como mostrado na figura 3.

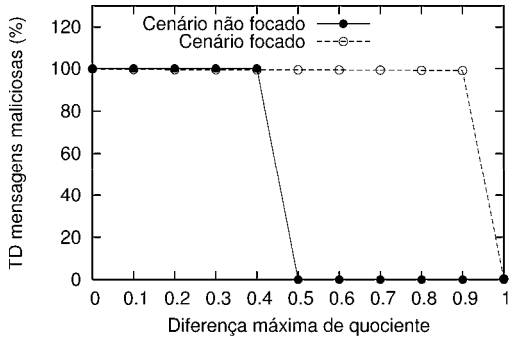

Figura 2: Taxa de detecção de mensagens maliciosas vs. diferença máxima de quociente

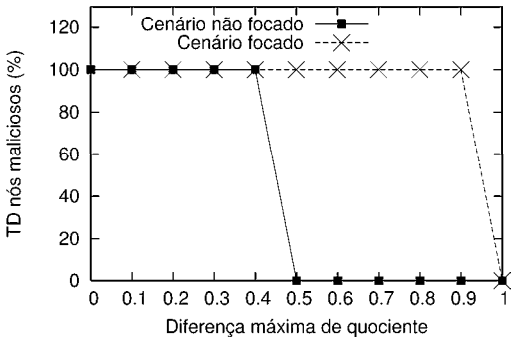

Figura 3: Taxa de detecção de nó malicioso vs. diferença máxima de quociente

5.2.4. Taxa de detecção vs. probabilidade de verificação de mensagem

Os resultados sobre a probabilidade de verificação de mensagens são mostrados na figura 4. Nestes experimentos, os nós da rede não verificam todas as transmissões escutadas. Ao invés disso, eles fazem a verificação com uma dada probabilidade definida por este parâmetro. Os resultados obtidos mostram que, no cenário não focado, uma probabilidade de verificação de mensagens de 0.7 garante uma detecção de nós maliciosos próxima de 90%. Isto mostra que não é necessário para um nó verificar todas as transmissões escutadas para ter uma boa taxa de detecção de nós maliciosos. Enquanto isso, no cenário focado, a taxa de detecção é de 100% em todos os casos.

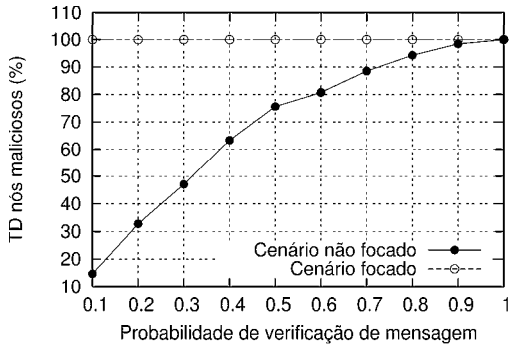

Figura 4: Taxa de detecção de nó malicioso vs. probabilidade de verificação de mensagem

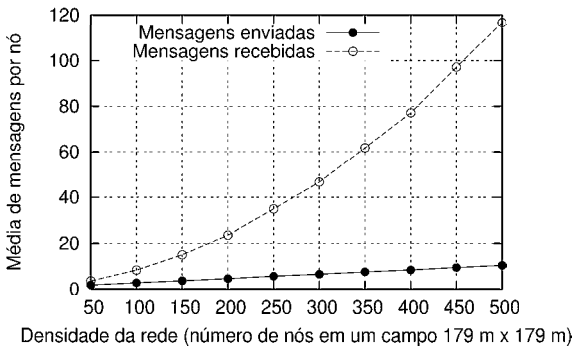

Figura 5: Número médio de recepções e mensagens recebidas vs. densidade da rede

5.2.5. Custo do SNIDP

A figura 5 mostra o número médio de transmissões e recepções de mensagens por nodo no cenário focado. Estes valores são restritos a trocas de mensagens requeridas pelo proto-

colo SNIDP quando mensagens suspeitas são detectadas. Estes valores são razoavelmente altos considerando-se as limitações de recursos de nós sensores, especialmente em termos de consumo de energia. A eficiência não estava no nosso foco durante o desenvolvimento deste protocolo: a preocupação inicial era implementar uma versão simples que pudesse funcionar corretamente.

6. Conclusões

Este esquema de detecção detecta ataques de enchente pois um nó malicioso S só pode enganar um nó N de cada vez utilizando-se do envio de uma mensagem na qual ele indica uma posição geográfica falsa e ajustando a potência de transmissão de forma adequada. Entretanto, a maioria dos vizinhos de N vai detectar esta transmissão maliciosa e disseminar esta informação entre seus vizinhos. Através deste mecanismo, N também descobrirá que S é malicioso. O esquema aqui proposto também detecta ataques de canalização porque mensagens que viajaram além do alcance de rádio do nó de origem são naturalmente descartadas, já que a diferença entre a potência recebida e a esperada do sinal será grande.

Ele pode ser facilmente integrado em outros protocolos. Ele se comunicaria com o resto do sistema através de uma interface de *software* que responde se um determinado nó ou mensagem são considerados suspeitos ou não. O MNDSS e o SNIDP não têm requisitos pesados sobre o *hardware* utilizado. Dispositivos de baixa precisão podem ser usados, já que este esquema trabalha bem mesmo com valores relativamente altos de diferença máxima de quociente.

O consumo de energia é diretamente correlacionado com o número de verificações de mensagens e o número de transmissões e recepções de mensagens ocorridas por causa da execução do SNIDP. Em relação ao número de verificações de mensagens, os resultados mostram que não é necessário que os nós chequem todas as transmissões escutadas para obter uma boa taxa de detecção de nós maliciosos. Em se tratando do número de transmissões e recepções de mensagens, o SNIDP ainda não foi otimizado e assim este número pode definitivamente ser reduzindo sem comprometer a eficiência do protocolo.

7. Trabalhos futuros

Vários aspectos deste trabalho podem ser objetos de trabalhos futuros. Um deles é a utilização de outros modelos de propagação de rádio e o seu impacto sobre as taxas de detecção. O modelo Two-Ray Ground não modela perda de potência de sinal devido a obstáculos, condições do tempo, interferência, etc. Um possível modelo a ser utilizado é o de sobreamento (*shadowing model*) [Rappaport, 2002]. Além dos estudos de simulação, este trabalho se beneficiaria muito com a comparação dos resultados com medidas de campo.

Podemos também melhorar o protocolo SNIDP. Outras versões podem ser sugeridas, abordando aspectos tais como número de mensagens trocadas, aumento de eficiência ou proteção contra outras formas de ataque contra a rede ou contra o próprio protocolo.

Outro trabalho futuro é a elaboração e implementação de novos cenários, modelando outras formas de ataque a RSSFs e aos protocolos aqui propostos. Em particular,

seria interessante relaxar o modelo de confiança, e permitir que nós maliciosos emitem opiniões enganosas quando da participação do protocolo SNIPD.

Neste trabalho, não são simuladas imprecisões na obtenção da posição geográfica. Deste modo, é muito importante estudar o impacto da precisão da localização nos resultados do MNDSS e do SNIDP. Este estudo nos permitiria saber como estes protocolos se comportariam se usados com diferentes formas de obtenção de posição geográfica propostas para RSSFs.

Outro aspecto a ser estudado é o impacto das camadas física e de enlace utilizadas em redes de sensores sem fio sobre a eficiência do SNIDP.

Referências

Banerjee, S. and Mishra, A. (2002). Secure spaces: location-based secure wireless group communication. *Mobile Computing and Communications Review*, 1(2).

Chipcon (2003). SmartRF CC1000 single chip very low power RF transceiver. http://www.chipcon.com/files/CC1000_Data_Sheet_2_1.pdf.

Debar, H., Dacier, M., and Wespi, A. (1999). Towards a taxonomy of intrusion-detection systems. *Computer Networks*, 31(9):805–822.

Hill, J. and Culler, D. (2001). A wireless embedded sensor architecture for system-level optimization. Technical report, University of California, Berkeley.

Hu, Y.-C., Perrig, A., and Johnson, D. B. (2003). Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)*.

Karlof, C. and Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *First IEEE International Workshop on Sensor Network Protocols and Applications*.

Lippmann, R., Fried, D., Graf, I., Haines, J., Kendall, K., McClung, D., Weber, D., Webster, S., Wyschogrod, D., Cunningham, R., and Zissman, M. (2000). Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation. In *Proceedings of the DARPA Information Survivability Conference and Exposition*, Los Alamitos, CA. IEEE Computer Society Press.

Marti, S., Giuli, T. J., Lai, K., and Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In *Mobile Computing and Networking*, pages 255–265.

Mica2 Radio Stack for TinyOS (2003). http://webs.cs.berkeley.edu/tos/tinyos-1.x/doc/mica2radio/CC1000.html.

Rappaport, T. S. (2002). *Wireless communications: principles and practice*. Prentice Hall, 2nd edition.

Tao, P., Rudys, A., Ladd, A. M., and Wallach, D. S. (2003). Wireless lan location-sensing for security applications. In *Proceedings of the ACM Workshop on Wireless Security*, San Diego, CA.

Zhang, Y. and Lee, W. (2000). Intrusion detection in wireless ad-hoc networks. In *Mobile Computing and Networking*, pages 275–283.