Detecção de Intrusos por Rotas Redundantes em RSSF

Wellington P. de Paula[1], **Sérgio de Oliveira**[1], **José Marcos Nogueira**[1], **Hao Chi Wong**[1]

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

{wpassos, sergiool, jmarcos, hcwong}@dcc.ufmg.br

Abstract. *Several types of attacks can be launched in wireless sensor networks (WSN). Some factors make the WSN more vulnerable to enemy action than the conventional networks: limited computer resources, hostile environment and wireless communication. This paper presents a mechanism for protection of WSN against some denial of service attacks in routing, like black hole and selective forwarding. This mechanism is able to detect intruders that promote these attacks, using alternative routes.*

Resumo. *Vários tipos de ataques podem ser executados em redes de sensores sem fio (RSSF). Alguns fatores fazem as RSSF mais vulneráveis à ação do inimigo que as redes convencionais: recursos de computação limitados, ambientes hostis e comunicação sem fio. Este artigo apresenta um mecanismo para a proteção de RSSF contra alguns ataques de negação de serviço no roteamento, como buraco negro e reenvio seletivo. Este mecanismo é capaz de detectar intrusos que promovem estes tipos de ataques, usando rotas alternativas.*

1. Introdução

RSSF têm surgido como uma proposta para diversos tipos de aplicações. Devido às restrições computacionais, um dos principais desafios que surgem é como garantir requisitos mínimos de segurança no envio dos dados dos nós para a estação base.

Este trabalho propõe o uso de rotas múltiplas para realizar a detecção de nós intrusos. Como as rotas criadas são usadas alternadamente, não há replicação de informações, o que faz com que o protocolo seja eficiente quanto à energia consumida. Com a adição de rotas alternativas, torna-se possível a descoberta de rotas que não entregam seus pacotes corretamente, através da análise das mensagens enviadas pelos nós à estação base.

Os nós intrusos atuam lançando diversos tipos de ataques. Este trabalho está interessado em ataques que promovem negação de serviço no roteamento. Nesse tipo de ataque, parte da rede fica em silêncio ou apenas parte das mensagens é entregue.

Nas próximas seções serão apresentadas as formas de estabelecimento das rotas múltiplas, distribuição dos pacotes entre essas rotas, aprendizagem da topologia da rede pela estação base e o algoritmo utilizado para detecção de intrusos.

2. Metodologia

2.1. Estabelecimento das Rotas Múltiplas

O trabalho desenvolvido tem como base o protocolo conhecido como *Tiny OS beaconing* [Karlof and Wagner 2003]. Esse método é baseado no uso de um *beacon*, enviado em modo de difusão pela estação base. Cada nó determina qual dos seus vizinhos será o próximo salto em direção à estação base a partir da recepção do *beacon*. Para a criação

de rotas múltiplas, o nó deve estabelecer mais rotas além daquela originada no nó que enviou o *beacon* primeiro. Assim, a segunda rota é estabelecida a partir do segundo nó vizinho que repasse o *beacon*. A rota criada após a recepção do primeiro *beacon* será tratada como rota padrão, enquanto que a outra será tratada como rota alternativa.

O algoritmo de roteamento dos nós deve tratar de forma diferente as mensagens originadas no nó e aquelas que estão apenas sendo repassadas. No primeiro caso, as duas rotas serão usadas de forma alternada. Já no segundo, apenas a rota padrão será utilizada.

2.2. Distribuição entre as rotas

Cada nó tem opções de destinos que podem ser usados para o envio das informações até a estação base. A escolha do caminho a ser seguido deve levar em consideração alguns requisitos, vislumbrando a detecção e o isolamento dos intrusos:

- O volume de dados deve ser equilibrado entre as duas rotas. Dessa forma, grandes diferenças entre suas taxas de perdas podem indicar a presença de um intruso;
- Não deve ser possível para o intruso conhecer a distribuição de pacotes entre elas;
- A estação base e o nó devem conhecer a priori qual rota deve ser usada para cada informação a ser enviada. Assim, na ausência de uma informação, a estação base sabe de onde deveria ter sido originada.

O uso de uma função pseudo-aleatória, baseada em uma semente pré-distribuída junto aos nós sensores, pode permitir a distribuição entre as rotas alternativas garantindo os requisitos exigidos. Essa função permite que seja imprevisível para o inimigo qual a rota a ser escolhida no envio de um pacote. O conhecimento da semente permite que a estação base conheça o caminho escolhido para o envio da mensagem.

A rota deve ser marcada em cada pacote para que a estação base conheça a origem da informação. Como a estação base conhece a rota que os pacotes devem tomar, a marcação dos pacotes permite à estação base avaliar a disponibilidade em cada rota.

2.3. Conhecimento da Topologia

Para identificar os intrusos, a estação base deve conhecer a topologia da rede. Mecanismos de conhecimento da topologia já estão disponíveis, como em [Staddon et al 2002].

Neste trabalho, para que a estação base possa aprender a topologia da rede, cada nó deve enviar uma mensagem indicando todos os seus vizinhos, ou seja, os nós alcançáveis diretamente e quais desses nós são os responsáveis pelas suas duas rotas.

Após receber essa informação, a estação base é capaz de construir e manter um grafo indicativo da conectividade com as rotas estabelecidas pelos nós.

Na adição de novos nós, o processo é o mesmo utilizado anteriormente, porém, a comunicação desses nós com a estação base só será possível após a atualização do roteamento, o que acontece em intervalos de tempo regulares.

2.4. Detecção de Intrusos

Para que seja possível para a estação base descobrir a existência de um nó sensor intruso são necessárias comparações entre o número de mensagens esperadas provenientes de cada nó e o número de mensagens efetivamente recebidas.

Assim, a partir das informações acima, mais o grafo de conectividade da rede, é possível propor um algoritmo para identificar a presença de intrusos. O algoritmo é

recursivo, partindo da estação base em direção aos nós folha no grafo. O resultado de sua execução é a marcação de nós com falha e de possíveis intrusos. Como o efeito da falha é o mesmo do ataque do tipo buraco negro eles serão tratados da mesma forma. Já os ataques do tipo reenvio seletivo, onde um nó envia suas mensagens mas não repassa mensagens de outros nós ou repassa apenas uma pequena parte das mensagens, podem ser distinguidos de falhas intermitentes pelo percentual de perdas na rota, pois, para que um ataque possa ser efetivo, ele deve ter altas taxas de perdas.

Em sua inicialização, o algoritmo calcula as perdas em cada uma das rotas dos nós da rede, além de inicializar as variáveis e chamar a função de detecção de intrusos a partir da estação base. Essa função é mostrada no algoritmo 1.

Cada execução do algoritmo 1 tem um nó em foco, na variável X. Esse algoritmo pode ser dividido em 3 partes: verificação das perdas nos vizinhos de X que o utilizam como rota padrão, verificação das perdas nos vizinhos que usam X como rota alternativa e a chamada da função, recursivamente, para os vizinhos que utilizam X como rota padrão.

Caso X seja um nó intruso, seus vizinhos devem apresentar taxas altas de perdas na rota que passa por ele. O mesmo não deve acontecer na outra rota. As duas primeiras partes do algoritmo 1 verificam a diferença entre as perdas das duas rotas. Caso exista uma diferença grande entre essas perdas, o nó é um provável intruso. Para possibilitar uma maior exatidão nessa identificação, nós suspeitos recebem uma pontuação que é incrementada sempre que houver a possibilidade do nó ser um intruso. Essa pontuação representa a extensão do seu ataque, pois ela será proporcional à abrangência do mesmo.

A partir do momento que um nó intruso é identificado, todos os indícios de intrusão percebidos nas rotas que dependem desse nó são associados a ele. Essa associação é realizada na terceira parte do algoritmo. Se um nó intruso já foi identificado, o segundo parâmetro da função *Detecta intruso* recebe o nó identificado como intruso. Se esse parâmetro estiver assinalado, então os indícios de intrusos são associados a esse nó.

2.5. Isolamento dos Nós Instrusos

Após a identificação dos instrusos, a estação base deve promover o isolamento destes nós, com as seguintes ações:

- Envio de mensagem informando a presença do intruso e seu devido isolamento;
- Atualização do roteamento, excluindo os intrusos. Isso pode ser feito com o envio do *beacon* desde que os vizinhos já os conheçam.

Esta última fase pode incluir a geração e envio de novas chaves aos nós sensores que dependem destas para comunicação.

3. Implementação

O trabalho aqui descrito está sendo desenvolvido no *network simulator (ns)*. O protocolo com rotas redundantes foi implementado e, através de experimentos, ficou comprovado que ele realmente não é mais caro em termos de energia que o *Tiny Os Beaconing*.

Os próximos passos no desenvolvimento do trabalho são:

1. Implementação de um protocolo que defina os intrusos na rede. Tais nós terão a função e prover os ataques de negação de serviço;
2. Implementação do algoritmo de detecção de instrusos acima descrito;
3. Testes exaustivos no sentido de verificar o funcionamento correto desse algoritmo.

Detecta intruso (Nó X, Nó Intruso, Pontos do Intruso)

1. *Para cada nó I, vizinho de X que o utiliza como rota padrão:*
   (a) *Se Perda padrão (I) $\gg$ Perda alternativa (I) então*
      i. *Se Pontos do Intruso = 0 então*
         Intruso $\longleftarrow$ X;
      ii. *Incrementa Pontos do Intruso;*
   (b) *Se Perda padrão (I) = Perda alternativa (I) = 100% então*
      i. *Marcar I como Falha;*
2. *Para cada nó I, vizinho de X que o utiliza como rota alternativa*
   (a) *Se Perda alternativa (I) $\gg$ Perda padrão (I) então*
      i. *Se Pontos do Intruso = 0 então*
         Intruso $\longleftarrow$ X;
      ii. *Incrementa Pontos do Intruso;*
3. *Para cada nó I, não marcado como falha, vizinho de X que o utiliza como rota padrão:*
   (a) *Se Pontos do Intruso = 0 então*
      i. *Detecta intruso(I, Intruso, Pontos do Intruso);*
      ii. *Se Pontos do Intruso $\neq$ 0 então*
         Marcar Intruso e Pontos do Intruso;
         Pontos do Intruso $\longleftarrow$ 0;
         Intruso $\longleftarrow$ vazio;

Algoritmo 1 - Detecção de intrusos

4. Trabalhos Relacionados

Vários trabalhos, como [Karlof, Li and Polastre 2002], [Deng, Han and Mishra 2003] abordam o uso de rotas múltiplas em RSSF. Tais rotas podem ser usadas de forma redundante ou alternada. Rotas usadas de forma redundante adicionam tolerância à falhas, porém aumentam o consumo de energia com a replicação de informações. O uso de rotas de forma alternada foi escolhido para manter o consumo de energia bem próximo daquele verificado sem os mecanismos de segurança.

O trabalho proposto por [Staddon et al 2002] identifica nós silenciosos que podem estar com falhas ou sem comunicação, devido a problemas em outros nós. Caso estejam sem comunicação por causa de outros nós, a comunicação é restabelecida através da criação de novas rotas. Não são levadas em consideração, nesse trabalho, as características diversas dos ataques. Apenas são identificados os nós que não enviam informações à estação base. Nesse caso, ataques como reenvio seletivo não poderiam ser detectados.

O trabalho proposto neste artigo é mais abrangente, pois possibilita que um nó sujeito a um ataque consiga enviar informações por uma rota alternativa, indicando que não existe falha nesse nó e sim a presença de um intruso que inibe o roteamento.

Referências

Karlof, C. and Wagner, D. (2003). *Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures*. on appear First IEEE International Workshop on Sensor Network Protocols and Applications, May.

Staddon, J., Balfanz, D, and Durfee, G. (2002). *Efficient Tracing of Failed Nodes in Sensor Networks*. Atlanta, Geórgia, USA.

Karlof, C., Li, Y., and Polastre, J. (2002). *ARRIVE: Algorithm for Robust Routing in Volatile Environments*. Technical Report UCB/CSD-03-1233, University of California.

Deng, J., Han, R. and Mishra,S. (2003). *INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks*. Poster paper - In the 23rd IEEE International Conference on Distributed Computing Systems , Providence, RI.