Aspectos de Detecção de Intrusos em Redes de Sensores sem Fio

Ana Paula Ribeiro da Silva , Fernando Augusto Teixeira, Hao Chi Wong , José Marcos S. Nogueira *

[1]Departamento de Ciência da Computação – Universidade Federal de Minas Gerais
Caixa Postal 702 – 30123-970 Belo Horizonte, MG, Brasil

{anapaula, teixeira, hcwong, jmarcos}@dcc.ufmg.br

Abstract. *Given their distinghishing characteristics, Wireless Sensor Networks (WSNs) require tailored intrusion detection systems. However, their design and implementation are challenging because of the resource constraints. In this paper, we take the first steps in characterizing a model for intrusion detection in WSNs, propose a modular, extensible and reconfigurable arquitecture for intrusion detection systems in these networks, and identify sources of hidden costs in deployments of such systems.*

1. Introdução

As Redes de Sensores Sem Fio (RSSFs) [Estrin et al., 2000] possuem características que as tornam altamente vulneráveis a ataques [Karlof and Wagner, 2003, Wood and Stankovic, 2002]. Além das conhecidas vulnerabilidades associadas à comunicação sem fio e organização ad-hoc, as RSSF são usualmente depositadas em áreas abertas e desprotegidas, muitas vezes hostis. Pode-se proteger as RSSF contra alguns tipos de ataques utilizando-se mecanismos preventivos, por exemplo métodos criptográficos, ou utilizar estratégias para tolerar intrusos [Deng et al., 2003]. Existem, entretanto, ataques para os quais não são conhecidos mecanismos de prevenção ou que não podem ser tolerados sob a pena de desperdiçar os recursos da rede ou de comprometer sua segurança. Tudo isso justifica a necessidade de desenvolver-se um Sistema de Detecção de Intrusos (*Intrusion Detection System* - IDS) para RSSFs.

Muitos trabalhos já foram desenvolvidos a respeito de IDSs, a maioria projetados para rede tradicionais [Debar et al., 1999] mas alguns projetados para redes ad-hoc [Zhang and Lee, 2000]. Os IDSs existentes não são diretamente aplicáveis às RSSF, nem mesmo aqueles projetados para redes que possuem recursos escassos, como as redes ad-hoc, pois as RSSF não dispõem dos mesmos recursos disponíveis naquelas redes.

Neste trabalho, procuramos investigar a questão dos IDSs para RSSF. Acreditamos ter dado o primeiro passo na caracterização de um modelo para detecção de intrusos em RSSF e propomos uma arquitetura modular e expansível que pode ser configurada de acordo com as particularidades da rede alvo. Além disso, levantamos as fontes de custo adicional para a implantação do sistema, assim como os serviços e pré-requisitos necessários. De acordo com nossas pesquisas, este é o primeiro trabalho sobre sistemas de detecção de intrusos em RSSF.

*O presente trabalho foi realizado com apoio do CNPq, uma entidade do Governo Brasileiro voltada ao desenvolvimento científico e tecnológico. 55.2111/2002-3

2. Modelo

Em qualquer IDS é preciso que se delimite os traços ou as características do sistema a ser monitorado, de onde se possa extrair informações sobre seu comportamento. A observação do comportamento do sistema pode levar à identificação de ações anômalas ou suspeitas de forma a caracterizar um indício de intruso. O modelo de uma RSSF para fins de detecção de intrusos consiste, então, na definição dos traços a serem monitorados e na caracterização de seu comportamento.

Alguns exemplos de traços que podem ser monitorados são a taxa de utilização da memória dos nós, o formato e o conteúdo das mensagens recebidas e o número de vizinhos de nó específico. Um intruso pode querer, por exemplo, consumir toda a memória disponível para causar algum tipo de negação de serviço (*Denial of Service - DoS* [Wood and Stankovic, 2002]) ou erros em algum protocolo. Ele poderá fazer isso enviando pacotes muito grandes ou agentes executáveis que rodem no nó e consumam toda a sua memória. Considerando que haja um padrão de utilização de memória considerado normal, a utilização da memória pode nos dar indícios de intrusos. Nos ataques de canalização e *hello flood* [Karlof and Wagner, 2003], o intruso utiliza transmissores potentes para levar uma mensagem de um extremo a outro da rede com uma baixa latência com o objetivo de comprometer o roteamento. Em redes onde a comunicação é vizinho a vizinho, receber uma mensagem de um nó que não seja vizinho é indício de intruso. Isso pode ser verificado no remetente da mensagem recebida, considerando que cada nó conhece seus vizinhos. Nesses ataques, o intruso pode ser detectado também pela potência do sinal recebido. [PiresJr et al., 2004]

Outros traços podem ser monitorados através de testes ou interrogação de nós da rede. Por exemplo, pode ser requisitado a um nó individual informações sobre sua identificação, localização, seu nível de energia e consumo de memória. Testes mais interessantes e abrangentes podem ser realizados sobre um conjunto de nós, por amostragem (por exemplo, 80% dos nós), sobre nós selecionados por hierarquia (por exemplo, apenas os líderes de grupos, ou apenas os nós pertencentes a um grupo de um líder específico), ou, até mesmo sobre a rede inteira. Podemos requisitar a um grupo de nós, a sua localização, distribuição hierárquica, distribuição do roteamento, entre outras coisas, para a formação de mapas com informações globais sobre a rede. O ataque de *sibyl* [Karlof and Wagner, 2003], por exemplo, pode ser identificado através de alterações no mapa de localização dos nós em redes estáticas. Outros indícios de intrusos podem ser detectados se o decaimento da energia ocorrer de uma forma anômala ou não esperada. Isso pode ser avaliado de uma forma global pelo nó requisitante através do armazenamento de mapas de energia.

Indícios de Intrusos considerados de forma isolada não identificam necessariamente um intruso. Eles podem estar relacionados, por exemplo, a um erro de configuração, um erro dos protocolos utilizados na rede ou a influência do próprio meio, sem que haja nenhuma tentativa de invasão. Para que possamos concluir sobre a presença de um intruso, os indícios devem ser relacionados de forma a nos dar um resultado preciso e completo.

3. Arquitetura

Ao se pensar em um sistema de detecção de intrusos para RSSF, deve-se levar em conta o compromisso entre a necessidade de segurança da aplicação e a escassez de recursos deste tipo de rede. Para endereçar essa questão de forma eficaz, a rede alvo precisa ser conhecida e o IDS precisa ser adaptado para suas necessidades. Tendo em vista o dinamismo e as limitações computacionais das RSSF, sugerimos uma arquitetura modular capaz de se adequar a cada tipo de rede.

A arquitetura proposta prevê a divisão do sistema em módulos específicos para cada tarefa a ser executada, conforme Figura 1. O módulo de Detecção de Indícios é responsável pela monitoração dos traços locais. O módulo de Análise de Indícios recebe indícios de intruso,

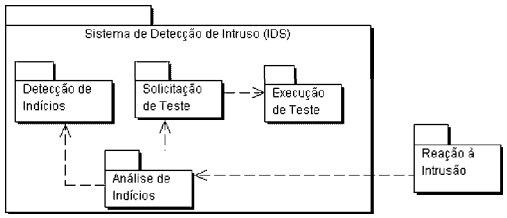

Figura 1: Arquitetura: Visão Lógica

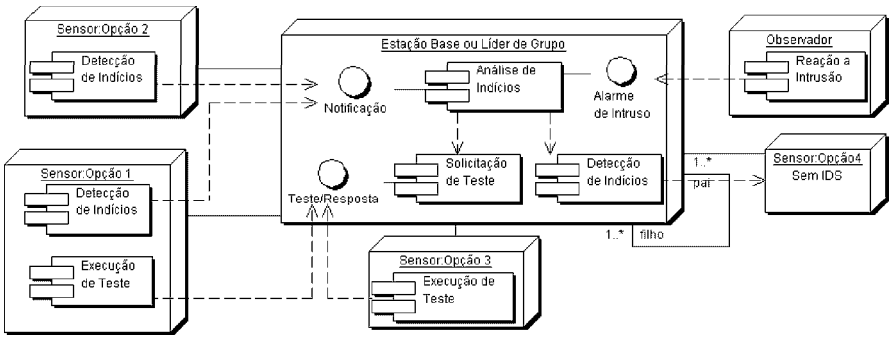

Figura 2: Arquitetura: Visão Física - Exemplo de Distribuição

analisa-os e define se há um intruso ou não. Caso necessário, o analisador de indícios aciona o módulo de Solicitação de Testes, que é responsável por auxiliar na detecção de traços remotos e na confirmação de indícios. A solicitações de testes são recebidas e processadas pelo módulo de Execução de Testes.

Para cada módulo definimos um componente, possibilitando que o IDS seja montado de acordo com a rede alvo e suas necessidades de segurança. Na Figura 2 apresentamos quatro exemplos de implantação desses componentes. A Opção 1 é indicada para RSSFs onde nós sensores são capazes de participar do sistema. A Opção 2 se aplica às redes onde os nós sensores não são capazes de responder a solicitações de testes, mas podem detectar indícios. Neste caso, os nós sensores detectam e propagam indícios para a estação base que os analisa e decide se há intruso ou não. A abdicação dos testes pode diminuir a precisão da detecção, mas pode ser necessária para viabilizar a implantação do IDS em RSSF mais limitadas. Na Opção 3 a estação base solicita a execução de testes ao invés de receber indícios espontâneos. A Opção 4 considera o caso onde os nós sensores não podem participar do IDS. A estação base passa a ser a única responsável por detectar os indícios e analisá-los. A detecção de intrusos torna-se mais difícil, já que alguns indícios podem não ser detectados e a estação base pode não ter a visão global necessária para tirar as conclusões corretas.

Além das opções destacadas, outros esquemas de implatação são possíveis. Se houver agrupamentos ou se tratar de uma rede heterogênea, os líderes ou os nós com maior capacidade podem abrigar mais módulos do IDS. Neste caso, além da estação base, outros nós poderiam solicitar testes ou analisar indícios, organizados hierarquicamente. Os nós intermediários poderiam fundir ou filtrar os indícios, de modo que apenas os relevantes fossem propagados até a estação base. Outra possibilidade seria a utilização de cooperação entre nós, para realizar conclusões locais antes de propagar um indício. Neste caso, haveria mais trocas de mensagens locais mas, por outro lado, o processamento também seria local, havendo menos mensagens inundando a rede como um todo.

4. Pré-Requisitos para o IDS

O modelo apresentado supõe a disponibilidade de certas informações. Algumas delas são facilmente obtidas, mas outras nem sempre estarão disponíveis numa RSSF. Por exemplo, cada nó pode conhecer sua própria reserva de energia em um determinado instante, pois trata-se de uma informação que pode ser obtida diretamente em seu hardware. Já o tempo de transmissão de mensagens entre nós não poderia ser determinado, a não ser que os relógios dos diversos nós da rede estivessem sincronizados, o que não é trivial nesse tipo de rede.

A necessidade dessas informações sugere que, em alguns casos, serviços sejam implantados para disponibilizá-las. Por exemplo seria necessário um serviço de sincronização de relógios para determinar o tempo de transmissão de uma mensagem. Se essa informação for de uso exclusivo do IDS, a implantação do serviço pode ser proibitiva, caso não consiga compensar os benifícios esperados com a detecção. Por outro lado, outros algoritmos ou subsistemas utilizados numa RSSF podem depender dos mesmos serviços, fazendo com que eles estejam previamente disponíveis. Dessa maneira, a disponibilização de serviços básicos como os que vem sendo propostos em [Silva et al., 2003, Elson and Romer, 2003] facilitará a implantação e influenciará o projeto do IDS.

A respeito do presente trabalho, vários estudos complementares estão em andamento, dentre eles: detalhamento do modelo apresentado; definição de regras e um método adequado para a detecção de indícios; detalhamento da estratégia de análise de indícios; detalhamento dos módulos lógicos propostos na arquitetura; validação do IDS através de simulações ou da implantação em RSSF reais.

Referências

Debar, H., Dacier, M., and Wespi, A. (1999). A revised taxonomy for intrusion-detection systems. Research Report 93222, IBM Research, Zurich Research Laboratory. 8803, Ruschlikon, Switzerland.

Deng, J., Han, R., and Mishra, S. (2003). A performance evaluation of intrusion-tolerant routing in wireless sensor networks. In *IEEE 2nd International Workshop on Information Processing in Sensor Networks (IPSN '03)*, Palo Alto, California. IEEE.

Elson, J. and Romer, K. (2003). Wireless sensor networks: A new regime for time synchronization. *ACM Computer Communication Review*, 33(1).

Estrin, D., Govindan, R., and Heidemann, J. (2000). Embedding the Internet. *Communications of the ACM*, 43(5):39–41. (Special issue guest editors).

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

PiresJr, W. R., Figueiredo, T. H. P., Wong, H. C., and Loureiro, A. A. F. (2004). Malicious node detection in wireless sensor networks. In *18th International Parallel and Distributed Processing Symposium*, Santa Fe, NM.

Silva, A. P. R., Teixeira, F. A., Lage, R. K., Loureiro, A. A., Nogueira, J. M. S., and Ruiz, L. B. (2003). Using a distributed snapshot algorithm in wireless sensor networks. In *The 9th International Workshop on Future Trends of Distributed Computing Systems*.

Wood, A. D. and Stankovic, J. A. (2002). Denial of service in sensor networks. *IEEE Computer*, 35(10):54–62.

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