Um Modelo de Gerenciamento de Segurança em Redes de Sensores Sem Fio

Sérgio de Oliveira[1, 2], Thiago Rodrigues de Oliveira[1], José Marcos Nogueira[1]

{ sergiool, thiagool, jmarcos }@dcc.ufmg.br

[1]Departamento de Ciência da Computação, Universidade Federal de Minas Gerais
Av. Antônio Carlos, 6627, Belo Horizonte, MG Brasil

[2] Universidade Presidente Antônio Carlos
BR 482, km 3, Cons. Lafaiete, MG Brasil

Abstract *- This paper proposes a security management framework to dynamically configure and reconfigure security components in sensor networks according to management information collected by sensor nodes and sent to decision-maker management entities. The goal is to give sensor networks tools to become self-managed and more autonomic. The security management model includes the definition of security levels, management information base, protocol messages and events.*

Resumo *– Este artigo propõe um modelo de gerenciamento de segurança para configurar dinâmica e autonomicamente redes de sensores para ativar e desativar componentes de segurança de acordo com as informações de gerenciamento coletadas pelos nós sensores e enviadas para as entidades responsáveis pela tomada de decisões. O objetivo do trabalho é fornecer condições para o auto-gerenciamento de uma rede de sensores no aspecto de segurança. O modelo de gerenciamento inclui a definição dos níveis de segurança, base de informações gerenciáveis, mensagens do protocolo e eventos.*

1 Introdução

Redes de sensores sem fio (RSSF) podem sofrer ataques e alguns fatores as tornam mais vulneráveis a ação de inimigos que redes convencionais, como recursos computacionais limitados, ambiente de operação hostil e comunicação sem fio. Vários tipos de ataques podem acontecer em uma RSSF, como escuta, inserção de pacotes falsos, e negação de serviço, entre outros.

Diversos trabalhos apresentam propostas de segurança em RSSF para evitar os efeitos da presença de intrusos na rede. Cada solução tem um custo, visto que recursos como processamento e comunicação gastam energia e tempo. As RSSF têm que economizar energia para estender seu tempo de vida, no caso mais comum de redes sem substituição ou recarga de bateria dos nós.

Sistemas de gerenciamento de rede podem agir na rede com o objetivo de aumentar o tempo de vida da mesma. Controle de densidade de nós sensores é um exemplo de serviço de gerenciamento de rede usado com esse objetivo na arquitetura Manna de gerenciamento de RSSF [Ruiz et al, 2003].

Um sistema de gerenciamento de segurança pode agir em uma rede da mesma forma, por exemplo, ativando ou desativando serviços e funções de segurança conforme necessário em resposta a alterações na rede. Mas a rede pode economizar energia

quando não há indicação ou suspeita de presença de intrusos. Sistemas de detecção de intrusos podem alertar a rede sobre intrusos e em resposta o sistema de gerenciamento pode ativar ou desativar funções ou serviços de segurança.

Este trabalho propõe um modelo de gerenciamento de segurança para RSSF, incluindo seleção de componentes de segurança, descrição de informação de gerenciamento, descrição de mensagens e definição de eventos de segurança. Em um modo autonômico, componentes de segurança podem ser agrupados em níveis, que podem ser alterados em resposta a eventos de detecção de intrusos. O objetivo é estender o tempo de vida da rede evitando o efeito de ataques e economizando energia com a ativação dos serviços de segurança somente quando for necessário.

O artigo está organizado da seguinte forma. A seção 2 apresenta os trabalhos relacionados. A seção 3 apresenta o modelo de rede estudado neste artigo. A seção 4 apresenta conceitos de gerenciamento de redes aplicados a redes de sensores. A seção 5 apresenta os componentes de segurança a serem abordados neste trabalho. A seção 6 apresenta as decisões autonômicas a serem tomadas. A seção 7 apresenta o modelo de gerenciamento, incluindo formato das mensagens, eventos e modelo de informações. A seção 8 apresenta uma validação do trabalho por simulação. Finalmente, a seção 9 apresenta uma discussão sobre os resultados e a seção 10 apresenta as conclusões.

2 Trabalhos Relacionados

Não existem muitos trabalhos sobre gerenciamento de RSSF. Savola e Uusitalo (2006) apresentam princípios de gerenciamento de segurança para redes ad hoc, que apresentam desafios diferentes para segurança em relação às RSSF. O principal problema em redes ad hoc é a falta de uma administração central confiável. RSSF não apresentam esse problema mas possuem mais restrições de energia e hardware.

Dimitriou and Krontiris (2005) apresentam uma visão geral dos atuais desafios em segurança para RSSF, destacando seus aspectos de comunicação autonômica. Eles apresentam os atuais debates nas pesquisas sobre segurança em RSSF: protocolos de estabelecimento e configuração inicial confiável de chaves, tolerância a ataques de negação de serviço, tolerância a nós alterados, roteamento seguro, segurança sensível a localização, fusão de dados segura e técnicas eficientes de criptografia. Na discussão, mostram como a comunicação autonômica oferece oportunidades para aumentar a segurança em RSSF. Este trabalho resume estas características autonômicas: auto-configuração, auto-reconhecimento, auto-adaptação, auto-organização e auto-otimização, bem como discute o que é necessário para prover uma solução integrada e completa para segurança em RSSF.

Alguns modelos de gerenciamento de redes foram propostos na literatura, entre eles o Manna [Ruiz et al, 2003], no qual políticas descrevem o comportamento desejado dos componentes de gerenciamento, como agentes e gerentes.

Song et al (2005) propõem um elemento que age como um mediador entre redes Universal Plug and Play (UPnP) e RSSF. Esse elemento, chamado BOSS (Bridge of the sensors), é um agente UPnP implementado na estação base e posicionado entre os controladores UPnP e os nós sensores não-UPnP a serem gerenciados. O objetivo é realizar a implantação de serviços em RSSF sem prover configuração para a rede.

3 Modelo de Rede

Este trabalho foi desenvolvido considerando RSSF estacionárias planas, onde todos os nós possuem os mesmos recursos computacionais e funcionalidades; nenhum nó possui funções especiais. Para ficarem condizentes com nós sensores reais, o trabalho referencia os nós sensores Berkeley Mica2 Motes, limitados para somente 4 Kbytes de memória RAM e 128 Kbytes de memória de programas [Crossbow, 2004]. A energia gasta para transmissão sem fio é maior que a energia consumida para recepção e processamento. Nesse nó, a transmissão com o alcance máximo consome 27 mA e a recepção 8 mA para uma taxa de transmissão de 38,4 Kbaud, e 8 mA de processamento para uma freqüência de CPU de 8 MHz.

Para o modelo considera-se ainda que o lançamento dos nós na sua área de operação é uniforme, seguindo o modelo conhecido como colméia, onde cada nós tem exatamente 6 vizinhos eqüidistantes. Porém, a vizinhança de cada nó não é conhecida previamente. A comunicação sem fio não é segura e está sujeita a escuta, inserção de pacotes e replicação de mensagens. Os nós são vulneráveis a violações físicas: se um nó é violado, o inimigo pode obter todas as suas informações. Há uma única estação base, que é fonte ou destino de todos os pacotes de dados e controle, possui recursos ilimitados e não pode ser violada.

4 Gerenciamento de Redes de Sensores Sem Fio

Em RSSF, o gerenciamento da rede é essencial para garantir o uso racional de todos os recursos. Funções de gerenciamento da rede podem ser configuradas e ligar ou desligar todos os componentes para conseguir um melhor consumo de energia.

O modelo Manna considera uma arquitetura de gerenciamento tri-dimensional, que consiste de áreas funcionais, níveis de gerenciamento e funcionalidades de RSSF. Essas dimensões são especificadas para o gerenciamento de uma RSSF e são a base para uma lista de funções de gerenciamento. O Manna inclui um protocolo de gerenciamento chamado MannaNMP, que descreve os serviços providos e o formato das mensagens, assim como a base de informações de gerenciamento.

Em uma aplicação demonstrativa, MannaNMP foi utilizado para controlar a densidade dos nós de RSSF. Com o serviço de controle de densidade próprio, é possível estender o tempo de vida da rede; setores com concentração excessiva de nós podem ter parte dos seus nós desligados, colocados em estado de espera para serem ligados depois de algum tempo, quando a bateria de um ou mais nós ativos da vizinhança se esgotar. Esses nós reservas substituem os ativos propiciando o aumento do tempo de vida de rede. Outro benefício do serviço de gerenciamento é a possibilidade de redução de tráfego na rede, que tem como conseqüência positiva a diminuição do consumo de energia necessário para repassar mensagens para a estação base e a redução das colisões de pacotes. Estudos sobre a adoção de técnicas de gerenciamento para RSSF têm mostrado outros benefícios, como uma baixa geração de mensagens adicionais de gerenciamento da rede e aumento do tempo de vida [Ruiz et al, 2004].

5 Componentes de Segurança

Diversas soluções de segurança são encontradas na literatura. Aquelas de maior interesse para este trabalho foram organizadas e classificadas em componentes de acordo com seus objetivos.

Existem soluções de seguranças preventivas e reativas. Algumas delas, como criptografia, são preventivas e impedem a ação de intrusos. Outras, como indicadores de detecção de intrusos a problemas de segurança, permitem ações corretivas, como a revogação de intrusos.

Este trabalho considera a possibilidade de criptografia salto-a-salto e fim-a-fim, a utilização de técnicas de gerenciamento de chaves, a existência de mecanismos de detecção de intrusos, roteamento seguro, fusão e agregação segura de dados, bem como um esquema de revogação de nós.

5.1 Técnicas Criptográficas

Encriptação

A encriptação pode ser um processo fim-a-fim, feito uma vez por mensagem, ou um processo salto-a-salto, feito cada vez que uma mensagem atinge um nó de repasse. Devido a restrições de recursos, é praticamente impossível utilizar algoritmos de chave pública para encriptar mensagens em RSSF. Esses algoritmos levariam vários minutos para encriptar e decriptar uma pequena mensagem em um nó sensor típico. Somente algoritmos de chaves simétricas podem ser utilizados sem causar grandes atrasos e muito consumo de energia.

Encriptação salto-a-salto implica em mais processamento nos nós intermediários e torna possível outros tipos de funções com processamento da rede, como a fusão de dados. A encriptação salto-a-salto, exige que os nós compartilhem chaves com vizinhos.

Encriptação fim-a-fim protege os dados contra ataques de espionagem durante sua transmissão para a estação base; todavia, limita o processamento na rede porque os nós têm de compartilhar chaves com a estação base. Nessa técnica, para transmitir uma mensagem de um nó para a estação base ou vice-versa, somente o nó e a estação base precisam de encriptar/decriptar a mensagem, o que implica em menos processamento que na encriptação salto-a-salto.

Assinatura

A assinatura também pode ser um processo fim-a-fim, verificada somente pela estação base, ou salto-a-salto. A assinatura de uma mensagem causa processamento extra no momento e local de sua geração, maior utilização da rede na transmissão e processamento extra no momento da verificação. O uso de técnicas de segurança pode evitar a inserção de pacotes falsos e a adulteração de mensagens.

TinySec

TinySec [Karlof e Wagner, 2004] é uma arquitetura de segurança totalmente implementado baseado no TinyOS, um sistema operacional para RSSF. TinySec especifica métodos criptográficos para assinar e encriptar mensagens, provendo propriedades de autenticação e privacidade para uma RSSF, ao custo de poucos bytes adicionais e baixo custo de energia.

O tamanho do cabeçalho do pacote, normalmente sete bytes no TinyOS, aumenta para oito bytes no TinySec com o aspecto de autenticação habilitado (TinySec-Auth mode). O campo de dados de um pacote TinyOS é de 0 a 29 bytes. No modo de encriptação, chamado TinySec-AE, o campo de cabeçalho tem tamanho de 12 bytes, incluindo um vetor de inicialização para prover controle de acesso; todavia, normalmente é suficiente habilitar somente o modo TinySec-Auth.

O TinySec requer o compartilhamento de chaves entre os nós vizinhos e diversas técnicas podem ser usadas, como compartilhamento global de chaves ou compartilhamento probabilístico de chaves. Um compartilhamento global de chaves não é seguro porque um único nó capturado pode revelar a chave global. Técnicas probabilísticas, onde dois nós compartilham a chave com certa probabilidade, também não são boas porque canais de comunicação podem não ser estabelecidos quando um ou mais nós do par não tiverem a chave própria.

Como uma técnica do nível de enlace, o TinySec tem que executar salto-a-salto e seu custo será considerado quando a criptografia salto-a-salto estiver habilitada.

Gerenciamento de chaves

Gerenciamento de chaves é um problema em RSSF porque esquemas de chaves públicas são inviáveis devido ao alto custo de processamento. Soluções de chaves simétricas são apresentadas em alguns trabalhos: chaves compartilhadas globais, chaves compartilhadas entre nós e estação base, pares de chaves estabelecidas entre nós vizinhos e chaves de grupos para aplicações em grupo.

Chaves par-a-par são mais difíceis de estabelecer porque a topologia da rede não é previamente conhecida e restrições de memória impedem total compartilhamento de pares de chaves.

Diversos protocolos de estabelecimento de chaves par-a-par são encontrados na literatura. Técnicas probabilísticas [Liu e Ning, 2005][Chan et al, 2003] [Eschenauer e Glicor, 2002] são boas propostas, mas não asseguram estabelecimento de chaves entre todos os nós vizinhos. Sem chaves, alguns canais de comunicação não poderiam ser usados, aumentando o caminho da rede e, consequentemente, o consumo de energia. Técnicas determinísticas [Oliveira et al, 2007][Zhu et al, 2003] assumem um início confiável de chaves globais compartilhadas para estabelecer todas as chaves necessárias para os pares.

Como solução para o estabelecimento de chaves, escolhemos as técnicas SPINS, para criptografia fim-a-fim, e NEKAP, para criptografia salto-a-salto. Essas técnicas foram escolhidas porque causam um consumo menor de energia para estabelecimento e são técnicas determinísticas, permitindo todas as ligações de comunicação.

SPINS

SPINS, *Security Protocols for Sensor Networks*, é um trabalho pioneiro que propõe dois blocos otimizados de construção de segurança para RSSF: SNEP e μTesla [Perrig et al, 2002]. SNEP, *Secure Network Encryption Protocol*, provê confidencialidade e autenticação fim-a-fim dos dados nas duas partes entre a estação base e cada nó. μTesla é um protocolo que provê comunicação por difusão da estação base. μTesla usa um caminho único da rede para autenticar suas mensagens. As chaves são anunciadas periodicamente. Todos os pacotes enviados antes do anúncio das chaves são autenticados com essa chave. SPINS inclui protocolo de distribuição de chaves, formatos de mensagens e uma implementação para o nó Mica Motes.

NEKAP

NEKAP, *Neighborhood-based Key Agreement Protocol*, [Oliveira et al, 2007] é um protocolo para estabelecimento de chaves par-a-par e de grupo para redes de sensores. Nesse protocolo, uma chave global K_G e uma chave mestra K_{Mi} são pré-carregada em cada nó. Após o lançamento, o nó *i* criptografa a chave mestra K_{Mi} com a chave K_G e

envia o resultado a todos seus vizinhos. K_G tem um tempo de validade pequeno, suficiente para permitir a troca das chaves mestras.

A chave de grupo é a primeira chave a ser estabelecida e é gerada a partir da chve mestra. Para envio de mensagens em *broadcast*, além da chave mestra, é necessária outra chave, tomada de uma cadeia de chaves de via única, para garantir a autenticação das mensagens.

Após a troca das chaves mestras, qualquer par de nós A e B tem um conjunto de chaves em comum: K_{MA}, K_{MB}, e também K_{MX} , para todo nó X que é vizinho, ao mesmo tempo de A e B. Para aumentar a segurança desse protocolo todas as informações conhecidas pelos nós são usadas, bem como os identificadores dos nós.

5.2 Sistemas de Detecção de Intrusos e Revogação de Nós

A detecção de intrusos em RSSF deve lançar mão de mais técnicas diferentes que nas redes convencionais, devido à diferença nos modelos, ataques e recursos. Dois tipos de técnicas podem ser utilizados para detecção de intrusos em RSSF: centralizada ou descentralizada. Na técnica centralizada, a estação base é responsável por detectar intrusos, iniciando o processo de coleta de informações da rede, especialmente a informação sobre a produção dos nós sensores (mapa de produção); a estação base possui um grande conjunto de informações à sua disposição, o que facilita o processo de detecção. Na técnica descentralizada, alguns ou todos os nós executam operações simples para detectar intrusos [Silva et al, 2005][Freiling et al, 2007]; a grande vantagem é a disponibilidade instantânea da informação, visto que os nós podem detectar os ataques exatamente no momento em que eles ocorrem.

A detecção de intrusos é normalmente seguida da revogação dos nós intrusos. A revogação é a exclusão do nó da rede, tornando impossível para ele a comunicação com seus vizinhos. Esse processo deveria ser autenticado para evitar a revogação de nós autênticos por intrusos. Como os nós não são protegidos contra violação física no modelo utilizado neste trabalho, é mais seguro permitir somente à estação base promover a revogação de nós. De outra forma, um nó intruso autenticado pela rede, provavelmente originado de uma violação física, poderia isolar nós autênticos, promovendo outros tipos de ataques de negação de serviço. O protocolo µTesla [Perrig et al, 2002] pode ser utilizado para autenticar mensagens de revogação.

5.3 Roteamento Seguro

Redes de sensores são baseadas na auto-configuração, auto-manutenção e auto-otimização. Assim, o roteamento é uma tarefa crítica porque um inimigo pode se inserir na rede para promover um ataque de negação de serviço. Três mecanismos foram considerados para proteger o roteamento: autenticação em difusão, fim-a-fim ou salto-a-salto, durante o estabelecimento de rotas [Perrig et al, 2002][Oliveira et al, 2007]; detecção de intrusos no roteamento [Silva et al, 2005] [Freiling et al, 2007] e rotas alternativas para aumentar a resiliência contra intrusão[Oliveira et al,2006].

5.4 Fusão Segura dos Dados

Eventualmente as leituras dos sensores podem ser imprecisas ou até mesmo inúteis. Mesmo sob condições ambientais perfeitas os sensores podem não prover leituras absolutamente perfeitas. As RSSF freqüentemente possuem um grande número de nós

sensores, trazendo um novo desafio de escalabilidade relacionado ao consumo desnecessário de energia provocado pela transmissão de dados redundantes e por colisões. A fusão de dados, técnica em que diferentes dados coletados por vários nós são transformados na rede antes de serem enviados ao usuário, possui pelo menos dois fatores que tornam importante a sua utilização em RSSF. O primeiro consiste na obtenção de leituras de maior precisão tornando a rede mais robusta e menos vulnerável a falhas e imprecisões de um único nó sensor. O segundo fator é a economia de energia pela da redução da quantidade de mensagens e de dados que são transmitidos pelos nós sensores [Luo et al, 2006].

Soluções de segurança podem interferir na fusão de dados. A encriptação fim-a-fim inviabiliza fusão de dados porque impede que qualquer nó intermediário tenha acesso à informação para executar a operação. Além disso, a fusão de dados pode confundir os mecanismos de detecção de intrusos, como o *watchdog* [Savola e Uusitalo, 2006]. Em aplicações de segurança crítica, a fusão de dados tem de ser desabilitada para se utilizar encriptação fim-a-fim e sistemas de detecção de intrusos.

6 Decisões Autonômicas

RSSF têm de ser auto-gerenciáveis, configurando seus componentes para estender seu tempo de vida e assegurar a produção dos dados. Neste trabalho, componentes de segurança são configurados baseados em eventos de segurança gerados por sistemas de detecção de intrusos.

Eventos de detecção de intrusos configuram componentes de segurança. Intrusos detectados pela estação base são revogados usando mensagens autenticadas da estação base. Intrusos detectados de maneira descentralizada não podem ser revogados pela estação base porque eles não são confiáveis, mas um evento de detecção de intruso é gerado, de forma a ativar componentes de segurança.

No trabalho relatado neste artigo, foram definidos níveis de segurança para facilitar decisões autonômicas baseadas em eventos recebidos. Em cada nível de segurança alguns componentes de segurança são ligados para proteger a rede dos intrusos. O nível de segurança da rede aumenta com a evidência de intrusos. O nível de segurança pode ser decrescido, também, em níveis críticos de energia. Para economizar energia, componentes de segurança, como a detecção de intrusos, podem ser desligados.

A Tabela 1 exibe eventos e ações autonômicas geradas nesses eventos. Em geral, um intruso é suficiente para alterar o nível de segurança, porque indica que o atual nível de segurança permitiu a entrada de intrusos; todavia, em algumas situações, o nível de segurança pode ser alterado após a detecção de mais de um intruso.

Tabela 1 – Eventos de detecção de intrusos e ações

Evento	Ação
Estação base detecta um novo intruso	- Intruso é revogado - Nível de segurança aumenta
Um nó sensor detecta um intruso	- Nível de segurança aumenta

A Tabela 2 mostra os níveis de segurança. O serviço de detecção de intrusos centralizado está sempre habilitado e não aparece na tabela. Quando a estação base detecta um nó intruso, ele é revogado. No primeiro nível, mais baixo, nenhum componente de segurança é habilitado. A fusão de dados é habilitada, o que pode reduzir significativamente o consumo da rede.

No nível Alto, a detecção de intrusos é estendida para 20% dos nós. A criptografia fim-a-fim desabilita o processamento na rede. Assim, a fusão de dados não pode ser utilizada. Na presença de intrusos, a fusão de dados não é um método confiável porque um intruso no processo de fusão de dados pode adulterar dados de vários nós. Esse modo somente tem de ser usado se nós intrusos ainda são detectados quando a criptografia salto-a-salto está ativa.

Tabela 2 - Níveis de segurança autonômicos

Nível	Componentes de segurança utilizados
Baixo	- Sem detecção de intrusos nos nós sensores - Sem utilização de criptografia - Fusão de dados habilitada
Médio	- 10% dos nós executam detecção de intrusos - Atualização de rotas autenticada fim-a-fim - Criptografia salto-a-salto habilitada - Fusão de dados habilitada - Rotas alternativas
Alto	- 20% dos nós executam detecção de intrusos - Criptografia fim-a-fim habilitada - Atualização de rotas autenticada salto-a-salto - Rotas alternativas - Sem fusão de dados
Crítico	- 30% dos nós executam detecção de intrusos - Sem fusão de dados - Criptografia fim-a-fim e salto-a-salto habilitadas - Atualização de rotas autenticada salto-a-salto e fim-a-fim - Rotas alternativas

Se ainda com o nível alto ativo, intrusos são detectados, o nível crítico é iniciado. Nesse nível, todos os componentes de segurança apresentados são utilizados, incluindo criptografia salto-a-salto e fim-a-fim. Nesse nível, considera-se que nós intrusos conhecem algumas chaves da rede. Assim, utiliza-se criptografia redundante, fim-a-fim e salto-a-salto. Dessa forma, um intruso terá de conhecer várias chaves para ter acesso às mensagens da rede.

Quando recursos de energia alcançam um nível crítico, os nós podem reduzir o nível de segurança para aumentar o tempo de vida. Nesse caso, os componentes de segurança têm um custo de energia maior que a rede pode gastar. Como os nós estão no fim dos seus tempos de vida, é melhor tentar trabalhar sem segurança do que gastar a energia restante com segurança.

A criptografia pode incluir encriptação e assinatura e os objetivos da rede devem determinar qual técnica tem de ser usada. Se os dados da rede são confidenciais, a encriptação tem de ser usada. De outro lado, somente assinatura pode ser utilizada para evitar adulterações e enganos.

7 Modelo de Gerenciamento

O modelo de gerenciamento deste trabalho segue as linhas gerais do modelo Manna, onde várias possibilidades são propostas para organizar o relacionamento entre gerente e agentes. Neste artigo, são propostas extensões ao MannaNMP, Manna Network Management Protocol, para incluir segurança. O modelo de gerenciamento, apresentado a seguir, é composto de uma base de informações de gerenciamento, mensagens trocadas e eventos. O modelo considera que os componentes de segurança

descritos anteriormente podem ser parte de situações de gerenciamento. Nesse sentido, a configuração dos componentes de segurança é dinâmica, o que significa que eles podem ser incluídos, excluídos, ativados, e desativados em tempo de operação. Eventos fornecem informações para a rede no sentido de tornar possível a configuração e a re-configuração dos componentes de segurança de uma maneira autonômica.

7.1 Base de Informações de Gerenciamento (MIB)

Para configurar componentes de segurança, um número de objetos de gerenciamento foi definido para a MIB. Os objetos são organizados de acordo com o tipo de componente de segurança que os utilizam: criptografia, chaves, dados e administração.

Criptografia

Objetos booleanos indicam se o sistema usa uma função específica de segurança; seus nomes são auto-explicativos; Encriptação fim-a-fim, Encriptação salto-a-salto, Assinatura fim-a-fim, Assinatura salto-a-salto, e Comunicação por difusão.

Gerenciamento de chaves

O próximo conjunto de objetos mantém informações sobre chaves e tem de ser armazenado nos nós sensores para os objetivos da criptografia. Os dados contidos nos objetos não podem circular pela rede por razões de segurança. Cinco objetos são definidos: Chaves de difusão (lista de chaves usada para difusão); Chaves par-a-par (lista de chaves usada para cada vizinho de um nó); Última chave (última chave revelada da cadeia de um nó vizinho); Chave fim-a-fim (chave para ser usada na encriptação fim-a-fim); Chave global (chave para ser usada por todos os nós vizinhos).

Dados

Vários tipos de controle de dados são enviados pela rede pelos nós ou pela estação base. Uma parte deles foi definida pela MIB:

-Nível de segurança (Choice) ⇒ Baixo (0), Médio (1), Alto(2), Crítico(3);
-*Fusão de dados?* (Boolean) ⇒ Indica se a fusão de dados é utilizada nos nós;
-*Intruso detectado?* (Boolean) ⇒ Indica se um intruso foi detectado na rede;
-*Identificador do intruso* (ID) ⇒ Identificador do intruso detectado;
-*Identificador de nó revogado* (ID) ⇒ Identifica o nó intruso para ser revogado;
-*Lista de nós revogados* (List) ⇒ Lista de nós suspeitos e revogados;
-*Lista de chaves revogadas* (List) ⇒ Lista de chaves revogadas por um nó.

Administração

-*Estado administrativo* (Choice) ⇒ Desbloqueado (0), Parcialmente bloqueado (1), Bloqueado (2);
-*Pacotes de gerenciamento enviados* (Integer) ⇒ mensagens de gerenciamento enviadas pelo nó;
-*Pacotes de gerenciamento recebidos* (Integer) ⇒ mensagens de gerenciamento recebidas pelo nó;

7.2 Definição das Mensagens

O modelo propõe um gerenciamento de segurança orientado por mensagens, onde mensagens de controle são usadas para ativar ou desativar componentes, como detecção de intrusos, criptografia, fusão de dados, assinatura digital. Uma mensagem indicando a presença de um intruso colocaria a rede em estado de alerta. Como a identificação precisa do intruso não é possível, a rede tem de reduzir as possibilidades de comunicação do intruso de forma a anular seus efeitos.

Um número de mensagens de gerenciamento foi definido e é listado a seguir. Em termos do modelo gerente/agente, elas são do tipo *set* e são usadas para estabelecer ou alterar os valores dos objetos, como definido no protocolo MannaMNP.

Mensagens para criptografia

As mensagens são para: ativação de encriptação fim-a-fim; ativação de assinatura fim-a-fim; ativação de assinatura salto-a-salto; utilização de difusão (para um específico período); mudança do protocolo de gerenciamento de chaves.

Mensagens de dados

As mensagens definidas são: *mudança no nível de segurança* (mudança de configuração dos componentes de segurança); *utilização de fusão de dados* (gera mensagem para desativar a encriptação fim-a-fim); *detecção de intruso* (coloca a rede em estado de alerta e envia o identificador do intruso para a estação base); *revogação de nós* (inclui o identificador do nó revogado na lista); *revogação de chave* (inclui a chave revogada na lista de chaves revogadas de nós recebedores).

7.3 Eventos

Na ocorrência de eventos, os nós sensores enviam mensagens para informar a estação base. Essas mensagens são usadas pela estação base para alterar a configuração da RSSF, o que pode ser feito imediatamente ou algum tempo depois. Mensagens de *trap* são usadas para informar eventos previamente programados. No caso de redes hierárquicas, as mensagens são encaminhadas para os maiores níveis de hierarquia até alcançar o gerente. Nós intermediários, quando possível, tomam decisões em resposta aos eventos informados, o que torna a rede mais inteligente e pode diminuir o fluxo de mensagens. Para reduzir o consumo de energia, a responsabilidade de monitoramento de alguns ou todos os eventos é atribuída à estação base ou somente a alguns nós. A comunicação baseia-se no protocolo MannaNMP.

Os eventos definidos são os seguintes: *Detecção de intruso* (nó sensor identificou um nó suspeito); *Revogação de chave* (um nó intruso foi revogado); *Desaparecimento de nó* (nó suspeita que um nó vizinho desapareceu); *Reativação de nó desaparecido* (um nó previamente suspeito de desaparecimento foi identificado e pode ser um intruso); *Nível crítico de energia* (um nível crítico de energia de um nó foi alcançado, as chaves desse nó têm de ser revogadas).

8 Validação

Para validar o modelo de gerenciamento aqui apresentado, um conjunto de simulações foi realizado, verificando o consumo de energia nos diversos níveis de segurança. Foi utilizado um simulador baseado em eventos discretos, desenvolvido no DCC-UFMG [Martins et al, 2005]. O objetivo é mostras as diferenças entre o consumo de energia em cada nível, para justificar a manutenção dos níveis inferiores sempre que a presença de intrusos não tiver sido constatada.

Para tanto, a simulação usou uma rede plana e homogênea, com o número total de nós variando entre 50 e 1000 nós. Os nós são distribuídos pela rede de forma uniforme, no modelo conhecido como colméia, onde cada nó tem exatamente 6 vizinhos eqüidistantes, a uma distância de 34 metros. A rede com baixa densidade consome muito menos energia que uma rede com alta densidade. De acordo com os dados

apresentados em [Crossbow, 2004], o consumo de energia para a recepção de pacotes é 8 mA, e para a transmissão é de 12 mA, correspondente a um energia média que garante a transmissão a uma distância média de 40 metros, que corresponde ao alcance do rádio. Considerando a proporção entre o número de mensagens recebidas e enviadas igual ao número médio de vizinhos, com 6 vizinhos, para cada pacote enviado, o nó receberá outros 6. Isso é fato, pois, em média, um nó recebe tantas vezes mais pacotes que envia quantos são seus vizinhos. Logo, em redes muito densas, com média de vizinhos acima de 6, o custo de recepção se torna certamente o maior custo, reduzindo o tempo de vida da rede. Por outro lado, em redes de densidade mais baixa, boa parte da rede pode ficar sem conectividade devido à escassez de ligações [Crossbow, 2008].

O sensoriamento é realizado por todos os nós a cada 14 segundos. O tempo para a transmissão de seus dados e recepção e repasse dos dados dos vizinhos é de 68,8 ms, o que representa 0,5% do tempo. Foram realizadas 45 fases de sensoriamento, com 3 etapas de restabelecimento de rotas, intercalando 15 fases de sensoriamento. Seguindo essas definições, uma bateria de 1000 mAh pode durar até um ano sem recargas ou trocas, atendendo aos objetivos das redes de sensores.

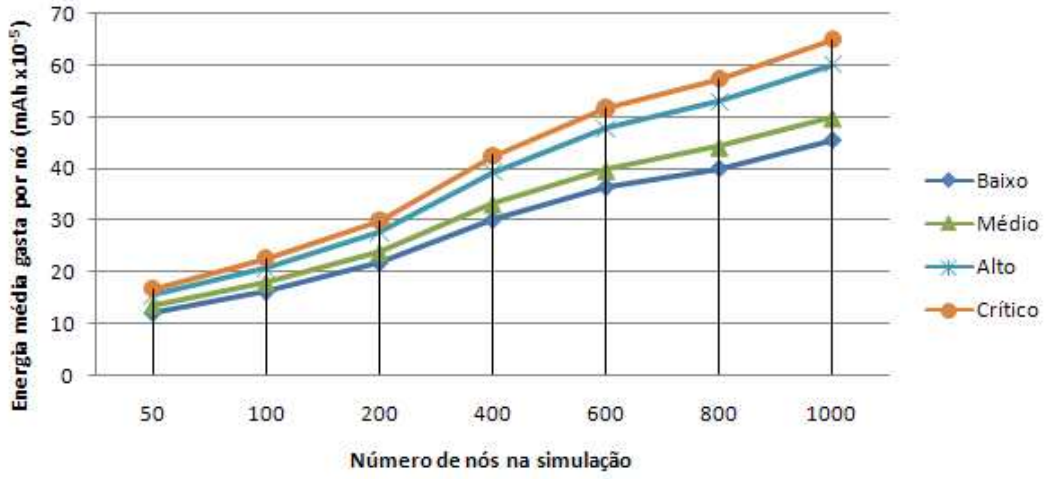

Figura 1 - Resultados das simulações

A cada simulação, foi medido a energia média dos nós, em mAh $x10^{-9}$ e apresentados no gráfico da Figura 1. Foram consideradas, na simulação, fusão de dados, rotas redundantes e a encriptação e assinatura criptográfica das mensagens para os níveis apresentados. Não foram consideradas as mensagens de gerência, como para mudança de nível, detecção de intrusos e revogação de intrusos. A energia gasta com as mensagens de gerência é muito baixa. Para alterar o nível de segurança da rede, a estação base propaga apenas uma mensagem pela rede, assim como na atualização de rotas. Já a detecção de intrusos gera uma mensagem do nó para a estação base, que gasta a mesma energia de uma mensagem de sensoriamento. Ou seja, normalmente essas mensagens não representam nem 1% do tráfego total.

A diferença média entre os níveis Baixo e Média é de 9,9%, entre Médio e Alto, 18,7% e entre Alto e Crítico 8,0%. Do nível baixo para o nível crítico, dois extremos, a diferença é de 40 %.

9 Discussão

Um requisito comum da maior parte das soluções propostas para redes de sensores é aumentar a disponibilidade do serviço oferecido pela rede. Para tanto, o prolongamento do tempo de vida da rede pelo baixo consumo de bateria tem sido o alvo principal dos trabalhos. Porém, problemas de segurança podem ser encontrados nesse ambiente, especialmente pelos ataques de negação que serviço, que pode reduzir os serviços da rede antes do término da capacidade das baterias.

Diversas soluções de segurança podem ser utilizadas para bloquear ataques de negação de serviço, aumentando a disponibilidade da rede. Cada solução aumenta o consumo de energia de 10 a 20%. Se essas soluções são sempre utilizadas, o tempo de vida da rede diminuirá por causa da exaustão das baterias.

Um modelo de gerenciamento de segurança, como apresentado neste trabalho, permitem equilibrar a disponibilidade da rede e o consumo de energia, ligando e desligando as soluções de segurança quando necessário. Entretanto, o gerenciamento também tem um custo de energia.

Considerando o modelo apresentado, é possível avaliar três cenários distintos:

1 - Rede sem segurança: Nesse caso, a disponibilidade da rede pode ser comprometida pela presença de intrusos, reduzindo a produtividade e o tempo de vida da rede;

2 - Rede com uso constante de algumas soluções de segurança: Nesse caso, a presença de intrusos é evitada ou reduzida, aumentando a disponibilidade da rede, mas o consumo de energia aumenta para executar essas soluções de segurança. Com algumas soluções de segurança, o consumo de energia pode aumentar em 40%, conforme a simulação, minimizando o tempo de vida pelo término das baterias;

3 - Rede com gerenciamento de segurança para ativar soluções de segurança somente quando necessário. Se nenhum intruso é detectado, a rede pode trabalhar sem componentes de segurança, minimizando o consumo de energia para prolongar o tempo de vida da rede. Quando a rede detecta um intruso, a solução de gerenciamento aumenta o nível de segurança evitando o efeito do intruso.

O consumo adicional de energia no terceiro cenário com mecanismos de segurança dependerá da presença de intrusos. No melhor caso, somente sistemas centralizados de detecção de intrusos executam, sem execução nos nós. Quando um primeiro intruso é detectado, o gerenciamento de segurança começa, enviando mensagens, a ativar soluções de segurança. As soluções de segurança serão ligadas gradualmente, aumentando o consumo da rede, mas evitando o efeito dos intrusos. Em grandes redes, a rede pode ser dividida em setores e as soluções de segurança podem ser ativadas somente onde intrusos são detectados.

Todas as soluções de segurança demandam processamento, memória e recursos da rede. Processamento e rede significam consumo de energia, porque processador e rede estão ociosos na maior parte do tempo. Recursos de memória podem ser críticos devido a fortes limites dos nós.

Mica2 Motes possui 128 Kbytes de memória de programas. Algumas avaliações mostram que soluções de segurança não ocupam tanta memória: NEKAP foi implementado com TinySec em 10 Kbytes e SPINS primitivo ocupa aproximadamente 2

Kbytes. Sistemas de detecção de intrusos como *watchdog* podem ser implementados em poucos bytes. Assim, as restrições de memória podem ser facilmente resolvidas.

10 Conclusão e Trabalhos Futuros

Este artigo apresenta um modelo de gerenciamento de segurança para RSSF. O objetivo é estender a disponibilidade da rede e o tempo de vida configurando soluções de segurança para executar somente quando é necessário.

O modelo de gerenciamento de segurança é uma extensão do Manna [Ruiz et al, 2003], um modelo de gerenciamento para RSSF. Algumas poucas mensagens são necessárias para implementar o gerenciamento de segurança.

De maneira autonômica, um gerente na estação base pode configurar níveis de segurança nos nós, ativando componentes de segurança para evitar o efeito dos intrusos. Um evento de detecção de intrusos gera decisão autonômica alterando os níveis de segurança.

Como trabalho futuro, propõe-se a otimização das soluções de segurança, compartilhando algoritmos, chaves e código, para reduzir recursos de memória e processamento exigidos.

11 Referências

Chan, H., Perrig, A. Song, D. – “Random key predistribution schemes for sensor networks”, 2003 IEEE Symposium on Security and Privacy May 11 - 14, 2003 Berkeley, CA, p. 197, 2003.

Crossbow Technology Inc – “Mica 2 wireless measurement system” - available at http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/6020-0042-04_B_MICA2.pdf, acessado em 10 de março de 2004, San Jose, CA, USA, February 2004.

Crossbow Technology Inc – “Mote Battery Life Calculator” – available at http://www.xbow.com/Support/Support_pdf_files/PowerManagement.xls acessed in March 20, 2008, San Jose, USA, March, 2008

Dimitriou, T, Krontiris, I. - "Autonomic Communication Security in Sensor Networks," 2nd International Workshop on Autonomic Communication, WAC 2005

Eschenauer, L; Glicor, V. D. – “A key-management scheme for distributed sensor network” – in Proc. of the 9th ACM conference on Computer and Communication Security, November 2002.

Freiling, F; Krontiris, I.; Dimitriou, T. – “Towards Intrusion Detection in Wireless Sensor Networks” - 13th EuropeanWireless Conference, Paris, France, 2007.

H. Song, D. Kim, K. Lee, and J. Sung, “Upnp-Based Sensor Network Management Architecture,” in Proc. ICMU Conf., Apr. 2005.

Karlof, N. Sastry, and D. Wagner – “TinySec: A Link Layer Security Architecture for Wireless Sensor Networks”, Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems (SenSys 2004). November 2004.

Liu, P. Ning, R. Li “Establishing Pairwise Keys” in Distributed Sensor Networks ACM Transactions on Information and System Security, Vol. 8, No. 1, February 2005

Luo, H.; Luo, J.; Liu, Y. and Das, S. - "Adaptive Data Fusion for Energy Efficient Routing in Wireless Sensor Networks," IEEE Transactions on Computers, vol. 55, no. 10, Oct. 2006.

Martins, M. H. T., Silva, A. P. R. da ; Loureiro, A. A. F. and Ruiz, L. B. (2005) An IDS simulator for wireless sensor networks. Sensornet Technical Report, Comp Sci Dept, Federal University of Minas Gerais, May 2005.

Oliveira, S.; Wong, H. C.; Nogueira, J. M. – "NEKAP: Intruder Resilient and Energy Efficient Key Establishment in Sensor Networks" – IEEE ICCCN'07 Workshop on Advanced Networking and Communications – Honolulu, Hawai, 2007

Oliveira, S.; Wong, H. C.; Nogueira, J. M.; Paula, W. P. – "Alternate Routes for Detection and Increase of Resilience to the Distributed Intrusion in WSN" - IFIP NETWORKING 2006 Workshop on Security and Privacy in Mobile and Wireless Networking (SecPri_MobiWi 2006), Coimbra, Portugal

Perrig, R. Szewczyk, J. D. Tygar; V. Wen; D. E. Culler – "SPINS: security protocols for sensor networks" – Wireless Networks 8, 2002, Kluwer Academic Publishers, Netherlands

Ruiz, L. B.; Nogueira, J. M.; Loureiro, A. A. F. - "Manna: A Management Architecture for Wireless Sensor Networks," IEEE Communications Magazine, vol. 41, no. 2, pp. 116–125, 2003.

Ruiz, L. B.; Silva, F. A.; Braga, T. R. M.; Nogueira, J. M.; Loureiro, A. A. F. - "On Impact of Management on Wireless Sensors Networks." IEEE/IFIP Network Operations and Management Symposium (IX NOMS 2004), ISBN 0-7803-8230-7, p. 657-670, 2004, Seul, South Korea

Savola, R; Uusitalo, I. – "Towards Node-Level Security Management in Self-Organizing Mobile Ad Hoc Networks" - International Conference on Internet and Web Applications and Services/Advanced International Conference on Telecommunications, 2006. AICT-ICIW - Volume , Issue , 19-25 Feb. 2006

Silva, P. R.; Loureiro, A. A. F.; Martins, M. H. T.; Ruiz, L. B.; Rocha, B. P. S.; Wong, H. C. – "Decentralized Intrusion Detection in Wireless Sensor Networks" - ACM Q2SWinet 2005.

Zhu, S; Setia, S; Jajodia, S. – "LEAP: efficient security mechanisms for large-scale distributed sensor networks" – 10th ACM Conference on Computer and Communications Security (CCS '03), Washington D.C., October 2003.