Universidade Nova de Lisboa
Faculdade de Ciências e Tecnologia
Departamento de Informática

Preparação da Dissertação

Mestrado em Engenharia Informática

Secure and reliable routing for dependable wireless sensor networks

Pedro Miguel Oliveira Marques da Silva (nº 26649)

1º Semestre de 2009/10

5 de Fevereiro de 2010

Universidade Nova de Lisboa
Faculdade de Ciências e Tecnologia
Departamento de Informática

Preparação da Dissertação

Secure and reliable routing for dependable wireless sensor networks

Pedro Miguel Oliveira Marques da Silva (nº 26649)

Orientadora: Prof. Doutor Henrique João Lopes Domingos

Trabalho apresentado no âmbito do Mestrado em Engenharia Informática, como requisito parcial para obtenção do grau de Mestre em Engenharia Informática.

1º Semestre de 2009/10

5 de Fevereiro de 2010

Resumo

As redes de sensores são uma tecnologia emergente no domínio da monitorização , de forma autónoma, de ambientes fisicos. São formadas por pequenos dispositivos que se auto-organizam por modo a cobrirem uma área geográfica. Esta autonomia e auto-organização apresenta alguns desafios relacionados com os aspectos de segurança, nomeadamente, no que concerne com o encaminhamento de dados. Assim, o trabalho a realizar pretende contribuir para a criação de um modelo sistémico para o estudo de protocolos de encaminhamento seguro em redes de sensores sem fios (RSSF). A definição do modelo de adversário é o passo inicial para o enquadramento das tipologias de ataque que se pretende avaliar. Aliado ao modelo formal de Dolev-Yao, orientado para os ataques ao meio de comunicação, o estudo de novos modelos de adversário, relacionados com a intrusão ou captura de nós, quer sejam bizantinos ou probabilisticos, é pertinente e apresentado dentro do âmbito deste trabalho.

Com vista a tornar as RSSF resistentes a algumas tipologias de ataques preconizadas no modelo de adversário, têm vindo a ser desenvolvidos diversos algoritmos de encaminhamento seguro. Pretende-se estudar alguns destes algoritmos, representantes do estado da arte neste domínio, estabelecendo uma matriz de medidas de resistência ao modelo de adversário. Os algoritmos alvo deste estudo são o SIGF, Clean-slate e INSENS, entendendo que no seu todo cobrem todas tipologias de ataque em análise, no entanto cada um tem lacunas no seu desenho quando direccionados alguns destes ataques. Ainda como contributo deste trabalho, pretende-se modelar um ambiente de simulação que permita avaliar/analisar, no quadro de ataques definido, as caracteristicas dos protocolos de encaminhamento em RSSF em máteria de segurança e resistência a ataques. Portanto, importa estudar e estabelecer critérios para análise de sistemas de simulação para RSSF das as caracteristicas conhecidas, por exemplo os recursos limitados dos modelos de energia, processamento e comunicação.

Palavras-chave: Redes de sensores sem fios,Protocolos de encaminhamento seguros,Simulação de redes de sensores, Ataque por intrusão

Abstract

The title "Abstract"font times-roman and bold. The text of the abstract with 20 to 30 lines, or 250 to 400 words, font times-roman 12 and 1.5 spacing as a reference.

.... and a blank line and the bar after the last sentence

Keywords: Wireless Sensor Networks,Secure Routing Protocols,WSN Simulation,Intrusion Atack

Conteúdo

Lista de Figuras

Lista de Tabelas

1 . Introdução

1.1 Introdução geral ou Motivação

Os recentes avanços no fabrico de *hardware* de pequena dimensão com capacidades para desepenhar tarefas específicas, tendo em conta também na diminuição do tamanho dos dispositivos de comunicação sem fios, fez surgir, nos ultimos anos um novo campo da investigação, as redes de sensores sem fios. Uma rede de sensores é um conjunto de pequenos dispositivos de computação de baixa potência destribuídos num determinado ambiente com a função de recolher sensorialmente (ou monitorizar) fenómenos fisicos na ausencia de um observador. Um ambiente pode ser um qualquer espaço onde uma RSSF possa ser instalada por exemplo: uma casa, um terreno de combate ou o próprio corpo humano. Entende-se por fenómeno como sendo uma entidade ou caracteristica que é do interesse do observador.

A componente básica e fundamental de uma rede de sensores é o nó sensor (*mote*) . Este pode conter diversos sensores para monitorizar, por exemplo, temperatura, luz ou movimento consoante as necessidades da aplicação. É caracterizado por ser pequeno, pouco poder de computação, baixa largura de banda de comunicação e energia limitada. Conhecidas estas limitações, os sensores têm de ser distribuídos em grande número como forma de aumentar a redundância.

1.1.1 Caracterização de RSSF

As redes de sensores sem fios são um caso especial de redes móveis *ad-hoc*(*MANET*)[2]. Têm surgido com um papel importante no campo da computação móvel e ubíqua. São constituídas por pequenos dispositivos (que vão das dezenas aos milhares de sensores), que podem ser distribuídos, autonomamente, em determinado local, com vista a desempenharem funções de monitorização de fenómenos físicos, como por exemplo, temperatura, humidade, detecção de presença. Estes dispositivos de baixa potência, também denominados sensores inteligentes(*Smart Sensors*)[15], são constituídos por um ou mais sensores, por processador, por memória, por bateria e por um mecanismo de comunicação por rádio-frequência (norma 802.15.4 [**?**]).

No entanto, dadas as características de auto-organização/configuração, encaminhamento

multi-hop, baixo custo, miniaturização e versatilidade de implementação (devido no necessidade de infraestrutura adicional de comunicação entre nós)[15], o seu uso tem-se estendido a outros campos, nomeadamente os do domínio militar, segurança e medicina.[**FALTA UMA REFERENCIA PARA AS aplicações**] Ao contrário do que acontece com as redes convencionais, as RSSF apresentam limitações de energia, alcance de comunicação, processamento, armazenamento e memória. Assim, todo o processamento e comunicação tem sempre em conta estas condicionantes, já que qualquer tarefa desempenhada penaliza o consumo de energia, com especial relevo para a comunicação, que consome muito mais energia do que o processamento. Com isto, a investigação centrada nas RSSF tem vindo a introduzir novos conceitos, a criar ou melhorar protocolos, a construir aplicações e a desenvolver novos algoritmos, com vista a ir ao encontro dos limites impostos pelas restrições das RSSF.

1.1.1.1 Componentes

As RSSF so constituídas, essencialmente, por pequenos dispositivos que desempenham funções diferentes na rede. O *hardware* implementado de pequena dimenso e com caractersticas muito especficas para a tipologia de aplicações s quais se aplica. Os *motes*(denominao dada aos ns de rede de uma RSSF) diferem uns dos outros consoante a sua função na rede, genéricamente poderão desempenhar dois papeis: nó genérico gerador de informação(*source-nodes*) ou nó base ou de sincronizao (n colector de dados da rede ou de execução de comandos de pesquisa)[**REFERENCIA**]. Outro tipo de componente tambm presente so os ns de interligao ou *gateways* que permitem ligar as RSSF a outras redes ou a outras infraestruturas que, com maior capacidade de armazenamento e processamento, permitem efectuar anlise de dados coligidos. Por fim, e no menos importantes, existem ainda os ns de desenvolvimento e teste de protocolos, que possuem ligações a computadores (ligao rede *ethernet*, RS232), podendo ainda funcionar como interligao para *gateways* [**REFERENCIA**]

1.1.1.2 Aplicações

Tendo em conta as caractersticas das RSSF, muitas foram as aplicações encontradas para a utilizao/explorao desta arquitectura distrbuida. O carcter autnomo destas redes oferece um sem nmero de vantagens que propicia a sua utilizao em locais remotos e sem necessidade de manuteno. Sendo assim, as aplicações podero ser divididas nas seguintes classes de funções:

Detecção de alvos/objectos(*Target Tracking*): Detecção de movimento (trajectória/presença) em àreas vigiadas (em teatros operacionais militares, na vigilância de infraestruturas);

Monitorização de fenómenos naturais: Detecção de eventos ou anomalias ambientais (agricultura, poluição, *habitats* naturais), controlo de fenómenos naturais (sismos, vulcões);

Recolha de dados: controlo de indicadores físicos de pessoas e animais (recurso a sensores especiais) normalmente associados a aplicações da medicina

1.2 Descrição e contexto (ou descrição do problema)

A segurança nas RSSF é uma problema *de facto*, com impacto na sua aplicação em sistemas críticos. Apesar da evolução do desenvolvimento de *hardware*, dos nós sensores, indicar que se pretende alcançar dispositivos de muito baixo custo, com menos constragimentos e mais capacidades, a investigação e desenvolvimento necessita de ferramentas que permitam testar novos algoritmos, protocolos, topologias sem que se tenha de instalar uma rede com sensores reais. A aplicação real de sensores, na investigação tem constragimento de ordem orçamental, que limita a dimensão das redes criadas e que não permite a repetição de experiências , variando apenas algumas condições predefinidas. Para suprir estas limitações surge a necessidade de criar sistemas de simulação de RSSF. O que se tem vindo a verificar é que, para cada problema cria-se uma ferramenta que permita testar/avaliar o problema especifico. No entanto, existem determinados modelos que são transversais a qualquer protocolo de encaminhamento que se queira avaliar, por exemplo: consumo de energia, taxa de cobertura, fiabilidade, escalabilidade. No domínio do estudo da segurança em RSSF, não existe uma plataforma que permita modelar protocolos de encaminhamento seguro enformados pelos ataques mais comuns dirigidos a estas redes, de forma simples em que só se esteja centrado no desenho do protocolo. Aliada a esta necessidade, surge também a necessidade de obter medições e resultados referentes a condições de execução das redes, que permitam afinar os protocolos mediante os resultados obtidos e a repetição de experiências nas mesmas condições.

1.3 Solução apresentada (ou âmbito do trabalho)

Assim, o desafio que se coloca é o desenho de um modelo de avaliação de protocolos de encaminhamento seguro em RSSF, que possibilite o desenho e implementação destes protocolos com vista proporcionar mecanismos que visem avaliar estes modelos. Por se tratar de questões de segurança, poder-se-á ainda proporcionar o estudo do impacto dos ataques enformados pelo modelo de adversário apresentado neste trabalho em cada um dos protocolos facilitando assim a avaliação possível adequação dos protocolos implementados.

1.4 Principais contribuições previstas

As principais contribuições previstas devem poder ser descritas em não mais do que uma página, podendo adoptar-se, por exemplo, um estilo de apresentação por itens, com uma pequena descrição de um parágrafo associado a cada item.

2 . Trabalho relacionado

Compete, neste capítulo, explanar o estado da arte em cada uma das vertentes do trabalho, por forma a sustentar a discussão da adequabilidade da solução proposta. Sabendo que a componente de análise crítica é de indispensável presença num trabalho científico, procurar-se-á, sempre que oportuno, acompanhar as explicações com uma interpretação técnica, como forma de justificar as opções efectuadas face panóplia de alternativas existentes na academia.

2.1 Desenho e Implementação de RSSF Seguras

Sendo o tema central do trabalho proposto o estudo das propriedades de segurança nestas redes, importa, em primeiro lugar, perceber, de forma consistente, a sua arquitectura de protocolos. Em segundo lugar, é necessário entender quais os serviços de segurança disponibilizados, por forma a poder adequar-se às aplicações para as quais são criadas e desenhadas as RSSF.

2.1.1 Arquitectura de uma RSSF

As redes de sensores têm uma arquitectura considerada minimalista porque, ao contrário de outras arquitecturas de redes, estão organizadas em menos camadas, fundindo algumas funções desempenhada por camadas inferiores para outras superiores (ex: a camada de aplicação pode desempenhar algumas funções da normalmente atribuídas à camada de transporte). Assim, é fundamental perceber qual a pilha de protocolos que as RSSFimplementam, bem como perceber quais os sistemas que compõem um sensor genérico para de seguida apresentar algumas implementações de sensores.

2.1.1.1 Pilha de Protocolos de uma RSSF

Uma arquitectura para a a pilha de protocolos em RSSF foi proposta por [1], esta pilha apresenta-se representada por cinco camadas: física, ligação de dados, rede, transporte e aplicação. Tendo em conta as características das RSSF, toda a pilha é acompanhada transversalmente por três planos, que devem ser atendidos por cada uma das camadas, de forma a lidarem de forma optima com a energia, mobilidade e recursos partilhados, e estes são os seguintes: plano de gestão de tarefas , plano de gestão de energia e plano de gestão de mobilidade.

Camada Física Esta camada é responsável por selecção de frequência, detecção de sinal e modulação, podendo ainda desempenhar algumas tarefas de encriptação. A minimização do consumo de energia é uma prioridade, as restantes tarefas assemelham-se às restantes redes sem fios. [1].

Camada de Ligação de Dados Das tarefas associadas a esta camada destacam-se as seguintes: multiplexação de dados, acesso ao meio, detecção de erros e detecção de frames. Uma RSSF tem um protocolo de MAC especifico de modo a atender o consumo de energia e os protocolos centrados nos dados. Assim sendo e porque os ambientes de operação têm ruído e os sensores podem ser móveis, o protocolo de acesso ao meio (MAC) tem que lidar com os constragimentos de energia por forma a minimizar colisões a quando do *broadcast* com os vizinhos[1].

Camada de Rede Sendo a energia um tema transversal a toda a pilha esta camada deve endereçar esta preocupação também. No entanto, o facto das RSSF serem essencialmente centradas nos dados, sensíveis à localização e com endereçamento baseado em atributos faz com que estes assuntos sejam também atendidos por esta camada[1]. Repare-se que se a camada de ligação de dados se preocupa com a comunicação entre dois quaisquer nós, a camada de rede deve decidir quais os nós a escolher. Um dos sistemas de encaminhamento mais simples é o baseado na inundação (*flooding*), no entanto, apesar da simplicidade não tem alguns problemas como por exemplo: a duplicação de mensagens e a total ignorância dos recursos da rede, nomeadamente os energéticos, pois se um evento é detectado por mais que um sensor essa informaçaõ vai enundar em duplicado pela rede. Um dos protocolos que minimiza o impacto da inundação é o SPINS[**?**], negociando e adaptando-se aos recursos existentes.

Camada de Transporte Nas redes convencionais a camada de transporte está responsável pela transmissão numa base ponto a ponto. Assim, uma das tarefas importantes a apontar é a de gestão da congestão de tráfego na rede, gestão da fiabilidade da comunicação[**?**][7].

Camada de aplicação Várias são as aplicações ou protocolos desenvolvidos para a camada aplicação normalmente estão associadas às capacidades sensoriais das plataformas, que naturalmente estão relacionadas com o fim para o qual se instala/desenha a RSSF. Alguns dos protocolos para camada aplicação referidos na literatura [1] são os seguintes: *Sensor Management Protocol* (SMP)[**?**] e Task Assignement and Data Advertisement Protocol

(TADAP)[**?**], realça-se no entanto, que nesta área ainda existe muito caminho por percorrer e explorar.

Note-se no entanto que na implementação de alguns protocolos para RSSF algumas camadas não estão presentes por exemplo um protocolo como o LESOP[**?**] as camadas de rede e transporte não são consideradas por forma a simplificar a pilha de protocolos em *motes*. Esta é uma das capacidades destas redes, que corresponde ao facto de adequar de forma especifica a infraestrutura às necessidades de determinada aplicação.

2.1.1.2 Modelo da plataforma genérica de uma RSSF - *Mote*

À semelhança do que acontece com as redes convencionais, existem nós de computação interligados por uma infraestrutura de comunicação. No caso da RSSF, esta infraestrutura corresponde a comunicação *multi-hop* em que cada nó da rede (*mote*) pode desempenhar pelo menos três papeis: 1) Nó gerador de dados, pela captação da eventos associados às especificidades dos sensores possuídos; 2) Nó encaminhador, que recebe dados de outros nós e os passa a outros nós por forma a que alcance o destino; 3) Nó de sincronização ou nó de agregação, embora estas duas caracterizações não correspondam à mesma tarefa por si só, a um nível mais macro, corresponde igualmente a colecção de dados da rede oriundos da detecção de eventos, por forma a faze-la seguir agregada para outro destino (interno ou externo à rede).

Desta forma interessa perceber qual o modelo inerente a estas pequenas plataformas de rede que apesar das características limitadoras da sua execução conseguem executar uma complexidade de aplicações tendo em conta sempre as limitações impostas pela arquitectura. Na figura seguinte apresent-se um modelo [**?**] que ilustra os diversos componentes que concorrem para a efectividade de serviço de um *mote* numa RSSF.

Como se pode observar pela figura, da qual se pode generalizar o modelo de uma plataforma genérica de RSSF, os sistemas que estão presentes são os seguintes: i) Sistema de processamento;ii) Sistema de energia; iii) Sistema de comunicação; iv) Sistema sensorial; v) Sistema de memória. Assim, importa perceber com mais algum detalhe alguns destes sistemas e não menos importante algumas caracterisiticas de sistemas operativos para estas plataformas existentes na actualidade bem como conhecer genéricamente algumas implementações usadas no desenho de RSSF.

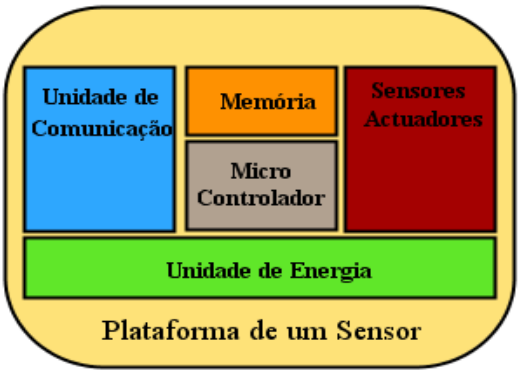

Figura 2.1 Modelo de um Sensor de uma RSSF (baseado em [**?**])

2.1.2 Arquitectura de Serviços de Segurança em RSSF

Muitas vezes considera-se que num sistema seguro, a segurança é um único componente da arquitectura do sistema[**?**]. Todavia, esta visão é redutora, pois, para se conseguir um sistema seguro, é necessário que a segurança esteja integrada em cada um dos componentes, se assim não se verificar cada componente pode corresponder a uma ameaça a partir da qual se pode desencadear um ataque.

Os desafios propostos pelas RSSF são específicos da própria tecnologia, assim sendo os mecanismos tradicionais de segurança podem não ser suficientes. Com isto surgem tecnologias que visam corresponder aos requisitos de segurança das RSSF. Assim, nesta secção pretende-se apresentar uma visão sobre os requisitos de segurança de uma RSSF e como estes são atendidos usando alguns serviços de segurança mais populares.

2.1.2.1 Requisitos de segurança de uma RSSF

Embora se apresente os requisitos de segurança de uma RSSF, estes requisitos podem variar consoante as especificidades da aplicação que a rede visa suportar. Por exemplos se se tratar de uma aplicação de monitorização de saúde uma pessoa, o óbvio é proteger a privacidade da pessoa, mas se se tratar de uma aplicação de monitorização de dados ambientais este requisito pode ser relaxado.
De seguida apresentam-se, de forma genérica, os principais requisitos de segurança de uma

RSSF:

Autenticação Considerando que as RSSF usam um meio de comunicação partilhado, é necessário recorrer à autenticação para garantir a detecção de mensagens alteradas ou injectadas no sistema com o intuito de obter acesso a alguma operação ou informação que é restrita a utilizadores não autorizados[**?**]. No que respeita a autenticação o requisito pode ter dois sentidos: autenticação da origem das mensagens (garantindo que a mensagem é gerada por quem se apresenta como sendo a origem) e autenticação dos dados (garantindo que os dados recebidos são exactamente os enviados). Note-se que a implementação de criptografia assimétrica pode contribuir para a garantia desta propriedade, mas ainda existe muito esforço a desenvolver neste campo dadas as limitações das RSSF e as exigências computacionais e energéticas destes mecanismos.

Confidencialidade Sendo a RSSF uma infraestrutura baseada fundamentalmente na disseminação de dados recolhidos apartir de sensores que se encontram distribuidos em ambiente não controlado e , normalmente, de fácil acesso, pode ser necessário garantir a confidencialidade dos dados que circulam na rede. Assim, o uso de mecanismos de criptografia é o mais usado para protecção de dados em comunicação ponto-a-ponto. O uso de criptografia por si só pode não ser suficiente, uma vez que um ataque pode fazer análise dos dados que circulam na rede (fazendo uma análise de padrões) e com este conhecimento violar as chaves que servem de base ao mecanismo. Desta forma, a utilização de algoritmos de encriptação fiaveis (ex:AES, ECC) para garantir um determinado nível de segurança, para isso existe a necessidade de partilhar chaves de sessão por todos os *end-points* e como tal deve-se recorrer a esquemas de distribuição de chaves.

Disponibilidade Para que consiga atingir um bom nível de disponibilidade é necessário garantir que uma RSSF funcione normalmente durante todo o seu tempo de implementação. Os ataques de negação de serviço (Denial of Service - DoS) são os mais frequentes para atingir a disponibilidade de uma rede. Para além de mecanismos que evitem a negação de serviço, é preciso garantir que a forma de degradação da rede (na presença de um ataque) seja controlada e que a degradação vá sendo tão grande quanto maior sejam o número de nós afectados.

Integridade In communication, data integrity ensures the receiver that the received data is not altered in transit by an adversary. In SPINS, we achieve data integrity through data

authentication, which is a stronger property.

Frescura Given that all sensor networks stream some forms of time varying measurements, it is not enough to guarantee confidentiality and authentication; we also must ensure each message is fresh. Informally, data freshness implies that the data is recent, and it ensures that no adversary replayed old messages. We identify two types of freshness: weak freshness, which provides partial message ordering, but carries no delay information, and strong freshness, which provides a total order on a request-response pair, and allows for delay estimation. Weak freshness is required by sensor measurements, while strong freshness is useful for time synchronization within the network.[**?**]

2.1.2.2 Serviços de Segurança

TinySec[9] TinySec é uma arquitectura de segurança para protecção ao nível de ligação de dados em RSSF. O objectivo principal, para o qual foi desenhado, é providenciar um nível adequado de segurança com o minimo consumo de recursos. Os serviços de segurança disponibilizados são: autenticação de dados (com a utilização de *Message Authentication Codes*(MAC), no caso CBC-MAC[1]) e confidencialidade (a encriptação é implementada com o recursotambém ao CBC-MAC). Para se adaptar às RSSF o MAC tem um comprimeito de 4 bytes ao contrário dos 8 ou 16 habituais. Uma vez que neste mecanismo as propriedades de segurança estão determinadas pelo comprimento do MAC os autores afirmam que para uma RSSF é suficiente uma vez que um atacante teria de efectuar 2^{31} tentativas, que demorariam cerca de 20 meses a realizar com um canal de 19.5Kbs. A frescura das mensagens não foi endereçado nesta arquitectura uma vez que os autores indicaram como demasiado exigente em termos de recursos o que contrariaria o objectivo inicial da arquitectura.

MiniSec[10]

SPINS[?] É um conjunto de protocolos de segurança, constituído por dois componentes principais SNEP[2] [**?**] e μTESLA [**?**]. O primeiro, fornece serviços de autenticação e confidencialidade entre dois pontos de comunicação, encriptando as mensagens e protegendo-as com um MAC. O SNEP gera diferentes chaves, de encriptação, que derivam de uma chave

[1] Cipher Block Chaining - Message Authentication Code (CBC-MAC))
[2] Secure Network Encryption Protocol

mestra partilhada entre os dois nós, ainda é incluido um contador nas mensagens para garantir a frescura. A encriptação é realizada com o modo CTR[3] e a autenticação com CBC-MAC. O segundo componente,o μTESLA, é um serviço de autenticação de *broadcast*, que evita a utilização de mecanismos, mais exigentes, de criptografia assimétrica, recorrendo a critografia simétrica, autenticando as mensagens com um MAC,

Sistemas de distríbuição de chaves[5] Confidencialidade e autenticação são aspectos críticos das redes de sensores com o objectivo de prevenir que um adversário compromenta a segurança de um sistema. Devido à natureza *ad-hoc* das redes, a comunicação intermitente e os recursos limitados, os mecanismos de gestão de chaves e autenticação de grupo tornam-se dificil de alcançar. Alguns esquemas para distribuição e gestão de chaves Key management services must ensure that confidentiality and group- level authentication services are available to authorized parties when needed. These services should not limit the availability of a network and should not create single points of failure.

2.2 Modelo de Adversário e Serviços de Segurança

Quando se tratam de questões de segurança, qualquer se seja o seu domínio, existe uma primeira pergunta que cumpre fazer: "quais são as ameaças/ataques a que está sujeito o objecto que se pretende manter seguro?". Esta pergunta possibilita, desde logo, encetar uma caminhada que visa a identificação de quais os possíveis atacantes, que capacidades estes possuem, quais os meios e modos que estes podem utilizar e em que momento o ataque se pode desencadear. Esta abordagem, um tanto ou quanto generalista, é suficiente para ilustrar a forma como se pretende orientar o estudo e com isto apresentar, nas mesmas vertentes, o modelo de adversário que enforma este trabalho.

2.2.1 Modelo de Dolev-Yao

Um dos modelos de adversário mais conhecidos, quando se trata de análise formal de protocolos seguros, é o modelo de Dolev-Yao [3]. Assim, neste modelo, é considerado que a rede está sobre o domínio do adversário, que perante este facto pode extrair, reordenar, reenviar, alterar e apagar as mensagens que circulam entre quaisquer dois principais legitimos. Com esta

[3] *Counter Mode*

assumpção, entende-se portanto, que o adversário transporta a mensagem e com isso adopta um ataque do tipo *man-in-the-middle*[**?**], com comportamento incorrecto, que o leva a poder alterar o destinatário, atribuir uma falsa origem, analisar o tráfego ou alterar as mensagens. Este funcionamento, entenda-se, não é comparado à intrusão mas sim à intercepção de mensagens que pode ser mitigado usando mecanismos de criptografia.

As tipologias de ataque, consideradas pelo o modelo de adversário de Dolev-Yao são instanciadas pela norma X800 [6] que pretende normalizar uma arquitectura de segurança para o modelo OSI, oferecendo uma abordagem sistemática para o desenho de sistemas seguros. Esta norma considera a segurança sobre três aspectos: ataque, mecanismo e serviço de segurança[**?**]. O primeiro refere-se à forma usada para comprometer um sistema, por exemplo, alterando ou tendo acesso não autorizado autorizado a dados desse sistema. Na literatura, algumas vezes usam-se os temos ataque e ameaça para denominarem o mesmo efeito, no entanto recorrendo ao RFC 2828 [**?**] podemos definir ameaça como uma potencial violação de segurança, ou seja é apenas uma possibilidade que pode ser usada para desencadear um ataque explorando uma vulnerabilidade; no caso do ataque, trata-se da exploração inteligente de uma ou mais ameaças que resultam na violação com sucesso de um sistema que se pretendia seguro. O segundo aspecto considerado, na norma X.800, são os mecanismos de segurança, que se entende como o processo que permite detectar, prevenir ou recuperar de uma ataque à segurança (ex: encriptação, controlo de acesso, assinatura digital)[**?**]. Por fim, o terceiro aspecto define os serviços que, fazendo uso de um ou mais mecanismos de segurança, permitem resistir a ataques dirigidos a determinada fonte de informação, quer seja durante o processamento ou durante a comunicação.

2.2.2 Modelo de Intrusão em RSSF

Considerando o estudo de segurança numa RSSF, e dada a sua exposição natural, nomeadamente a física, colocando cada sensor ao alcance de um qualquer adversário, torna relevante a consideração de novos modelos de ataque. Considerando que cada rede pode ser constituída por milhares de sensores, cada um deles é um ponto de ataque, na impossibilidade de se proteger ou monitorizar todos os sensores instalados[12]. Assim as RSSF vêm-se sujeitas a um modelo de adversário que difere das redes com/sem fios convencionais. Um adversário pode estar perto da rede e ter acesso aos sensores e com isto "roubar" um ou parte dos sensores da rede com

vista a explorar os segredos ou material criptográfico usados para a comunicação. Podemos então tipificar estes ataques como sendo por intrusão. Este tipo de ataques podem ser definidos por ataques desde o nível MAC[14] até ao nível de intrusão física em que um actor externo, tendo acesso a um ou más sensores legítimos, descobre os segredos criptográficos permitindo-lhe replicar[11] os segredos para sensores maliciosos, que depois de introduzidos podem agir de forma coordenada comprometendo a rede. Conseguida a intrusão, o atacante pode induzir nos sensores legítimos comportamentos incorrectos baseados na informação falsa introduzida pelos sensores maliciosos, influenciando o processo de encaminhamento (denominados de ataques ao encaminhamento). Note-se, por exemplo, que estes ataques têm características que os tornam difíceis de identificar quando instalados numa rede, uma vez que o carácter autónomo das RSSF, torna difícil distinguir um comportamento errado de uma falha. Um sensor malicioso pode respeitar o protocolo da rede, no entanto podem actuar de forma incorrecta levando a rede a criar topologias especificas para o ataque (por exemplo, criando partições) ou fazendo, por exemplo, toda a informação passar pelos nós maliciosos, suprimindo ou violando a informação. No que se refere aos ataques direccionados ao encaminhamento, por serem parte do objectivo do estudo deste trabalho, encontram-se definidos na próxima secção e são essencialmente instanciados pela participação colaborativa ou isolada de nós introduzidos com o intuito de afectar o normal funcionamento da rede.

2.2.2.1 Modelo bizantino: adversários bizantinos

2.2.2.2 Novos modelos de adversário - soluções probabilisticas

Sumário Mediante as vulnerabilidades de uma RSSF, é necessário estabelecer um modelo de adversário com vista a poder mapear as capacidades e tipologias de ataques deste em mecanismos de segurança com o propósito de lhes poder resistir ou mitiga-los. O modelo de Dolev-Yao é o modelo de facto quando se trata da análise de ameaças a redes , em que o meio de comunicação está sobre controlo do adversário. No entanto, tratando-se de RSSF, este modelo per si não se vislumbra suficiente para abarcar todas as problemáticas de segurança a que este tipo de redes está sujeita. Surge assim a necessidade de, face à insegurança que cada nó da rede representa, estender este modelo acrescentando-lhe um modelo de intrusão. Perante a exposição das RSSF, os ataques que se podem desencadear podem ser diferentes dos observados nas redes convencionais sendo assim necessário considerar outras tipologias de ataques.

Assim, podemos classificar os ataques como activos e passivos [13] e os atacantes como internos e externos[8]. Nestes ultimos ainda se pode classificar quanto aos recursos usados como *sensor-class* ou *laptop-class*[8]. Os ataques que se consideram para o estudo e relacionados com as RSSF são: falsa informação de encaminhamento, *blackhole*,*sinkhole*, *wormhole* e *sybil attack*[4].

2.3 Modelo de Adversário, Ataques ao Encaminhamento e Contra-medidas

São vários os ataques que se pode direccionar contra a pilha da arquitectura de uma RSSF. Cada uma das camadas da pilha tem vulnerabilidades próprias das funções que desempenha. No escopo deste trabalho o foco é a segurança ao nível dos protocolos de encaminhamento, representada pela camada de transporte, daí nesta secção se apresentar com algum detalhe as fases tradicionais de um protocolo de encaminhamento em MANETs[2] e em particular em RSSF.

Os protocolo de encaminhamento em redes de sensores, de uma forma geral dividem-se em três fases: descoberta dos caminhos, selecção dos caminhos, manutenção da comunicação pelos caminhos seleccionados. Importa neste momento realçar o facto de que os ataques a um algoritmo de encaminhamento normalmente exploraram as vulnerabilidades de cada uma destas fases de forma especifica. Daí, em seguida se proceder à associação dos ataques específicos que se podem desencadear em cada fase e como estes podem ser mitigados aplicando determinados mecanismos de segurança como contra-medidas.

2.3.1 Ataques à organização da rede e descoberta de nós

A fase de organização da rede e descoberta de nós é mais vincada em protocolos do tipo *table-driven*[REF] uma vez que estes desencadeiam a criação de tabelas de encaminhamento que se deverá manter actualizada durante a execução da rede. No entanto em protocolos do tipo on-demand[REF] também se verifica a existencia desta fase mas repete-se em cada inicio de comunicação ou de transmissão. Assim sendo, um ataque do tipo de introdução de informação de encaminhamento falsa, acaba por ter impacto na construção da rede e na descoberta dos nós. A falsificação de informação de encaminhamento permite criar entradas incorrectas nas tabelas de encaminhamento, podendo também fazer com que estas fiquem lotadas, isto em

protocolos que possuem este mecanismo. No caso dos protocolos on-demand o impacto é menos efectivo uma vez que o atacante terá de estar sempre a injectar informação errada a cada inicio de transmissão, mas ainda assim pode provocar danos na rede.

Outro ataque efectivo nesta fase é o *rushing attack* [REF]que é definido pela exploração por parte do atacante de uma janela de oportunidade para responder a um pedido de caminho para um destino. Esta operação é desencadeada quando um protocolo aceita a primeira resposta que recebe (exemplo do AODV[REF]), calculando isto o atacante é sempre um candidato a ser o próximo encaminhador, uma vez que não respeita temporizadores nem condições de resposta. Por fim, pode-se ainda tipificar ataques encetados por flooding de mensagens quer estas sejam HELLO, para os protocolos que usam este mecanismo para que os nós se anunciem aos seus vizinhos, quer sejam mensagens do tipo route-request (RREQ) para iniciar a descoberta de caminhos. O primeiro permite que um atacante com maior capacidade de comunicação se anuncie a todos os nós como seu vizinho (atacante laptop-class[REF]) e por isso toda a informação possa fluir através dele. O segundo, permite explorar as limitações energéticas[REF] da rede levando os nós legítimos da rede a estarem continuamente a responder e fazer as operações inerentes à descoberta de um caminho. Para mitigar ataques de HELLO flooding[**?**] pode-se simplesmente implementar um mecanismo de acknolege aos pacotes de HELLO. Assim, caso esteja a decorrer um ataque com uma capacidade comunicação abrangente de toda a rede, a resposta não será possivel porque os nós mais distanciados não possuiram capacidade de alcançar o atacante, anulando por isso o anuncio de vizinhança.Outra forma é a possivel que cada mensagem de HELLO obriga a autenticação da origem numa entidade central que ao detectar que um nó se está a autenticar com esta mensagem em vários nós então devem ser tomadas medidas para precaver um ataque desta natureza.

2.3.2 Ataques à estabelecimento de rotas

2.3.3 Ataques à manutenção de rotas

2.3.4 Ataques à reorganização da rede

2.4 Estudo de Protocolos de Encaminhamento Seguro para RSSF

2.4.1 *Secure Implicit Geographic Forwarding* (SIGF)

2.4.2 *Secure Sensor Network Routing: Clean-Slate*

2.4.3 *INtrusion-tolerant routing protocol for wireless SEnsor NetworkS* (INSENS)

2.4.4 Discussão

2.4.5 Aspectos em aberto e necessidade de avaliação experimental

2.5 Ambientes de Simulação

Algumas das limitações existentes nas plataformas das RSSF, devem-se ao facto de se pretender manter os sensores com um preço o mais baixo possível. Apesar de cada sensor por si não representar um investimento avultado quando se escala uma rede de 10 sensores para os milhares de dispositivos este valor pode representar valores bastante elevados. No campo da investigação estão a ser introduzidos novos protocolos de encaminhamento, novas aplicações, novos algoritmos e tecnologias de segurança. Como se trata de redes com tempo de vida limitado, devido ao fornecimento de energia ser limitado, o uso real de sensores apresenta-se como uma forma pouco eficiente para o desenvolvimento de novas tecnologias ou melhoramento das existentes.

Os ambientes de simulação de redes de sensores surgem como uma necessidade inevitável, para o rápido teste e desenvolvimento das redes de sensores e todas as tecnologias associadas, antes destas se implementarem. Alguns dos ambientes existentes foram adaptados de outros já existentes para redes sem fios ou *ad-hoc*, como é o caso do NS2[**?**] ou J-Sim[].As RSSF têm caracteristicas especificas que diferem das restantes redes, nomeadamente o modelo de comunicação, que tem avançado para a norma 802.15.4[**?**], bem como a necessidade de monitorizar eficiência energética de cada tecnologia. Outra propriedade importante destes ambientes é a

capacidade de rápidamente repetir experiências com determinadas variáveis configuraveis em cada ambiente (ex. nº de nós, modelo de rádio)

O que se pretende nesta secção é a apresentar diversos ambientes de simulação, mais comuns, e que suportem simular sistema de RSSF (em especial TinyOS). Correspondem a critérios de selecção especificos e enumerados seguidamente, com vista à avaliação de um ambiente que se mostre adequado para a utilização no trabalho de dissertação.

2.5.1 Critérios de Selecção

O número de ferramentas de simulação para RSF, tem vindo a aumentar, no entanto pretende-se analisar ferramentas que possuam as seguintes propriedades:

Portabilidade da Linguagem Devido às caracteristicas da linguagem de programação Java[**?**], inerente ao seu ambiente de execução e à consequente portabilidade para diversas plataformas e a programação orientada a objectos (reutilização) foram seleccionadas ferramentas apenas desenvolvidas nesta linguagem, ainda que algumas possam apresentar linguagem complementares para modelação de aplicaçãos (JSim com o JTcl).

Código Aberto e Livre Esta propriedade permite que se contorne obstáculos inerentes a licenciamento de *software*, bem como possibilita a análise e aproveitamento de todas as funcionalidades existentes, permitindo introduzir algumas melhorias ou alterações especificas.

Modularidade e extensibilidade Tendo em conta que os ambientes não possuem todos as mesmas caracterisiticas e funcionalidades, e considerando que a utilização na componente experimental da dissertação poderá introduzir novos mecanismos ou funcionalidades, o principio da modularidade e fácil extensibilidade facilitará o desenrolar do trabalho.

Documentação Sabendo que algumas das plataformas não se encontram muito bem documentadas este critério será importante como ponto de partida para o entendimento de cada uma das arquitecturas das ferramentas. No caso do JProwler, a simplicidade e a documentação do código é suficiente para ser considerado como adequado tendo em conta este critério.

2.5.2 Prowler/JProwler

Esta ferramenta resulta de uma conversão de um simulador de eventos discretos[4], implementado em MATLAB[**?**], pela universidade de Vanderbilt[**?**], para a linguagem Java. Este simulador pode ser configurado para simular de forma deterministica (permitindo a repetição de experiências) ou probabilistica (adequado para simular a forma não deterministica de comunicação entre motes). Permite a simulação com diversos nós podendo chegar aos 5000 (ainda que o número possa ser maior, por razões de performance é o valor máximo aconselhado) usando diversas topologias(dinâmicas) nas quais se podem implementar os mais diversos algoritmos.
O JProwler modela os aspectos mais importantes de todos os níveis do modelo de comunicação e de aplicação. A natureza não-deterministica da propagação rádio é caracterizada por um modelo de rádio probabilistico usando um modelo simples mas preciso para descrever a operação da camada MAC. Este ferramenta vem com uma janela de visualização da topologia RSSF. Para o desenvolvimento de aplicações ou protocolos são disponibilizadas classes base que se podem estender. Estão presentes dois modelos de rádio: um de Gauss para topologias estáticas e outro de reighXXX para topologias móveis.

2.5.3 J-Sim

J-Sim (anteriormente conhecido como JavaSim) é um ambiente de simulação baseado em componentes [**?**], implementado em Java. Não foi desenvolvido inicialmente com vista a sua utilização em RSSF como é o caso do ambiente SENSE[**?**], mas o objectivo para o desenvolvimento foi o mesmo: extensibilidade. Este ambiente é amplamente usado e implementa um modelo de rede em camadas. No entanto, este simulador não é adequado para o estudo do desempenho em RSSF visto que esta é condicionada pelo *hardware*, pelo sistema operativo, os protocolos de rede e as aplicações assim como optimizações especificas entre camada da pilha de protocolos (ex: implementação de mecanismos de transporte ao nível aplicação). Para além deste problema, J-Sim é um importante ambiente de simulação dada a natureza fracamente acupolada dos seus componetens que permite o rápido desenvolvimento e prototipagem rápida de aplicações.

[4]Fila global onde são inseridos todos os eventos da rede e que são tratados sequencialmente ou por prioridade, dependendo da implementação

2.5.4 Freemote

Fremote é uma ferramenta de emulação [5] leve e distríbuida, desenvolvida em Java, utilizada para o desenvolvimento *software* para RSSF. O emulador suporta motes (Squawk,Sentilla Point) e plataformas (Java cards, SunSpot) baseados em Java. Devide a arquitectura em três camadas bem definidas por interfaces: Aplicação, Encaminhamento e Ligação de Dados e Física. Sendo um emulador, os nós reais podem ser baseado na norma de comunicação IEEE802.15.4[**?**] (ex:MICAz, JMotes, Tmote Sky).

Trata-se de um emulador de RSSF, disponível com um interface gráfico para configuração que permite executar o código em motes baseados em Java. Pode ser usado para o desenvolvimento de algoritms para RSSF, uma vez que suporta experiências de grande escala (até cerca de 10.000 nós) incluindo a integração com nós reais baseados em Java e na norma IEEE802.15.4. Os principais pontos negativos são: 1) o modelo de propagação rádio é muito simples uma vez que não considera obstáculos entre os nós. 2) existe um modelo de comunicação realistico limitado a emulação simples e a plataformas especificas (JMote). 3) Não é orientada para a análise de performance, característica pode ser importante no desenvolvimento de algoritmos para RSSF.

2.5.5 ShoX

Trata-se de um simulador de redes sem fios, implementado em Java[**?**]. A ideia principal desta ferramenta é a de proporcionar, uma forma fácil e intuitiva, a implementação e desenho de protocolos de rede, modelos de mobilidade, modelos de propagação de sinal ou de tráfego de rede. Tal como outros simuladores incorpora um simulador de eventos discretos, que faz a gestão de todos os eventos da rede. Todos os conceitos conhecidos no dominio das redes sem fios são modelados neste simulador (modelo OSI, pacotes,modelos de mobilidade e energia). Uma das vantagens é a existência de classes abstractas para reimplementação de novos modelos de cada um dos componentes faciltando a programação de novos protocolos ou novas funcionalidades. A comunicação entre componentes é feita por intermédio de eventos, ou seja não existe acesso de um componente a outro.
Deve-se destacar o interface gráfico, que permite operar todas funcionalidades da ferramenta

[5] Técnica onde as propriedades de uma rede existente, desenhada, não ideal são simuladas com o objectivo de desempenho, previsão de impacte de modificações por forma optimizar decisões referentes à tecnologia

sem a necessidade de editar directamente os ficheiros de XML. Para além disso é ainda possível visualizar e extrair dados gráficos das simulação e da topologia de rede. O facto do modelo de propagação de sinal ser baseado na norma IEEE802.11, torna dificil a adaptação às condições das RSSF, no entanto a modularidade do sistema permite o desenvolvimento de uma camada IEEE802.15.4 para se aproximar da norma mais recente de comunicação das RSSF.

2.5.6 Discussão

A necessidade de recorrer a ambientes de simulação para desenvolvimento de tecnologias de RSSF é uma realidade difícil de contornar dadas as características das RSSF e a necessidade de estudar todas as suas caracteristicas. O que se tem vindo a observar é que, apesar das multiplicidade de simuladores existentes[**?**], todos os ambientes foram criados ou adaptados com caracteristicas muito ligadas para o fim a que se proponham testar ou avaliar nas RSSF. Analisando algumas destas ferramentas nota-se que não existe uma suficiente genérica e fléxivel que permita avaliar todos os aspectos de uma RSSF. No caso do Freemote, embora especificamente desenvolvida para as RSSF, não incorpora modelos importantes como é o caso da energia, factor altamente restritivo nestas redes, e que, devido ao impacto que tem em cada componente, merece ser modelado e dado alguma atenção. Ainda neste simulador notem-se as carências ao nível do modelo rádio.

Uma das caracteristicas dos simuladores estudados, exceptuando o Freemote, é o facto de serem orientados para redes sem fios em geral ou redes *ad-hoc*. Devido às diferenças que existem entre estas redes e as RSSF torna-se difícil a avaliação devida de protocolos ou aplicações. No entanto é de realçar que o ShoX se apresenta como uma plataforma com bastantes modelos de redes *ad-hoc*, alguns dos quais aplicados a RSSF, nomeadamente o modelo de consumo de energia e o modelo de rádio(ainda que a norma implementada seja IEEE802.11). Quanto à plataforma J-Sim esta tem de ser usada juntamente com um componente de RSSF e requer a implementação dos modelos numa linguagem de *script* que implica: a aprendizagem de uma nova linguagem e o *overhead* de se ligar duas linguagens, que podem penalizar o desempenho da simulação. Por fim, a simplicidade do JProwler pode servir de ponto de partida para a elaboração de um simulador para teste e avaliação de protocolos de encaminhamento seguro, uma vez que tem um comportamento baseado no TinyOS e com modelos do *Mica2* pode ser estendido a incorporar módulos de gestão de energia e de análise gráfica de comportamentos ou eventos que sirvam de indicadores como por exemplo: energia consumida, fiabilidade, tempo

de vida da rede e cobertura.

2.6 Discussão e Resumo do Trabalho Relacionado

3. Abordagem à fase de elaboração da dissertação

4. Plano de Elaboração da Tese

Bibliografia

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. *Computer Networks*, 38(4):393–422, March 2002.

[2] S Corson and J Macker. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, January 1999.

[3] D. Dolev and A. Yao. On the security of public key protocols. *Information Theory, IEEE Transactions on*, 29(2):198–208, 1983.

[4] John Douceur and Judith S Donath. The Sybil Attack. pages 251—-260, 2002.

[5] Laurent Eschenauer and Virgil D. Gligor. A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 41–47, Washington, DC, USA, 2002. ACM.

[6] ITU-T. Recommendation X.800: Security Architecture for Open Systems for CCITT Applications, 1991.

[7] Y.G. Iyer, S. Gandham, and S. Venkatesan. *STCP: a generic transport layer protocol for wireless sensor networks*. IEEE, 2005.

[8] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1(2-3):293–315, September 2003.

[9] Chris Karlof, David Wagner, and Naveen Sastry. TinySec: a link layer security architecture for wireless sensor networks. pages 162–175, Baltimore, MD, USA, 2004. ACM.

[10] Mark Luk, Adrian Perrig, Ghita Mezzour, and Virgil Gligor. MiniSec: a secure sensor network communication architecture. pages 479–488, Cambridge, Massachusetts, USA, 2007. ACM.

[11] B. Parno, A. Perrig, and V. Gligor. Distributed detection of node replication attacks in sensor networks. pages 49–63, 2005.

[12] Adrian Perrig and Haowen Chan. Security and Privacy in Sensor Networks.

[13] William Stallings. *Cryptography and Network Security (4th Edition)*. 2005.

[14] Yang Xiao, Hsiao-Hwa Chen, Bo Sun, Ruhai Wang, and Sakshi Sethi. MAC security and security overhead analysis in the IEEE 802.15.4 wireless sensor networks. *EURASIP J. Wirel. Commun. Netw.*, 2006(2):81–81, 2006.

[15] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal. Wireless sensor network survey. *Computer Networks*, 52(12):2292–2330, August 2008.