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, podendo formar uma rede de larga escala com milhares de nós. Esta autonomia e auto-organização apresenta alguns desafios relacionados com os aspectos de segurança, nomeadamente, no que concerne com o encaminhamento de dados. 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 e captura de nós 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 seguros. Pretende-se estudar alguns destes algoritmos, representantes do estado da arte neste domínio, estabelecendo uma matriz de medidas de resistência ao modelo de adversário, que permita então avaliar a efectividade destes .

Como contributo principal deste trabalho destaca-se a concepção de um ambiente de simulação inovador, uma vez que se pretende implementar funcionalidades não encontradas nos sistemas de simulação para as RSSF existentes. Este sistema proporcionará a possibilidade de desenhar e avaliar algoritmos de encaminhamento, concebidos para serem seguros, quando sujeito a ataques definidos no modelo de adversário. Esta avaliação estará centrada fundamentalmente na análise propriedades como o consumo de energia, fiabilidade, latência, correcção dos dados e correcção do comportamento do protocolo.

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

Abstract

Sensor networks are an emerging technology in the field of monitoring, independently of physical environments. They are formed by small devices that self-organize in order to cover a geographical area can form a network of large scale with thousands of us. This autonomy and self-organization presents some challenges related to security aspects, in particular, with respect to the routing of data.

The work undertaken aims to contribute to the creation of a systemic model for the study of secure routing protocols in sensor networks wireless (WSN). The definition of the type of player is the initial step in the framework of different types of attack that was assessed. Coupled with the formal model of Dolev-Yao, which focuses on the attacks on the media, the study of new models of opponent-related intrusion and capture us is relevant and presented within the context of this work. In order to make the WSN resistant to some types of attacks outlined in this type of opponent, have been developed several routing algorithms insurance. The aim is to study some of these algorithms, representatives of the state of the art in this field, establishing an array of measures of resistance to the type of opponent, which then allows to evaluate the effectiveness of these.

As a major contribution, this study highlight the design of an innovative simulation environment, since they intend to implement features not found in simulation systems for the existing WSN. It will provide the opportunity to design and evaluate routing algorithms are designed to be safe when subject to attacks in the model defined adversary. This evaluation will focus primarily on analysis of properties such as energy consumption, reliability, latency, accuracy of data and correction of the behavior of the Protocol.

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

Conteúdo

Lista de Figuras

Lista de Tabelas

1. Introdução

1.1 Introdução geral

Recentemente, tem-se observado avanços na concepção e fabrico de sistemas computacionais programáveis baseados em hardware de pequena dimensão[67] com capacidades para desepenhar tarefas específicas. Estes avanços permitiram integrar, nesses sistemas, processadores miniaturizados, memória, dispositivos de processamento de sinal e de conversão analógica-digital associada ao sensoriamento de diferentes fenómenos físicos (através de diversos tipos de sensores) e capacidades de comunicação sem fios por rádio frequência (baseados em normas como 802.15.4[16, 21] e Zigbee[21])). A possibilidade de construção destes dispositivos (que se designam mais simplesmente por nós sensores) fez surgir, nos últimos anos, um novo campo da investigação conhecido pela área das redes de sensores sem fios (RSSF).

Uma rede de sensores é formada por um conjunto de pequenos dispositivos com as características anteriores, distribuídos numa certa área geográfica, que podem funcionar de forma autónoma ou sem supervisão humana e que, com maior ou menor densidade, permitem monitorizar diferentes fenómenos físicos associados ao meio ambiente envolvente. Possuem características de auto-organização, podendo ser formadas por um menor ou maior número de sensores e permitindo cobrir desde pequenas a vastas áreas de monitorização. Um ambiente de instalação de uma rede de sensores sem fios tanto pode ser um edifício, uma instalação industrial, uma área de combate, uma vasta zona de monitorização de um habitat natural, um veículo, como o próprio corpo humano[65, 48, 49, 18].

A componente básica e fundamental de uma rede de sensores é pois o nó sensor (também designado por *mote*)[8, 1, 13, 9]. Cada um destes nós é visto como um substrato computorizado que pode possuir diversos sensores para monitorizar, por exemplo, temperatura, luz, movimento e outros fenómenos físicos, consoante as necessidades das aplicações. Sendo um dispositivo miniaturizado e concebido para possuir um baixo custo de produção, apresenta um poder de computação limitado, baixa largura de banda de comunicação, curto alcance de comunicação rádio e energia autónoma limitada[71]. Numa rede de sensores a energia pode constituir um recurso finito. Pois, em certos ambientes de instalação pode não ser possível, ou viável, realizar operações que exijam intervenção ou supervisão humana, por exemplo, para o carregamento ou substituição de baterias. Conhecidas estas limitações, para se poderem atingir distribuições de

grande cobertura geográfica, os sensores têm de ser distribuídos em grande número, podendo-se também, por esse meio, aumentar a redundância dos nós que assim formam redes de larga escala que chegam a atingir milhares de nós.

Sendo o hardware de pequena dimensão e com características muito específicas para a tipologia de aplicações às quais se aplica, os *motes*, diferem uns dos outros consoante a sua função na rede e poderão desempenhar, fundamentalmente, dois papeis: nó genérico gerador de informação (source-nodes) e nó base ou de sincronização (nó colector de dados da rede ou de execução de comandos de pesquisa). Numa RSSF os nós podem também actuar como nós de interligação (ou de encaminhamento e processamento intermédio através da rede) ou gateways (que permitem ligar o ambiente da rede de sensores a outras redes e sub-sistemas externos). Assim, uma RSSF pode ser concebida de forma a ser interligada a outras infraestruturas computacionais que, com maior capacidade de armazenamento e processamento, permitem efectuar análise de dados coligidos. Na tecnologia actual existem ainda nós de desenvolvimento, que possuem ligações a computadores (ex: ligação de rede ethernet, RS232 ou USB), permitindo o desenvolvimento e carregamento expedito de código desenvolvido em estações de desenvolvimento. Os sensores dotados de ligações Ethernet, RS-232 ou USB podem ainda funcionar como nós de tipo gateway, permitindo num cenário concreto ligar a rede de sensores a aplicações executando em sistemas de computadores usuais[3].

1.1.1 Caracterização de RSSF

As redes de sensores sem fios podem ser abordadas como um caso especial de redes *ad-hoc*, embora exibam características especificas que podem ser mais ou menos diferenciadas[24]. As RSSF para aplicações de larga escala fazem emergir algumas problemáticas inerentes a aplicações distribuídas, com especificidades e desafios próprios [25], nomeadamente ao nível dos mecanismos de gestão, da organização topológica autónoma, das necessidades de sistemas de encaminhamento *multi-hop*, de requisitos de tolerância a falhas, de requisitos de escalabilidade ou de necessidade de serviços de segurança.

1.1.2 Aplicações

Muitas foram as aplicações[18, 43] encontradas na investigação ou na utilização emergente de redes desensores com diferentes requisitos de escala[71]. O carácter autónomo destas redes

oferece um sem número de vantagens que propicia a sua utilização em locais remotos de acessibilidade difícil e onde não é possível a sua manutenção e supervisão. De entre as aplicações das RSSF, podem destacar-se as seguintes:

Detecção de alvos/objectos(*Target Tracking*): [65] associadas à detecção de movimento (trajectória/presença) em àreas vigiadas (como por exemplo, em teatros operacionais militares ou na vigilância e monitorização de recursos ou infraestruturas);

Monitorização de fenómenos naturais: [48]associadas à detecção de eventos ou anomalias ambientais (com aplicações na agricultura, monitorização de poluição ou monitorização de habitats naturais), bem como de vigilância ou controlo de fenómenos naturais (sismos, actividade de vulcões, etc);

Recolha de dados: [49] associadas ao controlo de indicadores físicos ou biomédicos de pessoas ou de animais (com recurso a sensores especiais associados a aplicações da medicina) ou como ambientes de monitorização de operação de infra-estruturas críticas (pontes, edifícios, sistema electro-mecânicos ou equipamentos de instalações fabris).

1.2 Segurança em RSSF

A segurança nas RSSF é uma problema *de facto*, quando se perspective a sua aplicação em sistemas críticos. A segurança deve ser pensada em tempo de concepção[57], tendo em vista a abrangência do sistema e tendo em atenção as particularidades específicas da tecnologia inerente e dos ambientes onde são implementadas. Importa analisar as hipóteses de desencadeamento de ataques a estas redes (a partir de hipóteses de modelos de adversário que devem ser considerados em cada caso) bem como as repercussões das potenciais tipologias de ataques[73, 41] a uma plataforma genérica de uma RSSF, de modo a reduzir as suas vulnerabilidades e de modo a antecipar o impacto desses ataques na operação da rede. Esta análise deve ser feita tendo em conta a pilha de protocolos[18] e de serviços associados ao *software*[14, 2, 42, 59] que executa em cada nó, uma vez que cada uma das camadas de serviços e protocolos pode ser vulnerável a esses ataques.

Na abordagem de uma plataforma usual e genérica para um nó de uma RSSF, verifica-se que, em geral, cada nó apresenta uma pilha de protocolos e serviço muito simplista ou minimalista, por comparação com uma pilha associada a uma rede de computadores usual (ex., TCP/IP ou pilha OSI[64]. As limitações impostas pelas dimensões e as capacidades de operação não

permitem uma arquitectura muito ambiciosa e, por outro lado, as RSSF possuem geralmente uma vocação orientada para aplicações específicas, que condicionam os serviços que devem ser suportados na pilha. As camadas de operação de um nó sensor são essencialmente cinco[18]: camada física, camada de ligação de dados, camada de rede, camada de transporte e camada de aplicação, embora na maior parte dos casos, a camada de transporte de dados e a funcionalidade inerente à camada de rede sejam concebidas e já estejam de facto associadas ao suporte da aplicação. Na investigação, verifica-se ainda que a própria camada de ligação de dados (nível MAC e protocolos data-link) tenham sido estudados e propostos em diferentes variantes que podem ter vantagens particulares dados os requisitos de operação das aplicações[60, 70, 26].

Alguns autores[68, 27, 55] têm vindo a desenhar algoritmos com vista a minimizar o impacto dos ataques ao encaminhamento, durante a operação das RSSF. Estes algoritmos, pretendem garantir algumas propriedades de segurança [62] (ex: confidencialidade, integridade, autenticação,frescura). Com este facto, tendo em conta que um único protocolo, pode não endereçar todas as tipologias de ataques, surge a necessidade de efectuar um estudo sistemático das suas características. Este estudo, normalmente é realizado com recurso a modelos matemáticos, análises teóricas ou experiências de pequena dimensão, que apenas permitem extrapolar medidas de resistências a ataques, ou outras características, nomeadamente as relacionadas com a performance, escala ou energia, medições estas que podem ser pouco representativas.

1.3 Objectivos e contribuições previstas para a dissertação)

Uma das vertentes do estudo da segurança em RSSF tem a ver com a possibilidade de se poderem efectivar ataques ao nível rede, na visão de estruturação de uma pilha de suporte de serviços de software. Diferentes tipologias de ataques [41, 36, 57] exigem diferentes tipos de contra-medidas, que normalmente são combinadas em mecanismos de segurança inerentes à proposta de sistemas de encaminhamento seguro apropriados às características e operação das RSSF[59, 45, 42].

Conhecidas que estão as dificuldades existentes no estudo de protocolos de encaminhamento seguro[41, 50], estes permanecem como um dos aspectos em aberto e de desafio à concepção de RSSF que operem em condições de segurança. Este desafio é tanto mais relevante quanto a análise de segurança pode envolver a avaliação de diferentes modelos e hipóteses de adversário[28, 54], e com implicações em diferentes tipologias de ataques [73, 41]

que nem sempre são estudados de forma sistemática e comparativa na abordagem de diferentes protocolos de encaminhamento seguro que vão sendo propostos. Por outro lado, existe uma dificuldade adicional em poder conjugar-se o estudo das contra-medidas de segurança de um protocolo de encaminhamento e a avaliação experimental face a uma implementação. Assim, para cada protocolo e de forma complementar a uma avaliação experimental, interessa medir o impacto que diferentes tipologias de ataques podem ter, nomeadamente, para cenários de grande escala. Portanto, é particularmente importante que se desenvolvam sistemas de simulação[10, 5, 11, 12, 6, 4] de RSSF que permitam simular diferentes hipóteses de ataque e antecipar o seu impacto, não apenas no comportamento dos protocolos de encaminhamento mas, complementarmente, no impacto que podem ter sobre a própria rede, nomeadamente no que se refere, à energia, à fiabilidade ou à latência, durante a operação. Um sistema que suprima estas dificuldades, contribui para um mais rápido desenvolvimento e uma afinação mais cuidada de determinados parâmetros dos protocolos com vista a garantir as propriedades de segurança desejadas para o ambiente de operação das RSSF.

No âmbito do trabalho que se pretende desenvolver na elaboração da dissertação, ao qual se refere este relatório, pretende-se conceber e desenvolver um sistema de simulação inovador que permita o estudo sistemático de protocolos de encaminhamento, desenhados com o intuito de providenciar mecanismos de segurança, que possua em particular as seguintes funcionalidades:

- Interface de visualização e configuração da rede, nomeadamente, com informações dos parâmetros de simulação e informação detalhada de cada nó, bem como o estado energético e o grau de ameaça a que está sujeito;

- Implementação de um modelo de energia que permita extrair consumos em diferentes momentos de operação: operação normal e operação perante determinado ataque;

- Motor de geração de topologias, sabendo que as topologias da rede podem ter influência no seu comportamento, introduz-se esta funcionalidade como forma de distribuir os nós de diversas formas na área de monitorização: distribuição aleatória, distribuição em grelha, distribuição controlada (estruturada);

- Mecanismos de introdução de falhas/ataques na rede. Com este mecanismo pretende-se capacitar o autor, de determinado protocolo, da possibilidade de introduzir ataques tipificados (ex: ao meio de comunicação ou intrusão) e de provocar mutação de código, com vista a induzir alterações no comportamento do protocolo;

- Utilitários de recolha de dados da simulação, em tempo real e em tempo diferido, que permitam a extracção de medições referentes a propriedades importantes como consumos de energia, latência, fiabilidade, correcção do protocolo e correcção dos eventos, diponibilizando-os de forma gráfica.

1.4 Principais contribuições e a sua avaliação

As principais contribuições resultantes da elaboração da dissertação são em especial duas: Concepção de uma plataforma de simulação para protocolos de encaminhamento seguro em RSSF e a prova de conceito, com a implementação de dois protocolos usando a plataforma concebida. No caso da primeira contribuição, pretende-se, com a implementação das funcionalidades anteriormente descritas, possibilitar a avaliação sistemática de algoritmos de encaminhamento. Esta avaliação permitirá a análise de propriedades tão importantes como: o consumo de energia, a fiabilidade da rede, latência das comunicações, correcção dos dados e a correcção do protocolo. Propriedades estas, que normalmente, são extrapoladas da implementação experimental em pequena escala ou da adopção de modelos matemáticos , que devido a variaveis externas, próprias do ambiente de operação, podem se afastar bastante dos resultados reais.

A segunda contribuição, decorre da primeira e consiste na implementação de dois algoritmos de encaminhamento seguro. Funcionando como prova de conceito, pretende aferir a usabilidade da plataforma, para o fim que foi concebida mas, pretende também, fazer um estudo comparativo entre os algoritmos implementados, pela observação das propriedades já referidas. Permitindo assim desenvolver uma análise crítica em relação a trabalhos publicados relacionados com estes algoritmos. Contribui ainda, com o estabelecimento de uma base de comparação, para futuras avaliações, de outros protocolos emergentes, no que se refere ao impacto que os mecanismos de segurança, têm sobre as propriedades mencionadas.

2 . Trabalho relacionado

Este capítulo apresenta uma visão do estado da arte relacionado com a segurança e modelos de simulação em RSSF. Assim, a primeira secção apresenta a definição do modelo de adversário e tipologias de ataques, a segunda, alguns protocolos de encaminhamento seguro e por fim, a terceira secção, apresenta diversos ambientes de simulação relacionados com as RSSF e *ad-hoc*. Culminando com uma discussão e análise crítica do trabalho relacionado.

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

2.1.1 Arquitectura de Serviços de Segurança em RSSF

Num sistema seguro, é necessário que a segurança esteja integrada em cada um dos seus componentes, não se confinando a um componente isolado do sistema[58]. Assim, nesta secção apresenta-se, introdutoriamente, alguns requisitos de segurança de uma RSSF e alguns serviços de segurança, que foram implementados com o objectivo de representarem um ponto de partida para a garantia de propriedades de segurança, a quando do desenho de RSSF seguras.

2.1.1.1 Requisitos de segurança de uma RSSF

Os requisitos de segurança de uma RSSF podem variar consoante as especificidades da aplicação que a rede visa suportar. No entanto, apresentam-se, de forma genérica, os principais requisitos de segurança de uma RSSF[58]:

Autenticação Devido ao meio de comunicação ser partilhado, é necessário recorrer à autenticação para garantir a detecção de mensagens alteradas ou injectadas no sistema por participantes não autorizados[58]. Note-se que a implementação de criptografia assimétrica contribui 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 a partir de sensores que se encontram distribuidos em ambiente não controlado e, normalmente, de fácil acesso, é necessário garantir a confidencialidade dos dados que circulam na rede. Assim, o uso de mecanismos de criptografia é o mais

indicado para este tipo de protecção.Desta forma, é necessária a utilização de algoritmos de encriptação fiáveis (ex: AES[1][63], ECC[63]) 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[30].

Disponibilidade Entende-se por disponibilidade de uma rede, a garantia de que esta funciona efectivamente durante o seu tempo de operação. Os ataques por negação de serviço (Denial of Service - DoS)[33] são os mais frequentes para diminuir a disponibilidade de uma rede. Então, para além de mecanismos que evitem a negação de serviço, é necessário garantir que a degradação da rede (ex: na presença de um ataque) seja controlada e que vá sendo proporcional ao número de nós comprometidos.

Integridade A integridade garante que os dados recebidos por um nó não foram alterados, por um adversário, durante a transmissão. Em alguns casos esta propriedade é garantida juntamente com a autenticação, usando mecanismos que permitam garantir ambos numa só operação. Por exemplo, o uso de CMAC's[63] é vulgar uma vez que permite autenticar (uso de critografia simétrica) a mensagem e para garantir a integridade da mensagem.[59].

Frescura A frescura de uma mensagem implica que estes sejam recentes, garantindo que esta não é antiga e não foi reenviada por um qualquer adversário. [59, 45] Podem-se considerar dois tipos de frescura: frescura fraca (garantindo ordem parcial e sem informação do desvio de tempo, usada para as medições dos sensores) e frescura forte (garante ordem total em cada comunicação permitindo estimar o atraso, usada para a sincronização de tempo).

2.1.1.2 Serviços de Segurança

Alguns serviços de segurança têm vindo a ser desenvolvidos para as RSSF com vista a garantir a segurança ao nível da comunicação (ex: criptografia, assinaturas, *digests*). Estes serviços permitem que o arquitecto de sistemas se centre em outras problemáticas relacionadas com o comportamento dos protocolos face outros ataques. Apresentam-se de seguida alguns serviços mais comuns:

TinySec[42] 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 mínimo consumo de recursos. Os serviços de segurança

[1] *Advenced Encryption System algorithm*

disponibilizados são: autenticação de dados (com a utilização de *Message Authentication Codes*(MAC)[63], no caso CBC-MAC[2]) e confidencialidade (CBC-MAC). Não implementa nenhum mecanismo que garanta a frescura das mensagens, tornando-o vulnerável a ataques de *replaying*).

MiniSec[45] Minisec é uma camada de rede concebida para possuir baixo consumo de energia, melhor que o TinySec, e alta segurança. Uma das caracteristicas principais, que a tornam mais eficiente, é o uso do modo *offset codebook* (OCB)[63] para encriptação de blocos. O que permite numa única passagem autenticar e encriptar os dados, sem com isso aumentar o tamanho da mensagem em claro, contribuindo para um menor consumo de energia. Esta arquitectura tem dois modos de operação: uma baseado paracomunicação *unicast* (MINISEC-U) e outro para *broadcast* (MINISEC-B). Sendo que a segunda não necessita de manter o estado (sincronização de contadores) por cada emissor por forma a proteger o reenvio escalando para grandes redes.

SPINS[59] Conjunto de protocolos de segurança, constituído por dois componentes principais SNEP[3] [59] e μTESLA [59, 46]. O primeiro, fornece serviços de autenticação e confidencialidade entre dois pontos de comunicação, encriptando as mensagens (com o modo CTR[4]) e protegendo-as com um MAC (autenticação com CBC-MAC). O SNEP gera diferentes chaves, de encriptação, que derivam de uma chave mestra partilhada entre os dois nós, com umcontador de mensagens para garantir a frescura. O segundo componente,o μTESLA[59, 46], 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,

Norma IEEE802.15.4[16] Esta norma define a especificação da camada física e de controlo de acesso ao meio das redes pessoais de baixa potência (*LRPAN*[5]). Foca-se essencialmente na comunicação entre dispositivos relativamente próximos, sem a necessidade de uma infrastrutura de suporte, explorando o mínimo de consumo de energia. É a norma que já se encontra implementada em algumas plataformas das RSSF. (ex: Micaz[9]). Esta norma, especifica alguns serviços de segurança[21], representam uma primeira linha de protecção contra ataques à infraestrutura. Estes mecanimos são os seguintes: i) Cada dispositivo mantém uma lista de controlo de acessos (ACL) dos dispositivos confiáveis

[2]Cipher Block Chaining - Message Authentication Code (CBC-MAC))
[3]Secure Network Encryption Protocol
[4]*Counter Mode*
[5]Low Rate Personal Area Networks

filtrando comunicações não autorizadas; ii) Encriptação de dados, partilha de uma chave criptográfica entre os intervenientes na comunicação; iii) Serviço de integridade de cada *frame*, adicionando a cada frame uma *Message Integrity Code* (MIC)[63]; iv) Garantia de frescura de mensagens (*Sequential Freshness*), utilizando contadores de frames e de chaves.

ZigBee[21, 15] Com a norma 802.15.4 orientada para as duas camadas mais baixas da pilha de protocolos das RSSF (física e MAC), a norma ZigBee define as especificações para a camada de rede e aplicação. Já incorpora alguns serviços de segurança, nomeadamente: i) Frescura, mantendo contadores associados a cada chave de sessão, que são reiniciados em cada mudança de chave; ii) Integridade, com opções de integridade de mensagens que vão desde os 0 aos 128 bits de verificação; ii) Autenticação, ao nível de rede e ao nível de ligação de dados; iv) Confidencialidade, com o algoritmo AES[63] com 128 bits. Esta arquitectura utiliza um *trusted center* para gestão da segurança na rede, implementando um coordenador de rede ZigBee. Este, acreditado por todos os nós da rede, pode desempenhar três funções: i) Autenticação de nós que pretendem participar na rede; ii) Manutenção e distribuição de chaves; iii) Providenciar segurança ponto-a-ponto entre nós da rede.

2.1.2 Modelo de Adversário

A definição do modelo de adversário permite desde logo identificar as características quanto às capacidades dos atacantes e os ataques que se podem desencadear na rede. Assim, nesta secção, caracteriza-se o modelo de adversário que enforma este trabalho.

2.1.2.1 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 [28]. 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 assumpção, entende-se portanto, que o adversário transporta a mensagem e com isso adopta um ataque do tipo *man-in-the-middle*[63], 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 [39] 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[63]. 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 [61] 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)[63]. 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.

2.1.2.2 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 adversário, torna relevante a consideração de novos modelos de ataque. Considerando que cada rede pode ser constituída por milhares de sensores, cada um destes sensores é um ponto de ataque[57]. Assim, as RSSF vêm-se sujeitas a um modelo de adversário que difere das redes com/sem fios convencionais. Pode-se então tipificar estes ataques como sendo por intrusão e por captura.

Este tipo de ataques podem ser definidos por ataques desde o nível MAC[69] até ao nível de intrusão física, em que um actor externo, captura um ou mais sensores legítimos, descobre os segredos criptográficos. Este facto permite-lhe replicar[54] os segredos para sensores maliciosos, introduzido-os na rede de modo a que, agindo coordenadamente, possam comprometer 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 (desencadeando ataques ao encaminhamento). Estes ataques, são de difícil detecção, uma vez que o carácter autónomo das RSSF, pode não permitir distinguir um comportamento errado de uma falha. Com a intrusão, um sensor malicioso embora respeite o protocolo da rede, pode actuar de forma incorrecta levando a rede a criar topologias especificas para determinado ataque ou forçando, toda a informação a passar por nós maliciosos, que podem suprimir ou violar a informação.

2.1.2.2.1 Modelo bizantino: adversários bizantinos O modelo de ataques por intrusão tem algumas parecenças com as denominadas falhas bizantinas[23], que são caracterizadas como falhas arbitrárias para as quais um sistema não está, à partida, preparado para lidar e que se pode traduzir em comportamentos inesperados. Transpondo esta realidade para as RSSF[47], é dificil detectar a introdução de nós maliciosos, autónomos ou replicados a partir de um nó que foi comprometido. No entanto alguns autores [54, 23] têm-se debruçado sobre esta problemática a fim de dotarem os algoritmos de mecanismos que permitam detectar a replicação de nós maliciosos numa RSSF. Para se lidar com os ataques com comportamentos bizantinos, implementam-se mecanismos probabilisticos que, ainda que não possam mitigar o ataque por completo, aumentam a resiliência e acabam por transformar um ataque num mal menor, definindo até onde pode ser comprometida a rede por forma a garantir a fiabilidade necessária para a operação.

2.1.3 Ataques ao Encaminhamento

Apesar de existirem ataques que podem ser dirigidos a qualquer das camadas da pilha da RSSF, em particular apresentam-se os ataques relacionados com a camada de rede, responsável pelo encaminhamento de dados. Os protocolo de encaminhamento em MANETs[24] e em redes de sensores, de uma forma geral, decompõe-se em três fases: descoberta dos caminhos, selecção dos caminhos e manutenção da comunicação pelos caminhos seleccionados. Os ataques a um algoritmo de encaminhamento, normalmente, podem explorar as vulnerabilidades de cada uma destas fases de forma especifica. Daí, em seguida se proceder à associação dos ataques específicos a cada fase apresentando as contramedidas que permitem mitigá-los.

2.1.4 Ataques à organização da rede e descoberta de nós

Após a descoberdos nós vizinhos é necessário recolher informação para a construção das tabelas de encaminhamento, isto nos protocolos do tipo *table-driven*[19]. No entanto, em protocolos do tipo *on-demand*[19] esta fase é desencadeada em cada início de transmissão.

Falsificação de Informação de Encaminhamento Este ataque tem impacto na formação da rede e na descoberta dos nós. Induz a criação de entradas incorrectas nas tabelas de encaminhamento, podendo também fazer com que estas fiquem lotadas e inválidas. Nos protocolos *on-demand*, o impacto pode ser menor, uma vez que obriga o atacante a injectar informação errada a cada ciclo de transmissão.

Rushing Attacks Outro ataque nesta fase é o *rushing attack*[37] que é definido pela exploração, por parte do atacante, de uma janela de oportunidade para responder a um pedido de caminho para um destino. Este ataque é efectivo quando o protocolo permite aceitar a primeira resposta que recebe (ex: AODV[56]). Explorando isto, o atacante é sempre um candidato a ser o próximo encaminhador, uma vez que não respeita temporizadores nem condições de resposta, podendo influenciar as rotas.

2.1.4.1 Contra-medidas

A aplicação de mecanismos de autenticação no protocolo de encaminhamento faz com que ataques de falsificação de informação seja minimizados. Os nós da rede podem partilhar chaves simétricas como forma de autenticar as mensagens de dados e controlo do encaminhamento (RREQ e RREP). Desta forma, o atacante como não possui a chaves necessárias para a comunicação, não poderá participar no protocolo.

Para fazer face a ataques de *rushing*, alguns autores [37] apresentam dois mecanismos de defesa: reenvio aleatório de RREQ ()*randomized RREQ forwarding*) e detecção segura (*secure detection*). No primeiro mecanismo, cada nó guarda um conjunto de mensagens RREQ escolhendo depois aleatóriamente um para reenviar. Ainda assim, pode ser seleccionada uma mensagem RREQ maliciosa, daí a existência do segundo mecanismo, que proporciona a troca de mensagens autenticadas entre dois nós garantindo que as mensagens pertencem a nós legítimos.

2.1.5 Ataques ao estabelecimento de rotas

HELLO Flooding Este ataque explora os protocolos que fazem anunciar a sua próximidade, aos vizinhos, emitindo mensagens de *HELLO*, [66, 41]. Os protocolos baseados na localização podem ser vulneráveis a este ataque, uma vez que, com um dispositivo do tipo *laptop-class*[41], que possua um alcance rádio suficientemente potente para cubrir toda a rede, permite anunciar-se a todos os nós como vizinho, forçando a informação fluir através dele.

Ataque Sinkhole Nas RSSF um dos modos de comunicação é de um-para-muitos(*one-to-many*). Este tipo comunicação apresenta algumas vulnerabilidades a ataques do tipo *sinkhole*[52]. Assim, um atacante informa os nós vizinhos, anunciando-se como um nó que tem boa comunicação com o nó *sink*, tornando-se assim um ponto de passagem de informação. O ataque é realizado enviando pacotes de RREQ, alterando a origem e aumentando o número de sequência como forma de garantir que a esta informação se sobrepõe a qualquer outra, legítima, da rede. Em determinada altura, um atacante poderá ter, a passar por ele, um número elevado de rotas, podendo, então, alterar ou encaminhar, de forma selectiva, a informação. Os protocolos *table-driven* são vulneráveis a estes ataques, enquanto os protocolos baseados em localização não o são, devido às suas rotas serem *on-demand*.[41, 66, 73]

Ataque Wormhole Neste tipo de ataque, apresentado por Perrig et al [35] a colaboração de dois nós maliciosos (normalmente a muitos *hops* de distância), colaboram para a realizaçãoefectividade do ataque. Assim, os atacantes estabelecem uma ligação (ou túnel, normalmente de melhor qualidade ou maior largura de banda) para comunicarem entre si. Permitindo a um nó malicioso capturar pacotes ou partes de pacotes e enviá-los pela ligação privada para o outro atacante no outro extremo da rede. Este ataque é particularmente eficaz em redes *ad-hoc* e redes baseadas em localização. Sendo estas compremetidas, não conseguiram estabelecer caminhos maiores do que dois hops, causando interrupções nas comunicações[72, 66]. Para além disso, este ataque transforma os atacantes em nós muito solicitados, pois apresentam-se aos outros nós participantes como tendo uma melhor ligação e estar a menor distância do destino.

Ataque Sybil Este ataque foi definido como um ataque que permitia atingir os mecanismos de redundância em armazenamento distribuído em ambientes de ponto-a-ponto[29]. Outra definição que surge, agora associada às RSSF, é a que o define como “um dispositivo malicioso que

ilegitimamente assume múltiplas entidades"[51]. Com estas definições e devido à sua taxonomia, é um ataque bastante efectivo contra protocolos de encaminhamento[41]. Em particular, os protocolos que adoptam múltiplos caminhos. Um nó ao assumir múltiplas identidades oculta o facto dos dados estarem a passar por um único nó malicioso[66, 73].

2.1.5.1 Contra-medidas

Uma das formas de prevenir um ataque HELLO flooding[41] é a implementação de mecanismos de respostas(*acknowlege*) a anúncios HELLO. Desta forma, caso o atacante esteja a usar um meio de comunicação potente, que cubra toda a rede, caso um nó legítimo se encontre fora do alcance de resposta, não considerará o anúncio como válido. Para além deste mecanismo, é possível proceder à autenticação da mensagem, certificando-a numa entidade central, que ao detectar que um nó se anuncia como vizinho de muitos outros nós, pode tomar precauções, repudiando o nó com a emissão de uma mensagem para toda a rede[66].

Alguns autores têm vindo a desenvolver algoritmos que visam a detecção de atacantes que desencadeam ataques do tipo *Sinkhole*[52], um desses mecanismos é o *Sinkhole Intrusion Detection Sistem* (SIDS)[52] orientado para a detecção destes ataques ao protocolo DSR[40]. Estes sistema propõe três mecanismos para detectar um atacante: i) Discontinuidade de números de sequência, tendo em conta que um atacante tentará usar números de sequência muito grandes, assim um nó pode identificar os que crescem rápidamente ou que não respeitam uma ordem crescente, considerandos um ataque; ii) Verificação de pacotes, os vizinhos podem certificar a origem dos pacotes enviados por um nó. Isto será dificil de realizar nos pacotes atacantes, uma vez que a origem é alterada. Assim, poder-se-á detectar que a rede está sobre ataque, se circularem muitos pacotes não certificados; iii) Número de caminhos a passar por um nó, cada nó pode observar a sua tabela de encaminhamento e se detectar que existem muitos caminhos a passar pelo mesmo nó, pode estar na presença de um ataque do tipo *Sinkhole* e reagir a este facto[66, 73]

A utilização de *packet leashes*[34] permite mitigar o ataque *wormhole*. Assim, existem dois tipos de condições para se aceitar os pacotes vindos de uma origem: baseado na localização e notempo. O primeiro, permite que um nó receptor, conhecendo a localização da origem, saiba se um pacote atravessou a rede por um *wormhole*, calculando a distância entre os dois pontos. No segundo caso, baseia-se essencialmente no tempo de transmissão do pacote, exigindo então a sincronização de relógios. Se for muito rápido a chegar ao destino, este nó assume que se está

perante um ataque de *wormhole*.

Para o ataque *sybil* em [51, 66], são possíveis dois esquemas de protecção: i) *Radio resource testing* (cada vizinho só pode transmitir num canal, selecciona um canal para receber e enviar uma mensagem, os nós que não responderem são tratados como falsos); *Random key distribution*(usando um modelo de *key-pool* são atribuidas n chaves de um conjunto de m. Se dois nós partilharem q chaves então estarão em condições de comunicar de forma segura. Uma função de dispersão, com base no identificador do nó, permite gerar chaves, evitando que um nó possa conhecer uma grande parte das chaves).

2.1.6 Ataques à manutenção de rotas

Ataque Blackhole No ataque *blackhole*[32] o atacante intercepta os pacotes destinados ao nó/área que pretende comprometer, informando a origem que este se trata de um caminho de melhor qualidade. Assim, força todo o tráfego, dirigido ao destino alvo do ataque, a circular através dele. Por exemplo, no protocolo AODV[56], por ser *on-demand* permite que, na fase de descoberta de uma rota, qualquer nó, que possua um caminho (suficiente recente), responda a uma mensagem de RREQ. Com isto, este algoritmo de encaminhamento pode ficar sujeito a um ataque de *blackhole*, pois um nó malicioso intermédio, pode responder com um caminho melhor, apesar de não ter sequer caminho para o destino, originando um "buraco negro", interrompendo o processo de comunicação[66, 73].

2.1.6.1 Contra-medidas

Para mitigar os ataques de *blackhole* existem várias propostas [20, 73, 32] das quais se destacam as que implementam os seguintes mecanismos: i) Confirmação do destino, é enviada uma mensagens ACK por cada pacote recibo pelo destino, pelo caminho inverso; iii) Definição de limites de tempo para receber as mensagens de ACK. por parte do destino, ou ao invés, receber mensagens de falha dos nós intermédios; iii) Mensagens de falha, quando num nó intermédio detecta o fim do temporizador de ACK, este gera uma mensagem de falha; iv) Caminho definido pela origem, ou seja, em cada pacote é indicado, na origem, o caminho que deve ser seguido pelo pacote até ao destino.

2.1.7 Ataques por Intrusão/Replicação

Alguns dos ataques tipificados anteriormente podem ser desencadeados a partir de nós maliciosos[52] introduzidos na rede de forma incorrecta e posteriormente replicados. Os ataques por replicação[54] são particularmente efectivos em sistemas do tipo de votação, ou cuja a operação da rede dependa de mecanismos de eleição. Pode-se então dizer que, mitigar os ataques por intrusão permite que, à partida, se possam reduzir algumas condições para a indução de outros ataques.

2.1.7.1 Contra-medidas

Apresentam-se algumas contra-medidas para ataques por intrusão, algumas das quais têm sido incorporadas em protocolos de encaminhamento:

Autenticação central Uma primeira forma de defesa contra replicação é a autenticação dos nós, usando os seus identificadores, realizada numa estação central, permitindo detectar inconsistências ou duplicações.

Múltiplas Rotas A existência de diversos caminhos para entregar uma mensagem no destino, faz com que se possa aliar a tolerância a falhas à resistência a intrusões. Assim, se a mensagem for interceptada por um intrusor, alta probabilidade desta alcançar o destino usando outro dos caminhos de envio[27].

Detecção de replicação Perrig *et* Parno em [54] apresentam mecanismos de detecção distribuída de replicações. Um dos mecanismos é de carácter aleatório *Randomized Multicast* e outro, denominado por *Line-Selected Multicast*, que se serve do modelo de comunicação multi-*hop* da rede para detecção de nós duplicados. Outro exemplo, é a criação de estruturas auxiliares (ex: àrvores binárias) como acontece no protocolo *Clean-Slate*[55].

2.2 Estudo de Protocolos de Encaminhamento Seguro para RSSF

Como ponto introdutório da discussão e apresentação de algoritmos de encaminhamento em RSSF, importa identificar algumas tipologias ou classes destes algoritmos.

2.2.1 Caracterização dos protocolos de encaminhamento em RSSF

Podem-se estabelecer três classes de protocolos[17]: os baseados na localização, os centrados nos dados e os hierárquicos. Os protocolos baseados na localização usam esta informação para tomarem as melhores decisões para alcançar os destinos(ex: IGF[22]). Os centrados nos dados, ou seja, os que exploram a redundância e a semântica dos dados, normalmente são baseados em algoritmos que efectuam pesquisas lançadas a partir de nós de sincronização (ex: Directed Diffusion[38]). Por fim, os protocolos hierárquicos, cuja concepção é baseada na construção de grupos de nós, normalmente definidos como *clusters*(ex: LEACH[31]), que funcionam no principio de agregação de dados do grupo e transferência da informação para os nós base.

Para além destas classificações podemos ainda considerar algoritmos quanto ao momento em que são determinadas as rotas de encaminhamento de dados[19]. Assim, consideram-se os protocolos como *table-driven* ou *on-demand*. Os primeiros referem-se a protocolos que mantêm as tabelas de encaminhamento trocando mensagens de controlo durante a sua operação. Assim, observa-se um maior consumo de energia devido à regular troca de mensagens. No segundo caso, nos protocolos *on-demand*, as rotas são determinadas em cada envio de mensagem. Apesar de representar alguma sobrecarga, em cada envio, acaba por compensar em redes mais móveis e com eventos mais espaçados.

2.2.2 Protocolos de encaminhamento seguro em RSSF

Muitos dos protocolos de encaminhamento para RSSF não foram desde logo concebidos tendo em conta o factor da segurança[41, 19], antes, pretendiam adaptar-se ao ambiente das aplicações e às características e capacidades das RSSF. No entanto, quando se pretende estender a sua utilização para outros domínios, cuja segurança é indispensável, estas preocupações aumentam, uma vez que os mecanismos de segurança implicam directamente um aumento da computação e pode implicar um aumento no custo da comunicação, reflectindo-se na autonomia dos sensores.

Nesta secção apresentam-se alguns protocolos de encaminhamento seguro em RSSF. Visam cubrir todo o espectro da temática deste trabalho e apresentam no seu todo os mecanismos de segurança que se pretende estudar.

2.2.2.1 *Secure Implicit Geographic Forwarding* (SIGF)

Conhecida a inexistência de mecanismos de segurança em alguns dos algoritmos de encaminhamento de RSSF, a implementação destes mecanismos correspondeu a um primeiro passo neste domínio. Um destes casos foi o algoritmo de encaminhamento *Implicit Geographic Forwarding* (IGF)[22], que deu origem a uma implementação segura o SIGF[68].

O IGF é um protocolo *on-demand*, baseado na localização, que não mantendo o estado ao longo do seu funcionamento, faz com que funcione sem que seja necessário o conhecimento da topologia da rede ou a presença de outros nós. O seu carácter não determinístico de encaminhamento, já representa um mecanismo de segurança perante determinados ataques, mas, não é de forma alguma suficiente para manter uma aplicação, com requisitos de segurança, a executar em ambientes críticos.

Funcionamento do protocolo IGF No protocolo IGF o ambiente está definido por coordenadas que permitem a cada nó saber exactamente a sua localização. Com a agregação do nível de rede com o nível MAC[6] num único protocolo *Network/MAC* é possível[22], no momento de envio do pacote, determinar qual o melhor próximo candidato por onde encaminhar os dados. O protocolo inicia com a origem a enviar uma mensagem do tipo *Open Request To Send* (ORTS) para a vizinhança (com a localização e o destino). Cada nó que se encontre no sextante válido [7] inicia um temporizador de CTS (*Clear To Send*) inversamente proporcional a determinados parâmetros (distância à origem, energia existente e distância perpendicular ao destino), favorecendo os nós com melhores condições. Ao expirar o temporizador, é enviada uma mensagem de CTS que, ao ser recebida possibilita o início de mensagens do tipo DATA apartir da origem. Como este protocolo não mantém estado,resiste a mudanças de topologia da rede, o facto de escolher em cada envio o nó seguinte constitui um mecanismo de tolerância a falhas e que, em caso de ataque, confina os danos, à vizinhança do nó comprometido.

Funcionamento do protocolo SIGF[68] A introdução de mecanismos de segurança, num protocolo existente, compreende um acréscimo de sobrecarga no funcionamento do protocolo. Contudo, o protocolo SIGF[68] pretende manter um bom desempenho e uma elevada taxa de sucesso de entrega das mensagens, mesmo durante um ataque. Uma das características deste

[6] *Medium Access Control*

[7] Ângulo de 60º centrado na origem orientado para o destino e determinado por cada nó com base na sua localização

protocolo é o facto de ser configurável e, como tal, permitir adaptar os mecanismos de segurança ao grau de ameaça. O protocolo tem três extensões ao protocolo IGF[22] que possibilita a evolução gradual de um protocolo seguro sem estado para um protocolo com manutenção de estado, e com isto mais pesado e exigente em recursos.

A primeira extensão é a mais simples e a menos exigente em recursos, o SIGF-0. Continua a não manter o estado e a ter um carácter não determinístico. No entanto, não sucumbe a ataques do tipo *rushing*[37] por não emitir logo para ao primeiro nó que envie o CTS mas sim manter um conjunto de possíveis candidatos a próximo nó. A extensão intermédia, SIGF-1 já mantém estado, mas ao nível local, podendo com isto constituir listas de reputação dos seus vizinhos por forma a escolher melhor próximo nó. Por fim, e tratando-se já de um protocolo mais robusto, mas mais exigente, o SIGF-2 partilha o estado com os seus vizinhos. Permitindo usar mecanismos criptográficos que permite garantir integridade, autenticidade, confidencialidade e frescura. Ainda assim, acumula as propriedades de segurança de cada um dos seus protocolos antecessores SIGF-0 e SIGF-1.

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

Este protocolo [27] foi concebido tendo em vista a tolerância a intrusões e como tal faz face a uma das tipologias do modelo de adversário preconizado neste trabalho. Para cumprir com este objectivo, foram identificados dois tipos de ataques: ataques por negação de serviço[33] e ataques ao encaminhamento. O protocolo assenta na existência de uma estação base, constituindo-se como um centro confiável, que partilha chaves criptográficas simétricas com cada um dos nós da rede. Este característica permite que, em caso comprometimento de um nó, o atacante não terá acesso a mais do que uma chave segura da rede, isolando, de alguma forma, o ataque.

O uso de caminhos redundantes permite aumentar a resiliência a atacantes não detectados. Bastando que exista apenas um caminho sem interposição de atacantes, para que as mensagens cheguem ao destino sem serem comprometidas. Note-se que neste protocolo não é possível a comunicação directa entre nós da rede, sem que esta não passe pela estação base.

O papel fundamental do protocolo, em termos de encaminhamento seguro, é desempenhado pela estação base. Uma das vantagens apontadas pelos autores é a redução das computações nos nós da rede (ex: para geração de chaves, tabelas de encaminhamento), cuja limitações são as conhecidas. Assim, a formação das tabelas de encaminhamento divide-se em três fases: Pedido de rotas (*route request*); Recolha dos dados de encaminhamento; Propagação das rotas.

A primeira fase, corresponde ao envio por parte da estação base de uma mensagen destinada a todos os nós da rede por forma a obter dados sobre as vizinhanças. Numa segunda fase, cada nó, responde com a sua vizinhança para estação base. Por fim, depois da estação base tratar toda a informação recolhida são elaboradas as tabelas de encaminhamento, que são depois propagadas para cada nó. Podendo prosseguir-se com o encaminhamento dos dados baseando nas tabelas recebidas.

2.2.2.3 *Secure Sensor Network Routing: Clean-Slate approach*

O algoritmo Clean-Slate[55] foi concebido para uso generalizado, desenhado desde de inicio, de forma sistemática, com características de segurança. É orientado para a comunicação ponto-a-ponto entre nós da rede, visando a resistência mesmo na presença de um ataque (ataque activo). Classifica-se como um protocolo *table-driven*.

Funcionamento do Protocolo Cada sensor da rede recebe um identificador único global, um certificado assinado por uma autoridade de certificação da rede (AR), a chave publica desta entidade e um conjunto de valores (desafios) baseados numa função de dispersão de um sentido (*one way hash function*). Neste protocolo, podem-se identificar três fases de operação: organização da rede, estabelecimento dos caminhos e manutenção das rotas.

O protocolo estabelece as tabelas de encaminhamento e os endereços dinâmicos (de tamanho variável) para cada nó da rede, usando um algoritmo recursivo de agrupamento, que executa de forma determinística mediante uma topologia. Os grupos são formados de forma recursiva e hierárquica fundindo-se até que a rede forme apenas um único grupo. Em cada fusão é acrescentado à esquerda um bit (0/1) que permitirá distinguir o endereço de cada nó. Dentro de um mesmo grupo a comunicação é feita usando *broadcast* autenticado inspirado nos protocolo μTESLA[59, 46].

Este algoritmo incorpora mecanismos de detecção de comportamentos incorrectos dos nós, por exemplo, caso pretendam assumir múltiplas identidades(*sybil*[51, 29]). Este mecanismo é desencadeado após a formação dos grupos, com cada nó a anunciar o seu endereço para os vizinhos, aplicando-se um algortimo de detecção de replicação de nós[54]. Outro mecanismo para a detecção de formação incorrecta de grupos é a utilização de *Grouping Verification Trees (GVT)*, baseado em tabelas de dispersão que providenciam autenticação ao nível das folhas usando a raiz para certificação. Cada nó tem uma GVT permitindo verificar qualquer comunicação

trocada com outros nós da rede.

Durante a fase de manutenção das rotas e encaminhamento, o algoritmo incorpora operações que permitem tratar a saida e entrada de nós. Um nó ao detectar a saída de outro, procura num dos vizinhos um novo nó fronteira que lhe permita alcançar o mesmo grupo antes acessivel pelo nó ausente. A definição de épocas (*ephocs*), permite que ao fim de algum temaopo o algoritmo de agrupamento se repita por forma a incluir novos nós. No que respeita ao encaminhamento usa múltiplas rotas, fazendo com que o protocolo possa contornar áreas comprometidas da rede. Os nós maliciosos são retirados do algoritmo usando uma técnica denominada por *Honeybee*, que corresponde a: quando um nó malicioso (pode ser replicado) é detectado, a rede é inundada com um pacote que indica que o atacante deve ser retirado das tabelas e, tratando-se de uma replicação, o nó replicado deve-se sacrificar.

De forma sumária, este protocolo incorpora os três conceitos para o desenho de protocolos de encaminhamento seguro: prevenção (autenticação), resiliência (multiplas rotas) e detecção/recuperação (GVT/Honeybee). Implementando-os todos, ao contrário do que acontece com alguns protocolos que apenas implementam um destes conceitos. Transformando-o num protocolo base, indicado para o estudo comparativo com outros protocolos.

2.3 Ambientes de Simulação

Os ambientes de simulação de RSSF surgem como uma necessidade, inevitável, para o teste e desenvolvimento das redes de sensores e todas as tecnologias associadas[53, 44]. Alguns ambientes têm sido desenvolvidos específicamente para determinados problemas. Outros são adaptados a partir de ambientes já existentes, como é o caso do NS2[10] ou J-Sim[5], que foram concebidos para simulações relacionadas com redes convencionais (ex: 802.3, 802.11). A característica importante, destes ambientes, que importa para a investigação, é a capacidade de repetição de experiências perante as mesmas condições, facilitando assim uma análise sistemática do objecto de estudo.

Nesta secção apresentam-se diversos ambientes de simulação, mais comuns, e que permitam simular sistema de RSSF. Foram seleccionados, em premeiro lugar, seguindo critérios relacionados com engenharia de *software*. Seguidamente, com vista à avaliação de um ambiente que se mostre adequado para a utilização no trabalho de dissertação, foram estabelecidos critérios relacionados com as RSSF.

2.3.1 Critérios Relacionados com Engenharia de Software

Portabilidade da Linguagem Devido às caracteristicas da linguagem de programação Java, inerente ao seu ambiente de execução, à consequente portabilidade e à programação orientada a objectos, foram seleccionados apenas ambientes desenvolvidos nesta linguagem.

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 específicas.

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

Documentação Alguns ambientes podem não se encontrar bem documentados. Este critério será importante como ponto de partida para o aprofundamento do conhecimento de cada uma das arquitecturas destas ferramentas.

2.3.2 Critérios Relacionados com as RSSF

Escalabilidade da Rede Uma das características mais importantes das RSSF é o conceito de escala, que se deve ao facto de estas compreenderem, normalmente, um grande número de sensores distríbuidos por uma vasta àrea. Assim, é importante que o ambiente de simulação possa suportar experiências com milhares de nós, uma vez que o factor escala é um das propriedades que se querem ver analisadas no trabalho a desenvolver;

Modelo de Colisões/Comunicação Rádio Este modelo é fundamental que se encontre modelado no sistema de simulação por ser um componente base das RSSF, relacionado com a camada de acesso ao meio e de ligação de dados(ex: B-MAC, S-MAC)[60, 70], e não se pretende que seja desenvolvido no âmbito da elaboração da dissertação;

Modelo de Gestão de Energia A existência de um modelo de energia permitirá adaptar a funcionalidade com vista à integração na plataforma final, visto se tratar de uma das propriedades que se deseja permitir estudar.

Capacidade de Emulação Alguns simuladores possuem a capacidade de emular um sensor real, permitindo efectuar o carregamento de código directamente para o *mote*, sem recurso a recompilação, não sendo um critério mandatório, reveste-se de grande interesse;

Modelo de Mobilidade Ainda que as RSSF sejam maioritariamente instaladas com características estáticas ou de pouca mobilidade, a existência de um modelo de mobilidade poderá possibilitar a avaliação dos comportamentos dos protocolos mediante esta propriedade;

Interface de Visualização É importante que o ambiente de simulação possua uma interface de visualização, permitindo uma mais fácil percepção dos comportamentos dos protocolos (ex: topologia, cobertura), bem como o controlo da simulação e extracção de resultados.

Modelo de Gestão de Topologia Um factor que pode influênciar o comportamento de um protocolo de encaminhamento, é a topologia. Como tal, é relevante a existência deste modelo por forma a avaliar os protocolos desenhados perante diferentes topologias.

2.3.3 Prowler/JProwler

[6]Esta ferramenta resulta da conversão de um simulador de eventos discretos[8] Prowler[7], 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 probabilístico simples e preciso que descreve a operação da camada MAC. Possui 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 Rayleigh para topologias móveis.

2.3.4 J-Sim

J-Sim (anteriormente conhecido como JavaSim) é um ambiente de simulação baseado em componentes [5], implementado em Java. Não foi desenvolvido inicialmente com vista a sua utilização em RSSF como é o caso do ambiente SENSE[11], mas o objectivo para o desenvolvimento

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

foi o mesmo: extensibilidade. Este ambiente é amplamente usado e implementa um modelo de rede em camadas. No entanto, este simulador não é o mais adequado para o estudo do desempenho em RSSF, visto que, esta é condicionada pelo *hardware*, pelo sistema operativo, pelos protocolos de rede e pelas aplicações assim como optimizações especificas entre camada da pilha de protocolos (ex: implementação de mecanismos de transporte ao nível aplicação). Apesar disto, o J-Sim é um importante ambiente de simulação dada a natureza fracamente ligada dos seus componentes que permitem o rápido desenvolvimento e prototipagem de aplicações.

2.3.5 Freemote

Fremote é uma ferramenta de emulação [4] distríbuida[9] desenvolvida em Java, utilizada para o desenvolvimento *software* para RSSF. O emulador suporta *motes* (Squawk, Sentilla) e plataformas (Java cards, SunSpot[13]) baseados em Java. Devide a arquitectura em camadas bem definidas por interfaces: Aplicação, Encaminhamento e Ligação de Dados/MAC. Sendo um emulador, os nós reais podem ser baseados na norma de comunicação IEEE802.15.4[16] (ex:MICAz[9]). Tem um interface gráfico para configuração. Suporta experiências de grande escala (10.000 nós) incluindo a integração com nós reais baseados em Java. Os principais pontos negativos são: 1) o modelo de propagação rádio é muito simples uma vez que não considera obstáculos entre os nós. 2) Só existe um modelo de comunicação real, limitado a emulação simples de plataformas especificas (JMote). 3) Não é orientada para a análise de performance das redes, característica pode ser importante no desenvolvimento de algoritmos para RSSF.

2.3.6 ShoX

Trata-se de um simulador de redes sem fios, implementado em Java[12]. A ideia principal desta ferramenta é a de proporcionar, de 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, mobilidade e energia). Uma das vantagens é a existência de classes abstractas para reimplementação de novos modelos em cada um dos componentes, faciltando a programação de novos protocolos ou novas funcionalidades. A

[9]Funciona em rede com a possibilidade de ter diversos clientes de visualização ligados a um servidor central

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 as configurações da ferramenta sem a necessidade de editar directamente os ficheiros de XML. Para além disso é ainda possível visualizar a topologia de rede e extrair resultados gráficos da simulação. 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[10]. Apesar deste facto se apresentar como uma desvantagem, a arquitectura apróxima-se bastante do que deve ser um simulador de RSSF, em que as camadas estão bem definidas, chegando ao ponto de poder simular a camada respeitante a um sistema operativo de um nó.

2.4 Discussão e Resumo do Trabalho Relacionado

As redes de sensores sem fios representam um enorme desafio para a investigação de sistemas e protocolos de segurança. As características que as tornam numa mais valia, para a operação em ambientes remotos, apresentam-se como sendo as suas maiores vulnerabilidades em termos de segurança. Este paradoxo é contornado com mecanismos de segurança inovadores e que se distinguem dos existentes nas redes convencionais. Assim, passada em revista as diversas dimensões que se pretende abarcar na futura dissertação: protocolos de encaminhamento seguro em RSSF e plataformas de simulação de RSSF, importa neste momento apresentar uma visão critica do trabalho relacionado como forma de enquadrá-lo como base teórica da dissertação.

Em primeiro lugar pode-se apresentar os ataques que foram estudados e apresentá-los, de forma estruturada, relacionando-os com as contra-medidas para os mitigar.

[10]Pode-se considerar este facto uma desvantagem, pois não cabe no âmbito da dissertação o desenvolvimento do módulo de comunicação

Fases do Protocolo	Ataque	Contramedidas
Organização e Descoberta da Rede	Falsificação de informação de Routing	Autenticação
	Ataques de *Rushing*	Encaminhamento aleatório de RREQ e autenticação
Estabelecimento de Rotas	HELLO flooding	Autenticação com confirmação(*acknowledge*)
	Ataques *Sinkhole*	Autenticação
	Ataques *Wormhole*	*Packet leaches*
	Ataques *Sybil*	Distribuição aleatória de chaves, testes aos canais de rádio
Manutenção de Rotas	Ataques de *Backhole*	Definição de temporizadores e mecanismos de confirmação (ACK) autenticados

Tabela 2.1 Tabela de Ataques *vs* Contramedidas

No ponto de vista dos protocolos estudados cabe relacionar as capacidades de cada um para fazer face a ataques definidos no modelo de adversário e tipificados nas diferentes fases dos protocolos em que estes se podem desencadear.

	Ataques ao Encaminhamento						
Protocolos	**Informação Falsa**	***Rushing***	**HELLO flooding**	***Sinkhole***	***Wormhole***	***Sybil***	***Blackhole***
SIGF	X		✓				
INSENS	X	X	X	X	X	X	X
Clean-Slate	X	X	X	X	X	X	X

Tabela 2.2 Tabela de Protocolos de Encaminhamento *vs* Ataques

Por fim e sendo a análise dos ambientes de simulação um dos focos do trabalho relacionado poder-se-á avaliar de forma comparativa os ambientes seleccionados para estudo comparandos com os critérios pensados como adequados para a avaliação.

		Ambientes de Simulação				
	Critérios	**Prowler/JProwler**	**J-Sim**	**Freemote**	**ShoX**	**Nova Plataforma**
Software	**Portabilidade da linguagem**	Java	Java	Java	Java	Java
	Código Livre Aberto	Sim	Sim	Sim	Sim	Sim
	Modularidade e extensabilidade	Sim	Sim, com recurso a JTcl	Sim	Sim	Sim
	Documentação	Apenas comentários no código	Papers e Online	Pouca	Pouca	
Propriedades das RSSF	**Escalabilidade**	Aprox. 5000 nós	Documentado na ordem dos milhares	Documentado na ordem dos milhares	Foram testados 100 nós sem sucesso	Na ordem dos milhares
	Colisões/Comunicação	Sim, modelo B-MAC	Sim, mas 802.11	Sim, mas muito simples	Sim, mas 802.11	Sim
	Gestão de Energia	Não	Não	Não	Sim	Sim
	Emulação	Não	Não	Sim, para plataformas Java *Based*	Não	Não
	Mobilidade	Sim, mas rudimentar	Sim	Sim	Sim	Não
	Visualização	Sim, mas só de visualização da topologia	Existem ferramentas auxiliares	Sim	Sim, mas não em tempo real. Apenas depois de executar a simulação	Sim
	Topologia	Não existe de raiz, pode ser modelado	Não existe de raiz, pode ser modelado	Não existe de raiz, pode ser modelado	Existem alguns de raiz, podendo ser estendido	Existirão de raiz alguns modelos, permitindo a adição de mais

Tabela 2.3 Tabela de Critérios de Avaliação *vs* Ambientes de Simulação

3 . Abordagem à fase de elaboração da dissertação

Tendo sido abordadas as temáticas relacionadas com a problemática da segurança numa RSSF, importa então, definir uma estratégia para a concepção de uma plataforma que vise a análise e avaliação de protocolos de encaminhamento, principalmente os concebidos com requisitos de segurança. Neste capítulo apresenta-se, de forma preliminar, as fases da elaboração da dissertação referentes à concepção dos modelos que suportam a arquitectura da plataforma. Adicionalmente, apresenta-se uma prova de conceito, referente à utilização da plataforma, com a implementação de dois protocolos Clean-Slate e INSENS e o conseguinte estudo comparativo.

3.1 Desenho e concepção da plataforma de simulação

3.1.1 Consolidação da avaliação de ambientes de simulação e a sua incorporação

Do estudo das plataformas de simulação existentes e apresentadas neste relatório, surgirá um motor de simulação com os modelos base de um ambiente de RSSF (comunicação, gerador de eventos discretos e plataformas de sensores). Assim, irá proceder-se à escolha de um simulador base com estas características, já fundamentadas e discutidas no capítulo anterior. No entanto, a fase de elaboração da dissertação deverá contar, inicialmente, com o aprofundamento da avaliação dos ambientes de simulação apresentados, com o intuito de certificar a selecção do simulador base. Uma mais valia deste estudo será o aproveitamento de características presentes em diversos ambientes e que possam ser aproveitadas para a implementação na plataforma final. Note-se que, a avaliação terá que ter em atenção sempre o objectivo do trabalho de modo a que, o tempo despendido a apreender determinada arquitectura não seja superior à possível implementação de raiz.

3.1.2 Apresentação preliminar da arquitectura da plataforma de simulação

A visão mais simples para representar a plataforma é sobre a forma de uma pilha de serviços. Como se pode ver na Figura 3.1, os principais serviços são: i) Mecanismo de Geração de Topologias; ii) Mecanismo de Gestão de Consumo de Energia; iii) Mecanismo de Injecção de Faltas/Ataques ao Encaminhamento; iv) Mecanismo de Configuração; v) Mecanismo de Visualização e Controlo de Simulação.

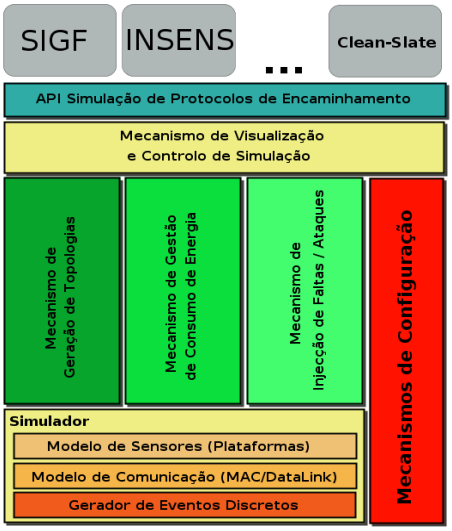

Figura 3.1 Arquitectura de Simulação

3.1.2.1 Mecanismo de Configuração

Para dotar a plataforma de maior flexibilidade, a existência de um componente gestor de configurações revela-se importante. Este componente, é transversal a toda plataforma. Pois, cada parte terá especificidades próprias que serão geridas por este componente. Para que as parametrizações possam ser persistentes e portáveis adoptar-se-à a tecnologia XML para definição dos ficheiros de configuração da plataforma. As principais funcionalidades que se prevêem existir vão desde as configurações dos parâmetros do simulador base, até à configuração de cada uma das simulações, que se pretende estudar, como forma de possibilitar a repetição de experiências nas mesmas condições.

3.1.2.2 Mecanismo de Geração de Topologias

As RSSF, normalmente, são caracterizadas por diferentes formas de distribuição dos nós sensores. Estas distribuições podem ser essencialmente divididas em dois modelos: aleatório e estruturado. Assim, para que se consiga acrescentar mais um grau de liberdade às características que se pretende observar na análise de um protocolo de encaminhamento, será fornecido um componente cuja função é gerar topologias na rede. Pois, sabe-se que a topologia da rede pode influenciar o comportamento de um protocolo. Pretende-se que este componente, possibilite a extensão para novas topologias (específicas para determinada simulação).

3.1.2.3 Mecanismo de Gestão de Consumo de Energia

As características fundamentais que se deverão implementar neste componente são: a definição de uma API para o desenvolvimento de novos modelos consoante as necessidades da simulação; a possibilidade de introduzir parâmetros relacionados com o consumo por parte dos sensores. Associadas a este componente estarão funcionalidades que permitirão a recolha de informação em tempo real dos consumos da rede, quer no seu total, quer individualmente, em cada sensor. Desta forma, este é um dos componentes de maior importância, uma vez que um dos indicadores que se pretende observar na análise de protocolos de encaminhamento, é o impacto sobre o tempo útil de operação da rede, quer em condições de funcionamento normais, quer em condições de ataque efectivo, tempo este que está dependente da energia.

3.1.2.4 Mecanismo de Injecção de Falhas / Ataques ao Encaminhamento

Sendo o tema central da futura dissertação o estudo de protocolos de encaminhamento seguros em RSSF, este componente é o de maior importância nesta plataforma e por diferentes ordens de razões: i) Não existe nenhum sistema de simulação que permita a indução de ataques de forma simples e intuitiva, consubstanciado-se num contributo para a inovação; ii) Deverá ser suficientemente flexível para se adaptar à lógica de cada algoritmo; iii) Poderá permitir a mutação de código em tempo de execução da simulação, por forma a alterar comportamentos do protocolo; iv) Idealmente deverá permitir a acrescentar mais modelos de ataques, dos já tipificados neste relatório ou outros que venham a ser desenvolvidos.

3.1.2.5 Mecanismo de Visualização e Controlo de Simulação

Como não poderia deixar de ser existe a necessidade de dotar a plataforma de um ambiente de operação. Como tal, é necessário implementar um componente correspondente à visualização gráfica de toda a simulação, bem como a possibilidade de controlar parâmetros de execução. Pretende-se desenvolver um ambiente gráfico integrado que permita a configuração da plataforma, a configuração e visualização das simulações e a extracção de resultados relacionados com as medidas que se pretendem avaliar: energia, fiabilidade, cobertura, principalmente sobre a forma de gráficos.

3.1.2.6 Avaliação da Solução

Uma vez que a contribuição efectiva para a componente de investigação de protocolos de encaminhamento seguros em RSSF, será obtida com a concepção de uma plataforma de simulação que suporte o estudo e a análise desta problemática, importa sujeitá-la a uma avaliação primária que permita comprovar a sua utilidade e/ou identificar eventuais lacunas neste domínio. Assim, tendo esta avaliação em vista, pretende-se contribuir com o estudo dos protocolos de encaminhamento seguro referidos. Para isso, definem-se duas fases complementares na elaboração da tese, uma que compreende a implementação de dois protocolos, seguidos da fase de experimentação usando as funcionalidades da plataforma. No final, será possível salientar as características de cada protocolo implementado analisadas à luz desta plataforma.

3.1.3 Implementação de Protocolos de Encaminhamento Seguro em RSSF

3.1.3.1 Fase de desenho dos algoritmos baseado nas especificações

No início desta fase, será necessário re-aprofundar o funcionamento de cada algoritmo a implementar, conhecer e identificar cada mecanismo, especificado, de modo a que se possa, dentro do possível, generalizar operações ou interfaces com vista a reutilização em outros algoritmos. Assim sendo, esta fase exigirá uma aprendizagem/conhecimento de cada algoritmo contribuindo também para a especialização neste domínio.

3.1.3.2 Fase de avaliação dos algoritmos

Recorrendo às ferramentas disponibilizadas pela plataforma deverá ser possível, no final da implementação, sistematizar as simulações por forma a extrair resultados, que por si só, caracterizem os algoritmos em matéria de segurança e a sua correcção em determinados parâmetros que se julgam ser fundamentais no estudo de protocolos de encaminhamento. Alguns dos quais, se indicam a seguir: i) correcção do protocolo; ii) análise do consumo de energia; iii) fiabilidade/entrega de mensagens; iv) correcção dos eventos; v) latência. Estes contribuem também, para a avaliação da usabiliadade da plataforma na avaliação/comparação de protocolos de encaminhamento seguro em RSSF.

4. Plano de Elaboração da Tese

A elaboração da tese realizar-se-à durante o 2º semestre de 2009/2010, iniciando a 22 de Fevereiro de 2010. O plano apresentado estabelece cinco grandes actividades: análise, desenvolvimento, prova de conceito, avaliação e relatório, como se apresenta na Figura4.1.

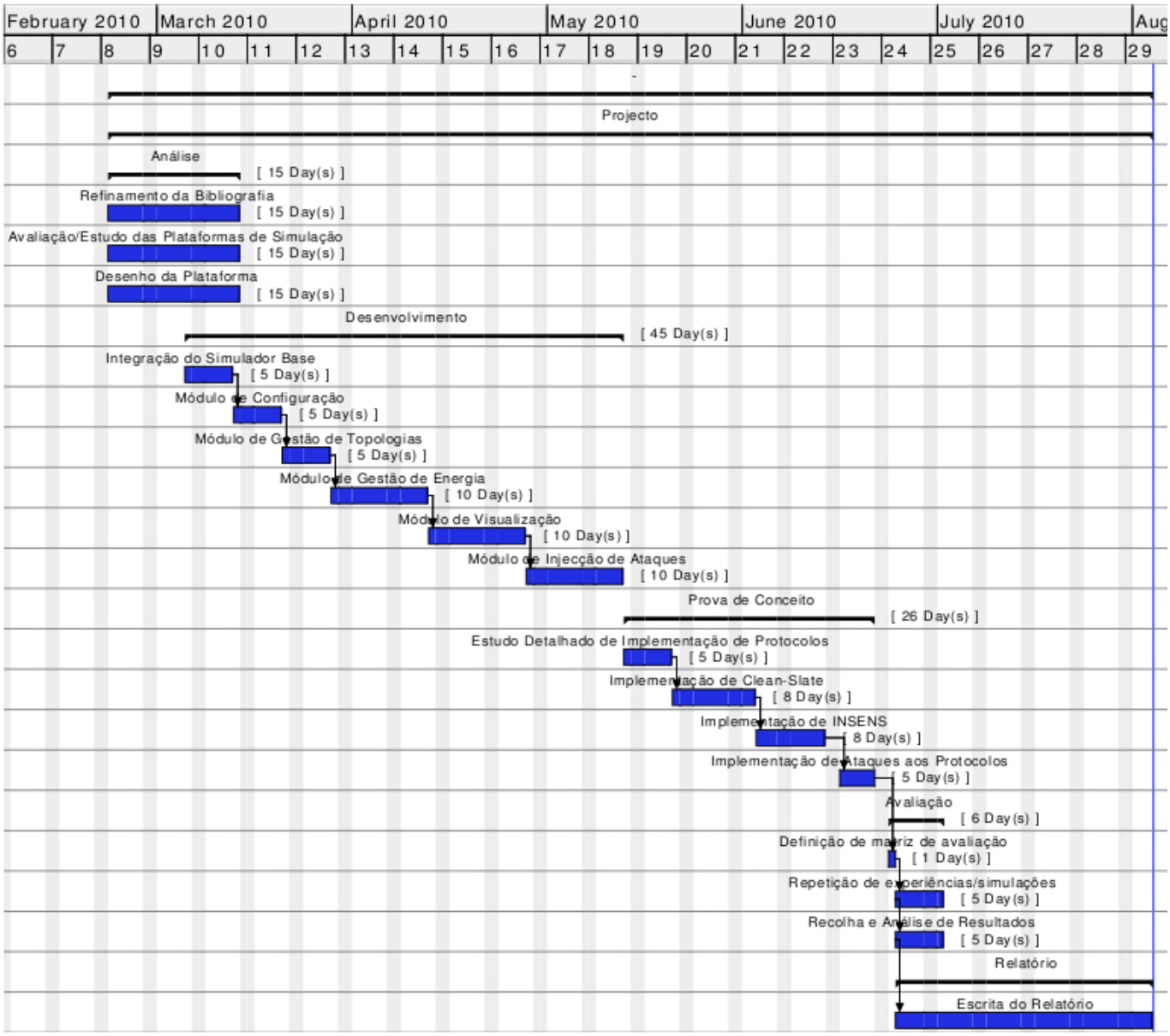

Figura 4.1 Plano da Dissertação

Apresenta-se em seguida uma breve descrição de cada uma das actividades.

Análise Esta actividade corresponde à revisão de bibliografia complementar, como forma de aprofundar o estudo de problemática, avaliação do simulador base como preconizado na secção 3.1.1. Inícia-se também o desenho da plataforma, consistindo numa visão mais técnica da solução, com a definição formal de algoritmos, interfaces e o modelo de interacção dos componentes da plataforma. Esta última tarefa permitirá iníciar a fase de desenvolvimento de forma mais sólida.

Desenvolvimento Esta actividade corresponde à concepção e implementação da arquitectura da plataforma como apresentada na secção 3.1.2, em que cada um dos componentes corresponderá às seguintes tarefas: Integração do Simulador Base, Módulo de Configuração (secção 3.1.2.1), Módulo de Gestão de Topologias (3.1.2.2), Módulo de Gestão de Energia (secção 3.1.2.3), Módulo de Visualização (secção 3.1.2.5) e Módulo de Injecção de Ataques (secção 3.1.2.4).

Prova de Conceito Esta actividade corresponde à implementação dos algoritmos de encaminhamento seguro propostos (ver secção 3.1.3.1): INSENS e Clean-Slate, que deverá ser precedida de um estudo mais aprofundado das particularidades de cada um. Consequentemente, cada protocolo será sujeito a um modelo de ataques que permitirão avaliar os comportamentos como forma de os mapear nas contribuições esperadas para esta dissertação.

Avaliação Esta actividade preconiza a avaliação dos protocolos implementados usando as ferramentas da plataforma como referido na secção 3.1.3.2. No entanto, esta avaliação permitirá, também, retirar conclusões acerca da usabilidade da plataforma (secção 3.1.2.6) e o grau de sucesso dos objectivos pretendidos que passam pela capacidade de estudo de protocolos de encaminhamento em RSSF em geral, e em particular, os com preocupações de segurança.

Relatório Esta actividade corrresponde à escrita da dissertação que poderá decorrer em paralelo com a avaliação e eventualmente com a prova de conceito. Que culminará com a entrega da dissertação até à data limite.

Bibliografia

[1] BTnodes - a distributed environment for prototyping ad hoc networks. http://www.btnode.ethz.ch/Documentation/BTnodeRev3HardwareReference.

[2] The contiki operating system - home. http://www.sics.se/contiki/.

[3] Gateways - crossbow technology. http://www.xbow.com/Products/productdetails.aspx?sid=159.

[4] Home | freemote emulator | assembla. http://www.assembla.com/wiki/show/freemote.

[5] Home (J-Sim official). http://sites.google.com/site/jsimofficial/.

[6] ISIS - JProwler. http://w3.isis.vanderbilt.edu/projects/nest/jprowler/.

[7] ISIS - prowler. http://w3.isis.vanderbilt.edu/projects/nest/Prowler/index.html.

[8] Mica2 Datasheet. http://www.xbow.com/Products/productdetails.aspx?sid=174.

[9] MicaZ Product Details. http://www.xbow.com/Products/productdetails.aspx?sid=164.

[10] The network simulator - ns-2. http://www.isi.edu/nsnam/ns/.

[11] SENSE-3.0: sensor network simulator and emulator. http://www.ita.cs.rpi.edu/sense/index.html.

[12] ShoX project page. http://shox.sourceforge.net/.

[13] SunSPOTWorld - documentation. http://sunspotworld.com/docs/index.html.

[14] TinyOS community forum || an open-source OS for the networked sensor regime. http://www.tinyos.net/.

[15] ZigBee alliance. http://www.zigbee.org/Default.aspx.

[16] IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - specific requirement Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications fo, 2007.

[17] Kemal Akkaya and Mohamed Younis. A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks*, 3(3):325–349, May 2005.

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

[19] J.N. Al-Karaki and A.E. Kamal. Routing techniques in wireless sensor networks: a survey. *Wireless Communications, IEEE*, 11(6):6–28, 2004.

[20] Mohammad Al-Shurman, Seong-Moo Yoo, and Seungjin Park. Black hole attack in mobile ad hoc networks. In *ACM-SE 42: Proceedings of the 42nd annual Southeast regional conference*, pages 96–97, New York, NY, USA, 2004. ACM.

[21] Paolo Baronti, Prashant Pillai, Vince W.C. Chook, Stefano Chessa, Alberto Gotta, and Y. Fun Hu. Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. *Computer Communications*, 30(7):1655–1695, May 2007.

[22] M. Blum, Tian He, Sang Son, and John A Stankovic. IGF: a State-Free robust communication protocol for wireless sensor networks.

[23] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance. In *OSDI '99: Proceedings of the third symposium on Operating systems design and implementation*, pages 173–186, Berkeley, CA, USA, 1999. USENIX Association.

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

[25] George F. Coulouris and Jean Dollimore. *Distributed systems: concepts and design*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1988.

[26] I. Demirkol, C. Ersoy, and F. Alagoz. Mac protocols for wireless sensor networks: a survey. *Communications Magazine, IEEE*, 44(4):115–121, April 2006.

[27] Jing Deng, Richard Han, and Shivakant Mishra. Insens: Intrusion-tolerant routing for wireless sensor networks. *Comput. Commun.*, 29(2):216–230, 2006.

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

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

[30] 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.

[31] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. *Hawaii International Conference on System Sciences*, 8:8020, 2000.

[32] Hongmei Deng, Wei Li, and D.P. Agrawal. Routing security in wireless ad hoc networks. *Communications Magazine, IEEE*, 40(10):70–75, 2002.

[33] Fei Hu and Neeraj K. Sharma. Security considerations in ad hoc sensor networks. *Ad Hoc Networks*, 3(1):69–89, January 2005.

[34] Y.-C. Hu, A. Perrig, and D.B. Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. In *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, volume 3, pages 1976–1986 vol.3, March-3 April 2003.

[35] Yih-Chun Hu, A. Perrig, and D.B. Johnson. Wormhole attacks in wireless networks. *Selected Areas in Communications, IEEE Journal on*, 24(2):370–380, Feb. 2006.

[36] Yih-Chun Hu and Adrian Perrig. A Survey of Secure Wireless Ad Hoc Routing. *IEEE Security and Privacy*, 2(3), 2004.

[37] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. In *WiSe '03: Proceedings of the 2nd ACM workshop on Wireless security*, pages 30–40, New York, NY, USA, 2003. ACM.

[38] Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin, John Heidemann, and Fabio Silva. Directed diffusion for wireless sensor networking. *IEEE/ACM Trans. Netw.*, 11(1):2–16, 2003.

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

[40] David B. Johnson and David A. Maltz. Dynamic source routing in ad hoc wireless networks. In *Mobile Computing*, pages 153–181. Kluwer Academic Publishers, 1996.

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

[42] 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.

[43] Mauri Kuorilehto, Marko Hännikäinen, and Timo D. Hämäläinen. A survey of application distribution in wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*, 2005(5), 2005.

[44] Johannes Lessmann, Peter Janacik, Lazar Lachev, and Dalimir Orfanus. Comparative study of wireless network simulators. In *ICN '08: Proceedings of the Seventh International Conference on Networking*, pages 517–523, Washington, DC, USA, 2008. IEEE Computer Society.

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

[46] Mark Luk, Adrian Perrig, and Bram Whillock. Seven cardinal properties of sensor network broadcast authentication. pages 147–156, Alexandria, Virginia, USA, 2006. ACM.

[47] Ruiping Ma, Liudong Xing, and H.E. Michel. Fault-intrusion tolerant techniques in wireless sensor networks. In *Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on*, pages 85–94, 29 2006-Oct. 1 2006.

[48] Alan Mainwaring, David Culler, Joseph Polastre, Robert Szewczyk, and John Anderson. Wireless sensor networks for habitat monitoring. In *WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pages 88–97, New York, NY, USA, 2002. ACM.

[49] Aleksandar Milenković, Chris Otto, and Emil Jovanov. Wireless sensor networks for personal health monitoring: Issues and an implementation. *Comput. Commun.*, 29(13-14):2521–2533, 2006.

[50] Wireless Networks. Security Vulnerabilities In Wireless Sensor Networks: A Survey. *Journal of Information Assurance and Security*, 5(2010):031–044, 2009.

[51] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In *Information Processing in Sensor Networks, 2004. IPSN 2004. Third International Symposium on*, pages 259–268, April 2004.

[52] E.C.H. Ngai, Jiangchuan Liu, and M.R. Lyu. On the intruder detection for sinkhole attack in wireless sensor networks. In *Communications, 2006. ICC '06. IEEE International Conference on*, volume 8, pages 3383–3389, June 2006.

[53] Sung Park, Andreas Savvides, and Mani B. Srivastava. Simulating networks of wireless sensors. In *Proceedings of the 33nd conference on Winter simulation*, pages 1330–1338, Arlington, Virginia, 2001. IEEE Computer Society.

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

[55] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig. Secure sensor network routing: a clean-slate approach. In *CoNEXT '06: Proceedings of the 2006 ACM CoNEXT conference*, pages 1–13, New York, NY, USA, 2006. ACM.

[56] C.E. Perkins and E.M. Royer. *Ad-hoc on-demand distance vector routing*. IEEE, 1999.

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

[58] Adrian Perrig, John Stankovic, and David Wagner. Security in wireless sensor networks. *Commun. ACM*, 47(6):53–57, 2004.

[59] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J. D. Tygar. Spins: Security protocols for sensor networks. In *Wireless Networks*, pages 189–199, 2001.

[60] Joseph Polastre, Jason Hill, and David Culler. Versatile low power media access for wireless sensor networks. In *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 95–107, New York, NY, USA, 2004. ACM.

[61] RFC2828. Internet Security Glossary, 2000.

[62] E. Shi and A. Perrig. Designing secure sensor networks. *Wireless Communications, IEEE*, 11(6):38–43, Dec. 2004.

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

[64] Andrew S. Tanenbaum and Maarten Van Steen. *Distributed Systems: Principles and Paradigms*. Prentice Hall PTR, Upper Saddle River, NJ, USA, 2001.

[65] Hua-Wen Tsai, Chih-Ping Chu, and Tzung-Shi Chen. Mobile object tracking in wireless sensor networks. *Comput. Commun.*, 30(8):1811–1825, 2007.

[66] Yong Wang, G. Attebury, and B. Ramamurthy. A survey of security issues in wireless sensor networks. *Communications Surveys & Tutorials, IEEE*, 8(2):2–23, Quarter 2006.

[67] B.A. Warneke and K.S.J. Pister. Mems for distributed wireless sensor networks. In *Electronics, Circuits and Systems, 2002. 9th International Conference on*, volume 1, pages 291–294 vol.1, 2002.

[68] Anthony D. Wood, Lei Fang, John A. Stankovic, and Tian He. SIGF: a family of configurable, secure routing protocols for wireless sensor networks. pages 35–48, Alexandria, Virginia, USA, 2006. ACM.

[69] 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.

[70] Wei Ye, J. Heidemann, and D. Estrin. Medium access control with coordinated adaptive sleeping for wireless sensor networks. *Networking, IEEE/ACM Transactions on*, 12(3):493–506, June 2004.

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

[72] Hu. Yih-Chun and A. Perrig. A survey of secure wireless ad hoc routing. *Security & Privacy, IEEE*, 2(3):28–39, May-June 2004.

[73] W. You-Chiun and Y Tseng. Attacks and defenses of routing mechanisms in ad hoc and sensor networks. In *Security in Sensor Networks*.