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

1. Introdução

1.1 Introdução geral

Os recentes avanços no fabrico de *hardware* de pequena dimensão [25] com capacidades para desepenhar tarefas específicas e a diminuição do tamanho dos dispositivos de comunicação sem fios, fez surgir, nos últimos anos, um novo campo da investigação, as redes de sensores sem fios (RSSF). Uma rede de sensores é um conjunto de pequenos dispositivos de computação de baixa potência distribuídos num determinado ambiente, de forma autonoma[1] e auto-organizada, com a função de recolher sensorialmente (ou monitorizar) fenómenos[2] físicos. Um ambiente de execução pode ser um qualquer espaço onde uma RSSF possa ser instalada por exemplo: uma casa, um terreno de combate ou o próprio corpo humano.

A componente básica e fundamental de uma rede de sensores é o nó sensor (*mote*)[2, 1, 3]. Este pode conter diversos sensores para monitorizar, por exemplo, temperatura, luz ou movimento consoante as necessidades da aplicação. É caracterizado por ser pequeno, ter pouco poder de computação, ter baixa largura de banda de comunicação e ter energia limitada. Conhecidas estas limitações, os sensores têm de ser distribuídos em grande número como forma de aumentar a redundância, formando redes de larga escala que podem ir até aos 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)[**REFERENCIA**]. Outro papel, que pode ser desempenhado, numa RSSF é o de nós de interligação ou *gateways*. Estes permitem ligar as RSSF a outras redes ou a outras infraestruturas que, com maior capacidade de armazenamento e processamento, permitem efectuar análise de dados coligidos. Por fim, e não menos importantes, existem ainda os nós de desenvolvimento, que possuem ligações a computadores (ex: ligação de rede *ethernet*, RS232), podendo ainda funcionar, também, como nó *gateway*. [**REFERENCIA**] Assim, verifica-se que apesar das limitações existentes, inerentes às caracteristicas do hardware e da sua aplicabilidade, os sensores, ao contrário do que acontece em redes convencionais,

[1] Sem a necessidade de monitorização ou vigilância por parte de uma entidade externa
[2] Entidades ou características do interesse do observador

não se encarregam somente de processar informação, mas possuem tarefas fundamentais no encaminhamento da informação. Estas particularidades, existentes também nas redes *ad-hoc*, tornado-se num desafio ainda maior nas RSSF, uma vez que as suas características e limitações expõe algumas vulnerabilidades ao seu funcionamento.

1.1.1 Caracterização de RSSF

As redes de sensores sem fios são um caso especial de redes *ad-hoc* que exibem características especificas que podem ser diferenciadas[**?**]. As RSSF têm particular interesse, dada a sua adequação a aplicações de larga escala, uma vez que a participação de milhares de nós faz emergir algumas problemáticas inerentes a aplicações distribuídas [9] e aos seus mecanismos de gestão, como tolerância a falhas, escalabilidade e segurança. Os nós sensores são dispositivos de baixa potência, também denominados sensores inteligentes(*Smart Sensors*)[28], são constituídos por um ou mais sensores, por processador, por memória, por bateria e por um mecanismo de comunicação por rádio-frequência baseados em normas (802.15.4 [4, 7] e Zigbee[7]) com base de comunicação orientada para protocolos de acesso ao meio e de ligação de dados (*MAC/Data Link*) que podem apresentar características mais ou menos específicas (ex: B-MAC[21, 10], S-MAC[27, 10]).

No entanto, dadas as características de auto-organização/configuração, encaminhamento *multi-hop*, baixo custo, miniaturização e versatilidade de implementação (devido à não necessidade de infraestrutura adicional de comunicação entre nós)[28], o seu uso tem-se estendido a outros campos, nomeadamente os do domínio militar, segurança e medicina[5]. Consciente das limitações impostas pelas RSSF, todo o processamento e comunicação tem-nas sempre, já que qualquer tarefa desempenhada penaliza o consumo de energia (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, traduzindo-se numa maior eficácia e na melhoria da sua utilização em inúmeras aplicações.

1.1.2 Aplicações

Muitas foram as aplicações encontradas para a utilização/exploração desta arquitectura distribuída de larga escala[28]. O carácter autónomo destas redes oferece um sem número de vantagens que propicia a sua utilização em locais remotos e sem necessidade de manutenção. Sendo assim, as aplicações poderão, genéricamente, ser divididas nas seguintes classes de funções:

Detecção de alvos/objectos(*Target Tracking*): [24] Detecção de movimento (trajectória/presença) em àreas vigiadas (em teatros operacionais militares, na vigilância de infraestruturas);

Monitorização de fenómenos naturais: [15]Detecção de eventos ou anomalias ambientais (agricultura, poluição, *habitats* naturais), controlo de fenómenos naturais (sismos, vulcões);

Recolha de dados: [16]controlo de indicadores físicos de pessoas e animais (recurso a sensores especiais) normalmente associados a aplicações da medicina

1.2 Segurança em RSSF

A segurança nas RSSF é uma problema *de facto*, com impacto na sua aplicação em sistemas críticos. Como tal, deve ser pensada em toda a abrangência do sistema e tendo em atenção as particularidades específicas da tecnologia inerente e dos ambientes onde são implementadas. Assim, importa, antes de mais, analisar a plataforma genérica de uma RSSF, sobre o ponto de vista da sua pilha de protocolos, uma vez que cada uma das camadas representa um pontencial ponto vulnerável a ataques. Neste momento não se pretende ser muito exaustivo na explanação das propriedades das camadas, visto que será alvo de descrição mais detalhada no decorrer deste trabalho.

Uma plataforma genérica possuí uma pilha de protocolos mais simplista, comparada com a pilha de protocolos perconizada no modelo OSI[23], uma vez que as limitações impostas pelas dimensões e as capacidades de operação não permitem uma arquitectura mais ambiciosa. As camadas de operação de um nó sensor são essencialmente cinco[5]: camada física, camada de ligação de dados, camada de rede, camada de transporte e camada de aplicação. No que respeita à camada física um dos ataques mais efectivo é o *jamming*[3][17], que pode ser mitigando usando mecanismos de salto de frequência. Ao nível da ligação de dados, sendo esta uma camada

[3]Transmissão de dados com o intuíto de confundir e introduzir ruído na comunicação

responsável pelo estabelecimento das comunicações ponto a ponto, verifica-se que ataques do tipo de exaustão ou de introdução de colisões são também bastante efectivos e podem ser combatidos com limitação das taxas de emissão e uma boa política de resolução de colisões. Ao nível transporte os ataques dirigidos por comportamentos de inundação aumenta o congestionamento da rede, no entanto esta camada não se encontra muito presente na pilha uma vez que as operações que por ela poderiam ser realizadas acabam por o ser na camada de aplicação.

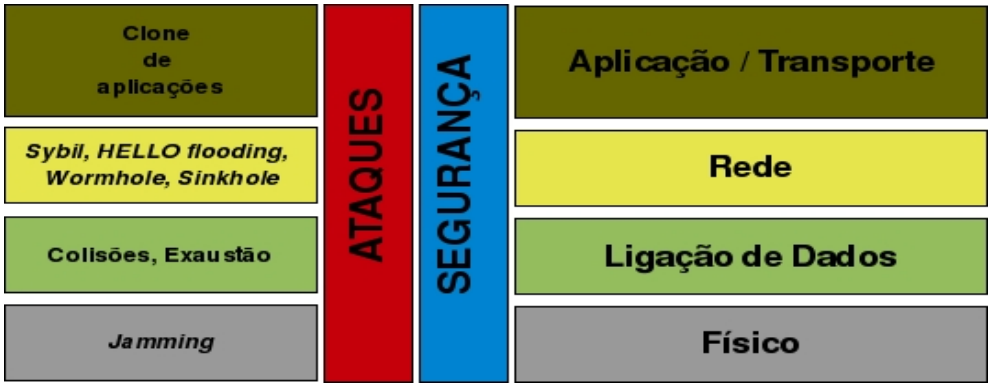

Figura 1.1 Pilha de protocolos de um nó sensor

No entanto a camada, na qual se pretende centrar a atenção, dentro do âmbito deste trabalho, é a camada de rede, responsável pelo encaminhamento dos dados numa RSSF. Nesta camada, as tipologias de ataques são essencialmente relacionadas com o meio de comunicação e com a intrusão. No primeiro tipo, os ataques verificados são os de introdução de informação de encaminhamento falsa, *wormhole*[13], *sybil*[12, 18] e HELLO *flooding*[14] e outros que serão mais detalhadamente apresentados à frente. No segundo caso e porque as RSSF têm características especiais (autonomia, auto-organização e localização remota) que as tornam susceptiveis a uma nova tipologia de ataques, tem-se os ataques por intrusão e captura de nós, materializados pelo ataque fisico ao sensor, que possibilita a usurpação de material criptográfico, bem como a replicação de nós maliciosos[19] que podem induzir comportamentos incorrectos, quer no protocolo, quer na aplicação.

Perante este cenário de novas ameaças, alguns autores têm vindo a desenhar algoritmos com vista a minimizar o impacto destes ataques na operação das RSSF. Estes algoritmos, efectivados com a especificação de protocolos de encaminhamento, com o intuíto de garantir algumas

propriedades de segurança[22] (ex: confidencialidade, integridade, autenticação, frescura) tem vindo a surgir na literatura. Importa, portanto, salientar os que irão ser alvo de estudo neste trabalho e que de uma forma geral correspondem ao estado da arte em matéria de segurança e de encaminhamento seguro em RSSF: *Secure Implicit Geographic Forwarding*(SIGF)[26], INtrusion-tolerant routing protocol for wireless SEnsor NetworkS (INSENS)[11] e *Secure Sensor Network Routing*(*Clean-Slate*)[20]. A selecção destes protocolos deve-se também ao facto de poderem ser enquadrados em diferentes classes de protocolos de encaminhamento (ex: hierárquicos, baseados em localização, *on-demand*[6], *table-driven*[6]), bem como o facto de terem diferentes mecanismos para fazer face aos ataques e, na generalidade, não protegerem contra todas as tipologias de ataques. O protocolo SIGF caracteriza-se por ser um protocolo inspirado num já existente, o IGF[8], incorporando neste, mecanismos de segurança. Por se tratar de um protocolo *on-demand*[6][4] e configurável, consegue estabelecer medidas de segurança adaptadas às necessidades da aplicação perante um ataque. Distingue-se do protocolo INSENS[11] porque este último é, em especial, orientado para a resiliência a ataques por intrusão, não descuidando os ataques ao meio de comunicação. É baseado na construção de tabelas de encaminhamento, portanto da classe *table-driven*[5][6], para além disto, deposita num nó base ou de sincronização um papel importante na criação e certificação das tabelas de encaminhamento, o que lhe permite implementar um sistema de multi-caminhos que o torna tolerante a intrusões. Por fim, o protocolo *Clean-Slate*[6][20] que procura abordar os conceitos principais para o desenho protocolos de encaminhamento seguro: prevenção, detecção/recuperação e resiliência. Assim, este protocolo pretende conseguir alta segurança, com alta disponibilidade, isto sem recorrer a *hardware* adicional e com o mínimo consumo de recursos.

Actualmente têm surgido muitos protocolos de encaminhamento para RSSF. Todavia, não conseguem endereçar todas as tipologias de ataques, assumindo, cada um, o compromisso de resistir a determinados ataques e garantir algumas propriedades de segurança tendo em vista a sua utilização em aplicações especificas. Dia após dia, com a generalização do uso das RSSF, com o baixo custo, com o carácter autonomo e a não necessidade de infraestrutura de comunicação, o estudo de protocolos de encaminhamento seguro por forma a avaliar os comportamentos das RSSF perante ataques e como estes influenciam a energia, fiabilidade e latência da rede.

[4]Em que as rotas são definadas a quando da comunicação

[5]Algoritmos que se baseiam numa tabela de encaminhamento que é mantida através da troca de mensagens de controlo por forma a manter a sua consistência em todos os nós da rede

[6]Esta designação deve-se ao facto do protocolo não ter um nome especifico mas, partir de uma abordagem de raiz para a garantia de segurança

Apesar do baixo custo do *hardware* a sua utilização em fases de investigação e desenho de protocolos torna-se impracticável, uma vez que dificilmente se consegue manter as mesmas condições de simulação. Considerando também, que o tempo útil de vida da rede é limitado, a utilização de sensores reais põe entraves relativos com os custos, já que os nós teriam de ser substituídos regularmente. Para suprir estas limitações surge a necessidade de conceber 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, permitindo a introdução de ataques de forma controlada. 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 Objectivos e contribuições previstas para a dissertação)

Conhecidas que estão as dificuldades existentes no estudo de protocolos de encaminhamento seguro, nomeadamente no que se refere à existência de um sistema de simulação de RSSF de larga escala, apresenta-se como desafio pertinente de se ver ultrapassado. 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, e pelo que consta inexistente de forma integrada, 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 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

Atingido o objectivo proposto de concepção de um ambiente de simulação que permita a avaliação/análise de protocolos de encaminhamento seguros em RSSF, pretende-se avaliar, com recurso a este ambiente alguns protocolos de encaminhamento existentes, nomeadamente os já indicados para estudo. Sendo este estudo uma contribuição, não só para a certificação da usabilidade do sistema, bem como para a complementariadade do estudo de cada um dos protocolos e verificação das propriedades enunciadas pelos autores, no que concerne à segurança. No que respeita à avaliação do ambiente em si e à sua utilização como ferramenta de estudo desta problemática, com a implementação de algoritmos de encaminhamento, será possível criar alguma sensibilidade para a efectividade e facilidade de utilização da plataforma para o desenvolvimento e estudo de protocolos de encaminhamento em RSSF em geral, e os que se revestem de preocupações de segurança, em particular.

Bibliografia

[1] BTnodes - a distributed environment for prototyping ad hoc networks : Documentation - b tnode rev 3 hardware reference browse. http://www.btnode.ethz.ch/Documentation/BTnodeRev3HardwareReference.

[2] MICA2_Datasheet.pdf.

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

[4] 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.

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

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

[7] 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.

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

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

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

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

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

[13] 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.

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

[15] 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.

[16] 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.

[17] A. Mpitziopoulos, D. Gavalas, G. Pantziou, and C. Konstantopoulos. Defending wireless sensor networks from jamming attacks. In *Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on*, pages 1–5, Sept. 2007.

[18] 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.

[19] B. Parno, A. Perrig, and V. Gligor. Distributed detection of node replication attacks in sensor networks. In *Security and Privacy, 2005 IEEE Symposium on*, pages 49–63, May 2005.

[20] 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.

[21] 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.

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

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

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

[25] 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.

[26] 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.

[27] 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.

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