Faculdade de Engenharia da Universidade do Porto

Segurança em Redes de Sensores Wireless

João Bento

Tese submetida no âmbito do
Mestrado Integrado em Engenharia Electrotécnica e de Computadores
Major Telecomunicações

Orientador: Prof. Dr. Armando Luís Sousa Araújo.

Julho de 2009

Resumo

As redes de sensores wireless possuem um enorme potencial de aplicação. Podem ser utilizadas em campos tão relevantes como a medicina e o sector militar. Seja a medir batimentos cardíacos, a fazer reconhecimento de terreno ou a medir a temperatura no interior de uma habitação, esta é uma tecnologia que, dia a dia, tem visto a sua utilização crescer. Tal deve-se não só à enorme gama de áreas em que uma rede de sensores wireless pode ser útil, mas também ao custo reduzido deste tipo de soluções [1]. É hoje possível adquirir quantidades numerosas de sensores a custos bastante reduzidos. No entanto, estas redes são implementadas muitas vezes em locais sem vigilância, estando portanto vulneráveis a uma variedade de potenciais ataques. Para além disso, os sensores envolvidos neste tipo de rede sofrem de fortes limitações, nomeadamente ao nível da capacidade de processamento, da memória e da própria bateria [2]. Estas limitações impedem a implementação das medidas tradicionais utilizadas nas redes wireless. É necessário, portanto, a implementação de medidas que consumam poucos recursos mas que ao mesmo tempo garantam a confidencialidade e fiabilidade necessária na comunicação, sem as quais esta tecnologia vê a sua aplicação bastante reduzida.

Este trabalho de investigação apresenta detalhadamente as ameaças mais frequentes, às quais as redes de sensores wireless estão sujeitas. São também descritas algumas medidas a implementar para que se consiga criar um nível de segurança elevado, assegurando a confidencialidade da comunicação. Para tal, são analisados protocolos de encaminhamento, assim como esquemas de encriptação e autenticação, sendo apresentadas soluções viáveis e respeitantes das limitações de hardware características das redes de sensores wireless.

Abstract

Wireless sensor networks possess a huge potential of employment. They can be used in such relevant fields as medicine or the military. They can be measuring heartbeats, doing terrain recognition or measuring the temperature inside a house, as the usage of this type of network has been growing quite noticeably. That is a direct consequence of the endless areas in which wireless sensor networks can be deployed, but also to the low costs involved. It is possible to build huge networks with thousands of nodes, while keeping the costs down. However, these networks are often deployed in unstable and unsecure environments, causing them to be vulnerable to a variety of potential attacks. Plus, sensors have generally severe limitations in terms of memory, energy and processing power, posing unique security challenges, as these limitations prevent the use of tradition wireless network security measures. As so, it is necessary to establish security measures that have in mind the hardware limitations of wireless sensor networks, while being able to assure the confidentiality and reliability of the communication channels.

This is an investigation project, with the purpose of determining and analyzing the most common threats that wireless sensor networks face. It describes also some measurements that are required in order to create the appropriated security level, ensuring the confidentiality of the network. With this in mind, some routing protocols are analyzed, as well as some encryption and authentication schemes, resulting in reliable security solutions that respect the unique characteristics of sensors in wireless networks.

Agradecimentos

Dedico este trabalho,

Aos meus pais, pela paciência que tiveram

À minha namorada, pelo apoio que me deu

Aos meus amigos, pelo motivação que me incutiram

Ao meu orientador pela ajuda e disponibilidade

Sem os quais nada disto era possível…

Índice

Lista de Figuras

Lista de Tabelas

Glossário

ACK	Acknowledgment.
ARC	Adaptive Rate Control.
BEB	Binary Exponential Backoff.
BKM	Basic Key Management.
CAM	Código de autenticação da mensagem.
Cluster	Conjunto / aglomerado / agrupamento.
CMDA	Code Division Multiple Access.
CSMA	Carrier Sense Multiple Access.
CTS	Clear To Send
Deadlock	Impasse / bloqueio.
DoF	Denial of Service.
GPSR	Greedy Perimeter Stateless Routing
Latência	Tempo decorrido entre o início de uma actividade e a sua conclusão.
LEACH	Low Energy Adaptive Clustering Hierarchy.
MAC	Medium Access Control.
Overhead	Custo adicional em processamento ou armazenamento.
QoS	Qualit of Service.
RKA	Random Key Assignment.
RKP	Random Key Pre-distribution.
RSW	Redes de Sensores Wireless.
RTS	Request To Send.
SAR	Sequential Assignment Routing.
SHARP	Sharp Hybrid Adaptive Routing Protocol.

Sinkhole	Depressão numa superfície, capaz aglomerar matéria no seu interior.
S-MAC	Sensors Medium Access Control.
SPIN	Sensor Protocols for Information via Negotiation.
SPINS	Security Protocols for Sensor Networks.
Spoofing	Imitação.
SYNK	Pacote de sincronismo
TDMA	Time Division Multiple Access.
TEEN	Threshold sensitive Energy Efficient sensor Network.
T-MAC	Timeout Medium Access Control.
Wormhole	Representa um “atalho” entre dois pontos distantes.

Capítulo 1

1. Introdução

Os recentes avanços na microelectrónica e nas redes wireless trouxeram a possibilidade de criar redes de pequenos sensores. Estes sensores, para além da reduzida dimensão, apresentam um baixo consumo, memória reduzida e pequena largura de banda. Uma rede de sensores wireless consiste num conjunto destes sensores, distribuídos espacialmente, com o objectivo de recolher e transmitir dados, onde não o é possível fazer com redes tradicionais, seja por motivos estratégicos ou por limitações do meio onde se inserem. Como tal, surgem áreas de aplicação bastante distintas, tais como habitações inteligentes (domótica), sistemas de estacionamento inteligentes, monitorização de instalações, robótica, indústria e segurança, entre outros [3].

A combinação do tamanho reduzido, baixo custo e a funcionalidade sem fios, faz das redes de sensores *wireless* uma tecnologia com enormes possibilidades de aplicação e evolução. À medida que os custos envolvidos forem descendo, o número de sensores numa rede poderá aumentar, tornando mais precisa e detalhada a aproximação ao fenómeno físico que se pretende monitorizar, do que até agora foi possível [5].

Embora todas as redes estejam sujeitas a ameaças, as redes wireless são substancialmente mais susceptíveis a ataques, uma vez que não existe a restrição física da cablagem, pelo que a informação se encontra fisicamente mais acessível aos atacantes. No entanto as claras vantagens da comunicação sem fios fazem da segurança uma necessidade ao invés de uma conveniência, pelo que a investigação nesta área é indispensável.

As limitações de memória, energia e largura de banda, são um grande obstáculo à implementação de medidas de segurança tradicionais. O facto de os meios de comunicação não serem fiáveis e os sensores frequentemente não estarem vigiados dificulta ainda mais o desenvolvimento de contramedidas adequadas [4].

1.1 Motivação

O uso crescente de sensores wireless torna necessária a investigação no campo da segurança, dado que a falta de fiabilidade nas suas aplicações pode inviabilizar o seu uso. Daí que para garantir a evolução e expansão desta tecnologia, seja necessário tornar a transmissão dos dados segura e fiável. Apesar de existirem bastantes abordagens aos ataques mais frequentes, a maioria das soluções aborda um problema, ignorando outros, pelo que uma solução que garanta os níveis de segurança necessários torna-se difícil de encontrar, sobretudo tendo em conta os limites dos sensores envolvidos, tanto ao nível da capacidade de processamento e da memória disponível, como da própria largura de banda [6].

1.2 Objectivos

O propósito deste trabalho é o de analisar a problemática da segurança em sistemas que usem redes de sensores wireless, tendo como principais objectivos:

- Estudar os protocolos usados em redes de sensores wireless;
- Investigar o nível de segurança oferecido pelos protocolos e software usados hoje em dia;
- Determinar as possíveis falhas de segurança e ataques contra este tipo de infra-estruturas;
- Determinar o "estado da arte" em termos de contra-medidas para evitar e repelir ataques.

1.3 Estrutura do Relatório

Este relatório encontra-se estruturado em cinco capítulos.

O primeiro capítulo serve de introdução à tese. Nele são apresentadas as Redes de Sensores Wireless e é explicada a motivação para este tipo de trabalho.

No segundo capítulo, as Redes de Sensores Wireless são explicadas com mais detalhe, juntamente com os tipos de ataques executados com maior frequência e os protocolos mais comuns.

O terceiro capítulo aborda alguns métodos de encriptação através de esquemas de gestão de chaves de segurança.

O quarto capítulo descreve com algum detalhe os ataques de encaminhamento, assim como analisa alguns algoritmos capazes de os contrariar.

As conclusões deste projecto são apresentadas no quinto e último capítulo, bem como sugestões para o que se poderá fazer, de futuro, como complemento a este trabalho.

Capítulo 2

2. Redes de Sensores Wireless

A tecnologia wireless aplicada às redes de sensores/computadores tem visto a sua utilização crescer imensamente. Esta tecnologia é utilizada hoje em dia, por exemplo, para monitorizar o ambiente numa fábrica ou, nas nossas casas, ligando em rede vários computadores [3]. Com o aumento do uso deste tipo de infra-estrutura, aumentou também o interesse em capturar os dados transmitidos ou mesmo em interromper a comunicação, por parte de indivíduos, ou organizações, com intenções menos nobres. Sem a existência de uma estrutura física, como as existentes nas redes com fios, os ataques podem ter origem em qualquer local, por qualquer indivíduo dentro do alcance da transmissão wireless, não estando restringidos a uma localização fixa. Isto torna a missão de detectar um intruso bastante complicada. Como tal, a permeabilidade em termos de segurança das redes wireless tornou-se um assunto importante, na medida em que a confidencialidade dos dados nas transmissões se torna ameaçada.

Neste capítulo serão analisados os protocolos mais frequentes, assim como os problemas de segurança que as redes de sensores enfrentam, derivadas das limitações dos próprios sensores e de outras restrições das redes. Serão apresentados os objectivos em termos de segurança, assim como os principais ataques realizados contra este tipo de rede.

2.1 Definição

Uma rede de sensores wireless é uma rede sem fios, consistindo num conjunto de dispositivos autónomos distribuídos espacialmente, usando sensores para monitorizar, de um modo cooperativo, fenómenos físicos ou condições ambientais, tais como a temperatura, o som, a vibração, a pressão, o movimento e a poluição, entre outros, em diversas localizações [7].

2.2 Aplicação

Apesar de os sistemas de instrumentação baseados em computadores já existirem há algum tempo, a produção em massa de sensores inteligentes veio tornar esta tecnologia barata e acessível, criando uma nova gama de possibilidades de aplicação.

Estas podem ser, a grosso modo, repartidas em três categorias [9]:

- Monitorização espacial;
- Monitorização de objectos;
- Monitorização de interacções entre objectos e o espaço que os rodeia.

A primeira categoria inclui monitorização ambiental, agricultura de precisão, controlo climático interior, vigilância e alarmes inteligentes, entre outros.

A segunda inclui monitorização de estruturas, ecofisiologia, manutenção de equipamento com base nas suas condições, diagnóstico médico e mapeamento de território urbano. As aplicações de maior relevo envolvem a monitorização de interacções complexas, como em habitats de vida selvagem, gestão de desastres, resposta em situações de emergência, procura de bens, cuidados médicos e controlo de linhas de produção [9].

Deve-se também destacar a aplicação das redes de sensores wireless na monitorização e controlo da vida selvagem oceânica, do ambiente florestal, como pode ser visto na figura 2-1 [10], desempenho de maquinaria de produção, aplicações militares e monitorização de actividade sísmica e vulcânica, como está ilustrado na figura 2-2 [13].

Figura 2-1:Monitorização ambiental na floresta tropical da Costa Rica

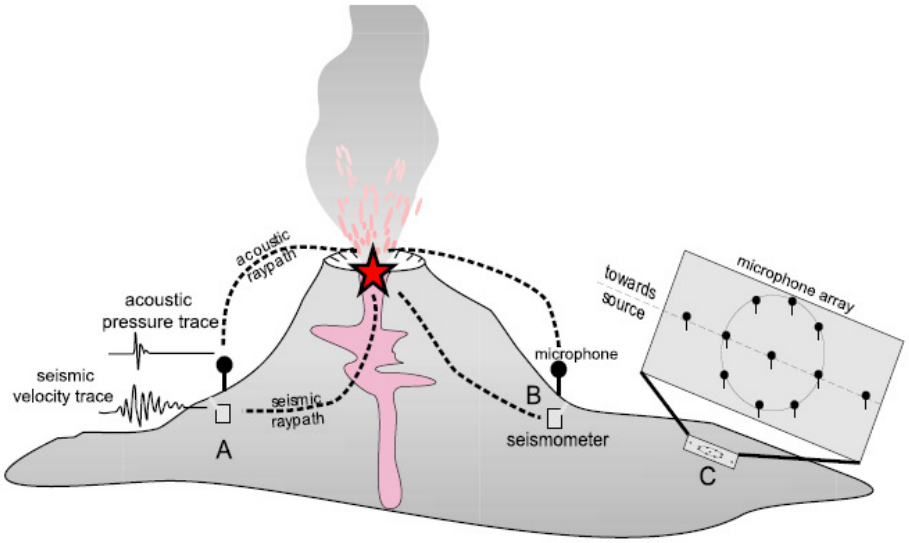


Figura 2-2:Rede de sensores wireless a monitorizar actividade vulcânica

É importante mencionar as possibilidades de aplicação no ramo da medicina. É possível a criação de interfaces para deficientes físicos, monitorização integrada, diagnóstico e administração de drogas para pacientes, monitorização de dados fisiológicos e monitorização de médicos e pacientes num hospital [11].

Em termos do meio ambiente, podem-se destacar as seguintes possibilidades de aplicação [12]:

- **Detecção de incêndios em florestas:** Redes de sensores podem ser densas e dispostas aleatoriamente sobre florestas, podendo a localização exacta do foco de incêndio ser encontrada pela rede, muito antes do fogo se tornar incontrolável.
- **Detecção de cheias:** Redes de sensores podem ser usadas para detecção de enchentes em locais menos acessíveis.
- **Agricultura de precisão**: É possível monitorizar a concentração de pesticidas na água, o grau de erosão do solo e o nível de poluição do ar, tudo em tempo real.

O ambiente doméstico é também um foco de possíveis aplicações [9]. Tais como:

- **Automação doméstica:** Conforme a tecnologia avançar, podem ser embebidos sensores em electrodomésticos, criando uma rede de cooperação entre eles.
- **Ambientes inteligentes:** Os electrodomésticos, móveis e portas de casa, por exemplo, poderão comunicar, cada um informando o outro sobre seu estado e possíveis eventos.

Este tipo de redes pode ainda ser uma parte integrante de sistemas militares de comando, controlo, comunicações, computação, inteligência, vigilância e reconhecimento. As características

presentes numa rede de sensores wireless, tornam-na ideais para tais aplicações onde o problema principal é a urgência. Segundo Quirino e Silva [35], a rápida instalação, a auto-organização e a tolerância à falha são exactamente aquilo que os militares têm vindo a procurar nas redes de sensores wireless. São exemplos de aplicações militares:

- **Monitorização de forças amigas, equipamento e munições:** Líderes e comandantes podem ter na sua mão, através de algo semelhante a um palmtop, informações instantâneas sobre os seus soldados, a situação do seu equipamento e munições.
- **Vigilância em campo de batalha:** Em caso de movimentação de tropas inimigas, são accionados sistemas de alarme e possíveis contra-medidas tomadas até mesmo automaticamente.
- **Reconhecimento de forças inimigas e terreno:** Sensores podem ser lançados de aviões em terrenos desconhecidos. Tais sensores podem fazer o rastreamento e mapeamento de estruturas cuja análise não possa ser feita por satélite.
- **Sistemas de pontaria:** Redes de sensores podem ser incorporadas em sistemas de pontaria usando munições inteligentes.
- **Avaliação de danos em batalha:** Antes, ou depois, de uma batalha podem ser espalhados sensores, na área de combate, para fazer uma avaliação de danos a estruturas ou terreno.
- **Detecção e reconhecimento de ataques nucleares, biológicos ou químicos:** Redes de sensores wireless dispostas em solo amigo podem ajudar no alerta para diminuir os danos causados por tais ataques.

De acordo com Perrig et al. [8], o espectro de actuação das redes de sensores wireless, RSW, tende a crescer. É de esperar a sua utilização em monitorização de tráfego automóvel, poluição, fogos florestais, segurança de instalações, qualidade da água e até no batimento cardíaco de cada indivíduo.

2.3 Limitações dos Sensores

Os sensores utilizados nas RSW são, tipicamente, limitados em termos de tamanho, capacidade de processamento e também de armazenamento. Isto vem dificultar imenso o desenvolvimento de medidas de segurança. Outro problema prende-se com a capacidade energética. Ocorrerá com alguma frequência a implementação de redes em locais de difícil acesso, pelo que a substituição das baterias dos sensores é uma tarefa que deverá ser realizada o mínimo de vezes possível. Outro factor que torna a poupança energética importante é o número de sensores. Numa rede com um elevado número de nós, o processo de renovação das baterias poderá ser extremamente demorado.

A figura 2-3 [27] apresenta alguns exemplos de sensores, sendo possível ver dimensões físicas que, tipicamente, estão envolvidas neste tipo de rede.

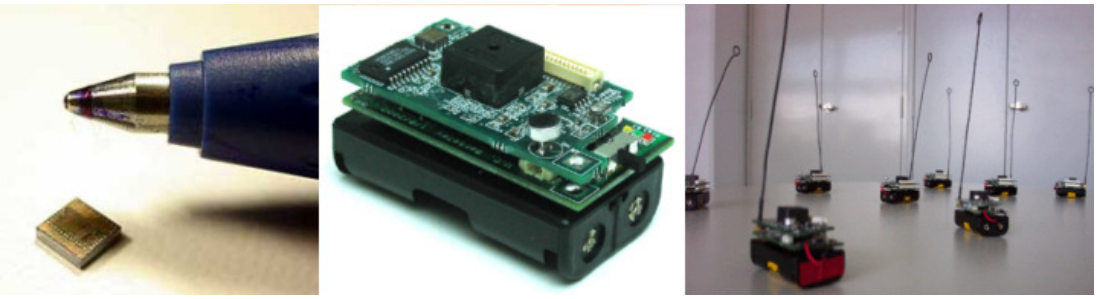


Figura 2-3:Redes e sensores wireless

Outro problema com o qual os sensores se prendem é a acessibilidade à sua localização. A captura de nós, ou seja a subtracção e/ou manipulação física de um nó por parte de um adversário, é uma ameaça à segurança da rede, uma vez que um atacante poderá extrair informação pertinente de um nó capturado.

A Tabela 2-1 [36] apresenta, a título de exemplo, as características de alguns sensores.

Tabela 2-1: Exemplos de sensores

Nome	**Microcontrolador**	**Emissor**	**Memoria Interna**	**Memória Externa**
BTnode	Atmel ATmega 128L (8 MHz @ 8 MIPS)	Chipcon CC1000 (433-915 MHz) and Bluetooth (2.4 GHz)	64+180 K RAM	128K FLASH ROM, 4K EEPROM
IMote	ARM core 12 MHz	Bluetooth with the range of 30 m	64K SRAM	512K Flash
IMote 1.0	ARM 7TDMI 12-48 MHz	Bluetooth with the range of 30 m	64K SRAM	512K Flash
SunSPOT	ARM 920T	802.15.4	512K RAM	4 MB Flash

Como se pode constatar, os nós possuem tipicamente processadores com baixas velocidades de relógio e, consequentemente, baixa capacidade de processamento, apresentando também uma limitada capacidade de memória, da ordem dos KBytes. Com estas limitações, a optimização de processos torna-se claramente um cuidado essencial.

2.4 Limitações das Redes

As redes de sensores sofrem das restrições das redes móveis ad-hoc, tais como a falta de fiabilidade do canal de comunicação, a falta de uma infra-estrutura física e problemas de colisão ou danificação de pacotes. Este último problema assume uma ainda maior relevância em redes de elevadas dimensões, que podem chegar aos milhares de sensores, e onde existe uma probabilidade elevada de ocorrerem colisões de pacotes e latência, ou seja, atrasos na comunicação. No entanto, ao contrário das redes tradicionais, as limitações energéticas dos nós tornam o reenvio de pacotes impraticável em situações de colisão [25].

2.5 Protocolos

Os nós das redes de sensores wireless possuem pouca capacidade de processamento, pouca memória e baterias com uma longevidade limitada. Como tal, os protocolos de comunicação tradicionais não podem ser aplicados às RSW.

Esta secção está dividida em três partes, abordando alguns dos protocolos utilizados em redes de sensores, assim como as suas características e funcionamento [35]. A primeira parte consiste numa descrição de alguns protocolos de acesso ao meio baseados em MAC, sendo a segunda parte referente a protocolos de encaminhamento plano, ou seja, encaminhamento em redes sem hierarquias estabelecidas. A terceira e última parte aborda o encaminhamento em redes hierarquizadas, onde alguns dos nós representam papéis de aglomeração e redireccionamento do tráfego.

2.5.1 Protocolos baseados em MAC

2.5.1.1 Protocolo, S-MAC

O Sensors Medium Access Control, S-MAC, é um protocolo criado para redes de sensores wireless [17]. Segue o princípio da alocação dinâmica do canal, havendo períodos em que parte dos nós estão “adormecidos”, acarretando assim uma diminuição do consumo energético da rede. O principal objectivo deste protocolo é a poupança de energia e a longevidade dos sensores.

Este protocolo é adequado para redes de sensores com aplicações dirigidas a eventos, onde há colecta de dados, sendo insensível à latência, ou seja, não é necessário o envio e processamento imediato dos dados, e tendo uma baixa taxa de envio de mensagens.

Tendo em mente a eficiência energética, o S-MAC permite a auto-configuração dos nós, com base na constituição da rede. O rendimento energético é afectado directamente por:

- **Colisões:** no caso dos nós transmitirem ao mesmo tempo para um mesmo destino, levando a um consumo adicional devido a retransmissões, aumentando consequentemente a latência e o consumo de energia;

- **Escuta inútil:** também chamado de *"overhearing"*, que é a escuta de tráfego de pacotes destinados a outros nós;
- **"*Overhead*" de controlo:** durante a comunicação, existem algumas trocas de pacotes, sendo que nem todos contêm uma mensagem propriamente dita. Alguns pacotes são utilizados como controlo da comunicação, tal como para confirmar recepções de mensagens, reservar o canal de comunicação, sincronização e outros;
- **Escuta ociosa:** o nó escuta o meio sem receber informação dos outros nós, mantendo o canal de comunicação aberto desnecessariamente.

O protocolo S-MAC utiliza as seguintes técnicas para ser energeticamente eficiente:

- Utiliza diálogo de comunicação RTS-CTS-DATA-ACK, ilustrado na figura 2-7, para evitar colisões. Isto permite contrariar problemas de terminal escondido e de estação exposta, sendo estes problemas descritos mais à frente;
- Para evitar a escuta inútil, desliga a comunicação do nó quando verifica que o pacote não lhe é destinado. Enquanto dois nós comunicam, os seus vizinhos ficam com a comunicação desligada;
- O tamanho dos pacotes enviados é reduzido com o objectivo de diminuir o "*overhead*";
- Baixos tempos de operação – os nós desligam os seus rádios periodicamente, "adormecendo" e reduzindo consequentemente o tempo de escuta ociosa como se pode ver na figura 2-4.

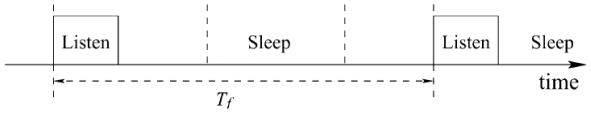


Figura 2-4: Comunicação em slots temporais

Quando dois nós tentam comunicar para um terceiro em simultâneo vai ocorrer uma colisão dos pacotes. Isto acontece quando os dois nós emissores estão fora do alcance um do outro e, como tal, não conseguem detectar que está a decorrer uma transmissão, como se pode ver pela figura 2-5. Este problema é conhecido como o problema do terminal escondido [15].

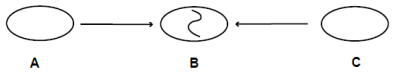


Figura 2-5: Problema do terminal escondido

Outro problema é o do terminal exposto. Na figura 2-6, o nó B está a transmitir para o nó A. O nó C não irá enviar nada ao nó D, uma vez que se encontra a aguardar que termine a transmissão de B. No entanto, uma vez que D se encontra fora do alcance de B, não existiria nenhuma interferência no receptor e, como tal, não haveria problema.

Figura 2-6: Problema do terminal exposto

Estes problemas são resolvidos através de um esquema de trocas de pacotes, RTS-CTS-DATA-ACK. Como ilustrado na figura 2-7, é enviado um pacote RTS (*Request To Send*) pelo nó que pretende enviar a mensagem, sendo seguido de um resposta CTS (*Clear To Send*) do receptor. De seguida, é enviada a mensagem propriamente dita, sendo que a comunicação termina com um pacote ACK (*Acknowledgment*) para confirmar a recepção da mensagem. Isto garante que dois nós não tentam comunicar para o mesmo destinatário simultaneamente. Na situação da figura 2-5, o nó C iria receber apenas o CTS do nó B e manter-se-ia em silêncio, eliminando o problema do terminal escondido. O problema do terminal exposto também é resolvido, porque um nó que recebe uma mensagem RTS, mas não a correspondente CTS pode transmitir a sua mensagem.

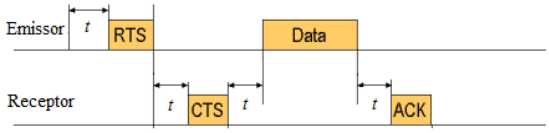


Figura 2-7: Troca de pacotes durante a comunicação

Antes que cada nó inicie o seu período de *Sleep* e *Listen*, necessitam de escolher uma calendarização para os seus períodos e de a transmitir aos seus vizinhos. Cada nó mantém uma tabela de calendarização onde armazena o calendário dos seus vizinhos. Para escolher este calendário e armazenar o dos seus vizinhos, cada nó segue os seguintes passos, exemplificados na figura 2-8 [17]:

1. O primeiro nó escuta por um determinado período de tempo. Caso não escute nenhum calendário de outro nó, escolhe aleatoriamente um período para dormir e transmite imediatamente o seu calendário numa mensagem SYNK, indicando que vai dormir após t segundos. Este nó é chamado de sincronizador, uma vez escolhe o seu próprio calendário, sendo que os outros nós sincronizam com este;

2. Se um nó receber um calendário de um vizinho antes de escolher o seu próprio, irá seguir este mesmo calendário. A este nó chama-se de seguidor. Após um intervalo aleatório t_d, este nó irá transmitir o seu calendário, indicando que irá dormir dentro de $t - t_d$ segundos. Este intervalo t_d é aleatório para evitar colisão de pacotes.

3. Caso um nó receba um calendário diferente após ter seleccionado e transmitido o seu próprio, vai adoptar ambos os calendários, ou seja, irá acordar no tempo que tinha previsto e também no tempo do seu vizinho.

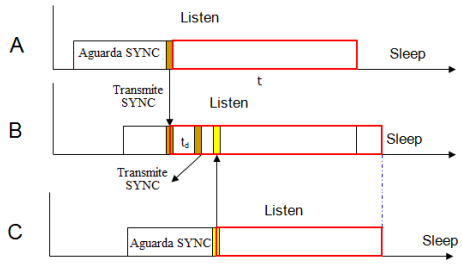


Figura 2-8: Sincronismo entre nós

O S-MAC prevê ainda o envio de mensagens longas divididas por várias mensagens pequenas, diminuindo assim o impacto da colisão de pacotes. No caso de ocorrer uma colisão, a mensagem tem que ser reenviada. A transmissão mensagens de grandes dimensões implica um custo elevado do ponto de vista energético, pelo que se forem pequenas, o custo de retransmissão é reduzido, conservando assim energia e prolongando o tempo de vida da rede.

2.5.1.2 Protocolo T-MAC

O protocolo *"Timeout Medium Access Control"*, T-MAC [15], é uma variante do S-MAC, referido no ponto 2.5.1.1, tendo sido criado para contrariar os níveis elevados de latência e baixa capacidade de transmissão do S-MAC.

Para se adaptar a níveis de carga (quantidades de tráfego) variáveis, o T-MAC utiliza um tempo de funcionamento adaptável, variando de acordo com as necessidades, contrastando com o tempo de funcionamento fixo do S-MAC. No T-MAC, os períodos de actividade dos sensores terminam quando nenhum evento de activação tiver ocorrido dentro de um limite de tempo *TA*

Um dos objectivos do T-MAC é ser energeticamente eficiente, considerando as limitações do hardware dos nós e os padrões de comunicação de troca de mensagens entre um nó e os seus vizinhos e entre os nós e a estação base. Para tal, é utilizado um ciclo de operação relativamente reduzido, possuindo tempos de actividade e de repouso variáveis que se adaptam à carga da rede. Um temporizador faz a variação dinâmica do tempo activo, que desliga o rádio do nó quando não existir transmissão durante um determinado intervalo de tempo *TA*. A ideia é reduzir o tempo de escuta ociosa para diminuir o consumo de energia do sensor.

As mensagens recebidas durante o tempo de repouso são armazenadas e transferidas em rajadas no início do tempo activo. A figura 2-9 descreve o ciclo de informação, onde as setas indicam transmissão e recepção de mensagens.

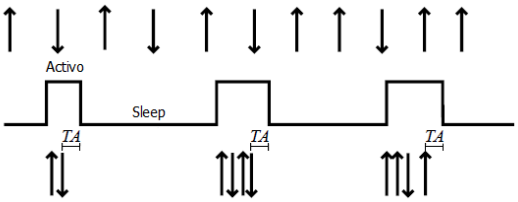


Figura 2-9: Ciclo adaptativo do protocolo T-MAC

Ao escutar a rede, o nó transmite e recebe dados durante seu tempo activo. O temporizador determina o final do tempo activo quando não ocorrem eventos durante *TA*. Este pode ser activado por início periódico, pela recepção de dados no rádio, pelo final da transmissão dos seus vizinhos, final da transmissão do seu próprio pacote de dados ou recebimento de pacotes de Acknowledgment, ACK, ou ainda por detecção de sinal no rádio.

Um problema do protocolo T-MAC consiste em um determinado nó adormecer quando um outro nó ainda tem uma mensagem para ele. Este problema é conhecido como o problema de dormir cedo. A figura 2-10 ilustra este comportamento.

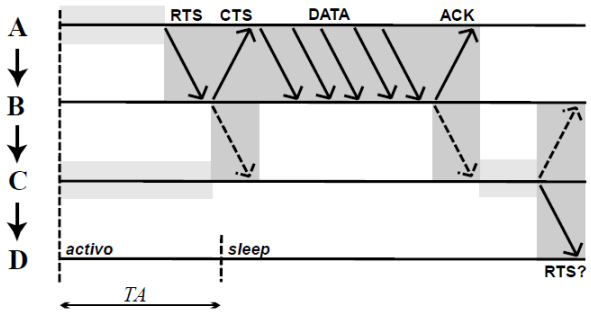


Figura 2-10: Nó adormecido

Considerando uma situação em que o tráfego na rede é tipicamente unidireccional, o nó C, sempre que este pretender enviar uma mensagem para D, terá que concorrer pelo canal de transmissão, podendo perder para o nó B (caso receba um pacote de RTS) ou para o nó A (indirectamente, ao escutar um pacote CTS do nó B). Se o nó C perder o direito ao canal por causa de um pacote RTS do nó B, irá responder com um CTS, que pode ser ouvido pelo nó D. Nesse caso, o nó D irá estar acordado quando terminar a comunicação entre C e B. No entanto, se C perder o canal por escutar um CTS de B para A, terá que permanecer em silencio. Uma vez que D desconhece que A está a comunicar com B, o seu tempo activo *TA* irá chegar ao fim e o nó irá adormecer. O nó C só terá uma nova hipótese de transmitir para D quando recomeçar o ciclo.

Este problema pode ser solucionado fazendo com que o nó envie imediatamente aos seus vizinhos um pacote, usando um esquema de prioridades para o esvaziamento do buffer quando este se aproximar da sua capacidade limite, ou seja, ao receber um *Request To Send*, RTS, em vez de responder com um *Clear To Send*, CTS, o nó transmitirá o seu próprio RTS para poder enviar as

mensagens armazenadas no seu buffer para o nó de destino das mesmas, como ilustrado na figura 2-11.

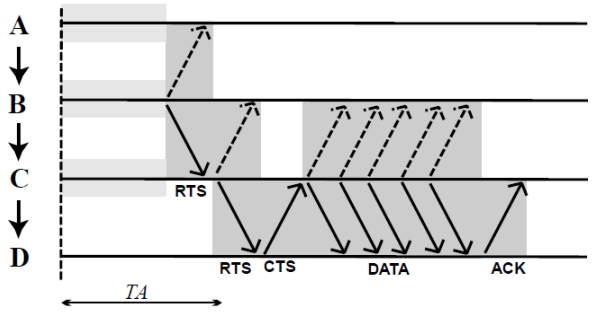


Figura 2-11: Prioridade após recepção de RTS

O T-MAC é mais eficiente em termos energéticos que o S-MAC, contudo é limitado em largura de banda e o seu algoritmo não é aplicável depois de uma fracção de largura de banda do canal ter sido utilizada.

2.5.2 Protocolos de Encaminhamento Plano

2.5.2.1 Protocolo Difusão Direccionada

O objectivo deste protocolo é estabelecer canais de comunicação eficientes entre os nós sensores e a estação base [18]. Baseia-se em dois conceitos:

- Encaminhamento baseado nos dados, onde, através da requisição de informação de interesse, é enviada a informação que um nó requisitou a um outro nó;
- Agregação de dados, onde os nós intermédios podem agregar os seus dados num simples pacote para reduzir as transmissões e o volume total de dados transmitidos. Tudo é centrado nos dados, logo, os endereçamentos dependem dos dados que monitorizam.

O protocolo de difusão direccionada é aplicável em redes orientadas a eventos e consultas, consistindo nos seguintes elementos:

- Interesses – uma mensagem de interesse é uma interrogação que especifica o que um utilizador pretende. Cada interesse contém uma descrição de uma tarefa de sensor que é suportada por uma rede de sensores para a aquisição de dados;
- Mensagens de dados – tipicamente, os dados numa rede de sensores são o resultado da colheita ou processamento de informação relativa a um fenómeno físico. Estes dados, podem ser um evento, que é uma descrição abreviada do fenómeno sentido. Na difusão directa, os dados são nomeados usando atributos e os respectivos valores. Por exemplo, uma tarefa de monitorização de um veículo pode ser descrita por:

tipo=Veículo terrestre	//Detectar localização do veículo
intervalo=20ms	//Enviar eventos a cada 20ms
duração=10s	//Nos próximos 10s
rect = [-100, 100, 200, 400]	//A partir de sensores dentro de um rectângulo

Uma tarefa de sensor é disseminada pela rede de sensores como um interesse em determinados dados. Intuitivamente, a descrição da tarefa especifica um interesse em dados que correspondentes a determinados atributos.

- Gradientes – a disseminação de interesses cria gradientes dentro da rede, com o propósito de atrair eventos, ou seja, procurando obter dados para satisfazer os interesses. Especificamente, um gradiente é o estado da direcção da comunicação em cada nó que recebeu uma mensagem de interesse. A direcção dos gradientes vai de encontro ao nó vizinho de onde se recebeu o interesse. Os eventos começam a fluir em direcção aos originadores dos interesses, através dos múltiplos caminhos de gradientes;
- Reforços – a rede de sensores reforça um, ou um pequeno número dos caminhos de gradientes ao nível da taxa de transferência, criando um caminho favorável para o envio dos dados na direcção da estação base.

A figura 2-12 ilustra a utilização destes elementos.

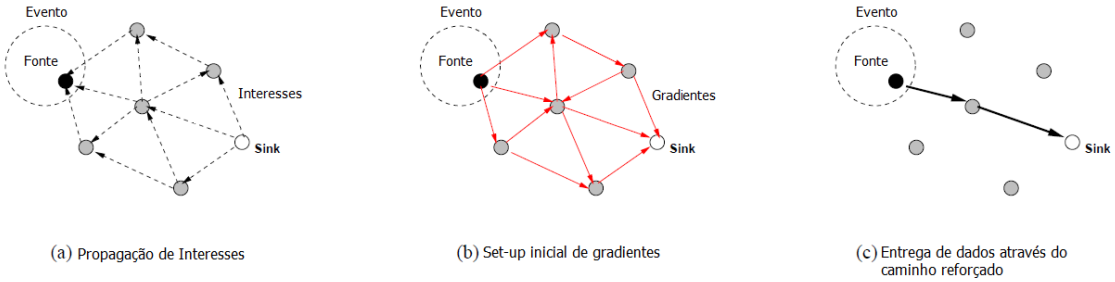


Figura 2-12: Protocolo Difusão Direccionada

2.5.2.2 Protocolo SPIN

O protocolo *"Sensor Protocol for Information via Negotiation"*, SPIN, assenta em duas ideias básicas [20]:

- Para operar de um modo eficiente e para conservar energia, os sensores necessitam de comunicar uns com os outros acerca dos dados que já possuem e dos dados que ainda necessitam. A troca de dados pode representar um elevado custo do ponto de vista de largura de banda e energia, mas trocar informação sobre os dados pode não o ser.
- Os nós numa rede devem monitorizar e adaptar-se aos seus próprios recursos energéticos para prolongar a vida operacional do sistema. Quando um nó percebe que sua

energia está perto de um limite preestabelecido, deverá adapta-se, participando menos da disseminação de dados.

Os sensores utilizam meta-dados para descrever completa e sucintamente os dados que recolhem. Se *x* representa os meta-dados do nó *X*, então o tamanho de *x* deverá ser menor do que o de *X* para o SPIN ser benéfico.

São utilizados três tipos de mensagens para comunicar:

- ADV – esta mensagem é utilizada para publicitar a existência de *novos dados (advertisment*). Quando um nó possuiu dados para partilhar, pode publicitar isto através da transmissão de mensagens ADV contendo meta-dados;
- REQ – pedido de dados. Um nó envia uma mensagem REQ quando pretende receber determinados dados do nó que os publicitou, através do envio de uma mensagem ADV;
- DATA – mensagem de dados. As mensagens DATA contêm dados obtidos pelos sensores com um cabeçalho contendo meta-dados.

Como as mensagens ADV e REQ apenas contêm meta-dados, o seu tamanho é reduzido e o custo de as enviar é mais baixo do que as correspondentes mensagens DATA. A utilização destas mensagens encontra-se ilustrada na figura 2-13.

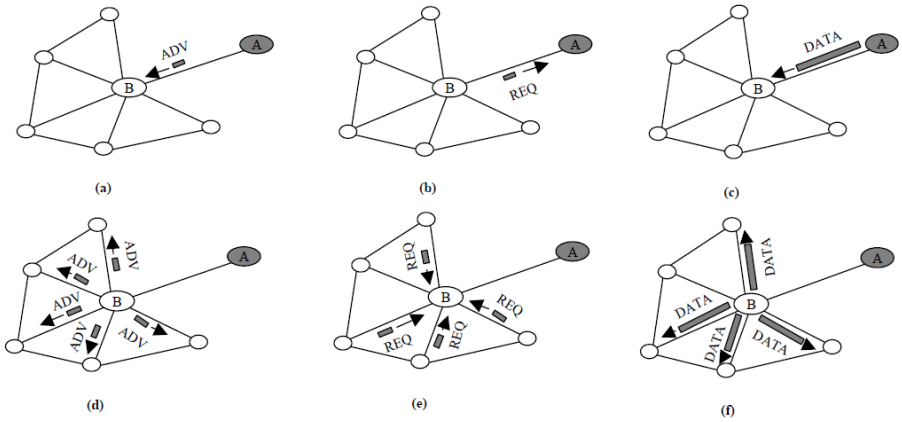


Figura 2-13: Protocolo SPIN

É possível observar que o nó A começa por publicitar os seus dados ao nó B (a). O nó B, por sua vez, responde enviando um pedido ao nó A (b). Após receber os dados pedidos (c), o nó B envia mensagens de publicidade aos seus vizinhos (d), que por sua vez enviam pedidos ao nó B (e,f).

2.5.2.3 Protocolo SAR

O *"Sequential Assignment Routing"*, SAR [21], tem como objectivo facilitar o encaminhamento multi-etapas (quando uma mensagem passa por vários nós entre o destino e a origem). Para este esquema, são levados em consideração o nível de prioridade de cada pacote, os recursos energéticos e a qualidade da transmissão, ou seja, *"Qualit of Service"* – QoS, em cada caminho.

A selecção do caminho é feita pelo nó que gera o pacote, a não ser que pelo caminho se altere a topologia, obrigando a que o pacote seja desviado. Cada ligação representa um custo energético e um atraso, e, como tal, representa uma resistência ao fluir de pacotes que pode assim ser contabilizada e somada ao longo de um dado percurso. Isto permite que um pacote com prioridade alta, por exemplo, seja encaminhado por percursos com baixa latência e evitando nós cuja bateria esteja perto do fim. Para cada pacote encaminhado pela rede, é calculada uma métrica ponderada QoS, como o produto da soma das métricas de QoS ao longo de um dado percurso com um coeficiente associado ao nível de prioridade do pacote, com o propósito de avaliar a performance. Quanto maior a qualidade do percurso, menor será a métrica ponderada de QoS do mesmo. No esquema da figura 2-14, o percurso do nó A para o nó C possui uma métrica QoS A-D que é o resultado da soma das métricas dos caminhos intermédios, sendo depois ponderada com a prioridade do pacote a transmitir.

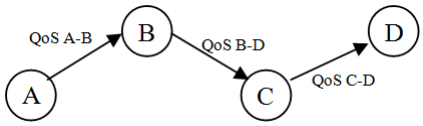


Figura 2-14: Métricas de QoS nas ligações

Esta métrica ponderada de QoS mede o QoS providenciado a cada pacote relativamente ao nível de prioridade do mesmo. Como tal, para manter a mesma métrica ponderada de QoS, caminhos com mais qualidade (com uma métrica de QoS mais baixa) serão usados para pacotes com mais prioridade (coeficiente de peso mais elevados). O objectivo do SAR é minimizar a média da métrica ponderada de QoS ao longo da vida da rede.

À medida que cada percurso vai sendo utilizado, com o tempo vão-se alterando os níveis energéticos disponíveis. Também é possível haver alterações do QoS nos percursos. Estas alterações são contabilizadas sempre que a estação base desencadear a actualização periódica das métricas.

2.5.3 Encaminhamento hierárquico

Com este tipo de encaminhamento, são estabelecidas duas classes distintas de nós: as fontes e os líderes de grupo (*cluster heads*). Os nós fonte apenas recolhem e enviam dados para o líder do grupo, que executa uma fusão ou agregação destes dados antes de os enviar para outro ponto de acesso, como ilustrado na figura 2-15.

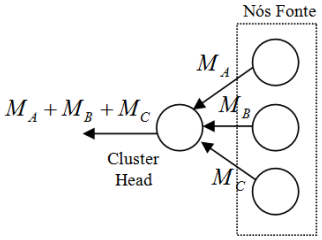


Figura 2-15: Agregação de mensagens no encaminhamento hierárquico

2.5.3.1 Protocolo LEACH

O protocolo "*Low Energy Adaptive Clustering Hierarchy*", LEACH, foi desenvolvido para reduzir o consumo de energia [22]. Trata-se de um protocolo que prevê a auto-organização e adaptação da rede durante ciclos de comunicação. Os nós organizam-se em clusters, com um nó a servir de estação base local ou líder de cluster. Este líder varia entre cada ciclo de comunicação de uma forma aleatória, evitando que se esgotem as baterias dos nós seleccionados. A decisão de se tornar líder de cluster depende do nível energético de cada nó. O processo de formação de clusters encontra-se ilustrado no fluxograma da figura 2-16.

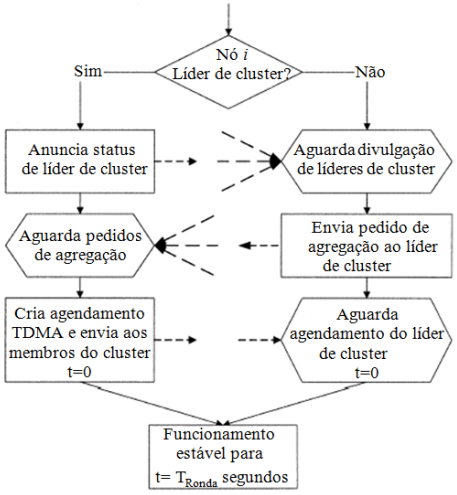


Figura 2-16: Fluxograma LEACH

O algoritmo do LEACH pode ser dividido nas seguintes fases:

1) Divulgação: cada nó decide se se torna um líder de cluster na ronda actual. Cada nó que se tiver auto-elegido como um líder de cluster transmite uma mensagem de divulgação ao resto dos nós;

2) Setup de clusters: cada nó decide a que cluster pertencer, tendo que enviar uma mensagem ao líder do cluster pretendido informando que faz parte do mesmo;

3) Agendamento: o líder de cluster cria um agendamento de TDMA (*Time Division Multiple Access*) que divide o acesso ao canal em slots temporais, indicando a cada nó qual o seu slot, ou seja, quando pode transmitir;

4) Transmissão de dados: o líder de cluster deverá manter o seu receptor activo para receber todos os dados dos nós do cluster. Quando todos os dados tiverem sido recebidos, o líder de cluster executa algumas funções de processamento de sinal para comprimir os dados num único sinal. Este sinal composto é enviado à estação base;

Para reduzir as interferências entre diferentes clusters, cada cluster comunica usando diferentes códigos CDMA (*Code Division Multiple Access*), sendo este um método de multiplexagem que codifica dados com um código associado a cada canal.

O LEACH é recomendado para redes em que se pretenda que a recolha de dados seja feita periodicamente.

2.5.3.2 Protocolo TEEN

O funcionamento do protocolo "*Threshold Sensitive Energy Efficient Sensor Network"*, TEEN [23], é semelhante ao LEACH, sendo que a auto-organização em clusters segue o mesmo método. No entanto, neste caso, os nós sensores podem não transmitir dados periodicamente. Segundo este protocolo, as redes são classificadas em redes pró-activas e redes reactivas. Nas redes pró-activas, os nós monitorizam o ambiente continuamente e existem dados a serem enviados com uma taxa constante. Já nas redes reactivas, os nós apenas enviam dados quando a variável que está a ser monitorizada ultrapassa um determinado valor limite H_T, *Hard Threshold*. Em ambos os casos, apenas são enviados dados quando o valor a transmitir difere do último valor transmitido em mais do que um valor S_T, *Soft Threshold*. Evita-se assim o desperdício de energia ao não enviar informação redundante.

Para evitar colisões neste protocolo, pode-se utilizar um escalonamento TDMA ou Code Division Multiple Access, CMDA, já descritos no ponto 2.5.3.1.

2.5.3.3 Protocolo GPSR

O protocolo GPSR, ou "*Greedy Perimeter Stateless Routing"* [24], explora a correspondência entre a posição geográfica e a conectividade numa rede de sensores wireless, através do uso da posição dos nós para decidir o encaminhamento dos pacotes. Este protocolo utiliza uma estratégia de encaminhamento chamada de *"greedy forwarding"*, ou encaminhamento ganancioso, para encaminhar informação pelos nós que se encontram sempre progressivamente mais próximas do destino. Os nós possuem informação sobre os seus vizinhos, enviando os pacotes para o nó (dentro do seu alcance) que se encontra mais próximo do nó ao qual se destina a mensagem. Na figura 2-17, o nó *x* possui um pacote para o nó *D*, enviando-o para o nó *y*, uma vez que este se encontra mais perto do nó *D* que qualquer outro nó dentro do seu alcance.

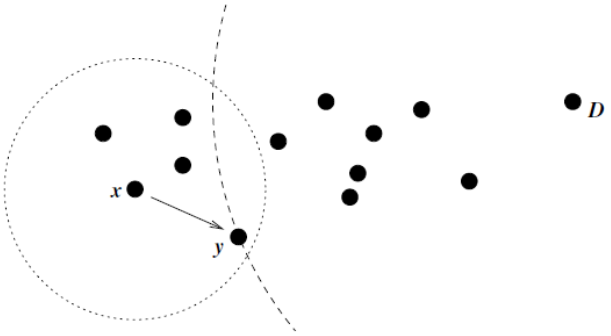


Figura 2-17: Greedy forwarding

Em regiões da rede onde não exista este percurso ganancioso, ou seja, o único caminho existente requer que se mova temporariamente para mais longe do nó de destino, o GPSR realiza o encaminhamento em *"perimeter mode"*, ou modo de perímetro, como ilustrado na figura 2-18.

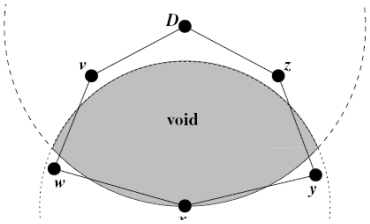


Figura 2-18: Região vazia

Neste modo, o caminho é definido através de um sub-grafo planar, que consiste num grafo que não contém intersecções de arestas, sendo que o caminho percorrido é estipulado pela regra da mão direita, como se pode ver pela figura 2-19. Segundo esta regra, é traçada uma recta *r* entre o nó de origem e o nó de destino e vai-se percorrendo a rede através das arestas no sentido anti-horário, desde que a aresta não intercepte a recta *r* [32]. Sempre que possível, deve ser retomado o *"greedy forwarding"*.

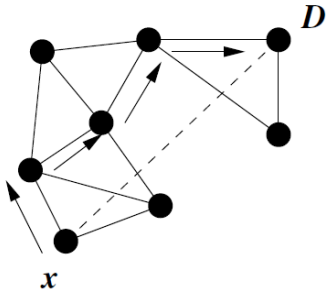


Figura 2-19: Modo de perímetro

Este protocolo apresenta uma boa latência, mas, em contrapartida, não consegue distribuir uniformemente a carga de tráfego pela rede.

2.5.3.4 Protocolo GAF

GAF significa *"Geographic adaptive fidelity"* [26]. Consiste num esquema de poupança de energia, baseado no conhecimento da localização dos nós. O protocolo GAF conserva energia ao desligar os sensores que não estejam a ser necessários, sem com isso prejudicar a qualidade do encaminhamento.

Neste protocolo, cada nó utiliza informação da localização baseada em GPS para se associar a uma grelha virtual, de modo a que toda a área da rede se encontre dividida em alguns quadrados, sendo atribuída a função de mestre da grelha ao nó que possua o nível de energia residual mais elevado. Os outros nós dentro de cada grelha, denominados de nós escravos, podem ser considerados de redundantes no que diz respeito ao encaminhamento de pacotes e, como tal, podem ser adormecidos sem por em causa a eficácia do encaminhamento. Os nós escravos alternam entre os estados de adormecido e à escuta, com a garantia que um nó mestre em cada grelha permanece acordado para encaminhar os pacotes. Por exemplo, na figura 2-20, os nós 2,3 e 4 na grelha virtual B são equivalentes, no sentido que um deles pode encaminhar pacotes entre os nós 1 e 5 enquanto que os outros dois podem dormir para conservar energia.

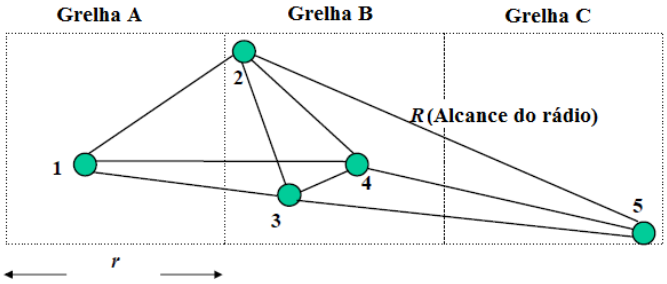


Figura 2-20: Grelha virtual no protocolo GAF

O tamanho da grelha *r* pode ser obtido através da relação entre *r* e o alcance do rádio *R*:

$$r^2 + (2r)^2 \leq R^2$$

A eleição dos mestres no GAF procede do modo que se segue. Os nós encontram-se num de três estados, como mostrado na figura 2-21: Adormecido, Activo ou em Descoberta. Inicialmente, um nó encontra-se no estado de Descoberta e troca mensagens de descoberta, que incluem o ID da grelha, para descobrir outros nós dentro da mesma grelha. Um nó torna-se mestre da grelha quando não ouve nenhuma mensagem de Descoberta durante um tempo T_d. Caso mais do que um nó se encontre no estado de Descoberta, torna-se mestre o nó que possuir uma longevidade prevista superior, do ponto de vista energético. O nó mester permanece activo durante um tempo T_a. Após este tempo, o nó altera o seu estado para Descoberta para dar a oportunidade a outro nó de se tornar mestre da mesma grelha.

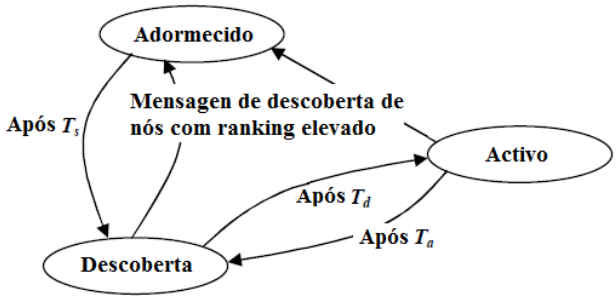


Figura 2-21: Diagrama de estados no protocolo GAF

2.5.3.5 Protocolo SHARP

O protocolo *"Sharp Hybrid Adaptive Routing Protocol"*, SHARP [33], representa um equilíbrio entre protocolos reactivos e proactivos, obtido com um ajuste do grau com que as informações de encaminhamento são propagadas na rede.

Entende-se por encaminhamento reactivo, a estipulação de percursos quando os mesmos são necessários, de acordo com as características actuais do sistema. Contrariamente, o encaminhamento proactivo consiste na determinação, reserva e estabelecimento prévio dos caminhos a percorrer até um dado destino.

Este protocolo permite que diferentes nós numa rede de sensores persigam objectivos diferentes em termos de encaminhamento. Cada nó pode procurar obter garantias de performance diferentes de acordo com a funcionalidade e utilização do próprio nó. Por exemplo, um nó pode direccionar o SHARP de modo a ajustar a sua disseminação de caminhos para reduzir as variações de latência, enquanto que outro nó pode usar em simultâneo o SHARP para minimizar o *"overhead"*.

Sendo o SHARP um protocolo híbrido adaptativo, deverá apresentar as seguintes características:

- **Adaptabilidade** – aplicável a uma grande variedade de características da rede. O comportamento do sistema deve alterar-se automaticamente de modo a atingir os objectivos estipulados face às alterações nos padrões do tráfego, mobilidade dos nós e outras características da rede;
- **Flexibilidade –** permite que os sistemas optimizem métricas específicas de cada aplicação ao nível do encaminhamento;
- **Eficiência e praticabilidade** – o protocolo deve atingir uma performance superior à de esquemas não híbridos.

As características mencionadas acima são asseguradas pelas seguintes propriedades do protocolo SHARP:

- Mecanismos de baixo custo energético para determinar o tamanho das zonas e controlar o encaminhamento proactivo;
- Monitoriza os padrões do tráfego de pacotes e as características locais da rede, tais como a taxa de falhas nas ligações, sem ocorrer em *"overhead"* excessivo;
- Determina o tamanho das zonas pelo isolamento de cada nó, baseando-se em informação local;
- O seu mecanismo de controlo permite aumentar ou diminuir as regiões de encaminhamento proactivo sem *"overhead"* de sincronização;
- Tira partido da sobreposição de zonas adjacentes para disseminar informação relativa ao encaminhamento proactivo de um modo mais eficaz;
- Não necessita de mecanismos de transmissão fiáveis e caros.

O SHARP alterna entre encaminhamento reactivo (específico de cada nó) e proactivo variando dinamicamente a quantidade de informação de encaminhamento partilhada proactivamente. Fá-lo através da definição de uma zona proactiva em redor de alguns nós, sendo que a dimensão desta zona é específica de cada nó e determina o número de nós nela contidos. Cada nó que se encontre a uma distância inferior ao raio da zona é um membro da zona proactiva desse nó. Todos os nós fora da zona proactiva de um dado destino usam encaminhamento reactivo para estabelecer percursos para esse nó. Os nós dentro de uma determinada zona proactiva mantêm percursos proactivos apenas em direcção ao nó central.

Ao aumentar o raio de uma determinada zona, o SHARP consegue diminuir a taxa de perda de pacotes e as variações na latência, mas terá um custo maior em termos de *"overhead"* para manter os caminhos numa zona de grandes dimensões.

Ao diminuir o raio, o SHARP reduz o *"overhead"*, uma vez que menos nós terão que ser actualizados proactivamente. No entanto, poderá causar valores mais elevados de perda de pacotes e variações de latência.

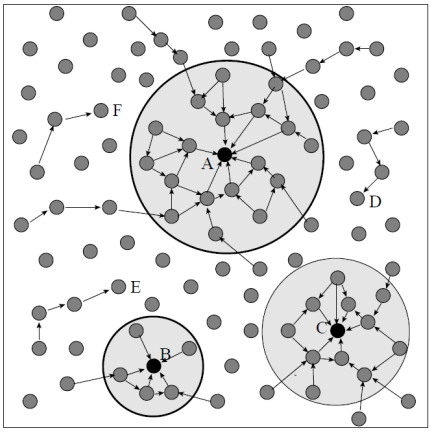


Figura 2-22: Zonas proactivas no protocolo SHARP

Na figura 2-22 é possível observar a existência de zonas proactivas em redor dos nós A, B e C, sendo o raio de cada zona dependente do nó central respectivo. O SHARP mantém zonas de encaminhamento proactivo em redor de destinos populares (A, B e C). Isto é alcançado através da adaptação dinâmica do raio da zona em cada destino com base na afluência de tráfego e mobilidade na rede. Consequentemente, cria zonas relativamente grandes em redor de destinos populares e zonas mais pequenas em redor que atraem menos tráfego. Por exemplo, nós que atraiam pouco ou nenhum tráfego, como os nós D, E e F, não terão sequer zona proactiva em redor e poderão apenas contar com encaminhamento reactivo.

Nesta secção foram abordados alguns protocolos de acesso ao meio e de encaminhamento que prevêem as necessidades energéticas e computacionais particulares das redes de sensores wireless. Facilmente se conclui que a escolha destes protocolos depende bastante do propósito de cada rede, do ambiente em que se insere, da sua necessidade de fiabilidade nos dados ou da rapidez com que obtêm os mesmos.

Na secção seguinte, é abordada a problemática da segurança nas redes de sensores wireless.

2.6 Objectivos de Segurança

As redes de sensores, possuindo capacidades de processamento, armazenamento, largura de banda e energia limitadas, necessitam de uma abordagem diferente em termos de segurança. As limitações de hardware e energia dos sensores criam dificuldades no que diz respeito à disponibilidade, confidencialidade, integridade e identificação [18].

De seguida, é explicado como estas características se enquadram numa rede de sensores segura.

2.6.1 Disponibilidade

A disponibilidade determina se um sensor tem a capacidade de aceder à rede e se as mensagens são comunicadas convenientemente pela mesma. Como qualquer medida de segurança complexa aumenta o consumo de energia dos nós de uma rede, a manutenção da disponibilidade dos sensores apesar dos seus recursos limitados é um desafio. Contudo, a falha de alguns dos nós principais pode ameaçar a rede na sua totalidade. Daí que a disponibilidade seja um factor importantíssimo de modo a manter a operacionalidade de uma rede de sensores.

2.6.2 Confidencialidade

A confidencialidade resulta da capacidade de uma rede esconder os seus dados de um atacante, de modo a que todas as mensagens transmitidas permaneçam confidenciais. Isto será talvez o aspecto mais importante no que diz respeito à segurança numa rede de sensores. Um nó não deve revelar o conteúdo das suas mensagens aos seus vizinhos [14], ou seja, a informação deve circular encriptada. Por exemplo, em aplicações militares onde um adversário introduziu nós maliciosos na rede, a confidencialidade da rede impedirá os nós introduzidos de ganharem acesso à informação dos outros nós. Estabelecer e manter a confidencialidade do sistema é de extrema importância quando os nós são identificados e as suas chaves de segurança são distribuídas, para estabelecer um canal de comunicação seguro entre os sensores.

2.6.3 Integridade

A integridade dos dados em redes de sensores wireless é necessária para garantir a fiabilidade dos dados transmitidos e refere-se à capacidade de confirmar que a mensagem não foi alterada indevidamente durante o seu percurso pela rede. Mesmo estando algumas medidas de confidencialidade implementadas, continuará a existir a possibilidade de os dados transmitidos se alterarem durante o percurso. Problemas de integridade de dados poderão dever-se a um nó malicioso presente na rede e a injectar dados falsos ou também a condições de transmissão wireless não ideais que podem comprometer ou causar a perda de dados.

2.6.4 Autenticação

A autenticação assegura a fiabilidade da mensagem, através da identificação da sua origem. Os ataques contra redes de sensores não envolvem apenas a alteração dos pacotes. Os atacantes podem também injectar pacotes próprios. Daí que aquando da recepção de uma mensagem, um nó necessita de confirmar que o pacote recebido provém de facto do nó que alega tê-lo enviado. Ou seja, a autenticação verifica a identidade dos nós emissores. A autenticação é conseguida através do envio e recepção de chaves secretas para em conjunto com um código *"Message Authentication Code"*, garantirem a autenticidade das mensagens.

2.7 Ataques

A circulação de informação potencialmente valiosa numa rede de comunicação vai atrair a atenção de entidades com meios e conhecimento para capturar esta informação. A única possibilidade de contrariar este facto, é analisar as fragilidades da rede, estudar os ataques que elas possibi-

litam e, com base nisto, criar medidas que contrariem estas mesmas fragilidades e tornem a rede segura.

Devido às características únicas das redes de sensores, tais como as limitações de memória e de bateria dos nós, a necessidade de segurança nem sempre prevalece sobre a da longevidade e de largura de banda da rede. Como tal, as redes de sensores são muitas vezes desenhadas sem a segurança em mente, possibilitando uma grande variedade de ataques.

Serão explicados de seguida os problemas e ataques e mais frequentes a redes de sensores wireless de acordo com Undercoffer et al. [31]. É feita uma breve descrição dos diferentes tipos de ataques passíveis de serem executados sobre uma rede de sensores, sendo dada especial atenção aos ataques de encaminhamento posteriormente no capítulo 4.

2.7.1 Captura de Nós

As redes de sensores são frequentemente implantadas em ambientes onde a natureza remota da sua localização ou mesmo a praticabilidade de acesso impedem a vigilância dos elementos da rede. Nestas situações, torna-se possível remover fisicamente um nó da rede. A captura de um nó pode revelar a informação contida no próprio, incluindo as chaves de encriptação. Isto, naturalmente, pode comprometer a segurança da totalidade da rede de sensores [29].

2.7.2 Recolha Passiva de Informação

Um atacante que disponha de meios adequados pode recolher informação que circule na rede, desde que a mesma não esteja protegida. Se a comunicação entre sensores, ou entre sensores e a estação base, for feita sem nenhum tipo de codificação, então um atacante com um receptor apropriado consegue apanhar facilmente o fluxo de dados. A intercepção de mensagens que contenham a localização física dos sensores permite a um atacante localizar os nós e destrui-los. Para contrariar esta ameaça, é necessário a utilização de mecanismos de encriptação, que tornem a informação ilegível a intrusos [30].

2.7.3 Nós Falsos

Um ataque de nó falso consiste na introdução de um nó por parte de um atacante com o objectivo de injectar informação maliciosa na rede. Este nó terá que possuir suficiente capacidade de processamento para fazer com que os outros nós lhe enviem informação e para conseguir lidar com o volume de dados.

2.7.4 Análise de Tráfego

Um adversário que pretenda atacar a estação base, consegue deduzir a localização física desta através da observação do fluxo das mensagens pela rede. Contrariamente às redes tradicionais, as RSW possuem padrões de tráfego assimétricos únicos. Uma vez que o principal propósito de uma rede de sensores é a recolha de dados, os nós sensores enviam persistentemente dados à estação base. Estes padrões providenciam informação suficiente acerca da localização da estação base a um adversário, mesmo que as mensagens circulem encriptadas [15].

2.7.5 Nós Avariados

Um nó avariado poderá gerar dados errados, que poderão por em risco a integridade da rede de sensores. Em redes estruturadas hierarquicamente, em que os nós estejam agregados por clusters, a avaria de um nó pode assim uma elevada relevância. Caso um nó líder de cluster avarie, toda a informação proveniente dos nós hierarquicamente inferiores poderá ser danificada ou perdida.

2.7.6 Mensagens Corrompidas

Qualquer tipo de alteração do conteúdo de uma mensagem por parte de um atacante compromete a integridade da própria mensagem. Caso um atacante tenha conseguido adquirir acesso e conhecimento suficiente sobre a rede de modo a conseguir alterar o conteúdo das mensagens, então toda a rede se encontra comprometida.

2.7.7 Nós Parados

Quando um nó deixa de funcionar, caso se trate de um nó de agregação numa rede hierarquizada, poderá haver uma perda da totalidade da informação enviada pelos nós aí agregados. Os protocolos das redes de sensores deverão ser robustos o suficiente para realizar um encaminhamento alternativo.

2.7.8 Denial of Service

"Denial of service", DoF, significa negação de serviço. Trata-se de um tipo de ataque que ocorre a um nível físico da rede. Inclui interferências no sinal de rádio, interferindo com o protocolo da rede e levando à exaustão da bateria, entre outros. Podem ser divididos em [32]:

- ***"Tampering"***, ou seja, adulteração – trata-se do resultado da captura física do sensor. Para contrariar estes ataques, os sensores devem ser capazes de detectar a sua captura e

apagar qualquer dado criptográfico que possam conter na sua memória, e que ponha em perigo a confidencialidade da rede. Uma prevenção contra os ataques de *tampering* pode passar pela camuflagem ou ocultação dos sensores.

- ***"Jamming"***, ou seja, interferência – este ataque pode ser facilmente detectado, uma vez que os sensores atacados não serão capazes de comunicar. Uma maneira de contrariar a interferência consiste em comunicar numa gama de frequências, não se estando restrito a apenas um canal. No entanto, isto acarreta custos mais elevados, maior consumo energético e uma maior complexidade de design.

2.7.9 Ataques de Encaminhamento

Muitos dos protocolos de encaminhamento das redes de sensores wireless são bastante simples. Esta simplicidade é necessária pelas limitações do hardware utilizado, mas torna as redes susceptíveis a ataques.

Os ataques de encaminhamento consistem geralmente numa alteração, limitação ou cessação do encaminhamento na rede. Estes ataques implicam tipicamente a existência de nós comprometidos, ou seja, nós sob o controlo de atacantes.

Um exemplo deste tipo de ataques é o encaminhamento selectivo, segundo o qual um ou vários nós comprometidos se recusam a encaminhar o tráfego que passa por eles para o resto da rede. É também de referir o ataque *"Sybil"*, consistindo este numa imitação de vários nós por parte de um só nó malicioso que apresenta identidades múltiplas e o ataque de *"Hello"*. Este último representa uma tentativa de um nó com elevadas capacidades de transmissão se fazer passar por vizinho de todos os nós da rede, através do envio de pacotes de *"Hello"* e fazendo com que estes façam o tráfego da rede passar por ele [34].

Esta foi apenas uma introdução aos ataques de encaminhamento nas redes de sensores wireless, pelo que uma análise mais pormenorizada de estes e de outros ataques será feita no capítulo 4, juntamente com uma descrição detalhada de vários protocolos de encaminhamento que os contrariam.

2.8 Conclusão do Capítulo

Este capítulo apresentou em detalhe as redes de sensores wireless, mencionando as possíveis aplicações desta tecnologia, assim como o hardware envolvido e as suas limitações. Foram também abordados os protocolos de encaminhamento mais frequentes, sendo estes maioritariamente

orientados para a eficácia energética. No entanto, estes protocolos não estão vocacionados para a problemática da segurança, pelo que estão sujeitos a diferentes tipos de ameaças e problemas.

Na ausência de medidas de segurança adequadas, uma rede de sensores permanece vulnerável a uma variedade de ataques. Como tal, os capítulos seguintes abordam algumas soluções de protecção, nomeadamente protocolos de encaminhamento seguro e esquemas de chaves de segurança, que procuram garantir os princípios da disponibilidade, confidencialidade, integridade e identificação referidos no ponto 2.6, tendo sempre em mente as limitações de memória e de processamento dos sensores.

Capítulo 3

3. Chaves de Segurança

Como foi mencionado no Capítulo 2, para que se possa considerar que uma rede de sensores wireless é segura, a rede terá que possuir quatro características: disponibilidade, confidencialidade, integridade e identificação [18]. Para tal, é essencial a existência de um sistema de encriptação e autenticação que mantenha a comunicação acessível apenas aos elementos que constituem a rede de sensores. Isto é possível através de chaves de segurança que, em conjunto com algoritmos de encriptação, tornam os dados transmitidos ilegíveis para terceiros. Os esquemas de gestão de chaves em conjunto com algoritmos de encaminhamento apropriados, sendo alguns destes analisados no Capítulo 4, permitem encriptar mensagens e enviá-las apenas aos nós identificados como funcionais e pertencentes à rede, fornecendo assim um nível de segurança bastante elevado e impermeável aos ataques mais comuns. Como tal, neste capítulo serão abordados alguns esquemas de gestão de chaves de segurança

Devido às limitações dos sensores em termos de capacidade de processamento e memória, é difícil conseguir um esquema de gestão de chaves eficaz, pelo que este é um processo de difícil desenho e implementação.

Segundo Hu et al., a gestão de chaves pode ser dividida em [37]:

- Pré-distribuição de chaves – carregar chaves de segurança na memória de cada sensor antes de os distribuir no terreno;
- Descoberta de vizinhos – análise da vizinhança por parte de cada nó para descobrir os nós vizinhos;
- Estabelecimento de chaves de "ponta a ponta" – estabelecer uma chave por parte de cada nó para comunicar com os sensores com os quais não está ligado directamente;

- Isolar nós erráticos – identificar e isolar nós que se encontrem danificados ou com comportamento errático;
- Latência do estabelecimento de chaves – reduzir a latência resultante da comunicação, assim como reduzir o consumo energético.

3.1 Esquemas de Gestão de Chaves

De acordo com Hu et al., a gestão de chaves têm o propósito de [37]:

- Inicializar os utilizadores de um sistema dentro de um domínio [38];
- Gerar, distribuir e instalar chaves;
- Controlar a utilização;
- Actualizar, revogar e destruir chaves;
- Armazenar, gravar/recuperar e arquivar chaves.

Nesta secção serão descritos alguns dos métodos de gestão de chaves actualmente utilizados, nomeadamente:

- *"Basic Key Management"* [39];
- *"Random Key Predistribution"* [41];
- *"Random Key Assignment"* [42];
- *"Pairwise Keys"* [74];
- *"Pairwise Key Pre-distribution"* [76];
- *"Deployment Knowledge"* [79];
- *"Group Key Management"* [80];
- *"Location-Based Keys"*;
- *"Secure Triple Key Scheme"*.

3.1.1 Basic Key Management

"Basic Key Management", BKM, significa gestão básica de chaves. Este esquema, proposto por Eschenauer e Gligor, pretende abordar a distribuição de chaves, revogação, redistribuição de chaves e resistência aos problemas de captura de nós [39].

Neste esquema, a distribuição de chaves é feita em três fases, nomeadamente, pré-distribuição, descoberta de chaves partilhadas e estabelecimento de chaves de percurso, sendo estas últimas

usadas para estabelecer uma ligação segura entre dois nós com nós intermédios. Esta distribuição envolve cinco passos anteriores à implantação da rede no terreno:

- Gerar um grande conjunto de *P* chaves de segurança, denominado de *Key Pool* (de 2^{17} a 2^{20} chaves);
- Recolher aleatoriamente uma quantidade *K,* de chaves da *Pool* para estabelecer um chamado "anel de chaves" para cada nó;
- Carregar o anel de chaves de cada nó para a sua própria memória;
- Guardar os identificadores das chaves e dos respectivos sensores num nó de controlo seguro;
- Para cada nó, carregar o identificador do nó de controlo e a chave partilhada entre ele e o nó.

A fase de pré-distribuição assegura que apenas um número reduzido de chaves necessita de ser colocado no anel de chaves de cada sensor, ao mesmo tempo que assegura que qualquer par de nós partilha pelo menos uma chave, com um grau configurável de probabilidade. Como tal, a quantidade de chaves, *K,* não corresponderá necessariamente ao número de nós activos da rede de sensores.

Na fase da descoberta das chaves partilhadas entre os nós, cada nó descobre todos os nós vizinhos, dentro do seu alcance, com os quais partilha uma chave. Cada nó difunde, em texto não encriptado, a lista de identificadores das chaves no seu anel de chaves. A descoberta das chaves partilhadas toma lugar durante a fase de inicialização da rede e estabelece a topologia da rede de sensores, assim como define o seu encaminhamento. Uma ligação entre dois nós só acontece se estes partilharem uma chave. Nesta situação, toda a comunicação entre os dois nós é assegurada por uma ligação encriptada.

Durante a fase de estabelecimento de chaves de percurso, uma chave de percurso é atribuída a pares de nós seleccionados, que estejam ao alcance um do outro e que não partilhem uma chave, mas que estejam ligados por duas ou mais ligações após a fase da descoberta de chaves.

A revogação de chaves é utilizada para eliminar o anel de chaves de nós que deixem de ser considerados seguros. Para executar uma revogação, um nó controlador difunde uma mensagem de revogação contendo uma lista assinada de *K* identificadores de chaves do anel de chaves do nó a ser revogado. Para assinar esta lista de identificadores de chaves, o nó controlador gera uma chave de assinatura, *Ke*, e comunica-a individualmente a cada nó, encriptando-a com uma chave *Kci* (chave de segurança entre o nó de controlo e um dado nó *i*) para o efeito. Depois de obter a chave de assinatura, cada nó verifica a assinatura da lista de identificadores de chaves (*K*), localiza os identificadores em questão no seu anel de chaves e remove as chaves correspondentes. A partir do momento que são removidas dos anéis de chaves, algumas ligações entre nós podem desaparecer e

os nós afectados necessitam de ser reconfigurados, através de uma nova etapa de descoberta de chaves partilhadas e, possivelmente, também de estabelecimento de chaves de percurso.

A re-atribuição de chaves consiste numa auto-revogação de uma chave por parte de um nó, quando o seu período de vida expira. Assim que a chave tiver sido removida, os nós afectados reiniciam a etapa de descoberta de chaves partilhadas e de estabelecimento de chaves de percurso.

A resistência à captura de nós enfrenta duas ameaças. A primeira envolve a manipulação dos dados do sensor quando um adversário injecta dados falsos dentro da rede. Detectar este tipo de ataques requer uma análise "*offline"* dos dados por parte de nós de controlo. A segunda ameaça ocorre quando um sensor está fisicamente sobre controlo de um atacante. Daqui pode resultar a manipulação dos dados transmitidos pelo nó atacado e pelos outros nós da rede. Algumas contra-medidas para os ataques em que acontece captura de nós passam por preparar o nó capturado para apagar o seu anel de chaves caso seja "vandalizado", fazendo eventualmente com que o sensor deixe de funcionar [40].

3.1.2 Random Key Pre-distribution

"Random Key Pre-distribution", RKP, significa pré-distribuição aleatória de chaves. Trata-se de uma variante do *"Basic Key Pre-distribution"*, desenvolvida por Chan et al., e introduz três esquemas novos [41]:

- *"Q-composite Random Key Pre-distribution";*
- *"Multi-path Key Reinforcement";*
- *"Random-Pairwise Keys".*

O esquema q-composite é uma variante do *"Basic Key Pre-distribution"*, onde são necessárias q chaves em comum ($q>1$) em vez de apenas uma. No esquema *"q-composite"*, o tamanho S da *"Key Pool"* é reduzido, uma vez que a utilização de múltiplas chaves irá criar combinações únicas para todos os pares de nós.

Para calcular a dimensão da *"Pool"*, considere-se $p(i)$ como sendo a probabilidade de qualquer par de nós ter em comum exactamente i chaves. Seja $P_{connect}$ a probabilidade de qualquer par de nós partilhar um número suficiente de chaves para criar uma ligação.

Se:

$$P_{connect} = 1 - (\text{probabilidade de 2 nós partilharem um numero insuficiente de chaves para formar uma ligação})$$

Então:

$$P_{connect} = 1 - (p(0) + p(1) + \ldots + p(q-1))$$

Para uma dada dimensão *m* do anel de chaves, um valor mínimo *q* de chaves em comum e uma probabilidade de conexão *p* mínima, a máxima dimensão *S* da *"Key Pool"* é escolhida de forma a obter $P_{connect} \geq p$.

Para inicializar o estabelecimento das chaves, um conjunto de *S* chaves aleatórias é seleccionado do conjunto total de chaves. Para cada nó, são seleccionadas *m* chaves aleatórias de *S*, em que *m* é o número de chaves que cada nó pode ter no seu anel de chaves. Estas *m* chaves são depois armazenadas no seu anel de chaves. Na fase de estabelecimento das chaves, cada nó descobre todas as chaves que tem em comum com cada uma dos seus vizinhos.

O esquema *"q-composite"* fortalece a robustez da rede contra a captura de nós, quando a o número de nós capturados é reduzido. No entanto, se um número elevado de nós for capturado, este esquema tende a revelar uma larga fracção da rede ao adversário [41].

No esquema *"Multi-path Key Reinforcement"* , ou seja, reforço de chaves multi-caminho, Chan et al. apresentam um método para fortalecer a segurança de uma ligação, estabelecendo-a através de múltiplos caminhos. Assumindo que o estabelecimento das chaves foi completado com sucesso, passam a existir múltiplas ligações seguras formadas a partir das chaves em comum existentes nos anéis de chaves dos vários nós, fazendo com que um atacante tenha que controlar um número mais elevado de nós para ter uma probabilidade elevada de capturar mensagens. A contrapartida é o aumento significativo do *"overhead"* dos pacotes.

Supondo que *A* possui uma ligação segura a *B* após o estabelecimento de chaves, esta ligação fica assegurada através de uma única chave *k* da *"Key Pool" S*. No entanto, *k* pode fazer parte do anel de chaves que se encontra na memória de outro nó qualquer da rede. Por isso, na eventualidade de algum desses outros nós ser capturado, a segurança da ligação entre *A* e *B* fica ameaçada. Quando isto acontece, a chave de comunicação é actualizada para um valor aleatório depois do estabelecimento das chaves. No entanto, a mensagem de actualização da chave não pode ser transmitida via a ligação directa entre *A* e *B*, uma vez que tendo controlo sobre esta ligação, um adversário poderia capturar a mensagem e desencriptar a actualização da chave e obter na mesma a nova chave de comunicação.

A abordagem *"Multi-path Key"* coordena as actualizações de chaves através de múltiplos caminhos independentes, partindo do pressuposto que pode ser trocada suficiente informação de encaminhamento de modo a que *A* conheça todos os caminhos distintos até *B* criados durante o estabelecimento de chaves inicial, e que têm um comprimento inferior ou igual a *h* saltos. Quantos mais caminhos existirem entre *A* e *B*, melhor será o nível de segurança conseguido com o *"Multi-path Key"*. No entanto, para qualquer percurso, a probabilidade de um atacante estar a escutar a comunicação aumenta com o tamanho do percurso, ou seja, com o número de saltos, uma vez que basta uma das ligações no percurso não estar segura para que todo o percurso esteja comprometido.

O terceiro mecanismo introduzido por Chan et al. é o *"Random Pairwise Keys"*, que significa chaves aleatórias par-a-par, através do qual é estabelecida uma autenticação nó-a-nó. Este esquema possui as seguintes características [41]:

- Resistência contra a captura de nós;
- Autenticação nó-a-nó;
- Revogação distribuída de nós;
- Resistência à replicação de nós;
- Possibilita o crescimento da rede.

Comparando estes três esquemas, nos dois anteriores, as chaves podiam ser retiradas múltiplas e vezes da *"Key Pool"* e a autenticação nó-a-nó não era possível. No *"Random Pairwise Keys"*, a distribuição de chaves aleatórias par-a-par atribui apenas uma chave única a cada par de nós.

Sendo, novamente, *m* o tamanho do anel de chaves de cada nó, e *p* a probabilidade de dois nós comunicarem com sucesso, o esquema *"Random Pairwise Keys"* procede da seguinte forma:

- Numa fase de inicialização, é gerado um total de $n = \frac{m}{p}$ identificadores únicos de nós. O tamanho *n* pode ser superior ao número de nós da rede, ficando os identificadores não usados disponíveis para nós que sejam adicionados posteriormente. Cada identidade gerada é depois emparelhada com *m* outras identidades, sendo gerada uma chave para cada par de nós. A chave é posteriormente guardada nos anéis de ambos os nós do par, juntamente com a identidade do outro nó, com o qual está emparelhado;
- Após a implantação da rede, cada nó difunde o seu ID aos seus vizinhos mais próximos, que por sua vez o pesquisam no seu anel de chaves para determinar se partilham uma chave de comunicação com o ID difundido, ou seja, determinam se podem ser emparelhados com algum dos seus vizinhos.

3.1.3 Random Key Assignment

"Random Key Assignment", RKA, significa atribuição aleatória de chaves. Este esquema proposto por Pietro et al., apresenta um modelo probabilístico composto por dois protocolos, sendo o primeiro denominado de protocolo Directo e o segundo de Cooperativo. O objectivo destes protocolos é estabelecer um canal de comunicação seguro entre quaisquer dois nós da rede de sensores [42].

Para que estes protocolos sejam eficientes em termos energéticos, consumam pouca memória e sejam resistentes à captura de nós, fazem parte dos mesmos:

- Um esquema de distribuição de chaves, que descreve como as chaves são carregadas nos sensores;

- Um procedimento de descoberta de chaves para calcular os conjuntos de chaves para um dado par de sensores;
- Um procedimento para o estabelecimento de um canal seguro, que permite que um par arbitrário de sensores determine uma chave comum aos dois, sendo esta usada para tornar o canal de comunicação seguro.

Para o protocolo Directo, o RKA utiliza o esquema *"Pseudo-Random Key Deployment"* [43], que significa distribuição pseudo-aleatória [44] de chaves. Este esquema apresenta uma maior eficiência no processo de descoberta de chaves do que um método aleatório. Utilizando uma estratégia de distribuição pseudo-aleatória, em que é utilizada uma semente [45] para gerar os valores aleatórios, é analisada a probabilidade de existir um canal entre dois sensores da rede. Caso este canal exista e os sensores pretendam comunicar de um modo seguro, é atribuída uma chave de sessão $K_{a,b}$ ao canal, tornando-o seguro.

Pietro et al. identificam algumas desvantagens no protocolo directo, afirmando que não é flexível o suficiente para se adaptar a circunstâncias que requeiram um nível de segurança mais elevado, e que para um anel de chaves de tamanho fixo, a probabilidade de ocorrer a corrupção de um canal pode não ser satisfatória, mesmo com um pequeno número de sensores corrompidos. Para contornar estes problemas, foi criado o protocolo Cooperativo, onde a fase de estabelecimento de chaves é cooperativa. A contra-partida é um aumento do *"overhead"*.

Se um sensor *A* quiser estabelecer um canal seguro com um sensor *B*, *A* escolhe um conjunto de sensores cooperativos $C = \{c1, c2..., c_n\}$ diferentes de *A* e *B*. Depois, *A* envia um pedido de cooperação a cada um dos sensores em *C*. O pedido contém o ID de *B*. Cada sensor *c* em *C* transforma a sua chave original do canal com *B*, K_{cB}, do seguinte modo: K_{cB} é gerada de acordo com o protocolo directo sendo posteriormente combinada com o ID de *A* e enviada para este. Quando *A* recebe todas as chaves combinadas, calcula K_{AB} e combina com as chaves recebidas, criando $K\underset{AB}{C}$. *A* tem depois que enviar a informação necessária a *B* para que o mesmo seja capaz de obter também $K\underset{AB}{C}$.

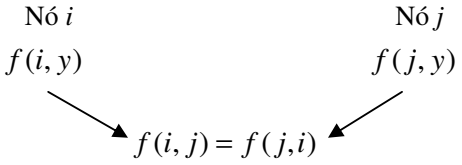
Este protocolo apresenta as seguintes características:

- Resistência à falha de sensores – se um sensor num grupo cooperativo de sensores não estiver disponível por qualquer motivo, o protocolo não irá falhar por *"deadlock"*;
- Inexistência de fuga de informação – no estabelecimento dos grupos cooperativos, a troca de chaves é feita através de uma transformada não invertível, pelo que não chega a ser transmitida nenhuma informação sensível;
- Adaptabilidade – o conjunto *C* pode ser escolhido de modo a assegurar todos os canais com a probabilidade desejada em conjunto com outros parâmetros da rede;
- Balanço de carga – a carga de trabalho gerada por este protocolo é distribuída praticamente de um modo igual por todos os sensores de *C*.

3.1.4 Pairwise Keys

Liu e Ning [74] propõem uma plataforma para estabelecer chaves de segurança entre pares de nós, baseando-se num protocolo polinomial de pré-distribuição de chaves, seguido por dois métodos alternativos: um esquema de pré-distribuição usando subconjuntos aleatórios de chaves e um esquema de pré-distribuição em grelha. Como complemento, apresentam uma técnica para reduzir o processamento ao nível do nó, de modo a que os seus esquemas possam ser implementados de um modo eficiente.

No esquema polinomial de distribuição de chaves [75], cada sensor *i* necessita de armazenar uma função polinomial *f(i,x)* de grau *t*, que ocupa *log (t+1)* no espaço de armazenamento *q* do nó. Para estabelecer uma chave num par de sensores, ambos os nós terão de considerar o polinómio como sendo o ID do outro nó. Para pré-distribuir chaves aos pares, o servidor de setup gera aleatoriamente um polinómio simétrico de grau *t* e de duas variáveis $f(x,y)=\sum_{i,j=0}^{t} a_{ij}x^i y^j$ sobre um campo finito F_q, onde *q* é um número primo suficientemente grande para acomodar a chave de encriptação, de modo a que se verifique que $f(x,y)=f(y,x)$. Para cada sensor *i*, o servidor de setup calcula a sua porção de $f(x,y)$, representada por $f(i,y)$. Para qualquer par de sensores *i* e *j*, o nó *i* consegue calcular a chave comum $f(i,j)$ ao avaliar $f(i,y)$ no ponto *j*, simultaneamente que o nó *j* consegue calcular a mesma chave $f(j,i)=f(i,j)$ ao avaliar $f(j,y)$ no ponto *i*, devido ao polinómio ser simétrico.



O estabelecimento de chaves par-a-par nesta plataforma é executado em três fases:

A fase de setup, que inicializa os sensores através da distribuição de conjuntos polinomiais;

A fase de estabelecimento de chave directa, que estabelece a chave directa para cada par de sensores;

A fase de estabelecimento de chaves de percurso, sempre que não se consegue obter uma chave directa comum entre dois nós.

A pré-distribuição usando subconjuntos aleatórios de chaves é uma extensão de um esquema probabilístico criado por Eschenauer e Gligor [39]. Em vez de seleccionar aleatoriamente chaves de uma grande *"key pool"* e de as atribuir aos sensores, este método escolhe aleatoriamente polinómios de uma *"pool"* e distribui as porções correspondentes a cada sensor. No esquema de Eschenauer e Gligor, a mesma chave é partilhada por múltiplos sensores, enquanto que neste esquema existe uma chave única para cada par de sensores.

A pré-distribuição em grelha é outro dos esquemas propostos por esta plataforma. Existem várias vantagens neste método. Em primeiro lugar, garante que quaisquer dois sensores conseguem estabelecer uma chave entre os mesmos, desde que não existam nós corrompidos e que os sensores consigam comunicar entre eles. Em segundo lugar, este esquema apresenta alguma resistência à captura de nós. Mesmo havendo alguns nós comprometidos, existe sempre uma alta probabilidade de se conseguir estabelecer uma chave entre quaisquer dois nós não comprometidos. Em terceiro lugar, um sensor pode directamente determinar se tem a possibilidade de estabelecer uma chave em conjunto com outro nó e, havendo essa possibilidade, saber que polinómio utilizar.

Supondo uma rede de sensores com um máximo de *N* nós, o esquema de pré-distribuição em grelha constrói uma grelha $m \times m$ com um conjunto de $2m$ polinómios $\{f_i^c(x,y), f_i^r(x,y)\}_{i=0,\ldots,m-1}$, com $m = [\sqrt{N}]$. Como pode ser observado na figura 3-1, cada linha *i* na grelha está associada a um polinómio $f_i^r(x,y)$ e cada coluna *i* está associada a um polinómio $f_i^c(x,y)$.

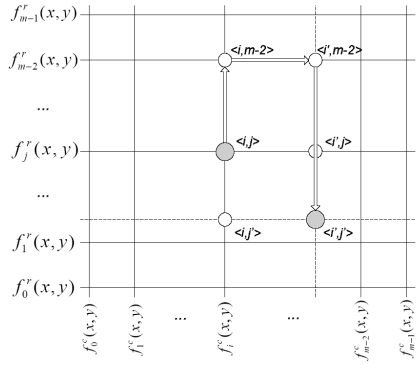


Figura 3-1: Pré-distribuição de chaves em grelha

O servidor de setup associa cada sensor na rede a uma única intersecção nesta grelha. Para um sensor nas coordenadas (*i*,*j*), o servidor atribui as porções polinomiais $f_i^c(x,y)$ e $f_j^r(x,y)$ ao mesmo. Como resultado, os sensores conseguem a executar a descoberta de chaves partilhadas e a descoberta de percursos com base nesta informação.

Para estabelecer uma chave partilhada com o nó *j*, o nó *i* verifica se os dois partilham uma linha ou uma coluna na grelha, ou seja, se $r_i = r_j$ ou $c_i = c_j$. Se de facto $c_i = c_j$, ambos os nós possuem porções polinomiais de $f_{ci}^c(x,y)$ e podem usar esquema polinomial de distribuição de chaves descrito anteriormente para estabelecerem uma chave de segurança directamente. Do mesmo modo, se $r_i = r_j$, ambos possuem porções polinomiais de $f_{ri}^r(x,y)$ e podem estabelecer uma chave convenientemente. Caso não se verifique nenhuma destas condições, os nós *i* e *j* terão que tentar estabelecer uma chave de percurso com a ajuda de nós intermédios.

3.1.5 Pairwise Key Pre-distribution

Du et al. [76] propõem um esquema de pré-distribuição baseado no método de Bloom [77] introduzido em 1985. Este método, apesar de não ter sido criado para redes de sensores, permite a qualquer par de nós numa rede encontrar uma chave secreta e, desde que não existam mais do que λ nós comprometidos, a probabilidade dos outros nós serem afectados é extremamente reduzida, pelo que a rede pode ser considerada como estando perfeitamente segura. Antes da entrada em funcionamento da rede, a estação base constrói uma matriz *G*, $(\lambda+1)\times N$, sobre um campo finito *GF(q)*, onde *N* é a dimensão da rede. A matriz *G* é considerada como informação pública, pelo que qualquer nó, e até mesmo adversários, consegue saber o seu conteúdo. Depois, a estação base cria uma matriz simétrica aleatória *D*, $(\lambda+1)\times(\lambda+1)$, sobre *GF(q)*, e calcula uma matriz $N\times(\lambda+1)$, $A=(D\cdot G)^T$. A matriz *D* deverá manter-se em segredo, sendo no entanto que uma coluna de $(D\cdot G)^T$ será carregada em cada nó. Devido a *D* ser simétrica, $A\cdot G$ também o será. Considerando $K=A\cdot G$, sabe-se que $K_{ij}=K_{ji}$, sendo este o valor da chave entre o nós *i* e *j*. A figura 3-2 ilustra a criação das chaves.

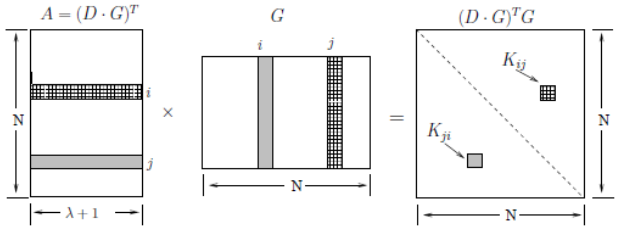


Figura 3-2: Criação de chaves no esquema de Bloom

O esquema de Du et al. é representado usando conceitos da teoria dos grafos [78], sendo dois nós unidos por uma aresta se e só se os mesmos conseguem estabelecer uma chave secreta comum. Poder-se-ia conseguir um grafo completo, ou seja, com todos os nós ligados por arestas, no entanto, apesar da conectividade total ser preferível, esta não é necessária. Para se conseguir o objectivo do estabelecimento de chaves, apenas é necessário um grafo ligado e não um grafo completo. Segundo Du et al., ao requerer que o grafo apenas esteja ligado, cada sensor necessitará de carregar menos informação.

Durante a fase de pré-distribuição, é atribuída informação sobre as chaves a cada nó, de modo a que, quando em funcionamento, os nós vizinhos consigam encontrar uma chave secreta em comum. Segundo este esquema, na fase de pré-distribuição é definido o espaço das chaves como um par ordenado (D,G), onde as matrizes D e G são definidas como descrito no esquema de Bloom. Dois nós conseguirão obter uma chave comum se os espaços de chaves que possuem se intersectarem.

Durante a fase de estabelecimento de chaves, após a entrada em funcionamento da rede, cada nó necessita de descobrir se partilha algum espaço com os seus vizinhos. Para realizar isto, cada nó transmite uma mensagem com o seu próprio ID, os índices do espaço que este carrega e a semente da coluna da matriz G que este carrega. De acordo com Du et al., comparativamente com outros esquemas como os propostos por Eschenauer e Gligor [39] e Chan et al. [41], um adversário necessitaria de corromper 5 vezes mais nós para conseguir obter os mesmos resultados, resultando daí um menor sucesso para um adversário num ataque em pequena escala.

3.1.6 Deployment Knowledge

Du et al. [79] desenvolveram uma extensão do BKM de Eschenauer e Gligor [39]. Este esquema consiste em saber de antemão a localização relativa dos nós, havendo uma maior probabilidade de se estabelecerem ligações entre vizinhos. Este conhecimento da posição relativa e ordem dos sensores é útil para a pré-distribuição de chaves. Quando os sensores vizinhos são conhecidos, a pré-distribuição de chaves torna-se trivial e simplesmente requer que para cada nó *n* seja gerada uma chave entre *n* e cada um dos seus nós vizinhos e que estas chaves sejam guardadas na memória do nó *n*. Isto garante que cada nó consegue estabelecer um canal seguro com cada um dos seus vizinhos após a inicialização.

3.1.7 Group Key Management

Neste esquema de Eltoweissy et al. [80], os nós da rede adquirem um identificador de grupo baseado na sua localização. Os nós dentro de cada cluster, no sistema pré-estabelecido de coordenadas, organizam-se exactamente em *l* sub-clusters. Este valor *l* é um parâmetro global da rede. A formação de sub-clusters é conseguida fazendo com que cada nó escolha, de um modo autónomo e aleatório, um número de sub-cluster local, sendo este número um inteiro entre $[0, l-1]$. Na prática, cada nó vai-se colocar num dos sub-clusters localizados dentro do cluster do próprio nó. Cada nó irá calcular então um identificador único para o sub-cluster ao qual se juntou em função do identificador do seu cluster e do número de sub-cluster ao qual aderiu. Este identificador global do sub-cluster actua como um identificador global do grupo para o nó. Os nós dentro do mesmo sub-cluster são apelidados de clones, uma vez que possuem identificadores de grupo idênticos e contêm as mesmas chaves em qualquer altura.

No *"Group Key Management"* , qualquer subconjunto de clones na rede pode ser organizado segundo grupos de comunicação segura, como ilustrado na figura 3-3.

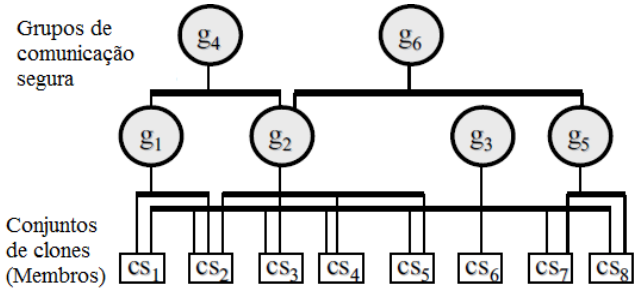


Figura 3-3: Modelo de organização segundo grupos de segurança

A inicialização das chaves de grupo é feita sem comunicações, uma vez que os nós calculam autonomamente o seu identificador de grupo com base na sua localização. O funcionamento deste esquema é depois assegurado por um servidor de chaves em que são implementadas algumas funções:

- Inicialização de chaves de sessão – para um dado grupo de comunicação *j*, esta função distribui por cada membro de *j*, de um modo seguro, as chaves iniciais de sessão para *j*;
- Revogação e redistribuição de chaves de sessão – esta função revoga a chave de sessão mais recente do grupo de comunicação *j* e distribui de um modo seguro uma nova chave de sessão a cada membro de *j*. A função apenas envia uma única mensagem, a qual contém a nova chave de sessão encriptada pela chave de sessão em vigor. Cada nó deverá considerar que uma chave foi revogada assim que receber uma chave de substituição;
- Exclusão de membros do grupo de segurança e da rede – para um dado membro *b*, a ser excluído, pertencente ao grupo *j*, esta função re-atribui chaves ao sistema de modo a que *b* deixe de ser capaz de enviar ou receber comunicações seguras dentro do grupo *j*. Cada nó possui um conjunto de chaves administrativas usadas somente para operações de redistribuição de chaves. Para que *b* não consiga obter as novas chaves, as mensagens de redistribuição são encriptadas com a chave de sessão mais recente e também com uma chave administrativa que *b* não contenha.

3.1.8 Location-based Keys

Zhang et al. [81] propõem a utilização de chaves baseadas na localização geográfica de cada nó. Este esquema é baseado na ideia de Corke et al. [82] de distribuir os nós no terreno usando robôs móveis e, consequentemente, conhecer antecipadamente a localização de cada nó. Estes robôs móveis deverão possuir funcionalidades de GPS e deverão são mais potentes em termos de comunicação e de capacidade de processamento do que os nós regulares.

Cada nó obtém a sua localização geográfica única do robô móvel e este propõe uma chave com base na localização. Para adicionar a chave, os robôs são carregados com os parâmetros do sistema

e com a chave primária do sistema *k*, de modo a que as outras chaves possam ser geradas para cada nó individual.

Zhang et al. também propõe um esquema de autenticação nó-a-nó baseado na localização, usando as *"Location-based Keys"*, segundo o qual, após a distribuição dos sensores, cada nó terá que descobrir os seus vizinhos e efectuar uma autenticação mútua com os mesmos.

A figura 3-4 mostra um exemplo de autenticação entre nós vizinhos, onde o nó *B* se encontra nas imediações dos nós *A* e *C*, ao passo que *A* e *C* não são vizinhos um do outro.

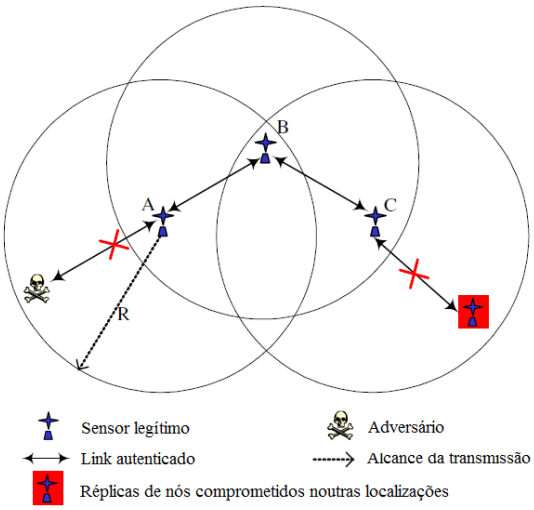


Figura 3-4: Autenticação mútua entre nós vizinhos

Para alcançar a autenticação, um nó *A* transmite localmente um pedido de autenticação que inclui a sua localização $posA =< x_A, y_A >$ e um número aleatório n_A. Após a recepção do pedido do nó *A*, o nó *B*, com localização $posB =< x_B, y_B >$, necessitará de confirmar que a localização *posA* está dentro do seu alcance de transmissão através de:

$$(xA - xB)^2 + (yA - yB)^2 \leq R^2$$

Esta verificação é necessária uma vez que, caso não fosse feita, um adversário poderia enviar a B um pedido de autenticação incluindo a localização de um nó *D*, por exemplo, que está fora do alcance de transmissão de *B*, através de um reforço da sua potência de transmissão. Neste caso, *B* poderia ser convencido de que *D* estaria de facto nas suas imediações.

Se esta verificação falhar, o nó B pura e simplesmente descarta o pedido, uma vez que o nó A não é seu vizinho. Caso contrário, o nó *B* envia uma resposta contendo a sua própria localização $posB =< x_B, y_B >$, um número aleatório n_B e um autenticador V_B, calculado através de $V_B = H_2(\hat{e}(LK_B, H_1(pos_A)) \| n_A \| n_B \| 0)$, em que $H_1, H_2, \hat{e}$ são alguns parâmetros públicos da rede e LK_B é a chave de localização de *B*.

Uma vez recebida a resposta de *B*, o nó *A* verifica se *B* está dentro do seu alcance. Caso se verifique, responde com um verificador $V_B^{'}$, calculado através de

$V_B^{'} = H_2(\hat{e}(H_1(pos_A), LK_A) \| n_A \| n_B \| 0)$. Após confirmar que $V_B^{'}$ e V_B coincidem, o nó *A* deve enviar o seu próprio autenticador V_A, calculado através de $V_A = H_2(\hat{e}(H_1(pos_B), LK_A) \| n_A \| n_B \| 1)$.

Zhang et al. também propõem o estabelecimento de chaves comuns a pares de nós, uma vez que são essenciais para garantir a segurança ao nível das ligações, ou seja, através da autenticação, protecção da integridade e encriptação das mensagens trocadas entre nós vizinhos.

Após o processo de autenticação, os nós *A* e *B* estabelecem implicitamente uma chave secreta partilhada entre os dois:

$$PK_{AB} = \hat{e}(H_1(pos_B), H_1(pos_A))^k$$, onde *k* é a chave primária da rede.

Um atacante pode escutar as mensagens de autenticação trocadas entre *A* e *B*, mas não consegue calcular PK_{AB} por não conhecer as *LKs* de *A* e *B*. Como tal, PK_{AB} é apenas conhecido para *A* e *B* e é definida como sendo a chave secreta do par daí em diante.

Uma vez que as chaves par-a-par são resultantes do processo mútuo de autenticação, não implicam comunicação extra para que sejam estabelecidas.

3.1.9 Secure Triple Key Scheme

Este esquema, proposto por Zia e Zomaya [83], prevêm uma organização hierárquica da rede em clusters que consiste na utilização de 3 chaves. Duas destas chaves são pré-colocadas em todos os nós, enquanto que a terceira é gerada já durante o funcionamento. Esta última é usada em questões relacionadas com a natureza hierárquica da rede de sensores.

É gerada uma chave de rede K_n na estação base. Esta chave é pré-distribuída por todos os nós e partilhada por toda a rede, sendo usada pelos nós para encriptar os dados antes dos passarem aos sensores vizinhos.

Outra chave gerada pela estação base é chave de sensor K_s. Também esta é pré-distribuída por todos os sensores e partilhada por toda a rede. A estação base usa esta chave para desencriptar e processar os dados e o nó líder de cluster usa esta chave para desencriptar e verificar os dados para os enviar à estação base após a reencriptação.

A chave de cluster K_c é gerada pelo líder de cluster e é partilhada pelos nós desse mesmo cluster. Esta chave apenas será usada pelos nós quando os mesmos forem líderes de cluster, caso contrário, não necessitam de desencriptar mensagens recebidas de outros nós, não desperdiçando assim capacidade de processamento e energia.

Este esquema de três chaves serve o propósito da confidencialidade e da autenticação.

a) Transmissão Estação Base – Nó

A estação base usa a chave de rede K_n para encriptar e transmitir uma mensagem. Quando um sensor recebe essa mensagem, utiliza a sua chave de sensor K_s para a desencriptar. A estação base encripta o seu próprio ID, uma marca temporal TS (*"Time Stamp"*) e a chave da rede K_n . É enviado também um campo MAC (*"Message Authentication Code"*) relativo à mensagem. O pacote transmitido contém os seguintes campos:

ID_{EB}	K_n	TS	MAC	Mensagem

Caso o pacote passe por um líder de cluster antes de chegar aos nós terminais, o ID da estação base é substituído pelo ID do líder de cluster.

b) Transmissão Nós – Líder de Cluster

Quando um nó envia uma mensagem para o seu líder de cluster, constrói um pacote da seguinte forma:

ID_{sn}	K_n	TS	MAC	Mensagem

O campo ID_{sn} é o ID do nó que envia a mensagem. Após a recepção da mensagem, o líder de cluster verifica a autenticidade e integridade do pacote através do campo MAC. Caso não se verifique, o pacote é descartado. O líder de cluster por sua vez, constrói a mensagem usando os mesmo campos, mas adicionando o seu próprio ID e K_n :

ID_{cln}	K_n	ID_{sn}	K_n	TS	MAC	Mensagem

c) Transmissão Líder de Cluster – Estação Base

A estação base recebe um pacote dos líderes de cluster ligados a ela directamente, verifica o ID do emissor e verifica a autenticidade e integridade do pacote através do MAC. Caso o pacote passe por mais do que um líder de cluster, vão sendo adicionados os respectivos IDs, como exemplificado a seguir:

ID_{cl1}	ID_{cl2}	K_n	ID_{sn}	K_n	TS	MAC	Mensagem

A figura 3-5 ilustra a circulação de mensagens na rede pelo método das *"Secure Triple Keys"*.

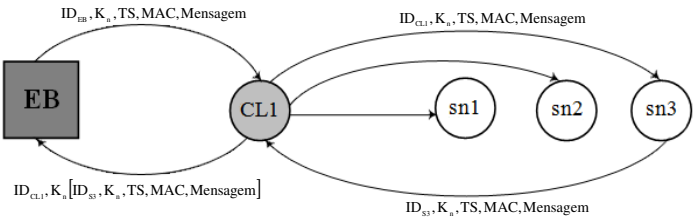


Figura 3-5: Transmissão com Secure Triple Keys

Os métodos de distribuição de chaves abordados neste capítulo, são agora apresentados em resumo na tabela Tabela 3-1: Resumo dos métodos abordados.

Tabela 3-1: Resumo dos métodos abordados

Abordagem	**Síntese**
"Basic Key Management"	Um esquema probabilístico de pré-distribuição, onde cada sensor recebe um conjunto aleatório de chaves de uma grande *Key Pool*. Para obterem uma chave para comunicação, dois nós têm descobrir uma chave comum dentro do seu conjunto de chaves.
"Random Key Predistribution"	Baseando-se no método anterior, acrescenta três esquemas de pré-distribuição: *"q-composite", "multi-path reinforcement" e "random pairwise schemes"*.
"Random Key Assignment"	Apresenta um modelo probabilístico e dois protocolos, Directo e Cooperativo, para estabelecer comunicação entre sensores, atribuindo para tal um pequeno conjunto de chaves aleatórias a cada sensor.
"Establishing Pairwise Keys"	Este esquema baseia-se numa *"Key Pool"* polinomial e numa pré-distribuição em grelha, altamente resistentes à captura de nós, apresentando no entanto baixo *"overhead"* na comunicação.

"Pairwise Key Pre-distribution"	Representa um esforço para melhorar a resistência da rede, fazendo com que um atacante tenha que capturar uma percentagem elevada da rede para a conseguir comprometer.
"Deployment Knowledge"	Este esquema, baseado no *"Random Key Predistribution"*, tira partido do conhecimento prévio da posição sequencial dos sensores. Devido à aleatoriedade da colocação dos nós, não é possível saber a localização exacta dos nós circundantes, mas consegue-se saber um conjunto de prováveis vizinhos.
"Group Key Management"	Baseando-se na posição relativa dos sensores, propõe uma auto-organização dos nós em grupos. Cada grupo deverá possuir um conjunto de chaves de segurança para comunicação, idêntico em todos os nós do mesmo, pelo que estes são apelidados de clones.
"Location-Based Keys"	Este esquema implica o conhecimento das coordenadas GPS de cada nó, obtidas na implantação da rede, sendo estas usadas para gerar as chaves de cada nó. A confidencialidade é assegurada pela autenticação entre os nós e pelas chaves par-a-par.
"Secure Triple Key Scheme"	Tem em vista redes organizadas hierarquicamente em clusters. A confidencialidade e a autenticação são asseguradas por um esquema de três chaves de segurança, sendo uma delas usada para a encriptação de todo o tráfego e as outras duas para desencriptar consoante o nível hierárquico de cada nó.

3.2 Conclusão do Capítulo

Neste capítulo foram examinados vários esquemas de gestão de chaves de segurança. Estes esquemas são capazes de fornecer chaves de encriptação que por sua vez permitem estabelecer ligações seguras nó a nó e nó a estação base, através da encriptação das mensagens, da autenticação e até mesmo do conhecimento e análise da posição dos nós. No entanto, são necessários algoritmos de encaminhamento seguro que façam bom proveito dos esquemas de chaves de segurança. Como tal, o capítulo que se segue apresenta alguns algoritmos de encaminhamento, sendo também explicados em detalhe alguns dos ataques de encaminhamento que as redes enfrentam.

Capítulo 4

4. Encaminhamento Seguro

Devido às limitações físicas dos sensores, analisadas no ponto 2.3, a maior parte dos protocolos de encaminhamento não têm em conta a segurança, mas sim o consumo de energia, procurando minimizar a comunicação e o processamento por parte dos elementos da rede. Como consequência, as redes de sensores wireless ficam vulneráveis a vários tipos de ataques, tornando esta tecnologia inviável para cenários onde a tolerância a falhas é reduzida. Para contrariar isto, é necessário implementar medidas impeçam a interferência de entidades exteriores à rede.

Nesta secção será feita uma análise em pormenor dos ataques de encaminhamento, alguns dos quais mencionados no capítulo 2. Esta análise é seguida pela descrição e comparação de alguns esquemas de encaminhamento seguro que contrariam os ataques referidos, não descurando as limitações de hardware inerentes às RSW. Por fim, é descrito em que medida os algoritmos de encaminhamento seguro servem de contra-medidas aos ataques mais frequentes.

4.1 Ataques de Encaminhamento

Nesta secção são descritos em detalhe os principais ataques de encaminhamento executados sobre as redes de sensores wireless.

4.1.1 Spoofing, Alteração da informação

Nas redes de sensores, o *"spoofing"* consiste em imitar ou replicar a informação de encaminhamento [34]. Tal é possível em redes *"had-oc"*, uma vez que todos os nós funcionam como um router. Este tipo de ameaça é utilizado para atacar a troca de informação entre os nós. Com isto

consegue-se gerar mensagens de erro falsas, encurtar e alongar percursos de encaminhamento, particionar a rede, entre outros. Os ciclos de encaminhamento podem também atrair ou repelir o tráfego da rede para ou de um determinado ponto da rede e podem aumentar a latência na comunicação nó a nó [49].

Este ataque também inclui os chamados *"Routing* Loops*"*, ou ciclos de encaminhamento. Estes consistem em encaminhar o tráfego em ciclo, fazendo com que o mesmo chegue à origem. Este processo pode ser visto na Figura 4-1, onde o nó A pensa que o nó B é o melhor caminho para determinado destino, enviando-lhe o pacote, Simultaneamente, o nó B considera que o melhor caminho é pelo nó C, que por sua vez considera que o melhor caminho é pelo nó A e envia-lhe o pacote, regressando assim à origem [50]. Esta "confusão" de localizações pode ser originada através do *"spoofing"* da informação de encaminhamento que os nós possuem, ou seja, um atacante envia informações erradas sobre a localização dos nós fazendo com que os pacotes fluam no sentido errado.

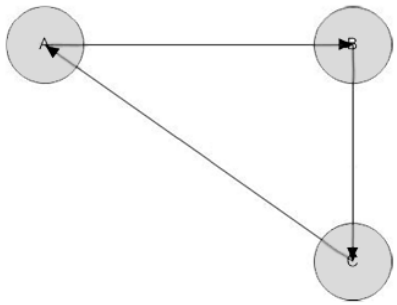


Figura 4-1: Routing Loop

4.1.2 Encaminhamento Selectivo

O encaminhamento selectivo, também conhecido por *"Selective Forwarding",* é uma forma de influenciar o tráfego na rede, de modo a que todos os nós aparentem estar a funcionar correctamente e que é seguro enviar-lhes mensagens. Nos ataques de encaminhamento selectivo, nós maliciosos podem recusar encaminhar determinadas mensagens e pura e simplesmente descartá-las. São difíceis de detectar pois podem ser confundidos com falhas normais do funcionamento da rede [51]. Quando um nó malicioso recebe mensagens, ele reduz a latência da sua ligação e faz com que os nós na sua vizinhança o vejam como parte de um caminho mais reduzido, ou seja, mais apetecível. Na Figura 4-2 é possível ver a estação base a enviar mensagens para D, onde um nó corrompido, B, faz o nó D crer que o caminho mais reduzido para a estação base é por B.

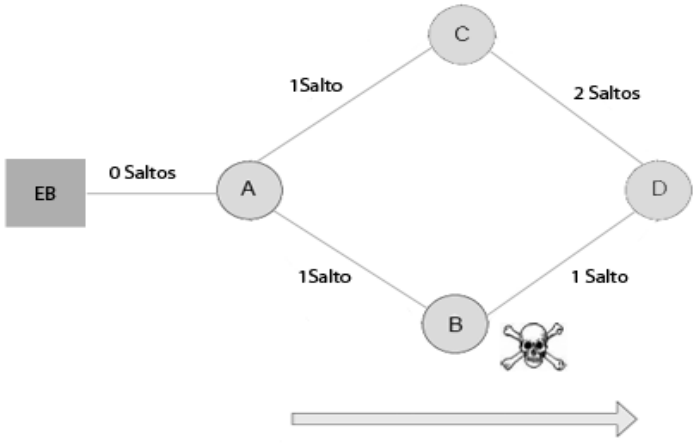


Figura 4-2: Encaminhamento até ao nó D

A eficácia do encaminhamento selectivo depende de dois factores [18] :

- Localização do nó malicioso, pois quanto mais perto se encontrar da estação base mais tráfego conseguirá atrair;
- Percentagem de mensagens que o nó malicioso descarta, uma vez que quantas mais mensagens o nó descartar, menos mensagens terá de encaminhar, poupando assim energia que será útil para enganar os nós vizinhos.

Uma forma simples deste ataque acontece quando um nó malicioso se comporta como um buraco negro, recusando encaminhar qualquer pacote que lhe chegue. No entanto, corre o risco de os nós vizinhos concluírem que o nó em questão falhou e procurarem caminhos alternativos. Uma forma mais subtil consiste em fazer o encaminhamento de apenas parte dos pacotes. Um adversário interessado em suprimir ou modificar pacotes originários de um determinado grupo de nós pode encaminhar o tráfego dos nós restantes da rede com fiabilidade, afastando assim suspeitas das suas reais intenções [34].

4.1.3 "Sinkholes"

Na Natureza, o termo *sinkhole* refere-se a uma depressão no solo, originada normalmente por motivos naturais [46]. Relativamente ao encaminhamento em redes de sensores wireless, trata-se de um tipo de ataques segundo o qual um atacante atrai o tráfego para um determinado nó da rede, que está sob seu controle, fazendo com que a estação base seja incapaz de obter dados da rede [52]. Este ataque tipicamente consiste em fazer com que o nó malicioso pareça especialmente atractivo aos nós em redor, no que diz respeito ao algoritmo de encaminhamento. Por exemplo, um

adversário pode falsamente publicitar a elevada qualidade do seu encaminhamento para a estação base. Alguns protocolos podem tentar verificar este encaminhamento da origem até ao destino, no entanto, se o nó malicioso se tratar de algo semelhante a um computador portátil, poderá facilmente fornecer a capacidade de transmitir a sua informação directamente para a estação base num único salto. Seja esta qualidade de encaminhamento falsa ou não, todos os vizinhos do nó malicioso irão encaminhar o tráfego por ele e propagar para os restantes nós a qualidade deste trajecto.

Um ataque deste tipo, pode ser visto na Figura 4-3, onde o nó 8 tenta induzir em erro os outros nós, de modo a que o considerem como o melhor caminho para a estação base, ou mesmo como sendo uma estação base.

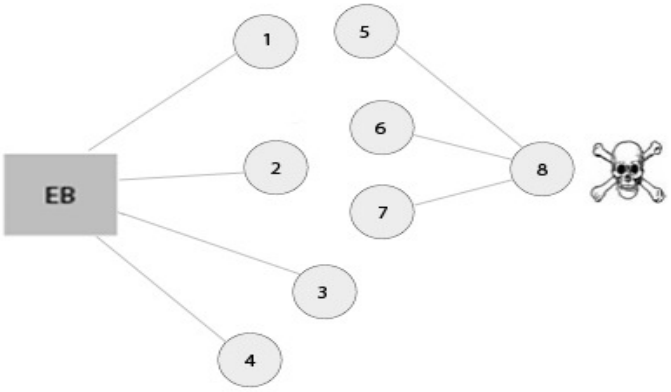


Figura 4-3: Nó 8 a durante um ataque de Sinkhole

Na Figura 4-4 é possível ver o resultado do ataque, onde todo o tráfego é encaminhado para o nó 8.

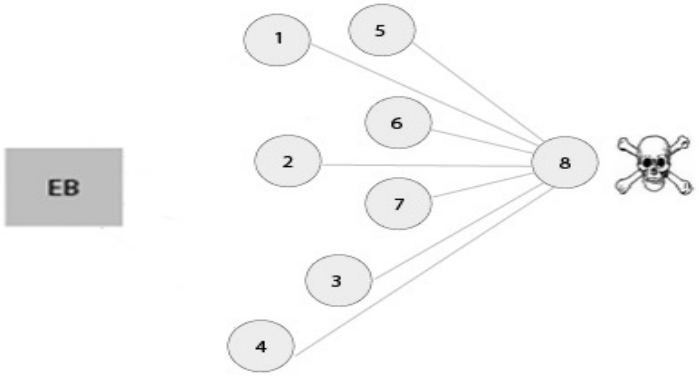


Figura 4-4: Rede após o ataque de Sinkhole

O método mais fácil de conseguir enganar os outros nós é colocar um nó malicioso na trajectória do fluxo de tráfego, ou seja na direcção de uma estação base e o mais perto possível desta, de modo a que o nó malicioso possa ser reconhecido ele próprio como uma estação base [52].

Uma das resultantes dos ataques *"Sinkhole"* é a possibilidade de fazer encaminhamento selectivo, de modo a atrair o tráfego em direcção a um nó comprometido. A natureza das redes de sensores wireless, onde o tráfego circula em direcção à estação base, possibilita o sucesso deste tipo de ataques [18].

4.1.4 Ataques "Sybil"

Num ataque "Sybil" [47], um nó malicioso cria múltiplas identidades falsas para si próprio dentro da rede de sensores, seja através do fabrico ou do roubo de identidades de nós legítimos. Os ataques "Sybil" podem ser usados contra os algoritmos de encaminhamento e reduzir a eficácia de esquemas tolerantes a falha, que utilizem redundância de encaminhamento [58] e armazenamento distribuído [59]. Estes esquemas assentam no pressuposto que os dados e o encaminhamento devem estar dispersos pela rede, distribuindo assim a carga uniformemente pelos nós. Como consequência, assegura-se um tempo de vida dos sensores uniforme, não se esgotando nenhum sensor em particular, e é criada redundância na rede. Esta redundância vai permitir que, em caso de ataque ou de falha de algum nó ou grupos de nós, o tráfego conseguirá circular por outros pontos [53]. No entanto, o que se pensa serem nós distintos, podem ser na verdade apenas um nó "Sybil" fazendo-se passar por um grupo de nós. Outra possível manifestação destes ataques acontece nos protocolos de encaminhamento baseados nas posições dos nós, onde pode acontecer de um nó aparecer simultaneamente em regiões diferentes [34], como está ilustrado na Figura 4-5.

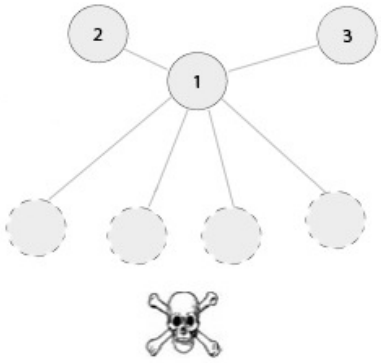


Figura 4-5: Ataque "Sybil"

4.1.5 "Wormholes"

O termo "*Wormhole*" significa buraco de verme, mas na verdade é um termo utilizado para descrever um atalho através do tempo e do espaço entre dois pontos [49]. Nas redes de sensores

wireless, corresponde a um ataque, segundo o qual um túnel é criado na rede por um atacante. O tráfego chega a esse túnel numa parte da rede e é propagado até outra parte. Normalmente, estes túneis apresentam um caminho com uma maior largura de banda e menor latência, sendo, do ponto de vista do algoritmo de encaminhamento, uma ligação de qualidade superior, e como tal, preferível para a circulação de tráfego [56].

O "*Wormhole*" é criado por dois nós maliciosos que se localizam nas extremidades do túnel, sendo que um dos nós se encontra normalmente perto da estação base, enquanto que o nó na outra extremidade atrai o tráfego para o "*Wormhole*", através da transmissão de pacotes com informação falsa de encaminhamento, tornando o túnel mais atraente, comparativamente a caminhos alternativos [56]. Este processo está ilustrado na Figura 4-6, onde é possível observar os dois nós maliciosos ligados entre si, sendo que grande parte do tráfego circula por esta ligação.

Este ataque vai originar, na verdade, um "*Sinkhole*", uma vez que o adversário fornece um caminho de alta qualidade para a estação base, atraindo todo o tráfego para si. Potencialmente, todo o tráfego das redondezas será atraído para ele, se as rotas alternativas forem substancialmente menos atractivas, podendo assim alterar completamente o encaminhamento da rede ao criar um "Wormhole" bem localizado [34].

Existe, no entanto, alguma resistência aos "*wormholes*" por parte de protocolos de encaminhamento baseados na localização geográfica dos sensores. Este tipo de protocolo constrói a topologia a partir de cada nó, sendo que estes enviam os dados na direcção da localização da estação base, procurando para tal os nós mais perto que se encontram nessa direcção. Este processo passa-se ao nível dos nós, não havendo qualquer interferência por parte da estação base. Como o tráfego é encaminhado numa direcção específica, torna-se complicado atraí-lo para qualquer outro lado [34].

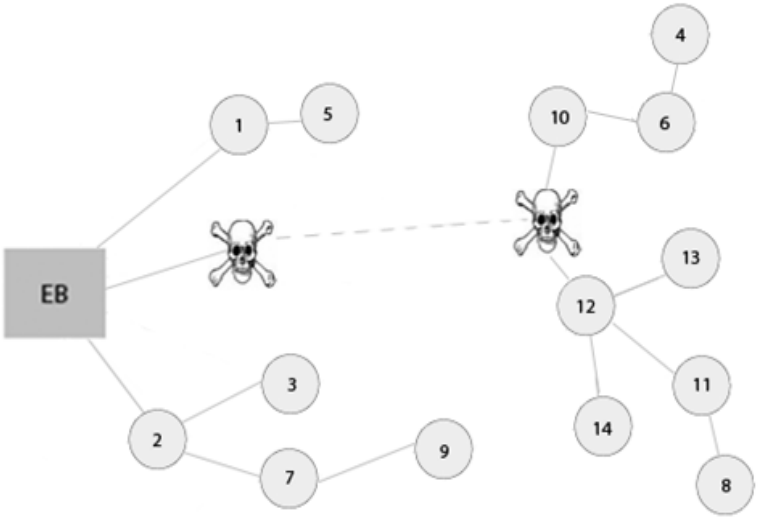


Figura 4-6: "Wormhole" para controlar o tráfego de dados

4.1.6 Inundação de "HELLO"

Muitos protocolos requerem que os nós difundam pacotes de HELLO para anunciarem a sua presença aos seus vizinhos. Um atacante pode difundir pacotes de HELLO, sendo que estes presumem que o sinal vem de um nó que se encontra dentro do alcance normal do sinal de um sensor. No entanto, isto pode não ser verdade, uma vez que um atacante com bastantes recursos em termos de hardware, possuindo por exemplo um computador portátil, poderá transmitir um sinal de tal forma forte, que todos os nós da rede pensem que é um dos seus vizinhos [34]. Por exemplo, um adversário publicitando um caminho de alta qualidade até à estação base para todos os nós na rede pode causar com que um elevado número de nós tente usar este caminho. No entanto, estes nós estarão suficientemente afastados do nó atacante para que os pacotes não cheguem a lado nenhum, estando apenas a desperdiçar energia, como ilustrado na Figura 4-7. A rede ficaria num estado de confusão. Um nó que se aperceba que a ligação ao adversário não é verdadeira, não possui muitas alternativas, uma vez que os seus vizinhos também estarão a tentar enviar os dados para o mesmo nó atacante. A estação base verdadeira também estará a enviar este tipo de pacotes, mas apenas receberá respostas de alguns nós.

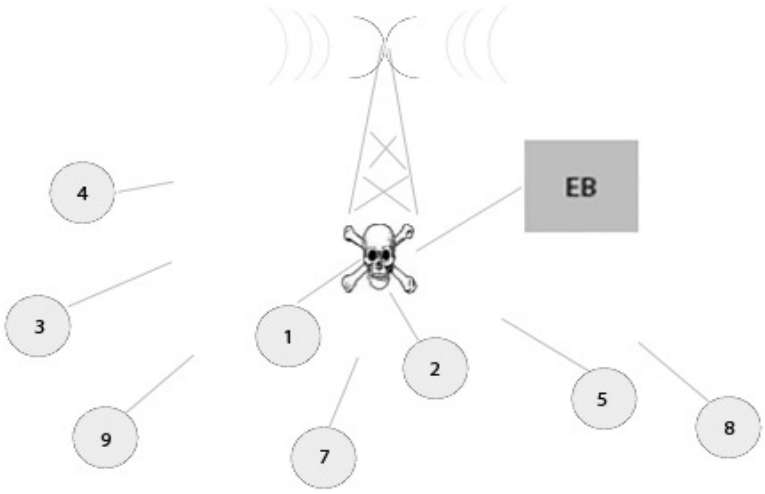


Figura 4-7: Nó malicioso a transmitir pacotes de HELLO

4.1.7 "Spoofing" de confirmação

Como foi referido em 4.1.1, "*spoofing*" consiste em imitar algo. Neste caso, refere-se à falsificação de pacotes de "*acknowledgment*" (ACK), ou seja, de confirmação, por parte de um atacante [31]. Muitos dos algoritmos de encaminhamento das redes de sensores dependem de confirmações implícitas ou explícitas quando os nós comunicam uns com os outros. Estas confirmações são

feitas através de trocas de pacotes com informação de controlo. Neste caso, pacotes de ACK. Devido ao meio de comunicação wireless, um atacante tem a possibilidade de falsificar instruções de confirmação nos pacotes de controlo da rede endereçados aos nós vizinhos [34]. Os objectivos desta acção consistem em convencer o emissor que determinado caminho fraco é na verdade forte ou que um nó "morto" ou desactivado está a funcionar. Por exemplo, um protocolo de encaminhamento pode seleccionar o próximo salto num caminho usando a fiabilidade da ligação. Reforçar artificialmente uma ligação fraca ou "morta" é uma forma subtil de manipular este esquema. Como os pacotes enviados por ligações fracas ou "mortas" são perdidos, um adversário poderá eficazmente montar um esquema de encaminhamento selectivo usando "*spoofing*" de confirmação, ao encorajar os nós a transmitirem pacotes por estas ligações [34].

4.2 Algoritmos de Encaminhamento Seguro

No ponto 2.5 foram analisados alguns protocolos de encaminhamento para as redes de sensores wireless. No entanto, devido às limitações dos sensores, estes protocolos têm em vista a economia de recursos, tornando-se portanto vulneráveis a ataques.

Esta secção contém uma análise a alguns algoritmos de encaminhamento seguro que, contrariamente à grande maioria dos protocolos analisados no capitulo 2, são capazes de fazer face às principais ameaças de segurança nas redes de sensores wireless, tendo em conta as limitações de hardware envolvidas.

Segue-se então a análise a algumas das soluções de segurança disponíveis.

4.2.1 Algoritmos de Chen

Chen et al. [60] propõem dois protocolos de segurança. O primeiro consiste num esquema para manter a confidencialidade e autenticação entre a estação base e os nós, através de um algoritmo de encriptação. O segundo consiste em autenticação da fonte, tendo sido baseado no protocolo TESLA (*"Timed Efficient,Streaming,Loss-Tollerant Authentication Protocol"*) [61], utilizando para tal uma função semelhante a uma *"hash chain"* [62] para gerar chaves, com o objectivo de conseguir implementar a autenticação ao nível dos nós.

Estes dois protocolos são baseados num algoritmo de chave partilhada [66], visto que este método requer menor capacidade de processamento que, por exemplo, um algoritmo de chave pública [67]. Pelo mesmo motivo, é utilizado o algoritmo RC5 [68] para realizar a encriptação.

Segue-se então a descrição dos dois métodos propostos.

4.2.1.1 Autenticação e Confidencialidade Estação Base-Nós

A autenticação entre a estação base e os nós é conseguida através de uma mensagem de 8 bytes denominada de *"Message Authentication Code"*, MAC, incluída em todos os pacotes enviados à estação base. O MAC é calculado com base na função de encriptação do protocolo RC5 e não é facilmente invertido. Uma vez que apenas o $nó_i$ e a estação base partilham a chave secreta para o $nó_i$, a estação base consegue verificar que a mensagem é genuinamente do $nó_i$ através do cálculo do MAC da mensagem, comparando-o de seguida com o MAC no pacote. Como tal, a estação base consegue verificar que o $nó_i$ é o verdadeiro originador da mensagem. Este protocolo assegura à estação base que a mensagem de facto vem de onde aparenta vir. Para além disto, o MAC também possui a funcionalidade de "*Cyclic Redundancy Code*", CRC [69], permitindo confirmar a integridade da mensagem. Se a verificação do MAC falhar, então a mensagem terá sido enviada maliciosamente ou então terá sofrido erros durante a transmissão. Em qualquer dos casos, a mensagem não é fiável e é assinalada como tal, sendo o seu destino depois dependente dos critérios do sistema.

A confidencialidade da comunicação é assegurada através do modo de *"Output-Feedback"*, OFB, do protocolo RC5. De acordo com este esquema, os nós usam as suas chaves secretas e um vector de inicialização para calcular uma "pad", ou chave aleatória [70]. O texto da mensagem sofre posteriormente um XOR com o "pad" para produzir o texto encriptado. Uma das vantagens deste método é que o texto encriptado possui o mesmo tamanho que o texto origina. Isto é um ponto muito favorável em aplicações com recursos limitados, como é o caso das redes de sensores wireless, em que a reduzida largura de banda é necessária para transmitir o maior volume de dados úteis possível.

Em cada pacote enviado para a estação base, o conteúdo útil da mensagem, chamado de *"payload"* [71], é encriptado (se a aplicação assim o pretender). Este *"payload"* encriptado, juntamente com o ID da aplicação, o número de sequência e o ID da fonte origina o MAC, permitindo a autenticação da mensagem. A confidencialidade, em conjunto com a autenticação entre a estação base e os nós, estabelecem um canal de comunicação seguro.

4.2.1.2 Protocolo de Autenticação da Fonte

O princípio básico deste protocolo é o de que o emissor gera uma sequência de chaves secretas, $\{ K_j \}$, em que cada chave K_j faz parte de uma *"hash chain"*. Esta *"hash chain"* consiste numa função recursiva, *F*, sendo que, através de uma chave inicial seleccionada aleatoriamente, K_N, são geradas outras chaves (únicas) com base na anterior, $K_j = F(K_j + 1)$. Neste caso, é usado o algoritmo MD5 [72] para o efeito. Esta função *F* é uma função de sentido único [73], ou seja, a partir de K_j não é possível obter o elemento que lhe deu origem.

O tempo é dividido em intervalos. Cada emissor associa a sua sequência de chaves com a sequência dos intervalos temporais, tendo uma chave por cada intervalo. No intervalo de tempo *t*, o emissor usa a chave do intervalo actual, K_t, para gerar o MAC para os pacotes nesse intervalo. O emissor irá posteriormente revelar a chave K_t após um atraso de δ_r, que se segue ao fim do intervalo de tempo *t*. O intervalo de revelação da chave δ_r deverá ser maior que o tempo de ida e volta da mensagem.

Quando o receptor recebe os pacotes com o MAC, guarda o tempo de chegada de cada pacote. É de referir que o receptor e o emissor necessitam de uma sincronização temporal aproximada. Após o emissor revelar a chave para o intervalo *i*, o receptor pode então autenticar os pacotes previamente guardados recebidos no mesmo intervalo de tempo, possuindo como tal a mesma chave.

A existência de um buffer de mensagens pode ser um problema devido às limitações de memória, pelo que este tamanho do buffer deve ser reduzido, assim como o intervalo temporal.

4.2.2 SPINS

O SPINS [62], ou *"Security Protocols for Sensor Networks"*, consiste num conjunto de protocolos de segurança intitulado de SNEP, *"Secure Network Encryption Protocol"*, em conjunto com um protocolo para a autenticação, o µTESLA. Este protocolo foi criado tendo em mente a utilização de equipamento simples do ponto de vista de memória e de energia, como acontece com as redes de sensores wireless.

O SNEP tem como objectivo a confidencialidade dos dados, autenticação e a garantia de que os dados recebidos não são antigos (sendo esta característica referida como frescura), apresentando no entanto baixo *"overhead"*. Para tal, esta plataforma apresenta as seguintes propriedades:

- Segurança semântica – com as mensagens, é enviado um valor de um contador, partilhado entre cada nó e a estação base, que é incrementado com cada envio. Como tal, a mesma mensagem é encriptada de um modo diferente de cada vez. O valor do contador é suficientemente longo de modo a que nunca se repita durante a vida útil do nó;
- Autenticação dos dados – isto permite ao receptor confirmar que os dados foram realmente enviados pelo suposto emissor. Para conseguir a autenticação, o emissor e o receptor partilham uma chave secreta para calcular um código MAC (*"Message Authentication Code"*);
- Protecção contra repetições – o contador incluído no MAC impede o reenvio de mensagens antigas. Se este contador não existisse, um atacante poderia facilmente repetir mensagens já enviadas;

- Frescura de dados – após uma mensagem ter sido verificada convenientemente, o receptor sabe que a mensagem é nova e que foi enviada depois da mensagem anterior que recebeu correctamente (que possuía um valor de contador inferior) e que não foi uma mensagem antiga repetida;
- Baixo *"overhead"* de comunicação – o estado do contador é mantido em cada terminal e não necessita de ser enviado em cada mensagem.

O SNEP utiliza criptografia simétrica, ou seja, a mesma chave é usada para encriptar e desencriptar, com uma função criptográfica (RC5) [68] para a encriptar, desencriptar, criar o MAC, gerar números pseudo-aleatórios e funções de "*hash*".

Os dados são encriptados no seguinte formato:

- $E = \{D\}_{<K_{encr}, C>}$, onde *D* são os dados, a chave de encriptação é K_{encr} e o contador é C
- Envio de A para B é $A \rightarrow B : E, \mathrm{MAC}(K_{mac}, C \mid E)$

A autenticação é importante para muitas aplicações nas redes de sensores. Dentro do processo de configuração da rede, a autenticação é necessária para muitas tarefas administrativas. Um atacante pode facilmente injectar mensagens, de modo que o receptor necessita de garantir que os dados vêm da fonte correcta. Quando a comunicação é entre apenas dois nós, a autenticação é conseguida simplesmente através de métodos simétricos. O emissor e o receptor partilham uma chave secreta para calcular um código MAC para todos os dados comunicados. Quando chega uma mensagem com o MAC correcto, o receptor sabe que a mensagem veio do emissor.

Este tipo de autenticação não pode ser aplicado a transmissões para todos os nós da rede. A utilização de métodos simétricos como o MAC implica que qualquer receptor conheça a chave e, como tal, pode imitar o emissor.

A autenticação assimétrica é conseguida através do protocolo µTESLA. Trata-se de é uma versão mais leve do protocolo TESLA, que por sua vez foi desenhado para computadores normais e não para ambientes computacionais limitados como os verificados nas redes de sensores wireless. As principais diferenças no µTESLA são:

- O uso de apenas mecanismos simétricos de encriptação;
- O tempo é divido em slots, sendo que a revelação da chave de encriptação é feita uma vez por cada slot e não em todos os pacotes.
- O número de emissores autenticados é restringido.

A transmissão autenticada requer um mecanismo assimétrico, que geralmente necessita de métodos de encriptação muito pesados. O µTESLA introduz a assimetria através de um revelar atrasado de chaves simétricas, resultando num método de transmissão autenticada eficiente. Em vez de adicionar uma chave revelada a cada pacote de dados, a revelação de chaves é independente

da transmissão de pacotes e está relacionada com intervalos de tempo. De acordo com este protocolo, o emissor transmite a chave actual periodicamente num pacote especial.

Na figura 4-8, os pacotes P1 e P2 são enviados no intervalo de tempo 1 e contêm um MAC com a chave K_1, enquanto que P3, enviado no intervalo 2, possui um MAC com K_2.

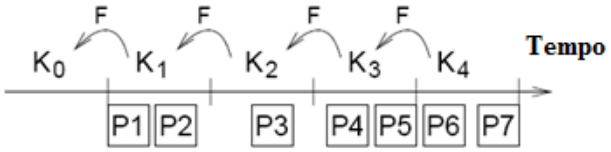


Figura 4-8:Utilização de sequência de chaves para autenticação

O receptor ainda não consegue autenticar a mensagem, tendo que armazenar os pacotes num buffer e aguardar pela chave. Se, por exemplo, os pacotes P4,P5 e P6 forem perdidos, assim como o pacote que revela a chave K_1, o receptor não será capaz de autenticar P1, P2 ou P3. No intervalo 4, a estação base transmite a chave K_2, que o nó autentica ao verificar que $K_0 = F(F(K_2))$, sendo que o nó conhece previamente K_0. Deste modo, o nó também consegue obter $K_1 = F(K_2)$, conseguindo assim autenticar P1 e P2 com K_1 e P3 com K_2.

As várias fases do µTESLA consistem em:

- Setup do emissor (gerar um sequencia de chaves secretas);
- Transmissão de pacotes autenticados (enviados em intervalos de tempo, com uma chave para cada intervalo);
- Inicialização de novos receptores (os receptores são inicializados com um chave inicial K_0, com a qual conseguem confirmar a veracidade das chaves seguintes através de $K_i = F(K_{i+1})$);
- Autenticação de pacotes.

A difusão de dados autenticados por parte dos nós é feita de dois modos, com o objectivo de minimizar o uso da memória e da bateria:

- Os nós difundem os dados através da estação base. Usam o SNEP para enviar os dados de forma autenticada à estação base, que por sua vez os difunde;
- Os nós difundem os dados. No entanto, é na mesma a estação base que possui a cadeia de chaves, enviando as chaves aos emissores sempre que necessário.

Resumindo, o protocolo SPINS baseia-se na utilização de criptografia simétrica leve, não usando esquemas simétricos e pesados como chaves públicas, para obter autenticação e encriptação da comunicação. Como tal, a troca de mensagens é feita com um baixo custo energético e requer equipamento pouco poderoso do ponto de vista de processamento e memória. No entanto, o

encaminhamento é feito sempre para a estação base, pelo que este protocolo é vulnerável a ataques de análise de tráfego.

4.2.3 Algoritmo de Undercoffer

Undercoffer et al. [31], propõem um protocolo de segurança relativamente leve em termos de recursos, tendo sido inspirado no SPINS. Consiste num protocolo a operar na estação base, permitindo à estação detectar e remover nós com um comportamento errático, tendo como objectivo:

1. Fornecer privacidade de dados;
2. Garantir a integridade dos dados;
3. Autenticar o emissor;
4. Impedir repetição de pacotes;
5. Prevenir contra ataques de análise de tráfego

Basicamente, este protocolo difere do SPINS em dois aspectos:

- O SPINS utiliza encaminhamento na fonte, ou seja, os nós emissores decidem o caminho que os pacotes percorrem, tornando a rede vulnerável a ataques de análise de tráfego. O protocolo de Undercoffer baseia-se em transmissões onde toda a comunicação é encriptada de ponto a ponto e o encaminhamento é decido pela estação base, de modo a reduzir a ameaça da análise de tráfego;
- O protocolo de Undercoffer fornece um mecanismo para detectar certos tipos de comportamentos aberrantes por parte dos nós, comportamentos estes que se podem dever a avarias ou a ataques de um nó individual. Em qualquer um dos casos, o protocolo é capaz de remover o nó da rede.

Estrutura de pacotes

Todos os pacotes enviados são constituídos por um preâmbulo, cabeçalho e *"payload"* (mensagem propriamente dita):

$$\overbrace{< \text{Addr\_1}()}^{\text{Preâmbulo}}, \quad \overbrace{\text{E}\, Key_j\{\text{Addr\_2(j)}, DTG, COMMAND\}}^{\text{Cabeçalho}} \quad , \overbrace{\text{E}\, Key_j\{\text{dados}\} >}^{\text{Payload}}$$

O preâmbulo é nulo se a comunicação originar da estação base e estiver direccionada para um sensor. Em qualquer outra situação, contem o endereço do nó emissor. O cabeçalho contem o endereço do receptor, um selo temporal (DTG) e um comando. Esta parte é encriptada pela chave Key_j, sendo esta partilhada entre a estação base e o nó *j*. O campo COMMAND pode tomar os valores apresentados na tabela 4-1. Por último, o *"payload"* contém os dados trocados entre o nó e

a estação base, sendo encriptado pela chave partilhada do nó de destino, que pode ser diferente da usada para encriptar o cabeçalho.

Tabela 4-1: Valores de comando

Comando	**Função**
HELLO	Mensagem de descoberta para averiguar a topologia da rede
HELLO-REPLAY	Resposta à mensagem de descoberta de topologia
RELAY	Concatenar Addr_1 ao *"payload"* e transmitir
UPDATE-PSI	Actualizar Ψ

Descoberta da topologia e setup da rede

A estação base possui um ID único e uma chave de encriptação simétrica com cada um dos nós da rede. Do mesmo modo, cada nó é inicializado com a chave única que partilha com a estação base, estando o seu relógio interno sincronizado com o da estação base.

Após a inicialização da rede, a estação base investiga a topologia da rede, cria e optimiza uma tabela de endereçamento e providencia um mecanismo para os nós fora do seu alcance a conseguirem alcançar de um modo seguro.

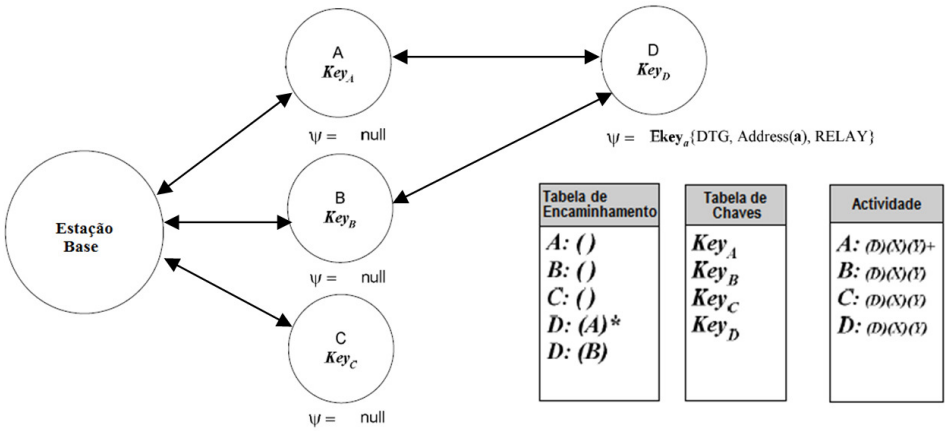


Figura 4-9: Exemplo de topologia

Na figura 4-9, é possível ver um exemplo da organização e encaminhamento da rede. A tabela de encaminhamento contém o caminho primário, indicado por um *, assim como contem os percursos alternativos até um determinado nó. Uma entrada do tipo A:() indica que o nó está directamente ligado à estação base, ao passo que, uma entrada do tipo D:(A) indica que A é um nó intermédio entre a estação base e o nó D.

A tabela de chaves contém as chaves únicas partilhadas entre um determinado nó e a estação base.

A tabela de actividade contém o selo temporal DTG (*"Date Time Group"*) mais recente recebido pela estação base de um determinado nó e um contador (Y) de outros nós dependentes do

reencaminhamento deste nó. Os valores de X e Y são usados para detectar comportamentos estranhos por parte de algum nó.

Criação da tabela de encaminhamento

Para os nós *j* dentro do alcance da estação base, é enviado uma mensagem de HELLO. Caso o nó responda com um HELLO-REPLY, então o nó é adjacente à estação base e esta adiciona-o à tabela de encaminhamento. Os nós que não responderem, são considerados como não adjacentes.

Para os nós *i* fora do alcance da estação base, a estação base envia uma mensagem aos seus nós vizinhos que contém o comando RELAY e um *"payload"*, de modo a serem encaminhados para o nó não adjacente de destino. Numa mensagem de RELAY, o cabeçalho é encriptado pelas chaves dos nós adjacentes e o *"payload"* dessa mensagem, que encapsula o cabeçalho e o *"payload"* destinados ao nó não adjacente, é encriptado pela chave do nó de destino:

$$\boxed{\text{EB} \rightarrow \text{i:}} \quad \overbrace{<\text{Addr\_1}(),}^{\text{Preâmbulo}} \overbrace{\text{E}\,Key_j\{\text{Addr\_2(j)}, \text{Null}, RELAY\}}^{\text{Cabeçalho}} \overbrace{, \text{E}\,Key_i\{\text{Addr\_2(i)}, \text{DTG}, HELLO\}>}^{\text{Payload}}$$

O nó responsável pelo reencaminhamento mantém o preâmbulo original e coloca o *"payload"* recebido como o novo cabeçalho. O *"payload"* a enviar contém um campo Ψ que será usado pelo nó não adjacente para alcançar a estação base através de um nó vizinho da estação base:

$$\boxed{\text{j} \rightarrow \text{i:}} \quad \overbrace{<\text{Addr\_1}(),}^{\text{Preâmbulo}} \overbrace{\text{E}\,Key_i\{\text{Addr\_2(i)}, \text{DTG}, HELLO\}}^{\text{Cabeçalho}}, \overbrace{\Psi = \text{E}\,Key_j\{\text{Addr\_2(j)}, \text{NULL}, RELAY\}>}^{\text{Payload}}$$

O campo Ψ contém o comando RELAY e é encriptado pela chave do nó adjacente. Em resposta à mensagem de HELLO, o nó não adjacente constrói uma mensagem de HELLO-REPLY encriptada com a chave que partilha com a estação base e coloca-a no *"payload"*. O preâmbulo que contém o endereço da estação base é adicionado ao Ψ (cabeçalho) e ao *"payload"*, formando a mensagem:

$$\boxed{\text{i} \rightarrow \text{j:}} \quad \overbrace{<\text{Addr\_1}(),}^{\text{Preâmbulo}} \overbrace{\Psi = \text{E}\,Key_j\{\text{Addr\_2(j)}, \text{NULL}, RELAY\}}^{\text{Cabeçalho}}, \overbrace{\text{E}\,Key_j\{\text{DTG}, \text{Addr\_2(i)}, HELLO - REPLY\}>}^{\text{Payload}}$$

Quando o nó adjacente recebe a transmissão, desencripta o cabeçalho e, após detectar o comando RELAY, adiciona o preâmbulo ao *"payload"* e transmite o pacote à estação base:

$$\boxed{\text{j} \rightarrow \text{EB:}} \quad \overbrace{<\text{Addr\_1(i)},}^{\text{Preâmbulo}} \overbrace{\text{E}\,Key_j\{\text{DTG}, \text{Addr\_2(i)}, HELLO - REPLY\}}^{\text{Cabeçalho}}, \overbrace{\text{null}>}^{\text{Payload}}$$

Assim que a estação base tiver conhecimento de quais nós que lhe são adjacentes e os caminhos para os nós que não o são, vai optimizar a sua tabela de encaminhamento de modo a não utilizar sempre os mesmos nós para o encaminhamento de mensagens. Caso o processo de optimização resulte em caminhos diferentes, a estação base envia aos nós em questão uma actualização do Ψ, através de uma mensagem com o código UPDATE-PSI.

Este protocolo também prevê a inserção de nós da rede, sendo realizada uma actualização à tabela de encaminhamento posteriormente. Para além disto, é possível detectar e isolar nós com comportamentos estranhos, podendo estes resultar de ataques, danos ou desgaste da bateria. Para tal, é mantida uma tabela com o registo da actividade de cada nó, verificando longos períodos de inactividade, ou o envio excessivo de mensagens corrompidas.

Resumindo, para evitar a análise do tráfego, toda a comunicação é encriptada, com a excepção do preâmbulo que é nulo, excepto para tráfego enviado para a estação base. Como tal, os nós têm que desencriptar toda a comunicação que recebem. Isto não representa um grande *"overhead"*, uma vez que quando o nó desencripta os primeiros 64 bits da mensagem, o endereço do receptor (Addr2) é revelado. Se um endereço válido é encontrado, então o nó vai continuar a desencriptar a mensagem, caso contrário, a mesma será descartada.

Como foi falado anteriormente, a autenticação é conseguida através do uso de uma chave secreta partilhada estação base e o nó j.

A garantia da integridade das mensagens é alcançada através do uso de um algoritmo de encriptação. Como tal, um ataque com a intenção de alterar a mensagem, apenas vai conseguir alterar a sua forma e não o conteúdo da mensagem propriamente dito

A negação de repetições é conseguida através do uso de um selo temporal, O DTG, fazendo com que o reenvio de mensagens por parte de um atacante não tenha sucesso.

Finalmente, a privacidade é alcançada como um resultado da encriptação de todas as comunicações.

4.2.4 Algoritmo de Slijepcevic

Slijepcevic et al. [63] propõem um algoritmo de segurança que classifica os tipos de dados existentes nas redes de sensores e identifica possíveis falhas de segurança. Para cada tipo de dados, existe um mecanismo de segurança correspondente, o que permite uma gestão de recursos eficiente.

São definidos três tipos de dados, sendo o primeiro referido como código móvel. Trata-se da transmissão de código em situações onde uma reprogramação dos nós é necessária. Devido à natureza esporádica e à sensibilidade destas situações, este tipo de dados pode ter um nível de protecção mais elevado e dispendioso do ponto de vista energético. O segundo tipo de dados enviados é relacionado com a divulgação da localização dos sensores, enquanto que o terceiro tipo engloba as trocas de informação relacionadas com a aplicação, tais como medições, alertas, entre outros. Estes diferentes tipos de dados estão sujeitos a diferentes tipos de ameaças:

- Código móvel – é possível injectar código malicioso nos sensores, podendo alterar o comportamento da rede;
- Localização de sensores – a transmissão da posição dos sensores pode facilitar a obtenção das mesmas por parte de um atacante;
- Dados específicos da aplicação – também podem incluir informação sobre a localização dos nós. Um atacante pode observar o conteúdo específico da aplicação nas mensagens, incluindo o ID da mensagem, selos temporais e outros campos. A confidencialidade destes campos é menos importante que a confidencialidade da informação da localização, uma vez que a informação relativa à aplicação não contém dados valiosos e a vida útil destes dados é relativamente curta;

Para cada um destes tipos de dados, foi criado um nível de segurança:

- Nível de segurança I para código móvel;
- Nível de segurança II para localização dos nós;
- Nível de segurança III para dados da aplicação.

Para implementar os diferentes níveis de segurança, foi utilizado o algoritmo RC6 [64]. O nível de segurança fornecido por este algoritmo é ajustável graças ao seu parâmetro "número de rondas", sendo que números de rondas mais elevados representam encriptação mais forte, com a contrapartida de maiores *"overheads"*.

É utilizado um modelo *"multicast"* de comunicação, ou seja, de um nó para vários. Isto evita que cada par de nós necessite de uma chave, como acontece nos modelos *"unicast"* (nó a nó) e minimiza o número de mensagens enviadas, sendo estipuladas chaves por grupos de nós.

Todos os nós da rede partilham inicialmente um conjunto de chaves mestras. O número de chaves depende da longevidade estimada do sistema. Uma destas chaves é activada a um dado momento, sendo seleccionada com base num algoritmo aleatório a correr em cada nó com a mesma semente. As chaves necessárias para os três níveis de segurança são derivadas da chave mestra activa.

4.2.4.1 Nível de segurança I

As mensagens que contêm código móvel são menos frequentes que as mensagens referentes à aplicação da rede. Isto permite a utilização de uma encriptação forte apesar do elevado *"overhead"* que daí resulta. Para a informação protegida por este nível de segurança, os nós utilizam a chave mestra actual directamente. Caso um atacante consiga quebrar a segurança deste nível, poderá inserir código malicioso e alterar todo o funcionamento da rede.

4.2.4.2 Nível de segurança II

O nível de segurança II é baseado num mecanismo de segurança que isola partes da rede, de modo a que uma quebra de segurança numa parte não afecte a rede na sua totalidade.

Neste nível, os nós utilizam chaves com base na sua actual localização. A área de cobertura da rede é dividida em células, sendo que os nós dentro de uma célula partilham uma chave obtida em função da chave mestra actual e de uma localização fixa da célula.

A divisão da área é feita em hexágonos, bastando para tal um ponto de referência (centro do hexágono) definido previamente. Os restantes pontos são derivados do tamanho definido das células. A dimensão das células deve ser suficientemente grande de modo a que a natureza localizada dos algoritmos na rede assegurem que o tráfego entre as células seja relativamente baixo, quando comparado com o tráfego global da rede.

Existe uma região de fronteira entre as células, cuja largura é igual ao alcance da transmissão. Todos os nós pertencentes a regiões de fronteira possuem as chaves de todas as regiões adjacentes. Isto assegura que dois nós dentro do alcance de transmissão um do outro possuem uma chave em comum. Isto encontra-se ilustrado na figura 4-10. A divisão hexagonal garante que um nó não necessita mais do que três chaves.

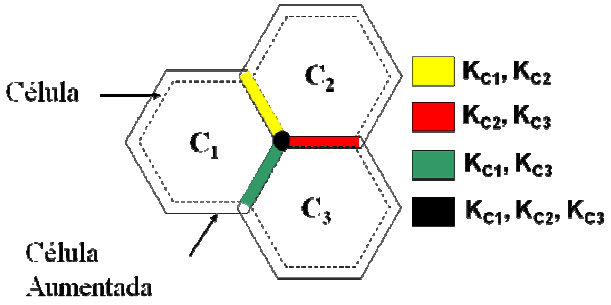


Figura 4-10: Divisão da rede por células

É chamada de célula aumentada à zona que engloba a célula propriamente dita mais a região de fronteira. Cada nó terá que comparar a sua localização com a de cada célula aumentada para determinar em que zona se encontra. Se se encontrar dentro da célula aumentada C_x, então irá possuir a chave de C_x, K_{Cx}. Os nós nas regiões de fronteira possuem mais do que uma chave. Por exemplo, os nós na zona amarela da figura 4-10 são adjacentes às células C_1 e C_2, possuindo portanto as chaves K_{C1} e K_{C2}. A contrapartida é que os nós nestas regiões terão que enviar a mesma mensagem mais do que uma vez.

Uma vez que o nível de protecção é mais reduzido para a informação sobre a localização do que para o código móvel, a probabilidade das chaves para o nível II serem decifradas é superior.

4.2.4.3 Nível de segurança III

Os dados específicos da aplicação são encriptados de um modo menos forte do que os dois tipos de dados mencionados anteriormente. A encriptação mais fraca implica um menor *"overhead"* computacional para este tipo de dados. Adicionalmente, o elevado volume de envio de mensagens com dados específicos da aplicação impede a utilização de encriptação mais forte, pois levaria à rápida exaustão dos recursos da rede. Como tal, é utilizado um algoritmo de encriptação que requer menos recursos, com a correspondente redução no nível de segurança.

A chave utilizada para a encriptação dos dados no nível III é derivada da chave mestra actual. A função de *"hash"* do protocolo MD5 [72] recebe a chave mestra e gera uma chave para o nível III. Uma vez que a chave mestra é alterada periodicamente, a chave correspondente a este nível segue estas alterações.

4.2.5 SRAs

O esquema SRAs, ou *"Secure Routing Algorithms"* [25], propõe um conjunto de dois algoritmos, sendo um para os nós e o outro para a estação base. Neste esquema, todos os nós possuem um ID único. Uma vez instalada a rede, a estação base constrói uma tabela com os IDs de todos os nós da rede. Depois, após um processo de auto-organização, a estação base passa a conhecer a topologia da rede. Este algoritmo utiliza o esquema de tripla chave, STKS, referido no ponto 3.1.9, para fazer a encriptação e a autenticação dos dados recolhidos e depois encaminhá-los para o líder do cluster, que por sua vez agrega e envia os dados para a estação base.

4.2.5.1 Algoritmo dos Nós

O algoritmo dos nós executa as seguintes funções:

- Os nós utilizam a chave K_n para encriptar e transmitir os dados;
- Transmissão de dados encriptados para os líderes de cluster;
- Concatenação do ID dos sensores aos dados e encaminhamento para os líderes de cluster. Numa topologia hierárquica, os líderes de cluster mais perto da estação base são designados como líderes de cluster de alto nível;
- Os líderes de cluster utilizam K_c (chave de cluster) para desencriptar e K_n para encriptar e enviar os dados para o nível hierárquico seguinte, chegando eventualmente à estação base.

O método de funcionamento do algoritmo pode ser descrito pelos seguintes passos:

Passo 1: Se o nó *i* pretender enviar dados ao seu líder de cluster, avança para o passo dois, caso contrário, sai do algoritmo;

Passo 2: O nó *i* solicita ao seu líder de cluster que lhe envie K_c;

Passo 3: Após a recepção, o nó *i* utiliza K_c e a sua K_n para calcular a chave de encriptação $K_{i,cn}$;

Passo 4: O nó *i* encripta os dados com $K_{i,cn}$, concatena o seu ID e um selo temporal *TS* aos dados encriptados e envia-os ao seu líder de cluster;

Passo 5: O líder de cluster recebe os dados, adiciona o seu ID ao pacote, juntamente com um *TS* e envia-os de seguida ao líder de cluster de alto nível, ou para a estação base caso esteja directamente ligado. No fim do processo, avança novamente para o passo 1.

4.2.5.2 Algoritmo da Estação Base

A estação base tem a seu cargo a responsabilidade de enviar aos outros nós as chaves da rede K_n e as chaves de sensor K_s, usadas respectivamente para encriptar e para desencriptar os dados. Possui também as funções de desencriptação e de autenticação dos dados. Estas funcionalidades são realizadas através dos passos seguintes:

Passo 1: Verifica a necessidade de transmitir alguma mensagem. Caso se verifique, transmite a mensagem encriptando-a com K_n;

Passo 2: Caso não haja necessidade de transmitir mensagens, então verifica se recebeu alguma mensagem dos líderes de cluster. Caso não existam dados a serem enviados para a estação base, volta ao passo 1;

Passo 3: Se existirem dados a serem enviados para a estação base, então são desencriptados usando K_s, o ID do nó e o *TS* contidos na mensagem;

Passo 4: Confirma que a chave de desencriptação K_s desencriptou os dados perfeitamente verificando a credibilidade do *TS* e o ID. Caso não se verifique, descarta o pacote e avança para o passo 6;

Passo 5: Processa os dados desencriptados e obtém a mensagem enviada pelos líderes de cluster e sensores;

Passo 6: Decide se deve pedir aos sensores que retransmitam os dados ou não. Se for concluído que não é necessário, retorna ao passo 1;

Passo 7: Se um pedido de reenvio for necessário, envia um aos sensores a pedir que retransmitam os dados. Caso a sessão tenha terminado, retorna ao passo 1.

A tabela 4-2 mostra um resumo dos níveis de segurança oferecidos por cada esquema.

Tabela 4-2: Resumo dos algoritmos de encaminhamento seguro

Esquema	**Encriptação**	**Autenticação**	***"Overhead"***
Chen	Chave única partilhada entre estação base e cada nó. Comunicação nó a nó não é encriptada.	Autenticação da fonte conseguida através de um campo MAC, incluído em todos os pacotes enviados à estação base, em conjunto com chaves simétricas divulgadas em atraso, simulando métodos assimétricos. Nós intermédios não autenticam os nós abaixo de si na hierarquia.	Baixo devido ao uso de chaves simétricas e tamanho reduzido do MAC (8 bytes)
SPINS	Chave única partilhada entre estação base e cada nó. Comunicação nó a nó garantida pela estação base.	Autenticação com base em chaves simétricas e MAC, com uma divulgação atrasada das chaves.	Baixo devido a encaminhamento na fonte e uso de chaves simétricas.
Undercoffer	Chave única partilhada entre estação base e cada nó.	Estação base com ID único e partilha com cada nó uma chave simétrica única. Detecção de comportamento errático.	Maior do que SPINS devido a encaminhamento pré-estabelecido pela estação base.
Slijepcevic	Três níveis de segurança para três tipos de dados. Nivel II utiliza chaves por cluster.	Não abordada.	Variável consoante o tipo de dados.
SRAs	Esquema de três chaves (STKS): chave de nó, chave da rede e chave de cluster.	Autenticação em dois níveis: estação base e líder de cluster. Utiliza selo temporal e IDs únicos.	O "*overhead"* resultante do SRAs é mais elevado que nos outros esquemas, mas oferece uma encriptação superior.

Da tabela 4-2 pode-se constatar que o nível oferecido pela maioria destes esquemas é semelhante, com a excepção do esquema de Slijepcevic que se concentra mais na encriptação do que na autenticação. Em termos de *"overhead"*, todas estas soluções foram criadas tendo em vista as redes de sensores e as suas limitações, pelo que a carga adicional de transmissão e processamento impostos por estes esquemas às redes é suportável e nalguns casos até configurável.

4.2.6 Algoritmos Vs. Ataques

Esta secção explica o modo como os algoritmos de encaminhamento seguros, em conjunto com esquemas de encriptação, fazem face a alguns dos ataques mais frequentes.

4.2.6.1 Ciclos de Encaminhamento

A replicação das identidades dos nós causa ciclos de encaminhamento (ver ponto 4.1.1). As mensagens falsas e enganadoras geradas pelos atacantes divulgam informação de encaminhamento alterando o normal comportamento dos nós da rede e esgotando os seus já de si limitados recursos energéticos, fazendo com a sua vida útil chegue ao fim antecipadamente. A defesa convencional contra este tipo de ataque consiste em ter uma autoridade central a guardar um registo com a localização de cada sensor [57]. Este tipo de solução cria um elevado *"overhead"* e pode tornar-se um problema para redes de elevadas dimensões.

Este tipo de ataques pode ser contrariado com a existência de esquemas de autenticação eficientes, como os abordados na secção anterior. Nestes esquemas, todas as mensagens de que um nó receba, são em geral descartadas se o nó emissor for um desconhecido, evitando assim a interpretação de mensagens maliciosas.

4.2.6.2 Ataques "Sybil"

Um ataque *"Sybil"* acontece quando um nó cria múltiplas identidades ilegítimas ao se fazer passar por outros nós da rede (ver ponto 4.1.4). Estes ataques reduzem a eficácia de esquemas tolerantes a falha, que utilizem redundância de encaminhamento [58], manutenção de topologia e armazenamento distribuído [59], entre outros.

Tal como nos ciclos de encaminhamento, estes ataques dão-se pela falta de autenticação apropriada. Se um nó não for quem afirma ser, não irá possuir o material de autenticação (chaves e IDs) necessário para se identificar como tal, sendo as suas mensagens descartadas. Por este motivo, um nó malicioso não pode aclamar múltiplas identidades e os esquemas propostos tornam um ataque *"Sybil"* praticamente impossível.

4.2.6.3 Encaminhamento Selectivo, Sinkholes e Wormholes

Os ataques de *"Sinkholes"* e *"Wormholes"* são ataques comuns contra protocolos, especialmente quando executados em simultâneo. Os *"Sinkholes"* atraem o tráfego da rede para um nó comprometido, colocando um nó malicioso mais perto da estação base e executando encaminhamento selectivo.

Num ataque de *"Wormhole"*, o atacante redirecciona mensagens de uma localização para outra com baixa latência.

A autenticação fornecida pela maioria dos esquemas propostos faz com que os nós não aceitem transmissões de nós maliciosos. Para além disso, alguns dos esquemas possuem mecanismos de detecção de nós com comportamentos erráticos, eliminando a possibilidade dos nós permanecerem na rede.

4.2.6.4 Inundação de HELLO

Atacantes com mais poder de transmissão, como por exemplo através de um computador portátil, tornam-se intrusos e inundam a rede com pacotes, induzindo os nós a interpretarem as mensagens como vindo da estação base. A autenticação da estação base perante os nós é uma característica importante da maior parte dos esquemas abordados, impedindo que um atacante se faça passar por ela. Um atacante pode, no entanto, reenviar pacotes enviados pela estação base (*"replay"* de mensagens), entre os quais se incluem os pacotes de HELLO para levantamentos de topologia, levando a respostas desnecessárias por parte dos nós da rede e à consequente exaustão de recursos. Para evitar isto, é essencial a incorporação de selos temporais nos pacotes enviados, assim como o sincronismo temporal dos nós, uma vez que permite confirmar que os dados são actuais. Esta característica está prevista em todos os esquemas abordados, com a excepção do proposto por Sliepcevic (ver ponto 4.2.4).

4.3 Conclusão do Capítulo

Neste capítulo foram descritos em pormenor os ataques mais frequentes contra o encaminhamento nas redes de sensores wireless, de onde se pode concluir que sem uma abordagem apropriada à problemática da segurança, as redes ficam extremamente vulneráveis a todo o tipo de ataques. Como tal, foram abordadas algumas formas de contrariar e prevenir os principais ataques, nomeadamente através de algoritmos seguros de encaminhamento. Estes algoritmos, em conjunto com esquemas de chaves de segurança como os descritos no capítulo 3, fornecem um nível de segurança capaz de fazer frente às ameaças mais frequentes.

O encaminhamento seguro é vital para a aceitação e uso das redes de sensores wireless em muitas aplicações. A autenticação é um factor fundamental para a fiabilidade dos dados recolhidos, uma vez que um atacante pode enviar informação propositadamente incorrecta se for reconhecido como constituinte da rede, falseando os resultados práticos do uso da mesma. Para além disto, a possibilidade da circulação de informação sigilosa na rede é por vezes essencial, pelo que um bom esquema de encriptação é necessário.

A encriptação da comunicação e os mecanismos de autenticação representam uma boa abordagem ao problema da segurança, no entanto não são suficientes. Um desenho cuidado dos protocolos usados é essencial, devendo estes ser adaptados à capacidade do equipamento usado, ao tipo de dados monitorizados, ao meio em que a rede se insere e ao propósito da implementação da mesma.

Capítulo 5

5. Conclusão e Trabalho Futuro

As redes de sensores wireless fazem parte de um grupo distinto dentro das redes móveis. Consistem em agregações de pequenos dispositivos capazes de recolher informação do ambiente em que se inserem e de monitorizar eventos e objectos. Estes dispositivos possuem, no entanto, algumas limitações profundas a nível capacidade de memória, de energia e de processamento. Estas fragilidades, em conjunto com as limitações do próprio meio de transmissão wireless e com a falta de vigilância sobre os sensores após terem sido colocados no terreno, tornam estas redes susceptíveis a uma variedade de ataques. Visto que a gama de aplicações possíveis inclui, entre outras, o campo da medicina e campo militar, a responsabilidade e importância dos dados que circulam em redes nestas áreas pode ser bastante elevada. Isto faz com que a falta de segurança possa ser um factor impeditivo da utilização desta tecnologia. As medidas de segurança tradicionais necessitam de uma capacidade de comunicação e de processamento bastante elevadas, o que impossibilita a sua utilização nas redes de sensores wireless. O baixo custo dos sensores permite a sua utilização em massa, o que inviabiliza actualmente o desenvolvimento de sensores mais poderosos, pois levaria a um aumento nos custos. Daqui conclui-se que é necessária uma solução de segurança ponderada que seja eficiente, eficaz e que não implique um aumento significativo do volume de dados de controlo transaccionados, para que não se desperdiçarem recursos.

Com este trabalho, foi possível concluir que uma rede desprotegida será facilmente controlada por um atacante e que, para obter um nível de segurança aceitável, é necessário satisfazer quatro objectivos:

- Disponibilidade;
- Confidencialidade;
- Integridade;
- Autenticação.

Concluiu-se também que através de um esquema de chaves de segurança, em conjunto com um algoritmo de encaminhamento apropriado, se consegue:

- Encriptar a comunicação na rede;
- Identificar os sensores individualmente;
- Garantir que estes conseguem encaminhar as suas mensagens.

Ficam assim satisfeitos os quatro objectivos mencionados. Com estes quatro factores garantidos, é criada uma barreira de segurança eficaz no combate às ameaças mais frequentes.

5.1 Satisfação dos Objectivos

Este trabalho teve como objectivo determinar os níveis de segurança que se conseguem obter nas redes de sensores wireless, assim como determinar as ameaças mais frequentes às quais estas redes estão sujeitas. Outro dos objectivos, foi determinar quais as medidas que se devem tomar para obter um nível de segurança desejável, contrariando os ataques revelados. Para tal, foi feito um trabalho de investigação, onde foram descritas em pormenor as ameaças a que as redes de sensores wireless estão sujeitas, tendo-se concluído que é essencial a implementação de esquemas de distribuição de chaves de segurança, e de algoritmos de encaminhamento apropriados. Satisfazendo estas duas necessidades, é possível assegurar um elevado nível de protecção contra os ataques mais frequentes. Com base nestas conclusões, é possível afirmar que foram satisfeitos os objectivos propostos inicialmente.

5.2 Trabalho Futuro

O uso crescente da tecnologia wireless nas redes de sensores implica a continuidade da investigação nesta área. Do mesmo modo que as medidas de segurança se tornam mais sofisticadas com o tempo, também os atacantes vão evoluindo e, regra geral, estão um passo à frente das medidas de segurança que procuram romper. Como tal, existirão sempre novos tipos de ataques, uma vez que a investigação por parte dos atacantes também não pára. Estando o "estado da arte" nesta área a alterar-se frequentemente com o tempo, é essencial que qualquer trabalho futuro passe sempre por uma actualização da informação relativa aos tipos de ataques, assim como das medidas de segurança disponíveis.

Sendo este trabalho direccionado às redes de sensores wireless em geral, seria interessante fazer uma análise individualizada às diferentes áreas de aplicação, tais como a medicina ou a domótica, uma vez que os níveis de segurança necessários dependem sempre das necessidades da aplicação e do meio em que se inserem, assim como do hardware envolvido. Este hardware também vai evoluindo com o tempo, pelo que será de esperar que futuramente a capacidade de processamento, memória e de energia não sejam um problema para as redes de sensores wireless, como acontece hoje em dia. Isto abrirá uma nova gama de oportunidades de pesquisa e desenvolvimento nessa área, uma vez que o grau de complexidade dos sistemas de segurança poderá aumentar,

aumentando consequentemente a fiabilidade das redes. Como tal, será importante seguir a evolução dos componentes utilizados nas redes de sensores wireless em trabalhos futuros

Referências

[1] Feldmeier, M., and Paradiso, J.A., "Giveaway Wireless Sensors for Large-Group Interaction". Procedings of the ACM Conference on Human Factors and Computing Systems (CHI 2004), Extended Abstracts, Vienna, Austria, Abril, 2004.

[2] Kaplantzis, Sofia. Security Models for Wireless Sensor Networks. Março de 2006.

[3] "O que é uma Rede de Sensores Sem Fio?", http://digital.ni.com/worldwide/brazil.nsf/web/all/EF115A37FDD4C3088625755F00524039 [Consultado em Março de 2009].

[4] H. S. Ng, M. L. Sim e C. M. Tan; "Security issues of wireless sensor networks in healthcare applications"; Junho 2006.

[5] Intel. 2008."The Promise of Wireless Sensors" , http://www.intel.com/research/exploratory/wireless_promise.htm [consultado em Abril de 2009].

[6] Zia, T.; Zomaya, A. (2006) "Security Issues in Wireless Sensor Networks". Proceedings of the International Conference on Systems and Networks ICSNC 2006, Nov 2- 4, Tahiti, French Polynesia.

[7] Wikipedia. Wireless sensor network. Wikipedia: The Free Online Encyclopedia. http://en.wikipedia.org/wiki/Wireless_sensor_network [Consultado em Março de 2009].

[8] Perrig, Adrian; Stankovic, John; Wagner, David. "Communications of the ACM" June 2004/Vol. 47, No. 6.

[9] Culler, David and Srivastava, Deborah. "Overview of Sensor Networks", Publicado por IEEE Computer Society, 2004;

[10] "Aerial robot uses wireless link to transfer sensor data"; http://www.machinebuilding.net/ap/a0486.htm; [Consultado em Março de 2009];

[11] Wozniak, B.; "Wireless sensor networks can address industrial, economic, and societal issues"; http://www.mbtmag.com/article/279047-Wireless_sensor_networks_can_address_industrial_economic_and_societal_issues.php.

[12] G. Barrenetxea, F. Ingelrest, G. Schaefer and M. Vetterli; "Wireless Sensor Networks for Environmental Monitoring: The SensorScope Experience"; 20th IEEE International Zurich Seminar on Communications (IZS 2008); Zurich, Suíça, Março 2008.

[13] Werner-Allen, Geoffrey; Johnson, Jeff; Rui, Mario; Lees, Jonathan; Welsh, Matt. "Monitoring Volcanic Eruptions with a Wireless Sensor Network";

[14] Carman, D.W., Krus, P.S. and Matt, B.J. (2000) Constraints and approaches for distributed sensor network security. Technical Report 00-010. Glenwood, Maryland, USA, NAI Labs, Network Associates;

[15] Jing Deng, Richard Han, Shivakant Mishra, "Defending Against Traffic Analysis Attacks in Wireless Sensor Networks", 13th USENIX Security Symposium, San Diego, CA, Agosto, 2004;

[16] Van Dam, J.M. "An Adaptive Energy-Eficient MAC Protocol for Wireless Sensor Networks", TUDelft, Junho 2003.

[17] Wei Ye, John Heidemann, e Deborah Estrin. "An Energy-Efficient MAC protocol for Wireless Sensor Networks". Proceedings of the IEEE Infocom, pp. 1567-1576. New York, NY, USA, USC/Information Sciences Institute, IEEE. Junho, 2002.

[18] Intanagonwiwat, C.; Govindan, R.; Estrin, D.; Heidemann, J.; Silva, F. "Directed diffusion for wireless sensor networking". Networking, IEEE/ACM Transactions. Volume 11, Issue 1, Fevereiro, 2003;

[19] Braginsky, David (2002) "*Rumor Routing Algorithm for Sensor Networks"*. In Proceedings of the First ACM Workshop on Sensor Networks and Applications.

[20] Kulik, J.; Rabiner Heinzelman, W; Balakrishnan, H. "Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks". Wireless Networks 8(2-3): 169-185, 2002;

[21] Sohrabi, K. Gao, J. Ailawadhi, V. Pottie, G.J.. “Protocols for self-organization of a wireless sensor network”. Personal Communications, IEEE, Volume: 7, Issue: 5, Outubro 2000;

[22] Rabiner Heinzelman,w.; Chandrakasan, A.;Balakrishnan H.; "Energy-efficient Communication Protocols for Wireless Microsensor Networks". Proceedings of Hawaaian Int'l Conf. on Systems Science, Janeiro 2000.

[23] Manjeshwar, A.; Agrawal, D. P.; "TEEN: A Protocol for Enhanced Efficiency in Wireless Sensor Networks", 15th International Parallel and Distributed Processing Symposium (IPDPS'01) Workshops, 2001;

[24] Karp, B.; Kung H.T.;"GPSR: greedy perimeter stateless routing for wireless networks", International Conference on Mobile Computing and Networking , Boston 2000;

[25] Zia, T.; Zomaya, A., “A Security Framework for Wireless Sensor Networks”, IEEE Sensors Applications Symposium Houston, Texas USA, Fevereiro, 2006.

[26] Xu Y.; Heidemann J.; Estrin D.; “Geography-informed Energy Conservation for Ad Hoc Routing,” Mobicom, 2001;

[27] Kaplantzis, Sofia. Security Models for Wireless Sensor Networks. Março de 2006;

[28] Wood, A.; Stankovic, J.; “Denial of Service in Sensor Networks”; IEEE Computer Society Press Los Alamitos, CA, USA, Outubro 2002;

[29] Tague, P.; Poovendran, R.; “Modeling node capture attacks in wireless sensor networks”; Proceedings of 46th Annual Allerton Conference on Communication, Control, and Computing; 2008;

[30] Saraogi, M., “Security in Wireless Sensor Networks”. Project Paper at Computer and Network Security, Sections 494/4 594/9. University of Tennesse, 2006.

[31] Undercoffer, J., Avancha, S., Joshi, A. and Pinkston, J. (2002) “Security for sensor networks”. In Proceedings of the CADIP Research Symposium, University of Maryland, Baltimore County, USA.

[32] Costa,O.;Vaz, I.. “Roteamento Geográfico”. http://www.gta.ufrj.br/grad/06_2/igor/index.html [consultado em Junho de 2009]

[33] V. Ramasubramanian, Z.J. Haas, and E.G. Sirer, "SHARP: A Hybrid Adaptive Routing Protocol for Mobile Ad Hoc Networks," Proceedings of MOBIHOC Conf. 2003, pp. 303-314, Junho 2003.

[34] Karlof, C. e Wagner, D. "Secure routing in wireless sensor networks: attacks and countermeasures". Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 2003.

[35] Quirino, Anderson de Jesus e Silva, Ronaldo Gabriel. "Rede de Sensores Sem Fio". 2007. Trabalho (Pós-Graduação em Redes Wireless) – Universidade de São Paulo, São Paulo.

[36] Wikipedia. Sensor node. Wikipedia: The Free Online Encyclopedia. http://en.wikipedia.org/wiki/Sensor_node [Consultado em Março de 2009].

[37] Hu, F., Ziobro, J., Tillett, J. and Sharma, N. (2004) "Secure wireless sensor networks: Problems and Solutions". Systemic, Cybernetics and Informatics, Volume 1, Nº 4.

[38] Wikipedia. Domínio. Wikipedia: The Free Online Encyclopedia. http://pt.wikipedia.org/wiki/Dom%C3%ADnio [Consultado em Junho de 2009]

[39] Eschenauer, L. e Gligor, V. (2002) "A key-management scheme for distributed sensor networks". Proceedings of the 9th ACM Conference on Computer and Communication Security, 2002, Washington DC, USA.

[40] Stajano, F. (2002) "Security for ubiquitous computing". New York, USA, John Wiley and Sons.

[41] Chan, H., Perrig, A. e Song, D. (2003) "Random Key Predistribution Schemes For Sensor Networks". Proceedings of the IEEE Symposium on Security and Privacy, 11-14 May 2003, Oakland, California, USA. Páginas 197-213.

[42] Pietro, R., Mancini, L. and Mei, A. (2003) "Random key-assignment for secure wireless sensor networks". ACM SANS.

[43] Zhu, S., Xu, S., Setia, S. e Jajodia, S. (2003) "Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach". 11th IEEE International Conference on Network Protocols (ICNP'03). Atlanta, Georgia, IEEE Computer Society.

[44] Testing Standards Working Party – Living Glossary. Definição de "Pseudo-Aleatório" http://www.testingstandards.co.uk/living_glossary.htm#P [Consultado em Junho de 2009]

[45] Wikipedia. Random Seed. Wikipedia: The Free Online Encyclopedia. http://en.wikipedia.org/wiki/Random_seed [Consultado em Junho de 2009]

[46] Wikipedia. Sinkhole. Wikipedia: The Free Online Encyclopedia. http://en.wikipedia.org/wiki/Sinkhole [Consultado em Junho de 2009]

[47] Wikipedia. Sybil. Wikipedia: The Free Online Encyclopedia. http://en.wikipedia.org/wiki/Sybil_%28book%29 [Consultado em Junho de 2009]

[48] Sherif Khattab (2004) "Security Issues of Wireless Sensor and Ad-hoc Networks" www.cs.pitt.edu/~skhattab/ [Consultado em Junho de 2009]

[49] Karlof, C. e Wagner, D. (2005) "Summary of Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures". Seminário sobre Theoretical Computer Science

[50] Wikipedia. Routing loop problem. Wikipedia: The Free Online Encyclopedia. http://en.wikipedia.org/wiki/Routing_loops [Consultado em Junho de 2009]

[51] L.B. Oliveira, E. Habib, D. Camara, H.C. Wong, A.A.F. Loureiro, and R. Dahab. "SecOverlay: Redes Overlay sobre Redes de Sensores Sem Fio para Transmissão Segura de Dados." 5th Brazilian Symposium on Information and Computer Systems Security, Florianopolis, Brasil, Setembro de 2005.

[52] E. C.H. Ngai, J. Liu, and M.R. Lyu. "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks," IEEE International Conference on Communications (ICC'06), Istanbul, Turquia, Junho de 2006.

[53] Rajeev Shorey, A. Ananda, Mun Choon Chan, Wei Tsang Ooi. "Mobile, Wireless, and Sensor Networks: Technology, Applications, and Future Directions". Wiley-IEEE Press. Abril de 2006.

[54] JR Douceur. "The Sybil attack" Proc. IPTPS'02, Março de 2002.

[55] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University, Tech. Rep. TR01-384, Junho de 2002.

[56] Campista, Miguel Elias Mitre; Duarte, Otto Carlos Muniz Bandeira. "Segurança em Redes de Sensores". Artigo submetido à Universidade Federal do Rio de Janeiro, Setembro de 2003.

[57] James Newsome, Runting Shi, Dawn Song, and Adrian Perrig. “The sybil attack in sensor networks: Analysis and defenses.” Proceedings of IEEE International Conference on Information Processing in Sensor Networks (IPSN 2004), 2004.

[58] K. Ishida, Y. Kakuda, and T. Kikuno, “A routing protocol for finding two node-disjoint paths in computer networks”. International Conference on Network Protocols, Novembro 1992.

[59] Castro e Liskov, “Practical byzantine fault tolerance”. OSDI: Symposium on Operating Systems Design and Implementation. USENIX Association, 1999.

[60] Chen, M., Chen W., Cui, W., Wen, V. and Woo, A.”Security and Deployment Issues in a Sensor Network”. Berkeley, California, USA, University Press. 2000.

[61] Adrian Perrig, Ran Canetti, J.D. Tygar, and Dawn Xiaodong Song. “Eficient authentication and signing of multicast streams over lossy channels”. IEEE Symposium on Security and Privacy. Maio de 2000.

[62] Perrig, A., Szewczyk, R., Wen, V., Culler, D. and Tygar, J.D. (2002) “SPINS: security protocols for sensor networks”. Wireless Networks Journal (WINE), Setembro de 2002.

[63] Slijepcevic S.; Potkonjak M.; Tsiatsis V.,;Zimbeck S. ;Srivastava M.; “On Communication Security in Wireless Ad-Hoc Sensor Network”; IEEE WETICE 2002, Pittsburg.

[64] R. L. Rivest, M.J.B. Robshaw, R. Sidney, e Y.L. Yin, “The RC6 Block Cipher”, AES submission, Junho 1998.

[65] Wikipedia. Hash Chain. Wikipedia: The Free Online Encyclopedia. http://en.wikipedia.org/wiki/Hash_chain [Consultado em Junho de 2009]

[66] Wikipedia. Pre-Shared Key. Wikipedia: The Free Online Encyclopedia. http://en.wikipedia.org/wiki/Pre-shared_key [Consultado em Junho de 2009]

[67] Wikipedia. Public Key. Wikipedia: The Free Online Encyclopedia. http://en.wikipedia.org/wiki/Public-key_cryptography [Consultado em Junho de 2009]

[68] Wikipedia. RC5. Wikipedia: The Free Online Encyclopedia. http://en.wikipedia.org/wiki/RC5 [Consultado em Junho de 2009]

[69] Wikipedia. Cyclic redundancy check. Wikipedia: The Free Online Encyclopedia. http://en.wikipedia.org/wiki/Cyclic_redundancy_check [Consultado em Junho de 2009]

[70] Wikipedia. One Time Pad. Wikipedia: The Free Online Encyclopedia. http://pt.wikipedia.org/wiki/One-time_pad [Consultado em Junho de 2009]

[71] Wikipedia. Payload. Wikipedia: The Free Online Encyclopedia. http://pt.wikipedia.org/wiki/Payload [Consultado em Junho de 2009]

[72] Ronald L. Rivest. "The MD5 message-digest algorithm". Internet Request for Comments, Abril de 1992. RFC 1321.

[73] Wikipedia. One Way Function. Wikipedia: The Free Online Encyclopedia. http://en.wikipedia.org/wiki/One-way_function [Consultado em Junho de 2009]

[74] Liu, D. e Ning, P. (2003) "Establishing pairwise keys in distributed sensor networks". Proceedings of ACM CCS '03, Outubro, Washington DC, USA.

[75] Blundo, C., De Santis, A., Herzberg, A., Kutten, S., Vaccaro, U. e Yung, M. (1992) "Perfectly secure key distribution for dynamic conferences". Proceedings of CRYPTO'92, Agosto, 1992, Berlin, Springer Verlag.

[76] Du, W., Deng, J., Han, Y.S. e Varshney, P.K. (2003) "A pairwise key predistribution scheme for wireless sensor networks". Proceedings of the ACM CCS '03, Outubro, 2003, Washington, DC, USA.

[77] Blom, R. (1984) An optimal class of symmetric key generation systems. Advances in cryptology. In Proceedings of EUROCRYPT 84, Abril, 1984, Paris, France. New York, USA, Springer Verlag.

[78] Wikipedia. Graph theory. Wikipedia: The Free Online Encyclopedia. http://en.wikipedia.org/wiki/Graph_theory [Consultado em Junho de 2009]

[79] Du, W., Deng, J., Han, Y., Chen, S.S. e Varshney, P.K. (2004) "A key management scheme for wireless sensor networks using deployment knowledge". Proceedings of the IEEE InfoCom, Março, 2004, Hong Kong.

[80] Eltoweissy, M., Wadaa, A., Olariu, S. and Wilson, L. (2005) "Scalable cryptographic key management in wireless sensor networks". Journal of Ad Hoc Networks, Special issue on Data Communications and Topology Control in Ad Hoc Networks, (3) 5, Setembro.

[81] Zhang, Y., Liu, W., Lou, W. and Fang, Y. (2005) "Securing sensor networks with location-based keys". Wireless Communications and Networking Conference (WCNC) 21-25 Março de 2004, Atlanta, GA, USA

[82] Corke, P., Peterson, R. and Rus, D. (2003) “Networked robots: flying robot navigation using a sensor net”. Proceedings of the 11th International Symposium of Robotics Research (ISRR), Outubro, 2003, Siena, Italy.

[83] Zia, T.A., and Zomaya, A.Y., “A Secure Triple-Key Management Scheme for Wireless Sensor Networks”. Proceedings of the IEEE INFOCOM 2006 Students Workshop, Abril, 2006, Barcelona, Espanha.