Universidade Federal de São Carlos

Centro de Ciências Exatas e de Tecnologia

Departamento de Computação

Programa de Pós-Graduação em Ciência da Computação

Utilização das Características Intrínsecas das Redes de Sensores Sem Fio na Detecção de Invasões

Luciano Bernardes de Paula

SÃO CARLOS – SP

Maio – 2006

Ficha catalográfica elaborada pelo DePT da Biblioteca Comunitária da UFSCar

D419uc

De Paula, Luciano Bernardes.
Utilização de características intrínsecas das redes de sensores sem fio na detecção de invasões / Luciano Bernardes De Paula. -- São Carlos : UFSCar, 2006.
82 p.

Dissertação (Mestrado) -- Universidade Federal de São Carlos, 2006.

1. Redes de computação – medidas de segurança. 2. Redes de sensores sem fio. I. Título.

CDD: 005.8 (20ª)

Universidade Federal de São Carlos

Centro de Ciências Exatas e de Tecnologia

Programa de Pós-Graduação em Ciência da Computação

"Utilização de Características intrínsecas das redes de sensores sem fio na detecção de invasões"

LUCIANO BERNARDES DE PAULA

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de São Carlos, como parte dos requisitos para a obtenção do título de Mestre em Ciência da Computação.

Membros da Banca:

Prof. Dr. Luis Carlos Trevelin
(Orientador – DC/UFSCar)

Prof. Dr. Hélio Crestana Guardia
(DC/UFSCar)

Prof. Dr. Mauricio Ferreira Magalhães
(DCA/FEE/UNICAMP)

São Carlos
Maio/2006

“Chewing bits, spitting bytes”

LBP

Dedico este trabalho:

À minha família, à minha namorada, aos meus amigos e, principalmente, aos estudantes de mestrado e de doutorado deste país que, apesar de todas as dificuldades e falta de incentivo, continuam a trilhar esse caminho.

Agradecimentos

A Deus, acima de tudo e de todos, por todas as oportunidades que tive e ainda terei na minha vida;

A meus pais (Ricardo e Raquel) e meu irmãos (Flavio e Henrique), pessoas sem as quais eu não seria o que sou hoje;

À Má, minha namorada, por todo o carinho.

A todos os meus familiares pela confiança irrestrita;

Ao Prof. Dr. Luis Carlos Trevelin pela orientação, motivação e amizade;

Aos meus amigos verdadeiros, que sempre estão ao meu lado, mesmo quando distantes;

Aos amigos do GSDR por toda ajuda e companheirismo;

Ao Bob Kane, Stan Lee, Jerry Siegel e Joe Shuster por suas criações.

Resumo

As aplicações para Redes de Sensores Sem Fio (RSSF) crescem de maneira acelerada e, cada vez mais, estas são aplicadas para solucionar problemas antes considerados intratáveis.

O maior desafio para os desenvolvedores de soluções que utilizem redes de sensores sem fio é como ultrapassar a barreira da limitação de recursos como energia, processamento e memória que essas possuem. Com o aumento da utilização dessas redes, incluindo em áreas militares e de segurança civil, aumentam também as ameaças de segurança que as visam. Em contrapartida, toda a segurança já desenvolvida para as redes de computadores convencionais não pode ser aplicada para as RSSFs devido à limitação destas.

A maioria dos ataques conhecidos contra redes de sensores sem fio é iniciada através da invasão da rede por sensores malignos, lançados pelo atacante na área de atuação destas. Algumas abordagens propostas na literatura visam identificar os ataques, e não a invasão pelos sensores malignos.

Essa dissertação de mestrado tem como objetivo especificar atributos que possam ser incorporados aos protocolos de camada de rede das RSSFs que tenham como característica de segurança a descoberta e identificação de invasões por sensores externos, não dependendo do tipo de ataque que estes aplicarão.

Abstract

The development of applications for Wireless Sensor Networks (WSNs) grows quickly and they are being applied to solve problems considered impossible before.

The great challenge for the developers of solutions that use WSNs is how to deal with the resources limitation like the low battery capacity, low processing power and small amount of memory that the sensor nodes have. The increasing in the utilization of this kind of network, including military and civil applications, makes the security menaces to them increase as well. On the other hand, every security strategy already developed to conventional computers network cannot be applied to the WSNs, because of their limitations.

The great part of the known attacks against WSNs is initiated by the invasion of the network by malicious sensor nodes, launched by the attacker inside the area of the network. Some approaches proposed in the literature seek to identify the attacks and not the invasion by the intruder nodes.

This work has as goal to define attributes that can be inserted in the network layer protocols for WSNs giving to the network the ability of detect invasions by external nodes, independently of the attack that they would perform.

Sumário

Lista de figuras

Lista de tabelas

1. Introdução

Cenário 1: Uma rede de sensores sem fio monitora a movimentação na área externa da residência de um grande empresário. Seqüestradores rastreiam o sistema e, antes de atacar, lançam próximo à área sensores invasores. Esses sensores se comunicam com os sensores de segurança, prejudicando a comunicação destes e, em pouco tempo, a rede de sensores da segurança se torna praticamente inútil, propiciando aos atacantes o momento ideal para a invasão, surpreendendo os seguranças.

Cenário 2: Na tentativa de evitar ataques químicos e biológicos, foi instalada uma rede de sensores sem fio por todo o complexo de metrôs de uma grande cidade. Esses sensores monitoram constantemente a presença de agentes químicos e biológicos no ar. Terroristas extremistas, munidos de alguns poucos sensores invasores, os acionam dentro da área de atuação da rede de sensores de proteção. Em pouco tempo, as comunicações falsas dos sensores malignos exaurem toda a energia da rede de sensores de segurança, permitindo que o grupo terrorista aja de maneira precisa e devastadora.

Os cenários descritos acima não são mera ficção. Em 18 de janeiro de 2005, foi publicada na Folha Online [FOL 05] uma reportagem a respeito das medidas de segurança tomadas para a posse do presidente americano, George W. Bush. Um dos trechos da reportagem [AND 05] cita:

"Dispositivos que detectam a presença de materiais químicos e biológicos serão espalhados em Washington --em mais estações de metrô que o normal, ao redor do National Mall e em prédios e ruas na rota percorrida na posse".

Cada vez mais as redes de sensores sem fio (RSSF) são empregadas em sistemas de segurança e monitoramento. Na mesma proporção crescem os ataques a essas redes que apresentam pouquíssimos ou até mesmo nenhum sistema de segurança contra esse tipo de

ameaça. Isso se dá pela própria natureza dos nós sensores que compõem a rede, pois se tratam de dispositivos com recursos limitados de energia, de processamento e de memória.

Todas as estratégias de segurança desenvolvidas para as redes de computadores convencionais devem ser reinventadas ou, no mínimo, reformuladas para as RSSFs, devido à escassez de recursos que estas apresentam.

Esse trabalho especifica características das RSSFs que, se monitoradas, faz com que a invasão da rede por sensores externos à ela seja identificada, evitando assim todo e qualquer tipo de ataque que tenha como característica o lançamento de sensores malignos dentro de uma RSSF. Para testar e validar a utilização dessas características, serão propostas extensões aos protocolos da camada de rede das RSSFs que as implementem e que considerem as características de roteamento de protocolos já amplamente utilizados nesse tipo de rede.

1.1 Motivações e Relevância

Algumas propostas foram feitas na tentativa de eliminar alguns tipos de ataques em RSSFs, como encontradas em [KAR 03][SAN 04][NEW 04][WOO 02] entre outros. O problema dessas abordagens situa-se na restrição que possuem, pois estas identificam apenas um tipo de ataque deixando a rede suscetível a outros. Uma característica marcante mostra que quase todos os ataques conhecidos em RSSFs são iniciados na invasão da rede por nós sensores malignos. O atacante insere nós invasores sobre o campo onde a RSSF se encontra, e estes nós invasores executam o ataque.

Através desse trabalho serão especificadas características a serem investigadas em uma RSSF para que esta esteja apta a identificar a invasão de nós malignos, de maneira que a solução não fique atrelada ao tipo de ataque, e sim à invasão em si. Essas características serão definidas de maneira que possam ser incorporadas em outros protocolos.

1.2 Organização

No segundo capítulo são apresentadas as RSSFs, suas principais características, aplicações e seus principais desafios. No capítulo 3 é abordada a segurança em redes de sensores sem fio, apresentando os principais ataques. O capítulo 4 discute as características intrínsecas das RSSFs utilizadas nesse trabalho e como explorá-las para detecção de intrusão. O capítulo 5 apresenta os mecanismos criados para o monitoramento das características da

rede. No sexto capítulo é apresentado em detalhes o mecanismo de contagem do número de elementos da rede. O capítulo 7 mostra em detalhes o mecanismo de monitoramento da energia residual da rede. O oitavo capítulo mostra a atuação dos dois mecanismos anteriores em conjunto e o nono conclui a dissertação.

2. Redes de Sensores Sem Fio – RSSFs

As redes de sensores sem fio – RSSFs – estão em grande crescimento atualmente, sendo utilizadas para monitorar e eventualmente controlar um ambiente. As RSSFs são formadas, geralmente, por centenas ou milhares de dispositivos de proporções reduzidas (cm^3 ou mm^3), chamados nós sensores. Esses nós sensores consistem em dispositivos com pequeno poder de processamento, baixo nível de energia (bateria) e capacidade de memória reduzida que, trabalhando em conjunto, podem executar tarefas complexas. Os nós sensores geralmente possuem módulos de sensoriamento, processamento e comunicação. As aplicações das RSSF se dão tanto em ambientes controlados, onde o posicionamento dos sensores pode ser feito de forma manual e planejada, ou até mesmo onde a atuação humana é impossibilitada como em ambientes hostis, necessitando que os nós sejam lançados de forma aleatória no ambiente. Ao serem lançados nesse tipo de ambiente, os nós sensores utilizam protocolos de auto-organização para formar uma rede sem fio, utilizando protocolos de acesso ao meio e roteamento fazendo com que a informação flua da maneira mais adequada possível até o nó sorvedouro (*sink node*), ou estação-base, ponto onde a RSSF faz a troca de informações com o mundo externo. A estação-base pode ser um nó especial, um computador que se comunique com a rede de sensor, ou até mesmo um computador portátil, inclusive podendo ser estática ou se movimentar durante o tempo. A figura 2.1 exemplifica a auto-organização de uma RSSF. A unidade de sensoriamento dos nós sensores possui uma grande gama de possibilidades, gerando uma grande diversidade de aplicações onde as RSSF podem atuar. Os sensores podem ser térmicos, sísmicos, acústicos, magnéticos, etc, possibilitando assim a medição de diversos fatores externos, como variações na temperatura, pressão, presença, movimentação, umidade, etc, e serem empregadas nas mais diversas aplicações. A maneira como a RSSF monitora o ambiente é bastante versátil, podendo assim, se adequar da melhor forma possível para cada aplicação. De acordo com a aplicação, o monitoramento pode ser contínuo, periódico, orientado a eventos, orientado a consultas, etc.

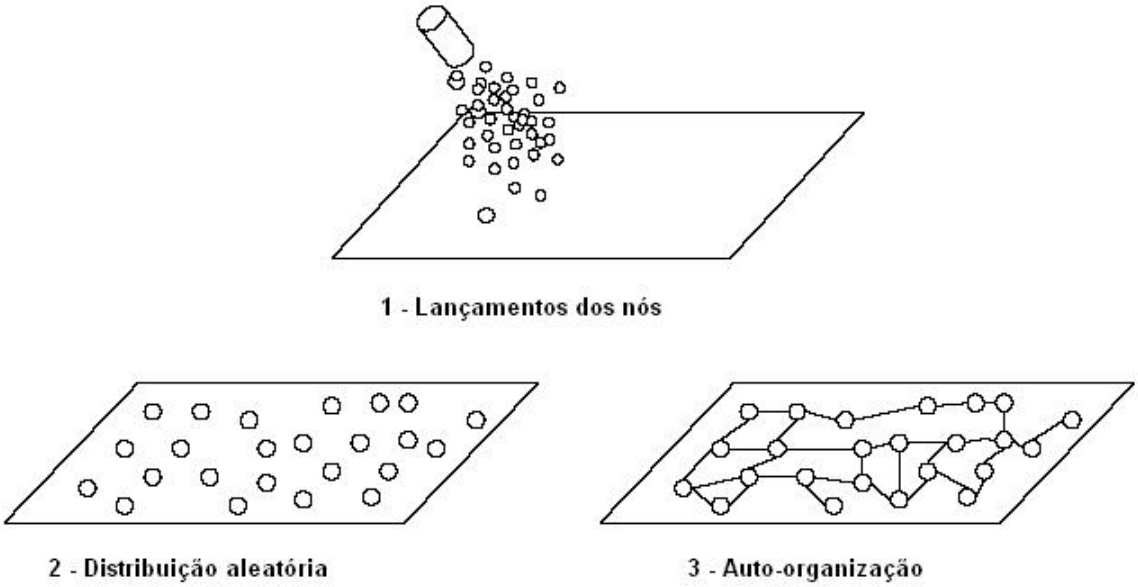


Figura 1: Auto-organização de uma RSSF [LIN 03]

Várias áreas possuem importantes utilizações para as RSSFs. Em [LIN 03] são apresentadas algumas destas:

- Rastreamento de contaminação química: Uma área pode ser monitorada por uma RSSF para a identificação de certos elementos químicos. Cada sensor é apto a "sentir" se há ou não a presença de um determinado elemento químico no ponto monitorado. Através do trabalho em conjunto dos vários sensores da rede, é possível identificar a forma da área contaminada e seu movimento de propagação [JIE 02].

- Rastreamento de área de desastre: Milhares de sensores são lançados de um avião em uma área que sofreu um desastre, formando uma rede *ad hoc* de comunicação. Grupos de respostas à emergência utilizam essa rede através da disseminação de consultas dentro desta com o intuito de coletar informações sobre o movimento de sobreviventes ou iminência de desabamentos, por exemplo. As consultas são automaticamente roteadas para os sensores mais apropriados e respostas são coletadas e enviadas para o mundo exterior. Em [CHI 01] é apresentado um modelo para RSSFs com essas características.

- Aplicações civis: A gama de aplicações desse tipo é muito grande. Um exemplo é o de detecção de poluição ao longo de praias com nós sensores distribuídos pela costa. RSSFs também podem ser usadas onde métodos tradicionais representam soluções impraticáveis ou

muito caras. Estas também podem ser usadas em cada artigo de um inventário em um complexo de armazéns ou de escritórios de uma fábrica, ser anexadas às paredes ou encaixadas nos assoalhos e tetos, seguindo o histórico da posição e uso dos artigos. As RSSFs podem automaticamente encontrar artigos, colaborar nos serviços de manutenção, analisar correlações a longo prazo entre o fluxo de trabalho e o desgaste [EST 99].

- Sistemas de transporte inteligentes: Kanaian [KAN 99] desenvolveu um pacote de sensores sem fio que conta a passagem de veículos, mede a velocidade média da estrada e detecta gelo e água na mesma. Conjuntos de sensores podem transmitir esta informação em tempo real às estações-base próximas, interligadas à rede de computadores, para controlar e predizer o tráfego e auxiliar na desobstrução de perigos na estrada. Os nós custam menos de US$30 para serem construídos e podem ser instalados sem a utilização de cabos sob a estrada. Os dispositivos observam os veículos, detectando perturbações causadas pelos mesmos no campo magnético da Terra. Outro exemplo seria o uso dos sensores em cada veículo de uma grande metrópole com vários sensores. Estes sensores são capazes de detectar suas posições, tamanho do veículo, velocidade e densidade, condições da estrada e assim por diante. Quando os veículos se cruzam, trocam informações. Estas informações são difundidas através das regiões da metrópole. Os motoristas podem planejar rotas alternativas, estimar o tempo de viagem e serem avisados sobre situações de dirigibilidade perigosa [EST 99].

- Monitoramento ambiental: Este tipo de aplicação fornece uma rica coleção de tipos de sensoriamento e condições ambientais. Cerpa *et al* [CER 01] propuseram uma aplicação em que o objetivo é dar suporte a uma coleção de dados e modelar o desenvolvimento de ecossistemas complexos. De acordo com eles, cientistas e autoridades de monitoramento de impacto ambiental poderiam monitorar os componentes químicos do solo e do ar, bem como populações e comportamento de espécies de plantas e animais. Imagens e acústica são utilizadas para localizar, identificar e rastrear espécies ou fenômenos baseando-se nos sinais implícitos (acústicos e sísmicos) ou sinais explícitos (colares de identificação, por exemplo). Devem ser implantadas nas posições remotas onde faltam infra-estruturas instaladas de energia e comunicação, motivado pela necessidade de comunicação sem fio de baixo consumo [EST 01].

- Monitoramento de florestas, vulcões, tornados: Sensores podem ser utilizados para reportarem eventos críticos na natureza, como por exemplo: fogo em uma floresta,

erupção de um vulcão, velocidade de um tornado, etc. Essas medidas têm um mínimo de atraso, informando também a localização da leitura.

- **Rastreamento de inimigos em aplicações militares:** Neste tipo de aplicação, são lançados no campo de batalha sensores para detectar a movimentação dos tanques inimigos. O movimento destes é detectado por sensores sísmicos [BAH 00].

Devido a essa grande gama de áreas que utilizam RSSFs, estas ficam sujeitas a funcionarem nos mais diferentes tipos de ambientes, como por exemplo:

- Dentro de máquinas, sob diferentes temperaturas;
- No fundo do mar, sob extrema pressão;
- Dentro de ciclones e furacões;
- Ambientes contaminados química ou biologicamente, impróprios para a atuação humana;
- Zonas de guerra;
- Ambientes domiciliares e empresariais;
- Em animais;
- Em veículos;

Como pôde ser notado, em vários desses ambientes, a colocação precisa dos nós sensores é praticamente impossível, necessitando o lançamento destes de forma aleatória no ambiente a ser monitorado.

Dessa forma, essas aplicações requerem técnicas de redes *ad hoc* sem fio. Devido às restrições de recursos dos nós sensores, os vários algoritmos e protocolos já existentes para esse tipo de rede, não se aplicam às RSSFs, necessitando mudanças e adequações.

2.1 Características e desafios das RSSFs

Algumas características marcantes das RSSFs, que as diferenciam das redes *wi-fi* e *ad hoc* do ponto de vista de topologia e comunicação de rede, são:

- Os nós sensores são extremamente limitados em energia, processamento e memória se comparados com computadores convencionais. Isso acarreta que todo projeto de protocolo, sistema de segurança, ou outro mecanismo qualquer para RSSFs deve levar em consideração esses fatores. Dentre essas características, destaca-se o fator energético. Quanto maior a economia de energia que um protocolo favoreça, maior será o tempo de vida útil da rede. Isso é mais importante ainda ao se pensar que, na grande maioria das aplicações, é totalmente inviável e fora de propósito a troca das baterias dos nós sensores ou até mesmo a substituição destes, o que os torna praticamente descartáveis.

- A quantidade de elementos em uma rede de sensores é muito maior que em uma rede *ad hoc* de computadores convencionais. Isso se dá pelo tipo de aplicação em que as RSSFs estão destinadas, envolvendo geralmente a cobertura de uma grande área, e quanto maior o número de sensores, maior a área monitorada.

- Os nós sensores são muito mais sensíveis que os computadores convencionais, sendo extremamente mais suscetíveis à falhas no seu funcionamento.

- A topologia de uma RSSF muda constantemente devido a vários fatores como: fim da bateria, falha no dispositivo, troca de líder (para os protocolos chamados hierárquicos), etc. Dessa forma, não há uma topologia fixa e todo o roteamento e as atividades da rede estão em constante mudança.

- O principal meio de propagação de mensagens em uma RSSF é o *broadcast*, sendo que nas redes *ad hoc* é utilizada principalmente comunicação ponto a ponto.

Existem atualmente vários projetos acadêmicos que pesquisam os nós sensores e as RSSFs. *COTS Dust* [HIL 00]*, Smart Dust* [DUS 02]*, Wins* [WIN 05]*, Sensor Webs* [MIL 05], são alguns deles, apresentados na figura 2.

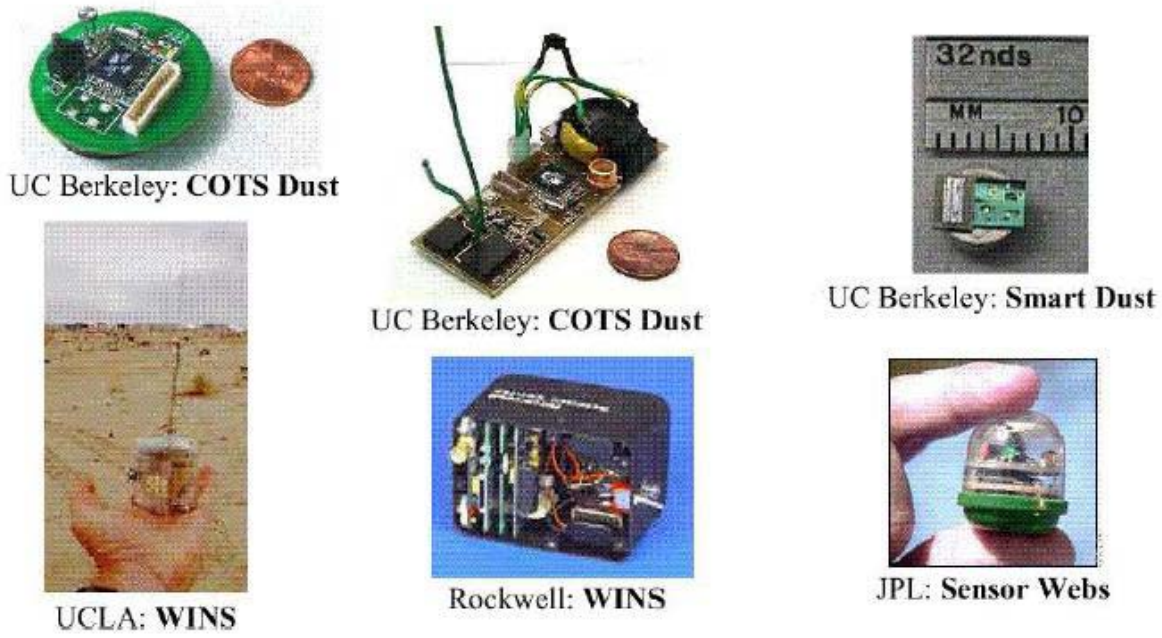


Figura 2: Alguns projetos de sensores

Um aspecto importante em todo sistema computacional é a segurança. Sistemas inseguros são suscetíveis a ataques, onde o atacante pode obter informações sigilosas do sistema, inserir dados falsos neste ou até mesmo inutilizá-lo. Em RSSFs esse fato não é diferente. Atualmente são conhecidos diversos tipos de ataques às RSSFs, onde o atacante pode tanto "roubar" informações da rede, prejudicar seu bom funcionamento ou até mesmo inserir informações falsas, eliminando a confiabilidade nos dados da rede. Um dos grandes problemas para a segurança das RSSFs situa-se nas restrições que estas possuem, do ponto de vista de *hardware*, que fazem com que todas as soluções já fundamentadas para segurança computacional de redes de computadores necessitem ser reinventadas ou no mínimo reformuladas para as RSSFs.

2.2 Pilha de protocolos

Sendo as RSSFs um tipo especial de rede, estas também possuem uma arquitetura de protocolos em camadas. Nas RSSFs as principais camadas são a camada física, camada de enlace de dados e a camada de rede. Apenas uma pequena quantidade de aplicações demanda a utilização de protocolos de camada de transporte. A seguir serão mostrados as camadas física, de enlace e de rede e seus principais protocolos.

2.2.1 Camada física

O objetivo da camada física é transmitir um fluxo bruto de bits de um dispositivo computacional para outro. Vários meios físicos podem ser usados pela transmissão real, cada uma possuindo seus próprios valores em termos de largura de banda, retardo, custo e facilidade de instalação e manutenção [TAN 03].

Em uma RSSF há três possibilidades para a comunicação sem fio:

- Ótica;
- Infravermelho;
- Rádio freqüência.

2.2.1.1. Comunicação ótica

A comunicação ótica é a que consome menor quantidade de energia por *bit* transmitido e não requer área física para instalação de antena, mas é necessário que o transmissor e o receptor estejam alinhados e sem obstáculos entre si (LOS – *Line of Sight*) para que ocorra a comunicação. Esse tipo de configuração não é viável em várias aplicações como, por exemplo, aquelas em que os nós são lançados aleatoriamente na área a ser monitorada. Esse tipo de comunicação também pode ser prejudicado por fatores atmosféricos. O nó sensor *Smart Dust* [DUS 02] utiliza esse tipo de comunicação de modo passivo, através de um *Corner Cube Reflector* (CCR) (0,5 x 0,5 x 0,1 mm3), transmitindo a uma taxa de 10 kbps, utilizando 1 mW de energia com uma área de alcance de 1 km. Outra opção no *Smart Dust* é a transmissão ativa através de *laser* (1,0 x 0,5 x 0,1 mm^3) transmitindo a 1 Mbps, com gasto de energia de 10 mW e área de alcance de 10 km. O volume total de um nó sensor *Smart Dust* chega a 1, 5 mm^3 e a massa total 5 mg, dimensões que tornam inviável o uso de transceptor de RF.

2.2.1.2. Infravermelho

As ondas milimétricas e infravermelhas sem guia são usadas em larga escala na comunicação de curto alcance. Os controles remotos utilizados nos eletrodomésticos utilizam comunicação infravermelha. Essas ondas são relativamente direcionais, baratas e fáceis de construir, mas possuem o inconveniente de não atravessarem objetos sólidos [TAN 03].

A comunicação infravermelha possui as seguintes características:

- Direcional;
- Alcance de aproximadamente um metro;
- Não é necessária área física para antena;
- Não atravessam objetos sólidos.

Ainda não há sensores disponíveis que utilizam esse tipo de comunicação.

2.2.1.3. Rádio Freqüência (RF)

As ondas de rádio são fáceis de gerar, percorrem longas distâncias, penetram objetos sólidos facilmente e, portanto, são largamente utilizadas para comunicação, sejam em ambientes fechados ou abertos. As ondas de rádio também são omnidirecionais, o que significa que elas percorrem todas as direções a partir da origem; ou seja, o transmissor e o receptor não precisam estar cuidadosa e fisicamente alinhados [TAN 03].

A comunicação em RF é baseada em ondas eletromagnéticas e um dos maiores desafios para o uso deste tipo de comunicação em RSSFs é o tamanho da antena. Para a otimização da transmissão e recepção, uma antena deve ser pelo menos "λ/4", onde λ é o comprimento da onda transmitida. Assumindo um nó sensor em que um quarto de comprimento de onda será 1 mm, a freqüência do rádio seria 75 GHz. Também é necessário reduzir o consumo de energia com modulação, filtragem, demodulação, etc. As vantagens da comunicação em RF são a facilidade de uso e a aceitação comercial, que tornam este tipo de comunicação viável para utilização em nós sensores. Vários aspectos afetam o consumo de energia do rádio, incluindo tipo de modulação, taxa de dados e energia de transmissão. Em geral, os rádios podem operar em quatro modos distintos: transmitindo, recebendo, "*idle*" (ativo, mas não executando nenhuma ação) e "*sleep*" (inativo, esperando algum evento para se tornar ativo). Muitos rádios que operam no modo "*idle*" consomem energia como se estivessem no modo de recepção, de forma que nestes casos é importante traçar outras estratégias para economia de energia [VIE 04].

Dois modelos de rádio têm sido usados comercialmente em nós sensores:

- TR1000 [TR1 04]: TR é um transceptor de rádio híbrido que suporta transmissão de dados em taxas superiores a 115.2 kpbs, possui alcance de 30 a 90 metros e opera em 3V. Consome aproximadamente 14.4 mW na recepção, 36 mW durante a transmissão e 15 μW no modo "*sleep*".

- CC1000 [CC1 04]: O rádio Chipcon CC1000 é um transceptor CMOS RF de baixo consumo de energia que atinge uma transferência de dados de até 76.8 kbps. Foi projetado

para modulação FSK (*Frequency Shift Key*) na faixa de banda ISM (*Industry Science Medical*) de 315, 433, 868 e 915 MHz. No modo de baixo consumo, a corrente consumida é de 0.2 μA. A tensão de operação varia de 2.1 a 3.6 V.

Outro exemplo que pode ser citado é o módulo de rádio do nó sensor WINS, o Conexant RDSSS9M que implementa uma comunicação RF *spread spectrum* em uma freqüência de 900 MHz (ISM *Industrial Scientific Medical*). O rádio opera em um dos 40 canais escolhido pelo controlador. O rádio é capaz de operar a vários níveis de energia para transmissão, podendo variar de 1 mW até 100 mW, permitindo assim o uso de algoritmos de otimização do consumo de energia para a transmissão.

2.2.2. Camada de Enlace

As RSSFs são diferentes das redes tradicionais mas herdaram os problemas de comunicação das redes sem fio. Na maior parte dos casos, as redes sem fio empregam um rádio de um único canal com modo de comunicação *half-duplex* (comunicação bidirecional e não simultânea). O rádio, utilizando a mesma freqüência, pode somente transmitir ou receber informações a cada instante. Sendo assim, o método empregado nas tradicionais redes Ethernet, CSMA/CD (*Carrier Sense Multiple Access with Collision Detect*) não pode ser empregado em redes sem fio [TAN 03].

As redes sem fio utilizam o protocolo CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) [KUR 06] para controle de acesso ao meio, o que evita a ocorrência de colisões. O CSMA/CA utiliza um diálogo de três passos: *RTS-CTS-DATA* (*Request To Send – Clear To Send - Data*) envolvendo a comunicação entre duas estações transmissora e receptora. É importante observar que nas redes sem fio as colisões só ocorrem no receptor, já que é impossível ao transmissor escutar o canal. As colisões podem ocorrer na recepção de pacotes de controle e de dados. As estações na rede ao escutarem pacotes de controle RTS ou CTS não destinados a elas, devem bloquear suas transmissões até o final da transmissão de terceiros. Este procedimento diminui a probabilidade de ocorrência de colisões na rede. As colisões em redes sem fio também ocorrem por um problema conhecido como terminal escondido: Uma estação A transmite uma mensagem RTS para uma estação B dentro de seu alcance de rádio. Uma outra estação C, que está dentro do alcance de rádio de B, mas fora do alcance de A, também envia um RTS para a estação B. Para esta situação haverá colisão na estação B.

As restrições dos protocolos empregados em RSSFs são ainda maiores que as restrições das redes MANETs (*Mobile Ad-hoc NETworks*), devido ao hardware empregado. Desta forma, não existe suporte pelo *hardware* para detecção de onda portadora, detecção de colisão, enquadramento específico, codificação ou balanceamento de energia. O rádio utilizado possui características de baixa potência, largura de banda limitada e um único canal na freqüência base ISM.

Alguns exemplos de protocolos de camada de enlace:

- S-MAC [YE 02]: protocolo de acesso ao meio que faz uso de alocação dinâmica do canal, mas utiliza sincronização para coordenação dos modos de operação do rádio. As aplicações ideais para a utilização do S-MAC são as dirigidas a eventos com coleta periódica de dados, insensíveis à latência e com baixa taxa de envio de mensagens.

- B-MAC [POL 03]: Ao invés de inserir o algoritmo de *backoff* inicial dentro da camada MAC, este protocolo estabelece uma política de gerenciamento em que a aplicação controle o *backoff* inicial antes de submeter um pacote para transmissão. O algoritmo de *backoff* binário exponencial não é usado, ao invés disso é verificado o estado do canal. O B-MAC utiliza a heurística chamada CCA (*Clear Channel Assessment*) para verificar se existe atividade no canal e para retornar a informação para a aplicação. O CCA emprega a técnica de julgamento de canal baseado em uma estimativa de ruído do canal obtida pela força do sinal recebido RSSI (*Received Signal Strenght Indicator*).

- TRAMA [RAJ 03]: O protocolo TRAMA (*Traffic adaptive Multiple Access*) é baseado em alocação estática de canal TDMA. É projetado para aplicações dirigidas a eventos com coleta contínua ou periódica de dados. Tem como objetivo ser eficiente em energia e o método de acesso ao canal garante que não existirão colisões em comunicações *unicast, broadcast* ou *multicast*. O TRAMA emprega um algoritmo de eleição para determinar qual nó pode transmitir em determinado intervalo de tempo (*time-slot*), e não faz reserva para os nós sem tráfego de envio.

- ARC [WOO 01]: O ARC (*Adaptive Rate Control*) tem como metas a alocação de largura de banda e eficiência em energia para condições de tráfego alto e baixo da rede. É proposto um mecanismo dinâmico que passivamente adapta as taxas de transmissão dos dois tipos de tráfego: de passagem e de dados originados. É utilizado um novo esquema CSMA, que é

composto pelas seguintes fases: atraso inicial aleatório, tempo de escuta – intervalo fixo de tempo, e mecanismo de *backoff* – tempo de atraso gerado com janela fixa, com incremento ou decremento binário exponencial.

O ARC em conjunto com este novo esquema CSMA fornece controle efetivo de acesso ao meio sem a utilização explícita de pacotes de controle. É eficiente para situações de baixo tráfego.

2.2.3. Camada de Rede

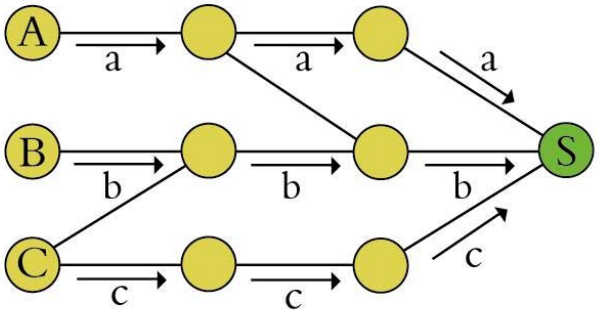
A principal função da camada de rede é prover o roteamento, que pode ser definido como o processo pelo qual a rede consegue identificar o destinatário das mensagens e encontrar um caminho entre origem e destino destas. Como em todos os tipos de redes de computadores, essa camada é muito importante, e em RSSF não poderia ser diferente. A camada de rede de uma RSSF é tão importante que grande parte da eficiência da rede será dada pela forma com que é feito o roteamento das mensagens que transitam nesta.

A comunicação típica de uma RSSF é direcionada no sentido dos nós fontes para o nó *sink*, como um *multicast* invertido. Os dados dos nós fontes em geral referem-se a um fenômeno comum (a leitura de um determinado valor de uma grandeza física, por exemplo), portanto, existe a probabilidade de redundância dos dados transmitidos. Outro aspecto que normalmente ocorre nas RSSFs trata da pouca ou nenhuma mobilidade dos nós sensores. Finalmente, a principal restrição nas RSSFs é a limitação de energia. Esta limitação é crítica, pois os dispositivos geralmente possuirão um funcionamento autônomo, não prevendo a recarga ou troca das baterias.

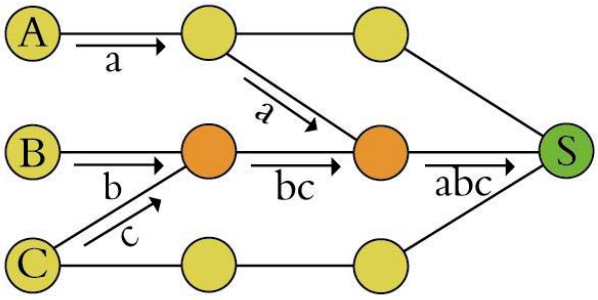
Neste contexto de severas limitações, a fusão/agregação de dados tem sido apontada como uma opção que permite otimizar a operação das RSSFs [HEI 01]. Essa abordagem visa reduzir a ocorrência de redundâncias e o número de transmissões para economizar energia através de um pré-processamento dos dados dentro da rede. Este paradigma modifica o foco da abordagem tradicional da camada de rede, centrada em endereço, para uma abordagem nova, centrada em dados, que permite a redução de dados redundantes. A figura 2.3 exemplifica uma operação de agregação de dados.

Na figura, os nós ***A***, ***B*** e ***C*** enviam mensagens para o nó *sink* ***S***. No roteamento centrado em endereços, sem fusão/agregação, a emissão desses dados gera nove mensagens. No roteamento centrado nos dados, utilizando fusão/agregação, a emissão dos mesmos dados gera seis mensagens. Isso se dá pelo fato de, ao passarem pelos nós em laranja, essas

mensagens são fundidas. O primeiro recebe as mensagens ***a*** e ***b*** e as funde na nova mensagem ***ab***. O segundo nó funde as mensagens ***ab*** e ***c*** na mensagem ***abc***. Dessa forma, claramente, há economia de energia na rede, já que o número de mensagens transmitidas é reduzido.



(a)- Roteamento sem fusão/agregação



(b)- Roteamento com fusão/agregação

Figura 3: Agregação de dados [LIN 04]

2.2.3.1. Endereçamento em RSSFs

O endereçamento em redes tradicionais tem como propósito prover informações referentes à topologia da rede, auxiliando assim a procura por rotas. Uma propriedade importante para as redes tradicionais é a existência de um endereço global único, que permite que qualquer nó seja identificado, permitindo assim o estabelecimento de conexões, por exemplo, como o endereço IP. Um custo referente a esse tipo de endereçamento dá-se na exigência de espaço (*bits*) suficiente para identificar cada um dos nós da rede. Assim, quanto maior o número de nós, maior deverá a quantidade de *bits* necessária para seus endereços. Nas redes tradicionais isso não chega a ser um problema, mas nas RSSFs, cada *bit* transmitido reduz o tempo de vida da rede [POT 00]. O tempo de vida da rede está diretamente ligado ao

consumo de energia desta. Portanto, se o consumo é minimizado, maior será o espaço de tempo que a RSSF se manterá em funcionamento. Outro fator que influencia é que em uma RSSF o número de elementos pode ser da ordem de milhares, fazendo com que os mecanismos de endereçamento tradicionais custem muito, do ponto de vista do consumo de energia. Uma característica das RSSFs é que geralmente as aplicações destas não necessitam a identificação de um nó específico, sendo as consultas feitas com o objetivo de extrair dados de uma região da área de cobertura da rede. Em conseqüência disso são necessários outros tipos de soluções que atendam às restrições das RSSFs, como o endereçamento espacial, baseado em atributos e de transações.

Endereçamento espacial: Tipicamente as aplicações de RSSFs estão interessadas na extração de dados de uma região, e não de um nó individual. Uma consulta é feita na região desejada, e qualquer nó presente nessa região pode respondê-la [EST 00].

O endereçamento espacial referencia nós individuais ou grupos de nós através da sua localização geográfica. O tamanho do endereço (codificação das coordenadas geográficas) depende de fatores como a granularidade (precisão) da localização, do tamanho da região a ser monitorada e da quantidade de nós a serem endereçados. Estes fatores podem dificultar a escalabilidade deste esquema, tornando o endereço muito grande em relação aos dados que estão sendo transmitidos.

Endereçamento baseado em atributos: A idéia de nomeação de dados para RSSFs tem origem em algoritmos como o pioneiro SPIN (*Sensor Protocols for Information via Negotiation*) [HEI 00a], onde os dados são identificados por metadados (descritores). Entretanto, o SPIN assume um endereçamento global dos nós sensores.

Na classe de endereçamento baseado em atributos, a comunicação baseia-se em atributos externos à topologia e relevantes para a aplicação. Esta forma de endereçamento utiliza a nomeação de dados mudando o foco do endereçamento dos nós e sua localização para os dados em si. Neste esquema, os atributos, utilizados para descrever ou nomear um dado, são identificados por chaves únicas que são distribuídas por uma unidade central. A solução proposta utiliza o protocolo de Difusão Direcionada [INT 02], regras de casamento de padrões e filtros para viabilizar a comunicação e disseminação de dados.

Endereçamento de transações: Em [ELS 01] é proposto um tipo de endereçamento para RSSFs chamado RETRI (*Random Ephemeral TRansaction Identifiers*). No RETRI os

nós selecionam identificadores probabilisticamente únicos para cada nova transação. Uma transação é definida por qualquer atividade computacional na qual é necessário manter algum estado entre os nós envolvidos.

O RETRI determina que quando for necessário um identificador único, esse é gerado de maneira aleatória. Se dois nós utilizarem o mesmo identificador ao mesmo tempo, ocorre uma colisão de identificadores, resultando na perda da transação que deve ser tratada como uma perda qualquer. Neste esquema, para cada pacote é atribuído um identificador aleatório e todos os seus fragmentos recebem o mesmo identificador, permitindo a sua reconstrução do lado do receptor. A cada novo pacote é atribuído um novo identificador aleatório. Nesse caso uma transação é considerada a transmissão de todo o conteúdo (fragmentos) de um pacote.

2.2.3.2. Protocolos de camada de rede

Os protocolos de camada de rede em RSSFs podem ser divididos em três tipos: plano, hierárquico e geográfico.

O **roteamento plano** [LIN 03] encara todos os nós como idênticos, do ponto de vista funcional, ou seja, a atividade de roteamento é tratada de forma idêntica por todos os elementos da rede. Alguns exemplos de protocolos de roteamento plano são:

- Difusão Direcionada [INT 00]: Propõe um algoritmo que possui como meta o estabelecimento de canais de comunicação eficientes entre os nós sensores e a estação-base. Este algoritmo introduz dois novos conceitos: roteamento baseado nos dados e a agregação de dados. O roteamento baseado nos dados ocorre através da requisição de informação de interesse. Quando algum nó possui alguma informação que é de interesse de outro nó, ele envia esta informação ao nó que requisitou tal informação. O outro conceito, agregação de dados, significa que nós intermediários podem agregar seus dados em pacotes mais simples, reduzindo assim as transmissões e o volume total de dados transmitidos.

O protocolo funciona através da disseminação de uma requisição de sensoriamento pela rede, na forma de um interesse. Os nós que originam o interesse determinam um valor mínimo para que este seja respondido e informam também um ou mais nós de um caminho preferível para a entrega dos resultados. Os nós que possuírem esse tipo de leitura, respondem ao interesse.

- SPIN [HEI 99]: O SPIN (*Sensor Protocols for Information via Negotiation*) utiliza informações sobre a quantidade de energia disponível em cada nó para executar o roteamento. Protocolos de negociação são utilizados para disseminar as informações de um nó sensor para todos os outros da rede. Quando um nó se encontra com um nível de energia próximo a um limite pré-estabelecido, ele passa a participar menos da disseminação dos dados.

O SPIN possui três estágios: se um nó possui novos dados a serem transmitidos, esse transmite uma mensagem ADV contendo meta-dados (estágio ADV) para seus vizinhos. Ao receber um ADV, os vizinhos verificam se possuem os dados requeridos ou se já requisitaram tal dado. Se não possuem, é enviada ao nó que iniciou a disseminação uma mensagem de requisição de dados (estágio REQ). O nó então responde ao REQ com uma mensagem de dados (estágio DATA). Após receber o dado, o nó vizinho envia uma mensagem ADV a todos os seus vizinhos, informando que possui um dado novo e que ele quer repassá-lo, dando continuidade ao ciclo.

- SAR [SOH 00]: O SAR (*Sequential Assignment Routing*) visa facilitar o roteamento *multi-hop*. O objetivo deste algoritmo é minimizar a média ponderada de métricas de qualidade de serviço (QoS – *Quality of Service*) através do tempo de vida da rede. Considera os recursos de energia e as métricas de QoS de cada caminho e a prioridade dos pacotes. A idéia é prover cada pacote com um coeficiente de QoS relativo a sua prioridade.

- Multi [FIG 04]: O Multi, Protocolo Adaptativo Híbrido para Disseminação de Dados em RSSFs, consiste em uma nova abordagem para os protocolos. O Multi leva em consideração, por exemplo, aplicações que são disparadas por eventos. Esse tipo de aplicação pode ter grandes períodos de inatividade, e em instantes, pode ocorrer uma grande quantidade de dados sendo transmitidos. O Multi atua na análise do tráfego e, para cada instante da rede, altera o protocolo de disseminação, visando uma maior economia de energia e otimização da rede.

- TinyOSBeaconing [BEA 04]: O TinyOS Beaconing é o protocolo de roteamento utilizado nos nós sensores da plataforma Mica Motes da Universidade de Berkeley, e tem como característica o funcionamento em redes com *hardware* restrito. O protocolo constrói periodicamente uma árvore de caminho mínimo (*Minimum Spanning Tree*) a partir da estação-base. A estação-base propaga uma mensagem, chamada de *beacon*, que é propagada na rede com o intuito de criar a árvore de roteamento. Por se tratar de um protocolo simples e geral, seu desempenho é inferior a protocolos desenvolvidos para aplicações específicas.

- PROC [MAC 04]: PROC (*Proactive Routing with Coordination*) é um protocolo de roteamento desenvolvido para redes de sensores homogêneas e estacionárias, onde nós enviam dados periodicamente para uma estação-base. Utiliza o conceito de coordenadores para construir um *backbone* de roteamento em forma de árvore com raiz na estação-base. Os nós que não pertencem ao *backbone* conectam-se diretamente a um nó coordenador. O *backbone* é reconstruído periodicamente, para que o consumo seja balanceado.

No **roteamento hierárquico** [LIN 03] da camada de rede das RSSFs há uma diferenciação entre os elementos que compõem a rede, podendo existir duas ou mais classes de elementos. Basicamente, uma classe de nós fica encarregada das atividades normais e a outra classe se encarrega de receber e transmitir as mensagens enviadas pelos elementos da primeira classe, destinadas à estação-base. Geralmente esse tipo de protocolo promove a formação de grupos (*clusters*) onde há um líder para cada grupo (*cluster-heads*). Os elementos centralizadores (líderes) executam operações de fusão e/ou agregação dos dados, diminuindo assim a quantidade de mensagens transmitidas pela rede, economizando energia. Tanto os elementos comuns quanto os elementos centralizadores podem ser idênticos do ponto de vista de *hardware*. Exemplos de protocolos desse tipo:

- LEACH [HEI 00a]: O LEACH (*Low-Energy Adaptive Clustering Hierarchy*) tem por objetivo reduzir o consumo de energia, sendo desenvolvido para redes homogêneas e utiliza ciclos durante os quais são formados agrupamentos de nós, denominados *clusters*, onde um nó é escolhido como líder. O líder do *cluster* é responsável por repassar os dados dos elementos de seu *cluster* para a estação-base com um único *hop*, o que limita o tamanho da rede em função do raio de alcance do rádio.

- LEACH-C [HEI 00b]: É uma variação do LEACH, que centraliza as decisões de formação dos grupos na estação-base. A maior vantagem desta abordagem centralizada é a criação e distribuição mais eficiente de grupos, na rede. Cada nó, na fase de inicialização da rede, envia sua posição geográfica e energia disponível para a estação-base. Baseando-se nesta informação, a estação através de processos de *simulated anneling*, determina os grupos de forma centralizada. Quando os grupos e seus líderes são determinados a estação-base envia uma mensagem que contém o identificador do líder para cada nó. Após isso, o comportamento é idêntico ao LEACH.

- PEGASIS [LIN 02]: O PEGASIS (*Power-Efficient Gathering in Sensor Information Systems*) é um protocolo para RSSF baseado no conceito de correntes. Cada nó troca informações apenas com os vizinhos mais próximos formando uma corrente entre eles, e apenas um nó é escolhido para transferir as informações coletadas ao nó *gateway*, dessa forma, o número de trocas de mensagens será baixo e a comunicação será realizada entre nós próximos uns dos outros. Com isso, a energia gasta é menor se comparada a outros protocolos que requerem muitas trocas de mensagens.

- TEEN [MAN 01]: O TEEN (*Threshold sensitive Energy Efficient sensor Network*) é um algoritmo similar ao LEACH exceto pelo fato de que os nós sensores podem não possuir dados a serem transmitidos de tempos em tempos. O TEEN utiliza a estratégia de formação de líder do LEACH, mas adota uma maneira diferente na fase de transmissão de dados. Há dois parâmetros chamados *Hard Threshold* (Ht) e *Soft Threshold* (St) para determinar a necessidade de transmissão do dado coletado. Se o valor exceder *Ht* pela primeira vez, ele é armazenado em uma variável e transmitido durante o intervalo de tempo alocado para a transmissão do nó. Se em seguida o valor monitorado exceder o valor armazenado por uma magnitude *St*, o nó transmite o dado imediatamente. O valor enviado é armazenado para comparações futuras.

O **roteamento geográfico** utiliza informações geográficas para rotear os dados. Estas informações podem incluir a localização dos nós vizinhos. Os dados de localização podem ser definidos a partir de um sistema de coordenadas globais (GPS – *Global Positioning System*) ou mesmo de um sistema local válido somente para os nós da rede ou válidos somente para um subconjunto de nós vizinhos. Exemplos de protocolos de roteamento geográficos:

- GEAR [YU 01]: O GEAR (*Geographical and Energy Aware Routing*) é um protocolo de roteamento geográfico que procura minimizar o consumo de energia da rede. O repasse de dados utiliza um algoritmo do tipo “guloso”, onde o nó que irá repassar os dados é aquele que possui o menor custo de envio até a região desejada. O custo de envio é calculado em função da distância e energia residual dos nós que compõem a menor rota até a região especificada. Esse protocolo diferencia-se dos outros algoritmos geográficos por utilizar informações de toda a rota até o destinatário.

- GeoMote [BRO 04]: No GeoMote (*Geographic Multicast for networked sensors*), o endereçamento dos destinatários é feito através de polígonos. Desta forma é possível realizar comunicações *multicast* localizadas. No GeoMote, cada nó possui uma função específica durante o tempo de vida da rede, definida no momento da sua programação. Há três categorias de nós sensores: GeoHosts (produtores de dados), GeoRouters (que repassam dados produzidos pelos GeoHosts) e os GeoGateways (que atuam como pontos de entrada e saída de dados).

- GPSR [KAR 00]: O GPSR (*Greedy Perimeter Stateless Routing*) utiliza dois algoritmos para rotear dados. Quando um nó identifica um vizinho que está mais próximo do destino, o protocolo repassa os dados para este vizinho. Se não existe um vizinho mais próximo, o pacote deve ser repassado para um nó mais distante, para evitar uma região onde a cobertura de nós é baixa. Como vantagens do protocolo podemos destacar o uso de informações locais da vizinhança para roteamento e o uso de algoritmos geométricos simples, que possibilitam a implementação do protocolo em nós sensores com poucos recursos de memória e processador. Para a criação da tabela com todos os nós da rede, os nós trabalham em modo promíscuo, armazenando as informações de localização contidas nos pacotes interceptados. Com isso, é facilitada a atualização dos dados geográficos, mas há um gasto adicional de energia, devido ao rádio estar sempre ligado.

2.3 Simulação de redes sem fio

Uma técnica amplamente utilizada em pesquisas de redes, inclusive as sem fio, é do uso de simuladores. Através destes é possível definir e controlar um cenário para testes e avaliações.

Devido às características peculiares das RSSFs, esse tipo de artifício torna-se ainda mais interessante. A simulação de RSSFs permite uma maior escalabilidade do sistema, podendo avaliar situações onde há de centenas a milhares de elementos, um cenário real que seria difícil de se obter.

Para simulação de RSSF destacam-se dois simuladores:

- J-SIM [JSI 06] - O J-SIM é um simulador Java baseado em componentes para simulação animada de ambientes. A entidade básica no J-SIM são os componentes, mas ao contrário de outros *softwares* baseados em componentes, neste simulador estes são autônomos. Desde 2003 possui suporte para simulações para RSSF.

- NS-2 [NS2 06] – O NS-2 (*Network Simulator*) é um simulador de eventos discretos projetado para pesquisas sobre redes. Possui suporte para as mais variadas simulações como TCP/IP, roteamento, protocolos multicast, redes cabeadas e sem fio. Utiliza a linguagem TCL [TCL 06] para a elaboração de *scripts* que definem o cenário e o comportamento das conexões. Por sua grande flexibilidade e customização, o NS-2 permite a criação de protocolos de diversos tipos e topologias de redes, incluindo as RSSFs, como descrito em [DOW 04]. O modelo de simulação de redes sem fio do NS-2 suporta movimentação de nós e restrições energéticas.

3. Segurança em RSSF

Uma das áreas com grande volume de pesquisa, em se tratando de RSSFs, é a segurança computacional destas.

As RSSFs apresentam dois problemas fundamentais no que diz respeito à segurança computacional, problemas que as diferem das redes sem-fio comuns: a drástica limitação de recursos energéticos e o *hardware* extremamente limitado. Esses fatores influenciam diretamente em qualquer abordagem que se queira propor para a segurança de RSSFs, fazendo com que o assunto se torne muito mais complexo do que nas redes convencionais.

3.1. Requisitos de segurança de uma RSSF

Como em todo sistema computacional, deseja-se que em uma RSSF haja segurança necessária para que sempre estejam garantidos os seguintes aspectos [GTA 04]:

- **Disponibilidade:** As RSSFs devem estar disponíveis sempre que forem necessárias. Devem ser evitados ataques do tipo *DoS*, pois estes exaurem os recursos dos nós.

- **Confidencialidade:** Os dados que trafegam nas RSSFs não devem ser "entendidos" por elementos fora desta (criptografia).

- **Autenticidade de nós e dados:** Garante que toda informação é inserida na RSSF somente por nós válidos, evitando-se que intrusos injetem informações falsas na rede.

- **Atualização dos dados:** Garante que os dados recebidos da RSSF são válidos e atualizados.

- **Integridade dos dados:** Garante que o dado recebido não foi alterado durante a transmissão.

Toda e qualquer tentativa de se violar qualquer um desses aspectos, prejudicando o correto funcionamento de uma RSSF, seja impossibilitando suas transmissões ou inviabilizando suas informações, é classificada como um ataque.

3.2. Ataques mais comuns a RSSF

A literatura apresenta vários tipos de ataques contra RSSF. Como a grande maioria dos protocolos utilizados nesse tipo de rede não possui nenhum mecanismo de segurança, a chance de sucesso desses ataques é muito grande. Em [KAR 03] são descritos os principais tipos de ataques às RSSFs como abaixo:

- ***Spoofing*:** Consiste em interceptar, alterar e gerar informações falsas tanto de roteamento quanto de leitura, causando problemas como *loops*, rotas falsas, dados irreais, etc. Geralmente essas informações são originadas por sensores invasores à rede.

- **Encaminhamento seletivo:** Um nó malicioso não repassa certos tipos de pacotes, causando perda de informação. O aviso que um certo evento ocorreu pode ser perdido.

- **Ataque buraco negro (*Black Hole*):** Um nó malicioso com valores atraentes de características como atraso, número de saltos ou potência de sinal é infiltrado na rede. Este nó se torna a melhor escolha, dependendo do protocolo de comunicação, e atrai para si todo o tráfego dos nós vizinhos. Dessa forma, o tráfego não chega a seu verdadeiro destino.
- **Ataque *Sybil*:** Em sistemas que estabelecem rotas redundantes, um nó malicioso se faz passar por vários, controlando assim grande parte da rede. Um nó qualquer da rede "enxerga" vários elementos onde na verdade só há um.

- ***Wormholes*:** Dois nós maliciosos podem criar um caminho clandestino entre si, como um túnel, particionando assim a rede. Cada um dos nós maliciosos convence os vizinhos através de métricas falsas de que são as melhores opções de caminho. O fluxo de informação é então desviado pelo "túnel", isolando as partições da rede. Geralmente um dos nós maliciosos se encontra dentro da rede atacada e o outro em uma rede à parte, controlada pelo atacante.

- **Inundação de *Hello*:** Alguns protocolos de roteamento utilizam mensagens para identificar os vizinhos (por exemplo, mensagens do tipo *Hello*). Um nó malicioso com um transmissor potente pode enviar esse tipo de sinal para a rede toda, atraindo grande parte do tráfego para si. Esse ataque também pode resultar em um *DoS*, exterminando os recursos dos nós, devido à grande quantidade de transmissões.

- ***Spoofing* de confirmação:** Um nó malicioso insere informações falsas, fazendo com que um nó fora de operação ou um canal ruim pareçam estar funcionando corretamente.

- **Anel da maldade (*Evil Ring*):** Vários nós maliciosos circundam a rede ou parte dela, dificultando e alterando as transmissões da região do interior do anel.

A figura 3.1 exemplifica alguns dos diversos tipos de ataques dentro de uma RSSF previamente estabelecida.

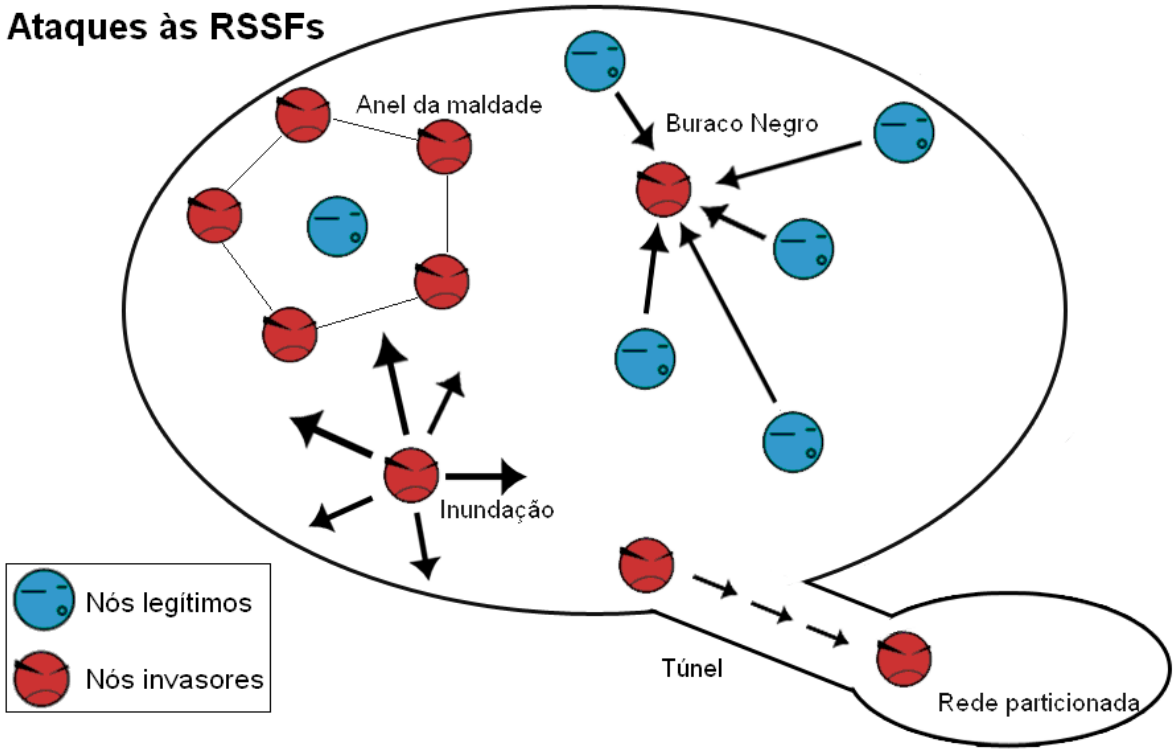


Figura 4: Alguns ataques às RSSFs

Como pôde ser constatado, todo ataque citado acima é originado através da inserção de nós maliciosos na rede, e esses nós interagem com a rede no momento do ataque. O invasor pode tanto retirar informações da rede para uso próprio, forjar informações (o que levaria à interpretação errônea dos fatos pela estação-base) ou até mesmo simplesmente impossibilitar que informações cheguem até a estação-base, inutilizando a rede e seu propósito. Algumas propostas foram feitas na tentativa de combater tais ameaças como em [KAR 03][SAN 04][NEW 04][WOO 02], mas essas sempre são específicas a um tipo de ataque, identificando-o e propondo uma solução através das conseqüências que esses acarretam.

Chris Karlof e David Wagner apresentam em [KAR 03] vários tipos de ataques e, para cada um deles, são propostas medidas de contenção específicas. São propostas para os ataques do tipo *Sybil*, inundação e *spoofing* soluções baseadas em criptografia, autenticação de nós e mensagens. É admitida a dificuldade de se lidar com ataques do tipo buraco negro e *wormhole*. Germano Guimarães e colegas avaliam em [GUI 04] alguns métodos de criptografia e sua viabilidade para as RSSFs, concluindo que é possível sua utilização, mas com um acréscimo no consumo de energia da rede. Em conseqüência disso, o uso de um método criptográfico em todo o tráfego da RSSF, faz com que sua vida útil seja reduzida.

Outro fator seria que, por ser mais simples e menos custosa, a criptografia para RSSFs deve ser de chave simétrica, sendo esta inserida no nó no momento de sua programação. Nesse caso, há a ameaça de um dos elementos da rede ser "seqüestrado" e, através deste, o atacante pode obter a chave utilizada, inserindo-a nos sensores invasores.

Serdan Sancak e colegas [SAN 04] apresentam uma solução para ataques do tipo *flooding* ou *spam attacks*. Os ataques são detectados mediante a análise da freqüência das emissões de mensagens em uma determinada região, assim como através da análise contra mensagens mal formadas. Trata-se de uma solução problemática, pois se um sensor invasor não gerar mensagens mal formadas e essas ocorrerem com uma freqüência tida como normal, não será identificado como invasor.

James Newsome e colegas [NEW 04] encarregam-se de ataques do tipo *Sybil*, propondo soluções para este tipo de ameaça específica. São propostas várias maneiras de se utilizar chaves simétricas na autenticação dos nós sensores. O próprio artigo não apresenta uma solução única para todas as variações do ataque, e sim uma solução para cada tipo e, por se tratar de uma solução baseada em criptografia, as mesmas observações para [KAR 03] podem ser feitas aqui.

Antony D. Wood e colegas [WOO 02] tratam da ameaça do *DoS* (*Denial of Service*) nas RSSFs. A análise do ataque é feita em vários níveis (camadas física, enlace e rede) propondo soluções como mapeamento da região, autenticação e autorização. Novamente, somente esse tipo de ataque específico é evitado, e a utilização de criptografia acarreta os mesmos problemas de [KAR 03].

O maior problema apresentado por todas essas abordagens situa-se na especificação do ataque que estas propõem solucionar. Dessa forma, cada solução fica atrelada a um tipo específico de ataque falhando na detecção de um outro qualquer. Além disso, a maioria identifica o ataque a partir de suas conseqüências, ou seja, após este ter sido aplicado dentro da rede. Os ataques citados possuem em comum o fato de serem iniciados através da invasão da rede já estabelecida, por nós maliciosos. Isso mostra que se esse acontecimento (a invasão da rede) for detectado resultará em vantagens no combate às ameaças tais como: antecipação do disparo de contramedidas, já que não é preciso que o ataque seja de fato aplicado para que se identifique que a rede está sob ameaça, e a generalidade da solução já que esta não identificaria especificamente um tipo de ataque.

Esse trabalho apresenta maneiras de se identificar o fato da rede ter sido vítima de uma invasão gerando soluções não atreladas aos ataques que por ventura os atacantes desencadeariam. Essa identificação é feita através do monitoramento de características

intrínsecas das RSSF, características essas que sofrem alterações no caso da rede ter sido invadida. Essas características serão discutidas no próximo capítulo.

4. Características intrínsecas das RSSFs.

As RSSFs constituem um tipo especial de rede devido a vários fatores como, por exemplo, a natureza dos elementos que as compõem, sua dinamicidade topológica, aplicações peculiares, locais de atuação, entre outros. Especialmente, nesse trabalho foram utilizadas duas dessas características:

- Número decrescente de elementos e

- Média energética residual decrescente.

As próximas seções apresentarão estas características em detalhes.

4.1. Número de elementos

Devido à fragilidade dos nós sensores, as RSSFs se tornam dinâmicas do ponto de vista topológico. Ao serem lançados no ambiente em que atuarão, vários fatores influenciam no número de sensores. Alguns nós podem perder contato com a rede, de maneira que fiquem isolados, outros podem sofrer anomalias físicas, como falha de *hardware*, e apresentar-se de forma inapropriada para o bom funcionamento. Com o decorrer do tempo, essa característica torna-se ainda mais marcante, mediante ao tempo de vida útil da bateria dos sensores, que faz com que alguns deles se tornem inoperantes primeiro que outros. Dessa forma, salvo o caso onde há inserções consentidas de novos elementos na rede, o número de nós sensores é decrescente durante toda a vida útil da rede. Se há inicialmente uma quantidade x de sensores lançados em um ambiente, esse número sempre se reduzirá da seguinte maneira:

x(t) = [nós iniciais – (nós isolados inicialmente + nós defeituosos + nós sem energia)](t)

Onde **x** é o número de nós sensores na rede no instante t.

Essa característica mostra que se, em um determinado momento, o número de nós sensores aumentar, mesmo que seja em uma simples unidade, uma invasão por sensores externos à rede original é caracterizada.

4.2. Média do nível energético dos elementos da rede

Todo dispositivo eletrônico consome energia para se manter em funcionamento. Os nós sensores não fogem a essa regra. Com o passar do tempo, a energia da bateria dos nós sensores diminui. Devido a esse fato, é possível afirmar que, ao longo do tempo, a média do nível de energia dos elementos de uma RSSFs é sempre decrescente. Esta média energética é calculada da seguinte forma:

$$y(t) = \frac{\sum \text{Nível de energia de cada elemento na rede } (t)}{\text{Número de elementos que iniciaram a rede em } t_0}$$

Onde **y** representa a média energética por elemento no instante t e t_0 é o instante inicial da rede. Por se tratar de uma razão entre a somatória de toda energia residual na rede no instante t pelo número de elementos que iniciaram a rede no instante t_0, o valor de **y** tende e sempre a decrescer. Esse fato indica que se, em um determinado momento, a média de energia residual existente na rede aumentar, houve o acréscimo de elementos no conjunto original.

Atualmente vários estudos sobre a energia remanescente de uma RSSF através do tempo têm sido feitos como, por exemplo, [MIN 04][SOU 05]. Esses estudos são desenvolvidos na tentativa de projetar novos protocolos de rede que tenham como característica uma melhor economia energética, ponto crucial em qualquer projeto de protocolos para RSSFs.

4.3. Detecção de invasão através das características intrínsecas da rede

As abordagens propostas em [KAR 03][SAN 04][NEW 04][WOO 02] visam detectar e prevenir ataques específicos, deixando toda a rede suscetível a algum ataque de outra natureza. O fato dos ataques apresentados possuírem como ponto em comum a invasão da

rede por nós maliciosos indica que, se detectado esse fato, é possível gerar soluções genéricas, que não sejam específicas para cada tipo de ataque.

Como mostrado nas seções anteriores, as RSSFs possuem características intrínsecas que são afetadas caso haja uma invasão. Isso indica que, através do monitoramento dessas características, é possível a identificação de invasões na rede no momento em que for constatada uma alteração nesses atributos.

4.3.1. Contagem dos nós

Para a utilização da primeira característica, que trata do número sempre decrescente de nós em uma RSSF, é necessário um controle de quantos elementos compõem a rede durante seu funcionamento. Dessa forma, a qualquer momento, o aparecimento de elementos extras ilegais no conjunto que forma a rede, claramente indica a presença de nós invasores. Para que essa característica seja utilizada, é necessário que todo o sistema esteja ciente do número de elementos que compõem a rede. A própria rede ou aplicações implementadas sobre ela devem possuir formas de estarem sempre cientes do número de elementos que a compõem possibilitando a identificação de um acréscimo neste número, denunciando assim uma invasão [PAU 05].

4.3.2. Monitoramento da média energética

A utilização da característica energética para detecção de intrusão pode ser feita através do monitoramento da média da energia residual presente na rede. Com o passar do tempo os nós sensores consomem energia para se manter em funcionamento, isso faz com que a energia residual da rede tenda sempre a decrescer. A constatação de que a média energética residual sofreu um acréscimo indica que novos elementos foram inseridos na rede de forma ilegal, o que caracteriza uma invasão. Para a utilização dessa característica, é necessário que a própria rede ou aplicações implementadas sobre ela possuam formas de estarem sempre aptas a monitorar a média energética, identificando invasões através do possível acréscimo deste montante.

4.4. Abordagem utilizada

A abordagem utilizada para a análise e avaliação dessas afirmativas foi a incorporação do monitoramento desses atributos em um protocolo de rede para RSSF, de forma que esta se torne apta a contabilizar o número de elementos que a compõem e monitorar a média energética desta durante seu tempo de funcionamento. O próximo capítulo apresenta detalhadamente todo o trabalho desenvolvido.

5. Mecanismos de monitoramento das características da rede

Como foi mostrado, a existência de um mecanismo que mantenha sempre em monitoramento o número de elementos da rede e a sua média energética auxilia na identificação de invasão em RSSFs. Dessa forma é criada uma solução genérica, não atrelada a um tipo de ataque ou às conseqüências desses, permitindo o disparo de contramedidas em um curto período, evitando-se assim a execução do ataque propriamente dito.

A abordagem utilizada neste trabalho para avaliação desse mecanismo foi a alteração de um protocolo de rede para RSSFs, de maneira que este se torne apto a agregar as informações necessárias para que sejam analisadas as duas características citadas.

Foi escolhido dentre os protocolos de rede um que possua características hierárquicas, por possuir um elemento centralizador [LIN 03]. O fato desse tipo de elemento existir faz com que seja facilitado o processo de captação das informações referentes aos elementos que constituem a rede.

Neste trabalho foi utilizada a implementação para o simulador de redes NS-2 [NS2 05] do protocolo LEACH [HEI 00], desenvolvido pelo MIT [MIT 05]. A próxima seção apresenta o funcionamento deste protocolo e as alterações propostas neste trabalho.

5.1. Protocolo LEACH

O protocolo LEACH (*Low-Energy Adaptive Clustering Hierarch)*, desenvolvido pelo MIT, foi escolhido devido ao seu comportamento hierárquico e relativa simplicidade, o que o torna bem conhecido. Este protocolo de camada de rede para RSSFs é organizado em grupos (*clusters*), sendo que dentro de cada grupo há um elemento que assume a função de líder (*cluster-head*). Todo o processo é feito em rodadas onde, no início de cada uma delas, os elementos da rede possuem uma certa probabilidade de se tornarem ou não líder de grupo. A cada rodada os líderes mudam, dessa forma há um consumo mais justo de energia entre os

elementos da rede, devido à função de líder ser mais dispendiosa. As rodadas são divididas em 4 fases: *Advertisement phase*, *Cluster set up phase*, *Schedule creation*, *Data transmission*.

- Advertisement phase

No início dessa fase, cada nó decide se será ou não líder de grupo. Essa decisão é feita baseada no percentual de quantos líderes são desejados na rede, definido anteriormente, e o número de vezes que o nó esteve na condição de líder até o atual momento. A decisão é feita através de um valor entre 0 e 1, definido por:

$$T(n) = \begin{cases} \dfrac{P}{1 - P * (r \bmod \dfrac{1}{P})} \\ \\ 0 \end{cases}$$

O primeiro caso é aplicado se n $\in$ G e 0 caso contrário.

Na equação, P representa o percentual desejado de líderes, r é a rodada atual, G é o grupo de nós que não foram líderes nas últimas 1/P rodadas. No começo da primeira rodada (rodada 0), todos os nós possuem probabilidade P de se tornar um líder de grupo. Os nós que se tornem líder não podem ser novamente pelas próximas 1/P rodadas.

Cada nó que se torna líder envia em *broadcast* uma mensagem (mensagem ADV-CH) para a rede, informando sua condição de líder de grupo. Os nós que não são líderes recebem as mensagens ADV-CH dos nós que se encontram nessa situação e escolhem a melhor opção para si. Essa escolha é feita através da força do sinal recebido, sendo o líder que teve o sinal mais forte no envio da ADV-CH para um determinado nó, será escolhido por este. O fato de ter recebido um sinal com mais força indica que a distância entre os dois é menor se comparada com a distância entre o nó e os outros líderes que tiveram menos força no sinal da mensagem ADV-CH, o que conseqüentemente sugere que o nó necessitará utilizar menos energia para transmitir sua mensagem ao seu líder.

- Cluster set up phase

Os nós que não são líderes enviam ao remetente da mensagem ADV-CH escolhida, uma requisição de ingresso em seu grupo através de uma mensagem chamada de JOIN-REQ. Os líderes então armazenam os elementos que fazem parte de seu grupo. Caso um elemento não receba nenhuma mensagem do tipo ADV-CH, este se torna sozinho, ou seja, não estará associado a grupo algum durante essa rodada e, quando possuir dados a serem transmitidos, com destino à estação-base, estes serão enviados diretamente.

- Schedule Creation

Os líderes, de posse dessas mensagens de requisição, criam um escalonamento TDMA (*Time Division Multiple Access*) entre os elementos que requisitaram o ingresso ao seu grupo, e enviam a estes o resultado desse escalonamento em uma mensagem chamada ADV-SCH. O escalonamento determina o intervalo de tempo de transmissão para cada elemento do grupo, a ser utilizado na próxima fase (*Data transmission*).

- Data transmission

Nessa fase é iniciado o processo normal da rede, onde os elementos que não são líderes começam o monitoramento e, ao possuírem informações a serem transmitidas à estação-base, as enviam ao líder do grupo, respeitando o escalonamento TDMA, e esse se encarrega de encaminhar a informação, executando operações de fusão/agregação nos dados recebidos visando economia de energia.

Para reduzir a interferência entre as transmissões entre grupos, cada um destes se comunicam utilizando um código CDMA (*Code Division Multiple Access*) diferente. Quando um nó se torna líder de grupo, este escolhe aleatoriamente um código CDMA e transmite esse código para todos os elementos que fazem parte de seu grupo. Dessa forma as mensagens recebidas por esse líder serão filtradas utilizando esse código (processo normal de uma transmissão CDMA) de maneira que as transmissões de grupos vizinhos não interferirão entre si.

Finalizada a rodada, todo o processo é repetido, mudando os líderes e compondo novos grupos. Cada rodada dura um tempo determinado, nesse caso, 20 segundos.

Segue abaixo o diagrama de estados que representa todo o funcionamento do protocolo LEACH.

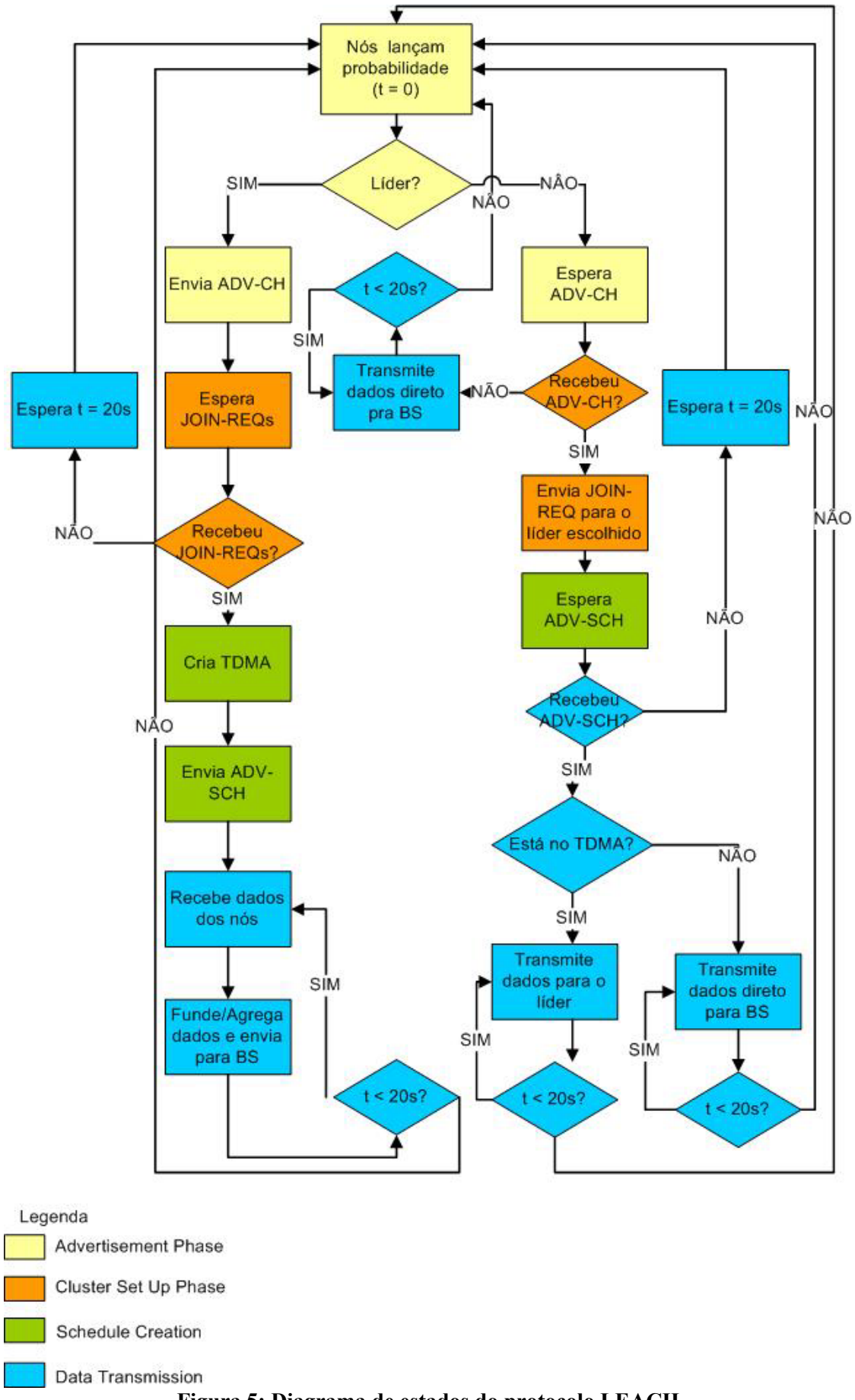


Figura 5: Diagrama de estados do protocolo LEACH

5.2. Alterações no protocolo LEACH

Para que o mecanismo envolvendo a contagem do número de elementos e a média energética da rede possa operar, durante o funcionamento desta, foram estabelecidas algumas alterações no protocolo LEACH. Para tanto foi utilizada a implementação do protocolo para o simulador de redes NS-2 [NS2 05] codificada e disponibilizada pelo MIT [LEA 05]. A próxima sub-seção apresenta como é a implementação do LEACH para o NS-2, feita pelo MIT.

5.2.1. Funcionamento do código do protocolo LEACH

O código do protocolo LEACH foi desenvolvido pelo MIT. A linguagem utilizada foi o TCL [TCL 06], linguagem utilizada para a criação de *scripts* entendidos pelo NS-2.

Todo o código pode ser encontrado em [LEA 05], sendo este compatível com a versão 2.1b5 do simulador NS-2.

O código foi desenvolvido em procedimentos, sendo que cada fase do protocolo (*Advertisement Phase, Cluster Set Up Phase, Schedule Creation* e *Data Transmission*) possui cada uma de suas ações representadas por uma ou mais funções.

Basicamente, o funcionamento se dá da seguinte forma:

Após a inicialização das variáveis que serão utilizadas, todo agente simulado (nesse caso, os nós sensores) executa a função

Application/LEACH instproc start {}.

Essa função, por sua vez executa a função

Application/LEACH instproc decideClusterHead {}.

Em *decideClusterHead{}*, cada nó lança a probabilidade para se tornar ou não um líder (*Cluster Head*). Cada nó que se torna líder, executa a função

Application/LEACH instproc advertiseClusterHead {}

onde enviam uma mensagem ADV-CH para toda rede, em *broadcast*, informando o fato de serem líderes.

A função anterior, para os elementos não líderes, ao terminar, executa a função

Application/LEACH instproc findBestCluster {}.

Essa função possui uma estrutura de decisão (*if*). Se o nó tiver sido definido como não-líder, este deve escolher entre as mensagens ADV-CH que recebeu a que tenha chegado com maior força de sinal e enviar para o remetente da mensagem escolhida uma mensagem JOIN-REQ através da função

Application/LEACH instproc informClusterHead {}.

Os elementos definidos como líderes recebem as mensagens JOIN-REQ e, de posse da lista de elementos que enviaram esse tipo de mensagem, cria um escalonamento TDMA executando a função

Application/LEACH instproc createSchedule {}.

Nessa mesma função o escalonamento é enviado para os elementos do grupo em uma mensagem ADV-SCH. Os elementos do grupo recebem o escalonamento e passam a transmitir seus dados ao líder, no momento determinado pelo escalonamento através da função

Application/LEACH instproc sendData {}.

O líder por sua vez recebe as mensagens de dados dos elementos do seu grupo, executa agregação/fusão nos dados e envia para a estação-base através da função

Application/LEACH instproc sendDataToBS {}.

Todos os elementos, líderes ou não, após 20 segundos de execução retornam à função *decideClusterHead {}*, onde uma nova rodada é iniciada. Dessa vez, os elementos que atuaram como líderes na rodada anterior não poderão atuar novamente dessa forma, fazendo

com que o gasto energético dessa função seja dividido de maneira mais justa com os outros nós da rede.

Basicamente, este trabalho consistiu em implementar as idéias aqui descritas, a respeito da contagem dos nós e do monitoramento do nível energético destes, através de alterações na implementação do protocolo LEACH descrita acima.

Todo o trabalho foi feito em três passos. Inicialmente foram feitas alterações no protocolo visando criar um mecanismo que monitorasse a quantidade de elementos existentes na rede. O segundo passo consistiu na criação de um mecanismo que monitorasse a média energética da rede. Finalmente, no terceiro passo foi criado um mecanismo que contemplasse as duas características ao mesmo tempo. Dessa forma foi possível a geração de resultados separadamente, tanto do mecanismo de contagem como do monitoramento da média energética, e por fim um mecanismo com os dois coexistindo ao mesmo tempo.

5.3. Avaliação e resultados

Todos os testes e simulações foram feitos através do simulador de redes NS-2, utilizando as implementações original e modificada do código do protocolo LEACH, desenvolvido pelo MIT.

Os testes foram feitos tendo como cenário uma área de 1000m x 1000m, uma rede contendo 100 nós sensores e uma estação-base (BS) localizada em x = 50 e y = 175. A propagação do rádio foi definida com valor de $3x10^8$ m/s. O rádio possui uma banda de 1 Mbps e o tamanho dos pacotes foi definido com 500 bytes. Os valores energéticos do rádio foram estipulados em 50 nJ/bit (para recepção e transmissão) e a propagação em 100 pJ/bit/m^2. A agregação dos dados gasta 5 nJ/bit/sinal do nó líder. O número de grupos é de 5% do total de elementos da rede (nesse caso, cinco grupos).

A avaliação foi feita comparando-se os resultados de simulações utilizando o protocolo LEACH original com os resultados utilizando o protocolo alterado, nos seguintes aspectos: o tempo de duração da simulação, a quantidade de dados transmitidos pela rede e a quantidade de energia consumida durante a simulação.

Os mecanismos foram implementados de forma independente. Em primeiro lugar foi produzido um código do protocolo LEACH que utiliza o mecanismo de contagem para a identificação de invasões. Após a obtenção de sucesso nessa primeira etapa, foi produzido um segundo código que utiliza o monitoramento energético para tal tarefa. Finalmente, após os

resultados positivos dos dois mecanismos previamente citados, foi gerado um código do protocolo LEACH que possui um mecanismo de identificação de invasões que utiliza tanto o número de elementos como a média energética destes. Para os três mecanismos foram simuladas situações de invasão na rede, testando assim a eficácia na detecção dos intrusos.

Os próximos capítulos apresentam cada mecanismo em detalhes e os resultados obtidos com cada um deles.

6. Mecanismo de contagem dos nós

O mecanismo de contagem consiste em alterações no protocolo LEACH que possibilitam à estação-base estar ciente da quantidade de elementos que compõem a rede a cada rodada. Dessa maneira é possível identificar caso haja um aumento nesse número.

6.1. Alterações no protocolo para a contagem dos elementos

O mecanismo de contagem dos elementos foi feito a partir da adição de novas mensagens no procedimento do protocolo. Basicamente, os líderes passaram a contabilizar a quantidade de elementos existentes em seu grupo e informar tal valor à estação-base. As alterações foram feitas nas seguintes fases do protocolo:

- Cluster Set Up Phase

Após ter decidido qual será seu líder, cada nó envia a este uma mensagem, requisitando a participação no grupo através de uma mensagem JOIN-REQ.

Uma situação que pode ocorrer durante o funcionamento do LEACH é a possibilidade de um nó não receber nenhuma mensagem do tipo ADV-CH. Nas simulações do código do MIT, é determinado que quando esta situação ocorre, o nó se torna sozinho e transmite seus dados diretamente para a estação-base. A alteração determina a adição de uma mensagem do nó que se encontre nessa situação destinada à estação-base, informando-a desse fato. Dessa forma a estação-base pode contabilizar quantos nós estão sem grupo na rodada atual. Essa mensagem é chamada de ADV-AL (*ALone*). Em termos de implementação, esse fato consistiu na criação de uma nova função chamada

Application/LEACH instproc SendNumToBS {num}

onde o elemento que se encontre nessa situação envia uma mensagem para a estação-base para que seu número seja contabilizado. O argumento *num* trata-se do número a ser informado para a estação-base. O valor igual a "1" desse argumento significa uma mensagem ADV-AL.

- Schedule Creation

Nessa fase, os líderes receberam as mensagens JOIN-REQ de cada nó que deseja fazer parte de seu grupo. Dessa forma é possível que este contabilize a quantidade de elementos que fazem parte de seu grupo. Uma alteração foi feita nessa fase: antes que o líder envie a mensagem ADV-SCH, este envia à estação-base o número de elementos que estão sob sua responsabilidade em uma mensagem chamada ADV-LIST. O envio dessa mensagem é feita pela *SendNumToBS {num}*, onde o líder envia a quantidade de elementos no seu grupo (argumento *num*).

Outro fato que pode ocorrer é um nó não ser incluído no escalonamento TDMA. Isso pode acontecer se a mensagem JOIN-REQ enviada ao líder colidir durante a transmissão, por exemplo. Se o nó receber a mensagem ADV-SCH e notar que não possui um *slot* de tempo atribuído para si no escalonamento TDMA, esse fato significa que o líder não está ciente da sua participação no grupo. A extensão propõe que esse nó envie uma mensagem ADV-AL à estação-base, sendo contabilizado como um nó que não possui grupo (também através da função *SendNumToBS {1}*). Outra mudança diz respeito à ocorrência de múltiplas colisões durante a transmissão das mensagens de JOIN-REQ de vários nós. Isso pode resultar em um líder que acredita não existirem nós sob sua responsabilidade, mas vários nós acreditam fazer parte do seu grupo. O líder, então, envia uma mensagem ADV-AL à estação-base (*SendNumToBS {1}*, em *broadcast*) devido ao fato de seu grupo não possuir elementos. Os nós que acreditam fazerem parte desse grupo e por isso esperam uma mensagem ADV-SCH, também recebem a mensagem ADV-AL enviada por seu suposto líder, pelo fato desta ter sido enviada em *broadcast*. Ao receberem esta mensagem de seu suposto líder, estes assumem que houve falha no envio do JOIN-REQ e passam a se comportar como se não possuíssem grupo, enviando uma mensagem ADV-AL à estação-base, informando-a do fato e possibilitando sua contagem (*SendNumToBS {1}*).

Desta forma, a cada início de rodada os líderes contabilizam o número de elementos de seu grupo e enviam à estação-base. A estação-base por sua vez, através dessas novas informações, se torna apta a contabilizar o número de elementos de toda a rede, executando a somatória dos valores enviados pelos líderes somados com o número de mensagens ADV-AL.

Isso faz com que seja possível a detecção do aumento do número de elementos, o que denuncia uma invasão. A figura abaixo apresenta o diagrama de estados do protocolo LEACH com o mecanismo de contagem.

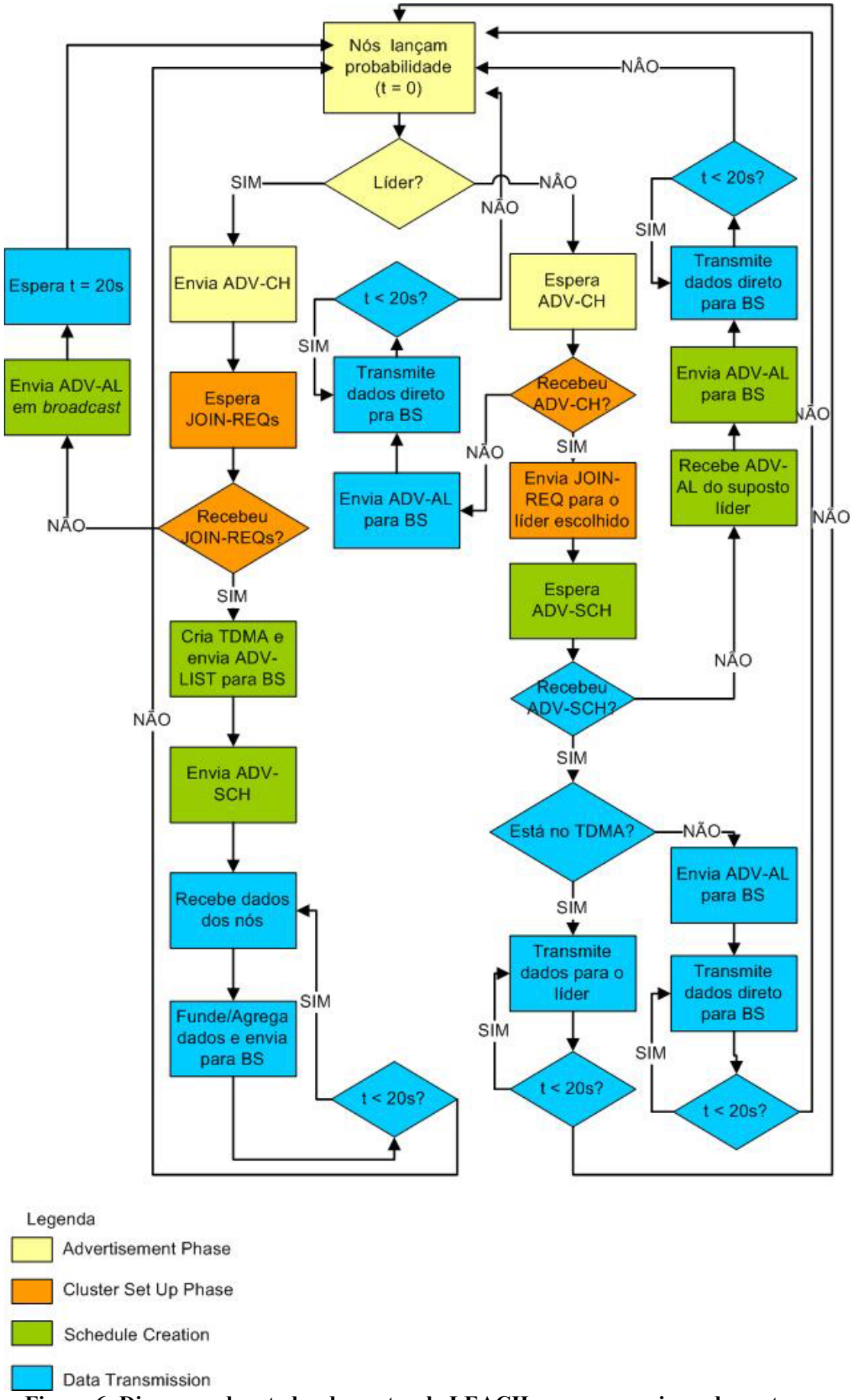


Figura 6: Diagrama de estados do protocolo LEACH com o mecanismo de contagem

6.2. Resultados do mecanismo de contagem

Foram feitas simulações para avaliação do impacto do mecanismo no rendimento do protocolo, comparando-se os resultados de simulações com o protocolo LEACH original e uma versão deste alterado.

	Total de dados (bytes)		**Total de energia (J)**		**Tempo Total (s)**	
Simulação	**Leach**	**Leach/cont.**	**Leach**	**Leach/cont.**	**Leach**	**Leach/cont.**
1	8250	28672	199,65015	199,39956	194,9	401,1
2	45546	47555	199,67071	199,51197	550,3	525,1
3	37975	45308	197,97661	199,16482	521,2	485,3
4	45732	30771	199,21771	200,18235	542,5	374,7
5	41717	47142	199,46124	198,97012	492,9	561,7
Média	**35844**	**39889,6**	**199,19528**	**199,44576**	**460,36**	**469,58**

Tabela 1 – Resultado dos testes do mecanismo de contagem

A tabela 1 mostra os resultados de 10 simulações, sendo 5 com o protocolo LEACH original e 5 com a versão alterada.

A tabela mostra que a performance do LEACH e sua versão alterada com o mecanismo de contagem são muito similares. Devido à simulação possuir fatores aleatórios, todos os valores são diferentes uns dos outros, mesmo se comparado os resultados de dois testes utilizando o mesmo protocolo. Isto ocorre devido à aleatoriedade da maneira de como é determinado qual nó irá assumir o posto de líder, o que pode resultar em líderes dispostos distantes dos nós do grupo, implicando em uma maior quantidade de energia utilizada por esses nós na transmissão de suas mensagens ao líder, se comparado com a situação onde este se encontra mais próximo.

A tabela 1 mostra que os resultados das simulações das duas versões do protocolo estão dentro de um mesmo intervalo. A média resultante de todos os testes mostra que o impacto negativo do mecanismo na performance do protocolo é pequeno, provando que é possível implementá-las sem prejudicar o rendimento da rede.

O total máximo de bytes transmitidos em uma simulação com o protocolo LEACH original foi de 45732, com média de 35844, enquanto na versão com o mecanismo de contagem temos no máximo 47555 bytes transmitidos, com média de 39889,6.

Nas simulações com o LEACH original, o maior valor de energia gasto foi de 199,21771 J com média de 199,19528 enquanto na versão com a contagem o máximo foi de 200,18235 J e média de 199,44576.

A duração, em média, das simulações foi de 460,36 segundos para o LEACH original e de 469,58 para a versão modificada com a contagem.

Um fato digno de nota é visto nos resultados, onde o pior deles foi obtido através da simulação de uma rede utilizando o protocolo LEACH original (simulação 1 da Tabela 1). Isso mostra que, apesar do acréscimo no custo da rede pela adição das mensagens aqui descritas, isso não levou o rendimento para um extremo negativo, sendo este obtido com o protocolo original. Este resultado extremo foi obtido devido à aleatoriedade da maneira que os líderes são escolhidos podendo resultar, em algumas simulações, líderes distantes dos elementos do grupo, fazendo com que estes necessitem consumir mais energia na comunicação.

Os gráficos abaixo mostram a quantidade de elementos que compõem a rede durante a simulação nos casos onde a rede não sofreu invasão (Figura 5) e quando este fato ocorreu (Figura 6). Os gráficos foram gerados a partir das informações recebidas pela estação-base durante a simulação do protocolo LEACH com o mecanismo de contagem.

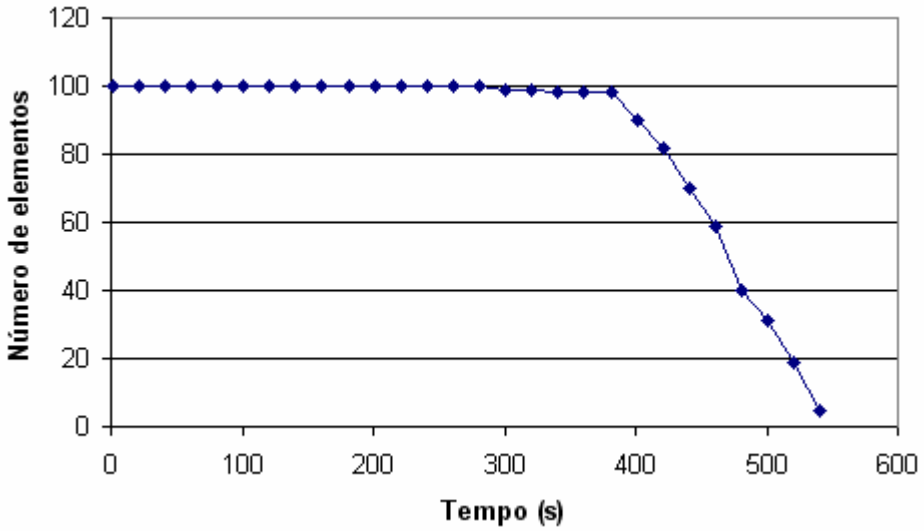


Figura 7: Quantidade de elementos em uma rede sem invasores

A figura 5 mostra que até pouco antes de 300 segundos de simulação havia 100 elementos na rede. Em 300 segundos esse número cai para 99 e, logo após, 98 elementos. Pouco antes de 400 segundos, a quantidade de elementos na rede começa a cair até que não há mais elementos disponíveis.

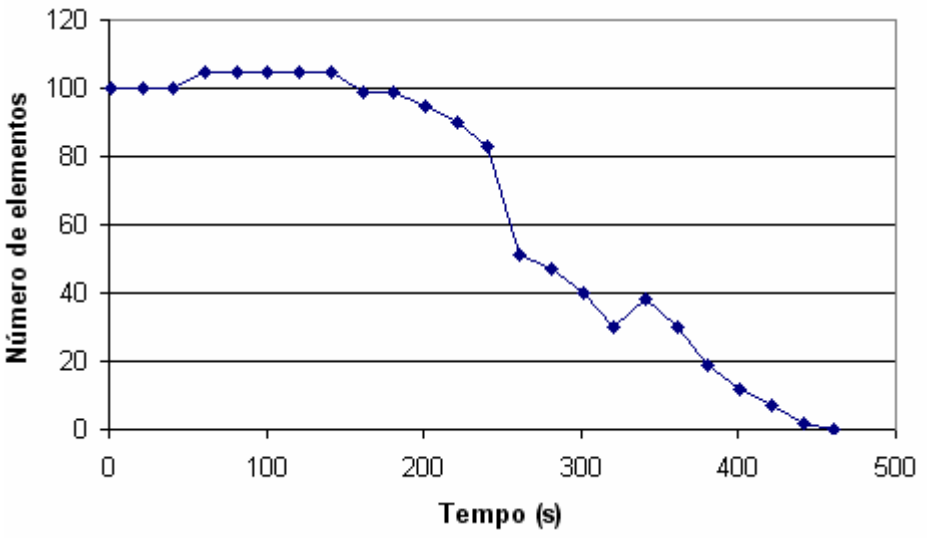


Figura 8: Quantidade de elementos em uma rede com invasores

A figura 6 mostra como é possível identificar invasões através do número de elementos da rede. Após 60 segundos de simulação, 5 nós intrusos aparecem na rede, o que faz com que o número de elementos suba de 100, valor inicial, para 105. Esse aumento no número de elementos claramente denuncia a invasão. Após isso, o número de elementos segue decrescendo até que em 340 segundos de simulação uma nova invasão ocorre. A quantidade de elementos na rede volta a subir, de 30 para 38 elementos, fato que indica a nova invasão.

O resultado obtido, como pôde ser visto, foi positivo, pois com poucas alterações no protocolo, que resultaram em apenas uma pequena sobrecarga neste, foi possível obter um controle sobre a quantidade de elementos que compõem a rede durante sua vida útil.

É interessante dizer que nos testes foi utilizado um espaço de tempo de 20 segundos entre duas consultas à quantidade de elementos da rede devido à implementação do LEACH estabelecer rodadas que durem essa quantidade de tempo. Em uma RSSF, dependendo da capacidade desta, o espaço de tempo entre uma consulta e outra pode ser reduzido, permitindo assim um maior controle do número de elementos da rede em espaços menores de tempo.

7. Mecanismo de monitoramento energético

O mecanismo de monitoramento energético visa prover à estação-base a capacidade de estar sempre ciente do nível energético que existe na rede. Dessa forma é possível identificar caso haja um aumento no nível de energia da rede, o que denuncia a existência de novos elementos nesta.

7.1. Alterações no protocolo para o monitoramento energético

O monitoramento energético dos elementos da rede foi feito através da adição de novas mensagens e da utilização de mensagens já existentes no protocolo, agora contendo informações sobre o estado atual do nível energético do remetente. Seguem abaixo as alterações no protocolo para este mecanismo:

- Cluster Set Up Phase

Quando um nó envia a mensagem JOIN-REQ ao líder escolhido, esta passa a conter o nível energético atual do remetente. Essa alteração foi feita na função já existente no código, *informClusterHead {}*, responsável pelo envio das mensagens JOIN-REQ. No caso de um nó não receber nenhuma mensagem do tipo ADV-CH este nó se torna sozinho e transmite seus dados diretamente para a estação-base. O mecanismo determina a adição de uma mensagem do nó que se encontre nessa situação destinada à estação-base, informando-a desse fato, enviando o seu nível energético. Dessa forma, a estação-base pode contabilizar o nível de energia dos nós que estão não estão associados a grupo algum na rodada atual. Essa mensagem será chamada de ADV-AL (*ALone*). A nova função criada, responsável por essa mensagem, é

Application/LEACH instproc SendEnToBS {en}.

Onde o argumento *en* consiste no valor energético atual do remetente, que irá no conteúdo da mensagem.

- Schedule Creation

De posse das mensagens JOIN-REQ dos nós que compõem seu grupo, o líder cria um escalonamento TDMA. Este então envia uma mensagem ADV-SCH com o escalonamento TDMA a todos os nós que fazem parte do seu grupo.

Antes que o líder envie a mensagem ADV-SCH, este envia à estação-base a soma do nível energético recebido de cada um dos elementos do grupo nas mensagens JOIN-REQ. Essa mensagem é chamada ADV-EN (*ENergy*) e enviada através da função *SendEnToBS {en}*, onde *en* nesse caso é a soma do nível energético dos elementos do grupo.

Caso o nó receba a mensagem ADV-SCH e note que não há um *slot* de tempo atribuído para si no escalonamento TDMA, esse fato significa que o líder não está ciente da sua participação no grupo. Com o mecanismo, esse nó envia uma mensagem ADV-AL à estação-base, contendo seu nível energético atual, de forma que a energia deste pode ser contabilizada (*SendEnToBS {en}*). Outra mudança diz respeito à ocorrência de múltiplas colisões durante a transmissão das mensagens de JOIN-REQ de vários nós, o que resulta em um líder que acredita estar sozinho, sem nós sob sua responsabilidade, mas vários nós acreditam fazer parte do seu grupo. O líder, então, envia uma mensagem ADV-AL à estação-base (*SendEnToBS {en}* em *broadcast*) enviando o seu nível energético atual. Ao receberem uma mensagem do tipo ADV-AL do seu suposto líder, estes assumem que houve falha no envio da mensagem JOIN-REQ. Os nós, então, passam a se comportar como se não possuíssem grupo, e todos os elementos que se encontram nessa situação enviam uma mensagem ADV-AL à estação-base, informando seu nível energético, sendo assim contabilizados (*SendEnToBS {en}*).

Dessa forma, o mecanismo propicia à estação-base capacidade de estar ciente do nível de energia remanescente na rede a cada rodada, podendo identificar caso esse montante sofra um acréscimo, o que denuncia uma invasão.

A figura abaixo apresenta o diagrama de estados do protocolo LEACH com o mecanismo de monitoramento energético.

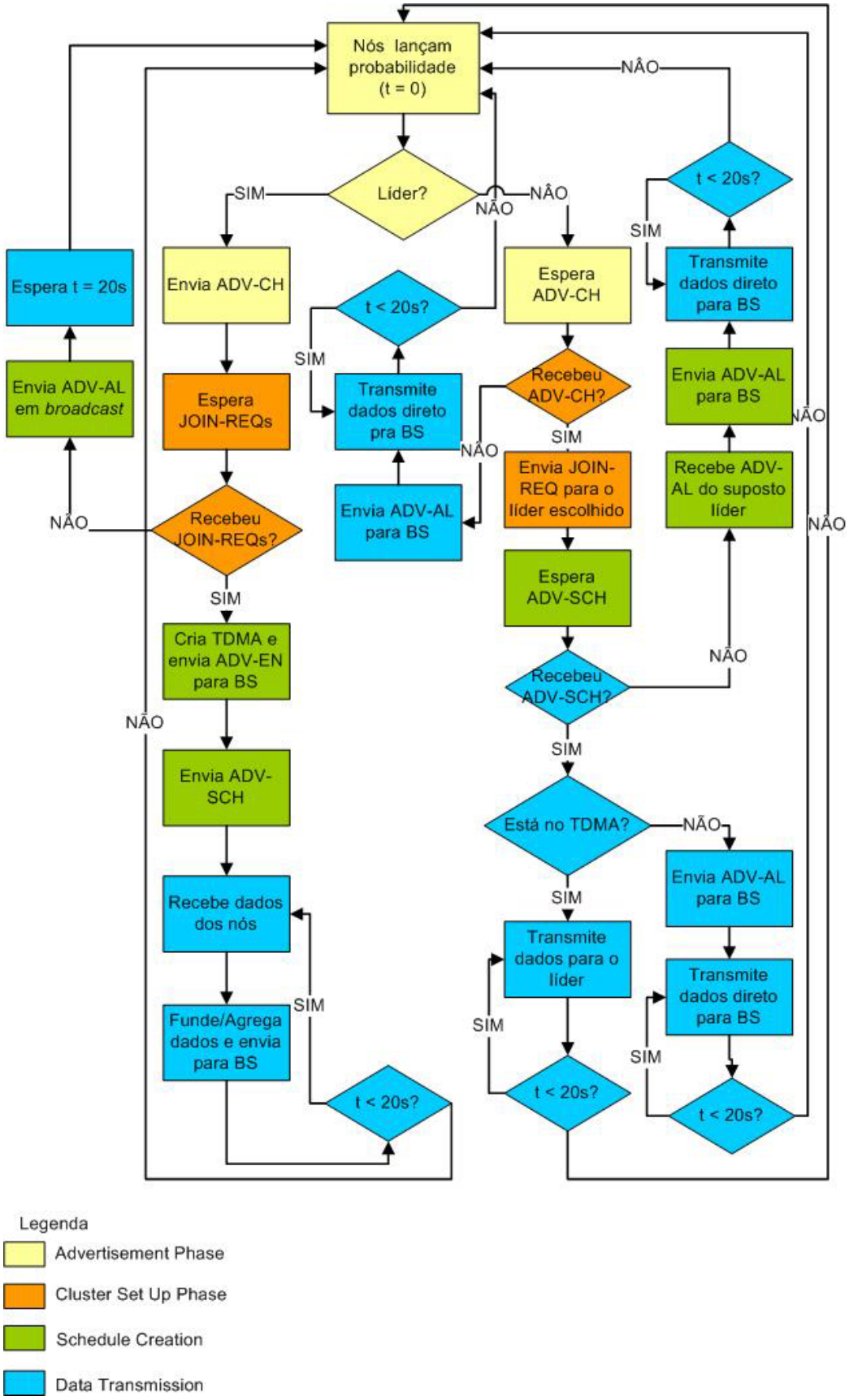


Figura 9: Diagrama de estados do protocolo LEACH com o mecanismo energético

7.2. Resultados do mecanismo de monitoramento energético

Os resultados foram obtidos comparando-se o rendimento do protocolo alterado com o mecanismo de monitoramento energético e o original.

Como apresentado na tabela 2, o mecanismo de monitoramento energético não teve um impacto negativo no rendimento da rede, se comparado com o protocolo LEACH original. A tabela mostra resultados de 5 simulações com o protocolo original e 5 com o protocolo tendo o mecanismo de monitoramento de energia implementado.

	Total de dados (bytes)		**Total de energia (J)**		**Tempo Total (s)**	
Simulação	**Leach**	**Leach/En.**	**Leach**	**Leach/En.**	**Leach**	**Leach/En.**
1	42062	42401	199,02261	198,21052	481,2	489,9
2	41595	45392	198,86348	200,32102	506,5	563,1
3	44311	39865	199,54662	199,48609	469,6	401,3
4	42020	47786	198,14959	200,28842	470,2	563,6
5	40496	41758	199,01238	198,92572	475,9	561,1
Média	**42096,8**	**43440,4**	**198,91893**	**199,447286**	**480,68**	**515,8**

Tabela 2 – Resultado dos testes do mecanismo de energia

O máximo total de bytes transmitidos pelo protocolo LEACH foi de 44311 bytes, com média de 42096,8, enquanto no protocolo com o mecanismo energético o resultado foi de máximo de 47786 bytes transmitidos e média de 43440,4 bytes.

A energia despendida pelo protocolo original teve como valor máximo 199,54662 J, com média de 198,91893 J. O protocolo que contém o mecanismo de monitoramento consumiu no máximo 200,32102 J e teve em média um consumo de 199,447286 J.

A duração da simulação foi de no máximo 506,5 segundos e média de 480,68 segundos para o protocolo original e máximo de 563,6 segundos e média de 515,8 segundos para o protocolo com o mecanismo de monitoramento de energia.

Os resultados obtidos mostram que tanto o rendimento do protocolo original quanto o do LEACH utilizando o mecanismo de monitoramento energético são similares, existindo pouca variação. Isso mostra que a implementação do mecanismo no protocolo LEACH não teve um impacto negativo significativo no rendimento da rede, o que torna o mecanismo viável.

As figuras abaixo mostram como é possível a identificação de uma invasão através desse mecanismo.

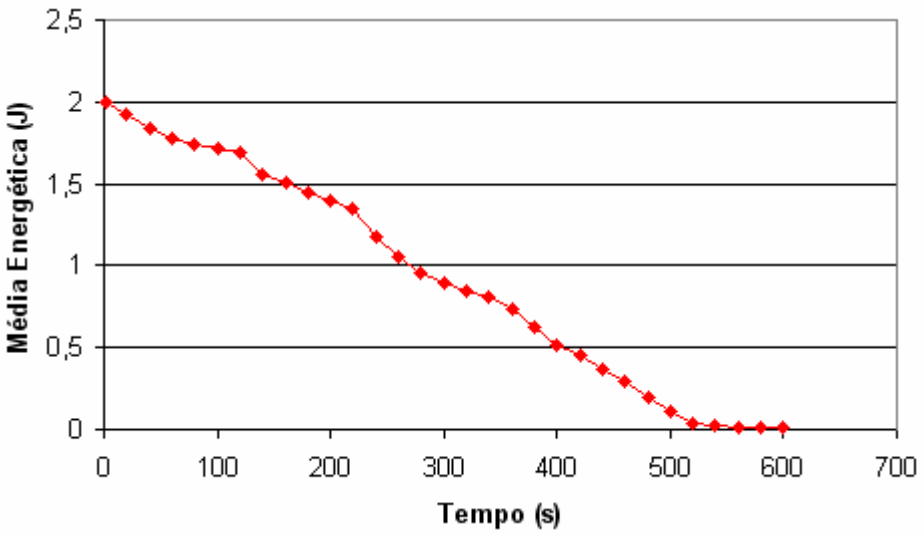


Figura 10: Média energética da rede em uma simulação sem invasores

A figura 7 mostra um gráfico feito a partir das mensagens recebidas pela estação-base, de acordo com as mudanças feitas no protocolo. Devido ao fato de que todos os elementos da rede iniciam com 2 J de energia, a média energética da rede no instante 0 equivale a esse valor. À medida que o tempo passa, os nós consomem energia e a estação-base, recebendo essa informação, monitora o nível de energia da rede. Durante o funcionamento da rede, a média energética tende sempre a decrescer, até não restar energia suficiente nos nós, impossibilitando o seu funcionamento.

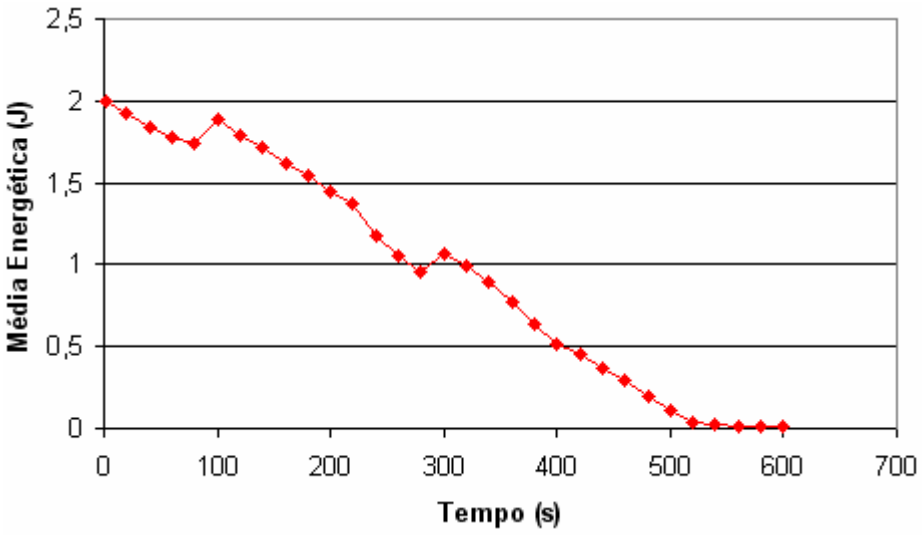


Figura 11: Média energética de uma rede com invasores

A figura 8 mostra como a média energética é afetada caso haja uma invasão na rede. Em 100 segundos de simulação, novos nós aparecem na rede, o que faz com que a média

energética desta sofra um acréscimo de aproximadamente 1,75 J para aproximadamente 1,9 J. No instante 300, novamente há um acréscimo na média energética da rede, que aumenta de 0,95 J para 1,05 J aproximadamente. Não havendo nenhum acréscimo legítimo de nós na rede, esse incremento na média energética da rede claramente denuncia uma invasão de novos e ilegais elementos nesta.

O resultado obtido com esse mecanismo foi positivo, com poucas alterações no protocolo foi possível monitorar a energia residual da rede e, conseqüentemente, calcular a média energética dos elementos que a compõem, possibilitando assim a identificação de qualquer acréscimo nesse valor, o que denuncia uma invasão.

Novamente é interessante citar que as consultas referentes às informações energéticas da rede foram feitas a cada rodada, estabelecida no protocolo LEACH tendo duração de 20 segundos. Dependendo da aplicação e do protocolo em que esta estratégia for inserida, o tempo entre uma consulta e outra pode ser menor, aumentando assim as chances de identificação de alguma alteração nesse atributo.

8. *Mecanismo completo de análise*

Nessa fase do trabalho foi criado um mecanismo que monitore tanto o número de elementos da rede quanto a média energética desta ao mesmo tempo. Basicamente foi feita a união do mecanismo de contagem com o mecanismo de monitoramento energético, possibilitando a análise da atuação dos dois em conjunto.

8.1. Alterações no protocolo para o mecanismo completo

O mecanismo completo basicamente faz uso das alterações feitas no protocolo LEACH para o mecanismo de contagem juntamente com as mudanças que possibilitaram o monitoramento energético dos elementos da rede. Para isso foram feitas as seguintes alterações no protocolo:

- Cluster Set Up Phase

A primeira alteração ocorre da seguinte forma: a mensagem JOIN-REQ passa a conter o nível de energia atual do remetente. Dessa forma, o líder do grupo receberá, junto da requisição de ingresso ao grupo, suficiente para a contagem dos elementos, os dados necessários para contabilizar a energia que existe nos nós sob sua responsabilidade. Essa alteração foi feita na função *informClusterHead {}*.

Uma situação que pode ocorrer é a possibilidade de um ou mais nós não receberem nenhuma mensagem ADV-CH (enviada na *Advertisement Phase* pelos líderes da rodada atual aos outros nós). Um nó que se encontre nessa situação simplesmente não se associa a nenhum líder e, quando possui informações a serem transmitidas à estação-base, transmite-as diretamente. Para que as informações deste nó, tanto numérica quanto energética, sejam contabilizadas, uma alteração foi necessária. Um nó que se encontre nessa situação envia uma mensagem à estação-base, informando este fato através de uma mensagem do tipo ADV-AL (*ALone*). Nessa mensagem é enviado o nível energético atual do nó, de forma que mesmo os

nós sem grupo podem ser contabilizados tanto em número quanto em energia. A função criada para esse fim foi

Application/LEACH instproc SendClusterInfoToBS {info}

onde *info* contém o nível de energia do remetente e a quantidade de elementos que o grupo possui, nesse caso, "1".

- Schedule Creation Phase

Nessa fase, os líderes de grupo receberam as mensagens JOIN-REQ de todos aqueles que desejam se associar ao seu grupo. Como foi feita a alteração citada acima, as mensagens JOIN-REQ possuem o nível energético de cada nó. Dessa forma é possível para o líder somar o nível de energia de todo o grupo e contabilizar o número de elementos que o compõem. Essas informações são enviadas em uma mensagem denominada ADV-CI (*Cluster Information*) à estação-base que, de posse de todas as mensagens ADV-CIs de todos os grupos e das mensagens ADV-ALs dos elementos sem grupo da rede, contabiliza o número total de elementos e a média energética existente na rede. O envio da mensagem ADV-CI é feito pela função *SendClusterInfoToBS {info}*, sendo *info* nesse caso trata-se da soma dos valores energéticos dos elementos do grupo e o número de elementos que o compõe.

Caso haja falha no envio da mensagem JOIN-REQ de um nó ao líder, ao receber o escalonamento, esse nó em particular não encontrará um período de tempo destinado às suas transmissões. Nessa situação o nó se torna sozinho e envia uma mensagem ADV-AL à estação-base para que possa ser contabilizado (*SendClusterInfoToBS {info}*).

Outra situação que pode ocorrer é o caso de múltiplas falhas no envio do JOIN-REQ dos nós ao líder. Isso resulta em nós que acreditam estarem associados a um grupo, mas o líder deste não sabe deste fato e considera que em seu grupo não há elementos. Esse fato leva à situação onde os nós comuns permanecem esperando a mensagem ADV-SCH (que contém o escalonamento TDMA) que nunca é recebida ficando inativos por toda rodada. Para que os nós nesse estado possam ser contabilizados e terem seus níveis energéticos computados, o protocolo foi alterado de forma que, se um líder acredita não possuir elementos no seu grupo, este envia em *broadcast* para a rede uma mensagem ADV-AL, informando a estação-base desse fato. Os nós que estão esperando uma mensagem ADV-SCH deste líder, ao receberem uma mensagem ADV-AL no lugar desta, entendem que não estão sendo considerados pelo

líder como sendo elementos do grupo, dessa forma se tornam elementos sem grupo, enviando uma mensagem ADV-AL para a estação-base (*SendClusterInfoToBS {info}*).

Após isso, a estação-base possui toda informação necessária para que sejam feitas a contabilidade do número de elementos e a média energética de toda a rede. Para a contabilidade da quantidade de elementos da rede, basta executar a soma do número de elementos de cada grupo (mensagens ADV-CI) mais os elementos que se encontram sem grupo (mensagens ADV-AL). No caso da média energética, o cálculo é feito somando-se o nível energético de cada grupo mais o nível energético dos elementos sem grupo e divide-se esse montante pelo número de elementos que existiam quando a rede foi iniciada. Dessa forma é possível identificar a qualquer momento se houve um acréscimo no número de elementos ou se a média energética aumentou.

A próxima figura apresenta o diagrama de estados que representa o protocolo LEACH com o mecanismo completo implementado.

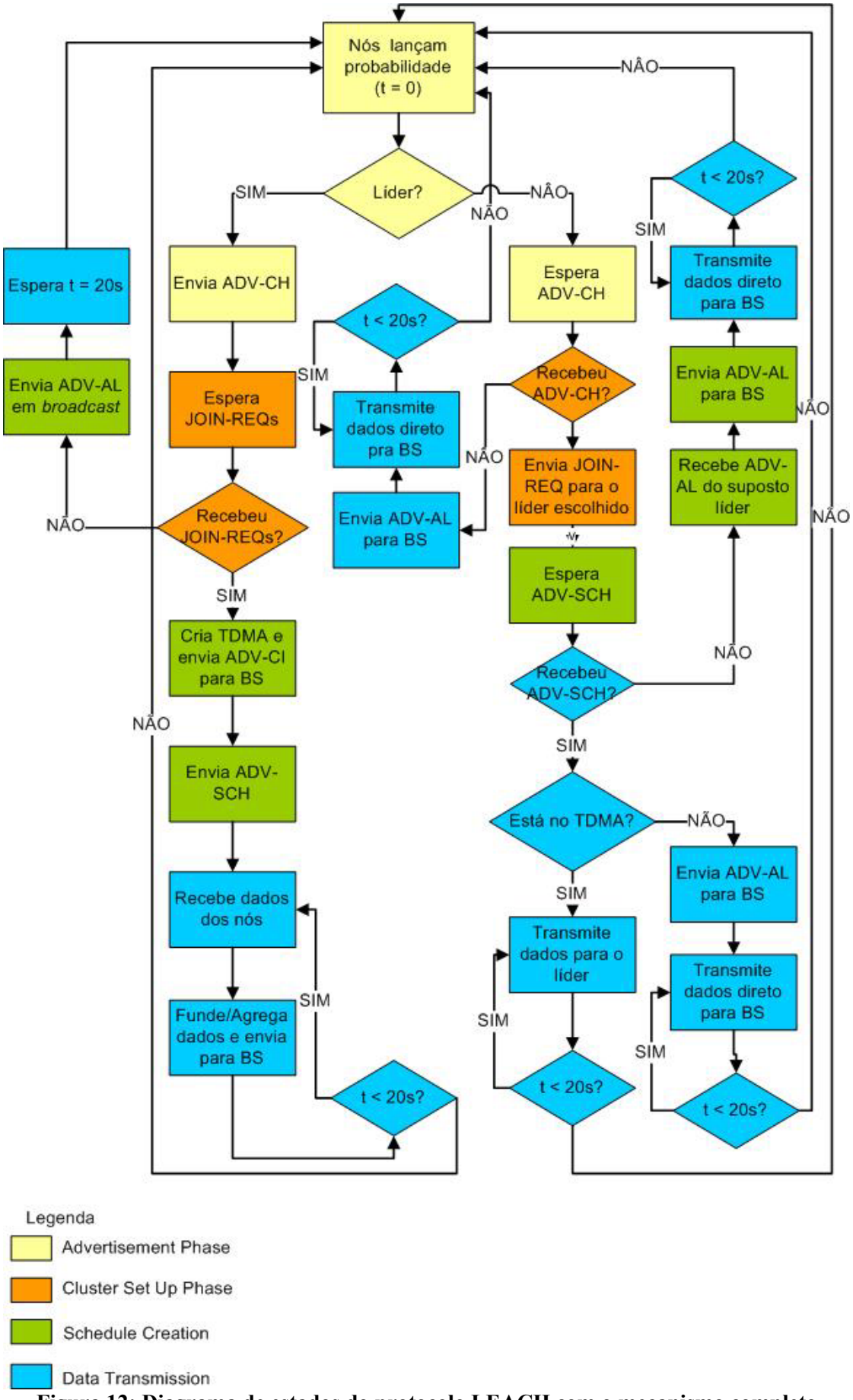


Figura 12: Diagrama de estados do protocolo LEACH com o mecanismo completo

8.2. Vantagem da utilização dos dois métodos em conjunto

A importância de se utilizar os dois parâmetros para identificação de uma invasão se dá na possibilidade de falha em um dos métodos. Por exemplo, no caso de uma quantidade *x* de nós invadirem a rede ao mesmo tempo em que *y* nós legítimos "morrem", onde $y > x$, isso resulta em uma situação onde o mecanismo de contagem de nós falha, mas por outro lado, esse tipo de invasão é possível ser identificada pelo monitoramento da média energética. Em contrapartida, caso os nós invasores divulguem informações falsas a respeito do seu nível energético, de maneira que a média da rede não sofra acréscimo, esse tipo de invasão pode ser identificado pela contagem dos nós.

A próxima seção apresenta os testes e a análise dos resultados obtidos nas simulações. Foram comparados resultados de simulações utilizando o protocolo LEACH na sua forma original e uma versão deste que contém as alterações aqui descritas implementadas.

8.3. Resultados do mecanismo completo

Nessa fase do trabalho o protocolo LEACH foi alterado de maneira que os dois mecanismos (contagem de nós e monitoramento da média energética da rede) coexistam. A idéia é constatar a eficiência dos dois mecanismos sendo utilizados em conjunto, assim como medir se há impacto negativo destes no rendimento da rede.

	Total de dados (bytes)		**Total de energia (J)**		**Tempo Total (s)**	
Simulação	**Leach**	**Leach Alt.**	**Leach**	**Leach Alt.**	**Leach**	**Leach Alt.**
1	42002	48429	199,02000	200,2819	461,2	532,9
2	41595	38702	198,86509	199,2370	506,5	397,2
3	44281	46397	199,04462	198,3022	509,6	511,2
4	42120	46924	198,00950	200,1031	480,2	526,1
5	40296	37847	199,05247	201,8539	435,9	350,4
Média	**42056,8**	**43659,8**	**198,81653**	**199,95562**	**478,68**	**463,56**

Tabela 3 – Resultado das simulações com o mecanismo completo

A tabela 3 mostra resultados de dez simulações, cinco utilizando o protocolo LEACH sem alterações e cinco utilizando o protocolo LEACH alterado utilizando os mecanismos de contagem de nós e monitoramento energético em conjunto.

É possível notar que os rendimentos das simulações que utilizaram o protocolo alterado foram bem parecidos com os apresentados pelas simulações que utilizaram a versão original deste.

O total máximo de dados transmitidos foi de 44281 bytes e mínimo de 40296 bytes para o protocolo original e máximo de 48429 bytes e mínimo de 37847 bytes no protocolo alterado com o mecanismo completo de análise. A média ficou em 42056,8 bytes para o protocolo original e 43659,8 bytes para o protocolo alterado.

A energia gasta nas simulações foi, em média, de 198,8165 J para o protocolo original e de 199,9556 J para o protocolo alterado.

A duração da simulação foi de no máximo 509,6 segundos e mínimo de 435,9 segundos para o protocolo original e de máximo de 532,9 segundos e mínimo de 350,4 segundos para o protocolo com o mecanismo completo. Em média, a simulação da rede que utiliza o protocolo original durou 478,68 segundos e a simulação da rede com o protocolo alterado durou 463,56.

Os dados da tabela mostram que não houve um impacto negativo na rede devido às alterações no protocolo. Houve um pequeno acréscimo no gasto energético da rede, na quantidade de dados transmitidos e uma pequena queda na duração da rede, mas esses fatores não se traduzem na inviabilidade operacional do uso de tais artifícios.

As figuras abaixo ilustram a detecção de intrusão através do monitoramento de tais atributos da rede. As figuras 9 e 10 mostram o comportamento de uma rede onde não houve invasões. Como pode ser visto na figura 9, a quantidade de elementos da rede no início da simulação é de 100, e esse número vai decrescendo à medida que o tempo vai passando. Semelhantemente, a figura 10 mostra a média energética dos elementos da mesma rede. No início, com todos os elementos iniciando a simulação com 2 J, a média da rede é aproximadamente este valor. Com a passagem do tempo, os elementos consomem energia e essa média decresce, chegando a próximo de 0 perto dos 400 segundos de simulação.

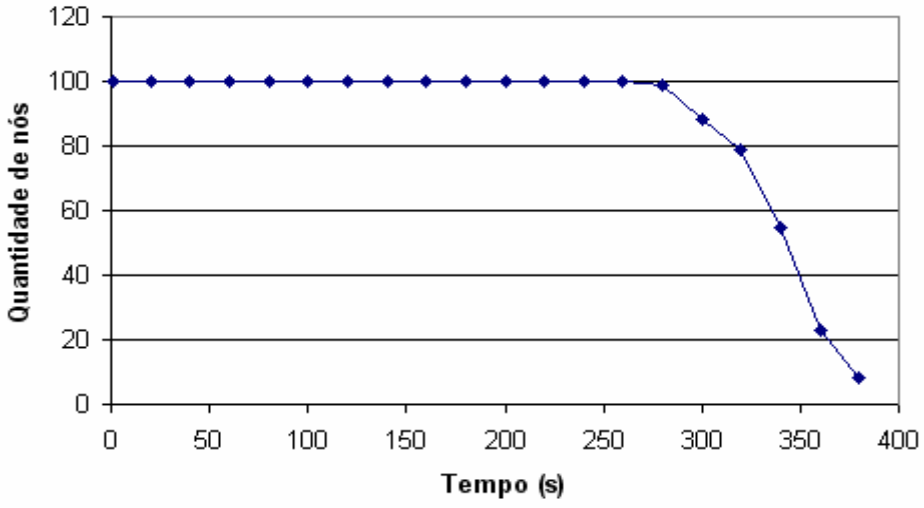


Figura 13: Quantidade de elementos em uma rede sem invasores

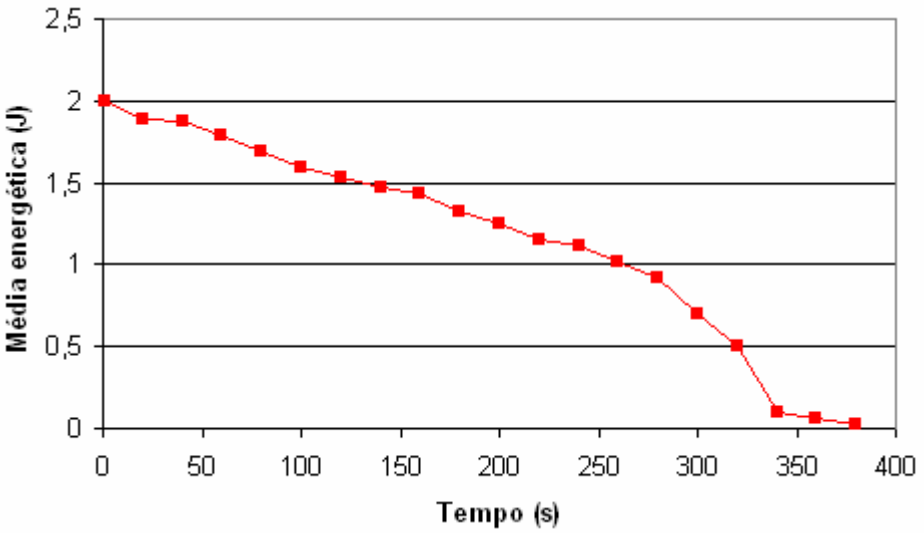


Figura 14: Média energética da rede em uma simulação com invasores.

As figuras 11 e 12 mostram o comportamento de uma simulação onde foram inseridos dois grupos de 10 elementos intrusos na rede. Na análise da quantidade de elementos da rede (figura 11), é possível ver que no instante 100 segundos de simulação, o número de elementos da rede que era de 100 passa para 110, e em 200 segundos, este número é incrementado novamente, de 110 para 120. Como não houve uma inserção legal na rede, isso indica que a rede foi alvo de uma invasão.

O mesmo pode ser dito para a média energética da rede (figura 12). No instante 100 segundos, a média de energia da rede sobe de 1,75 J para 1,9 J aproximadamente, e em 200 segundos, este número sofre outro incremento, de 1,7 J para 1,8 J aproximadamente. Isso indica que novos elementos penetraram na rede, aumentando assim a energia residual desta.

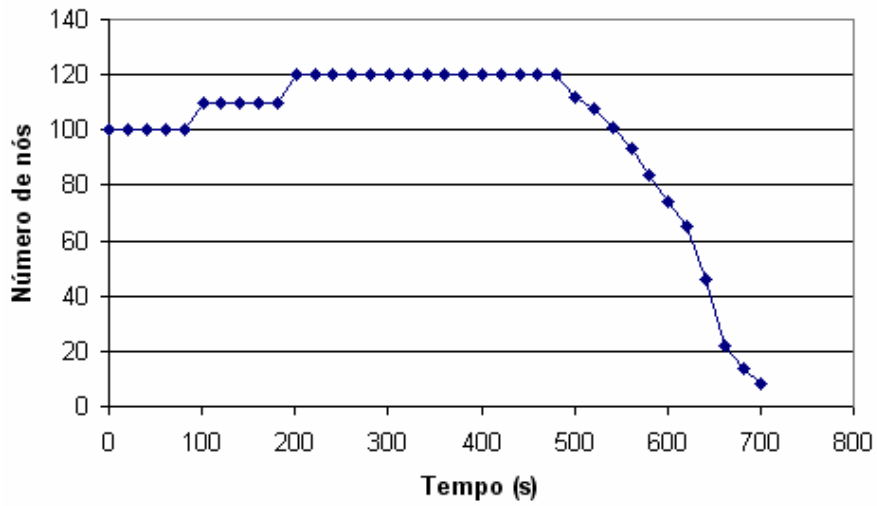


Figura 15: Quantidade de elementos em uma rede com invasores

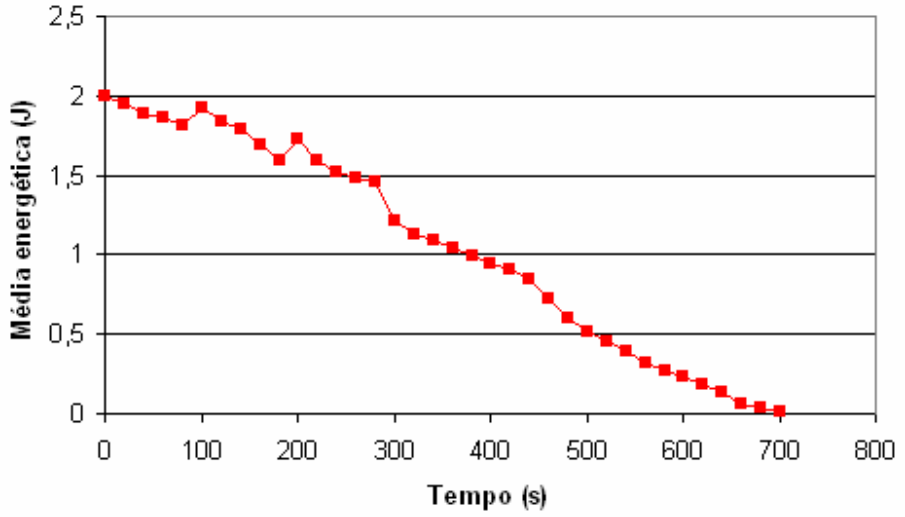


Figura 16: Média energética de uma rede com invasores

É dedutível que cada uma dessas características pode ser utilizada separadamente como mostrado nos capítulos 6 e 7 dessa dissertação, mas como em todo sistema de segurança, quanto mais fatores forem investigados, maior a chance de se descobrir uma ameaça. Os próximos gráficos apresentam uma situação específica.

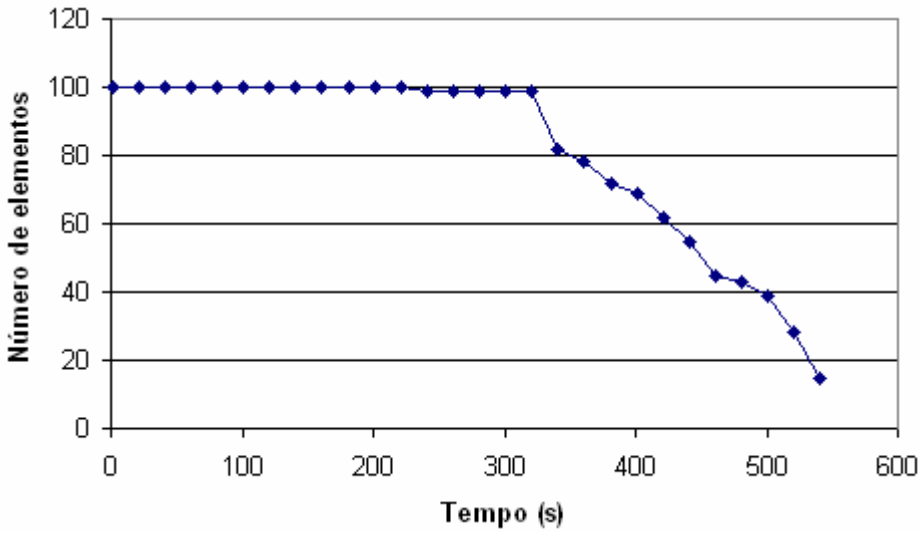


Figura 17: Quantidade de elementos em uma rede

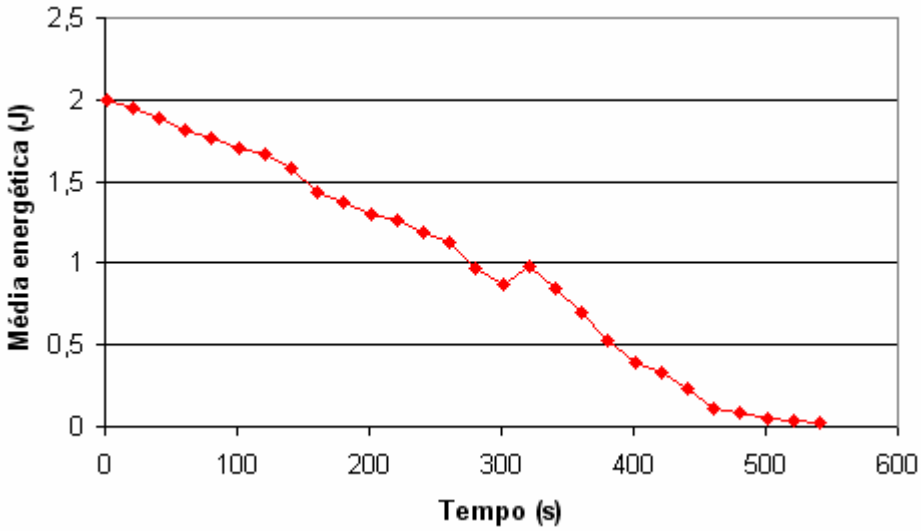


Figura 18: Média energética em uma rede

A figura 13 mostra um fato específico e com chances remotas de ocorrer. Coincidentemente, no momento em que 10 nós invasores entraram na rede, 25 nós legítimos "morreram" (320 segundos de simulação). Como o número de elementos invasores é menor que o número de elementos legítimos que “morreram”, o mecanismo de contagem não pôde identificar o ocorrido. Essa situação, apesar de possível, seria muito difícil de ser usada pelo atacante, já que a predição da “morte” de elementos na rede é algo totalmente impreciso. Por outro lado, o mecanismo energético obteve sucesso na identificação (figura 14), pois foi possível detectar no mesmo instante (320 segundos) um acréscimo na energia da rede (cerca de 0,15 J aproximadamente).

As figuras 15 e 16 apresentam uma situação inversa.

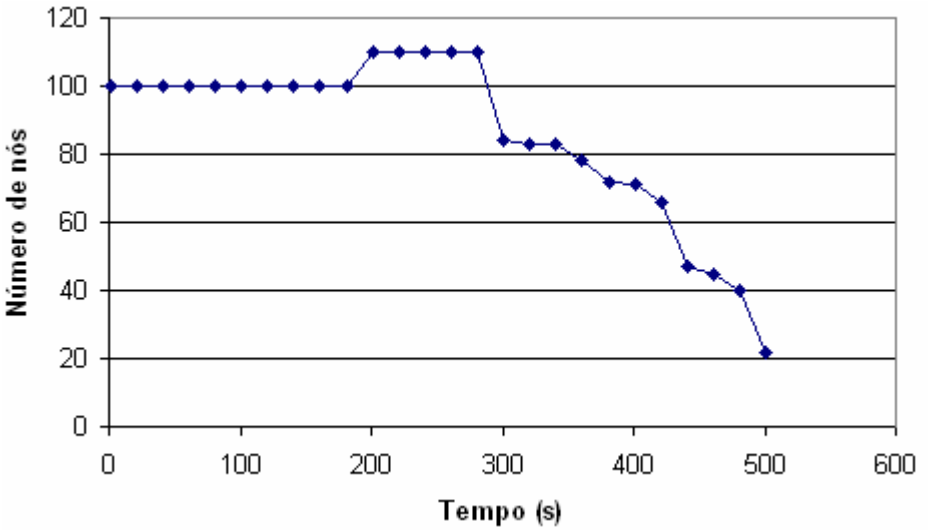


Figura 19: Quantidade de elementos em uma rede

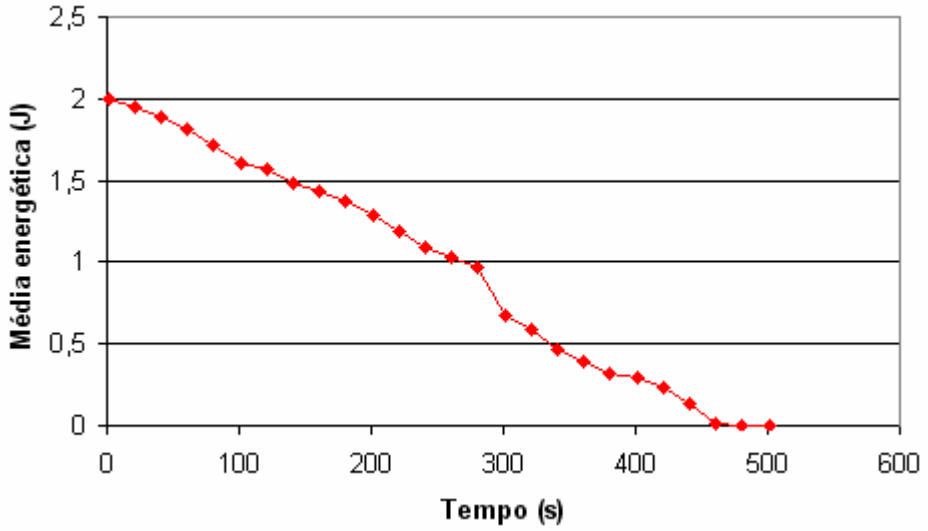


Figura 20: Média energética em uma rede

Os nós invasores forjaram seu nível energético de maneira que é divulgado um valor muito menor de energia de forma que não influencie na média energética da rede, nesse caso, os invasores forneciam 0 J como energia atual. Por esse motivo, a figura 8 apresenta o gráfico energético como uma linha sempre decrescente. Por outro lado, o mecanismo de contagem identificou elementos extras na rede descobrindo assim a invasão, tendo a quantidade de elementos acrescida de 10 unidades após 200 segundos de simulação. Nós invasores que omitem seus dados energéticos podem também ser descobertos através do monitoramento de mensagens mal-formadas, como sugerido em [SAN 04]. Dessa forma, a divulgação de um nível energético de 0 J já caracterizaria uma situação anormal.

Uma situação imaginável que ludibriaria os dois mecanismos seria a ocorrência dos dois fatos ao mesmo tempo: no exato momento que uma quantidade x de elementos na rede "morrem", y invasores aparecem nesta, sendo $x > y$ e esses invasores divulguem seu nível energético de maneira maliciosa. Como já dito acima, a criação dessa situação de maneira intencional demandaria um prévio conhecimento do sistema e levaria em conta predições imprecisas.

Como era esperado, o resultado da união dos dois mecanismos já apresentados nos capítulos anteriores também obteve resultados positivos, inclusive foi demonstradas vantagens da utilização destes em conjunto, devido ao fato de um poder auxiliar o outro, em situações específicas.

9. Conclusão

Conforme apresentado, grande parte dos ataques conhecidos para RSSFs iniciam com a invasão da rede por nós maliciosos. As soluções apresentadas na literatura para evitar e combater esses ataques não são genéricas, ou seja, propõem-se somente a solucionar um tipo específico de ataque, deixando a rede vulnerável a outro diferente do primeiro.

A invasão da rede por nós sensores maliciosos, que interagem com a rede como se fossem legítimos, apresenta-se como um ponto em comum a esses ataques. Isso indica que, se for identificada a intrusão, é possível gerar uma solução genérica que não esteja atrelada a um tipo específico de ataque.

Esse trabalho mostrou que, ao ser alvo de uma invasão, a RSSF sofre alterações em algumas de suas características intrínsecas, como o número de elementos que a compõem e o nível de energia remanescente na rede, fatores que podem ser utilizados na detecção de uma invasão.

Para provar tal afirmativa, a abordagem desse trabalho consistiu em apresentar um mecanismo simples de detecção de invasão pelas características da rede, através de pequenas alterações no protocolo de rede LEACH, de forma que foram incorporadas mensagens que enviam dados sobre a quantidade de elementos e da energia residual na rede à estação-base. Dessa forma, a estação-base torna-se apta a detectar invasões possibilitando o disparo de contra-medidas de forma imediata.

Os testes foram feitos utilizando o simulador NS-2, comparando o resultado de simulações com o protocolo LEACH original e com as alterações sugeridas aqui.

O trabalho foi desenvolvido em três fases:

- Na primeira fase foi implementado, testado e avaliado somente o mecanismo de contagem de elementos;

- Na segunda fase, o mecanismo de monitoramento de energia foi implementado, testado e avaliado;

- A terceira fase consistiu em implementar um mecanismo que agregasse os dois outros, gerando uma solução mais abrangente.

Os resultados de cada uma dessas fases foram positivos e mostraram que realmente os atributos citados são afetados no caso de uma invasão, possibilitando a identificação de novos elementos. As alterações no protocolo não tiveram um impacto negativo no rendimento deste, acarretaram apenas uma pequena sobrecarga no protocolo o que possibilita sua utilização.

Os atributos mostrados podem ser utilizados separadamente ou em conjunto, aumentando assim a eficiência na detecção. Não foi definido o protocolo ou o método a ser utilizado para o monitoramento das características da rede, deixando a solução flexível para cada tipo de RSSF e protocolo que possam conter o mecanismo.

9.1. Trabalhos futuros

O presente trabalho pode ser estendido nos seguintes aspectos:

- Descoberta de outras características das RSSFs que podem ser investigadas para a detecção de uma invasão;

- Implementação e testes das características aqui abordadas em outros protocolos das RSSFs;

- Estudo da eficiência de se ter a abordagem para detecção de invasores aqui descrita em conjunto com outras técnicas de identificação de ataques em RSSFs discutidas no capítulo 2.

- Planejamento de um mecanismo que valide a entrada legal de novos elementos na rede, sem que estes sejam identificados como nós invasores. Isso pode ser feito através de um protocolo de entrada de novos elementos, utilizando autenticação criptográfica.

- Estudo de contramedidas a serem adotadas no caso de uma invasão ter sido identificada. Tais medidas podem ser tão somente alertas da estação-base, informando o fato da invasão, como também medidas reativas como, por exemplo, o isolamento da região ou do grupo no qual a invasão foi identificada. Esse isolamento pode ser feito descartando as mensagens provenientes desse grupo/região da rede.

Referências

[AND 05] Kevin Anderson, BBC – *Posse de Bush terá esquema de segurança inédito* – reportagem publicada na Folha Online em 18 de janeiro de 2005. (http://www1.folha.uol.com.br/folha/bbc/ult272u38839.shtml). (consultado em 08 de abril de 2006)

[BAH 00] Bahl, P. e Padmanabhan, V. N. (2000). *RADAR: An In-Building RF-based User Location and Tracking System*, IEEE INFOCOM, 2000.

[BEA 04] Beaconing, T. *Tiny os: A component-based os for the networked sensor regime*. http://www.webc.cs.berkeley.edu/tos, 2004.

[BRO 04] Broadwell, P., Polastre, J., and Rubin, R. *Geomote: Geographic multicast for networked sensors.* Disponível em http://citeseer.csail.mit.edu/541776.html, 2004 (acessado em 08 de abril de 2006)

[CC1 04] CC 1000. Chipcom corporation. CC1000 low power FSK transceiver. http://www.chipcon.com, 2004 (consultado em 08 de abril de 2006).

[CER 01] Cerpa. A., Elson, J., Hamilton, M., Zhao, J., Estrin, D. e Girod, L. *Habitat monitoring: application driver for wireless communications technology.* In ACM SIGCOMM Workshop on Data Communication in Latin America and the Caribbean, p. 20 - 41, San Jose, Costa Rica., 2001.

[CHI 01] Chien-Chung Shen, Chavalit Srisathapornphat, and Chaiporn Jaikaeo. *Sensor Information Networking Architecture and Applications.* IEEE Personel Communication 150 REFERENCES Magazine, 8(4):52 59, August 2001.

[DOW 04] Downard, Ian – Simulating Sensor Networks In NS-2 – Naval Research Laboratory – Washington DC, EUA - 2004

[DUS 02] Dust, S. Smart Dust: Autonomous sensing and communication in a cubic millimeter. http://robotics.eecs.berkeley.edu/~pister/SmartDust/, 2002 (consultado em 08 de abril de 2006)

[ELS 01] Elson, J. and Estrin, D. Random, ephemeral transaction identifiers in dynamic sensor networks.In *Proceedings 21st International Conference on Distributed Computing Systems (ICDCS-21)*,pages 459.568, Phoenix, Arizona, 2001.

[EST 99] Estrin, D., Govindan, R. e Heidemann, J. *Scalable coordination in sensor networks*. Technical Report 99-692, University of Southern California, 1999.

[EST 00] Estrin, D., Govindan, R., and Heidemann, J. Embedding the internet. *Communications of theACM*, 43(5):39.41, 2000.

[EST 01] Estrin, D., Girod, L., Pottie, G. e Srivastava, M. *Instrumenting the world with wireless sensor networks.* In International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2001), 2001.

[FIG 04] Figueiredo, C. M. S., Nakamura, E. F., and Loureiro, A. A. F. *Protocolo Adaptativo Híbrido para Disseminação de Dados em Redes de Sensores sem Fio Auto-Organizáveis.* In Aceito para Publicação no SBRC04, 2004.

[FOL 05] Folha Online – www.folha.com.br (consultado em 08 de abril de 2006)

[GUI 04] Germano F. Guimarães, Cláudia B. L. N. da Silva, Eduardo J. P. Souto, Reinaldo C. M. Gomes, Judith Kelner, Djamel Sadok – Impacto da utilização de macanismos de segurança em nós sensores – VI Workshop de Comunicação Sem Fio e Computação Móvel, 2004.

[HEI 99] Heinzelman, W. R., Kulik, J., and Balakrishnan, H. *Adaptive protocols for information dissemination in wireless sensor networks.* In Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking, pages 174.185, Seattle, WA, USA, 1999.

[HEI 00a] Heinzelman, W. R., Chandrakasan, A., and Balakrishnan, H. *Energy-efficient communication protocol for wireless microsensor networks.* In Proceedings of the Hawaii International Conference on System Sciences, Maui, Hawaii, USA, 2000.

[HEI 00b] Heinzelman, W. R. – *Application-Specific Protocol Architectures for Wireless Networks"* – Tese de doutorado, Instituto de Tecnologia de Massachussets (MIT), USA, 2000.

[HEI 01] Heidemann, J., Silva, F., Intanagonwiwat, C., Govindan, R., Estrin, D., and Ganesan, D. *Building efficient wireless sensor networks with low-level naming.* In Proceedings of the Symposium on Operating Systems Principles, pages 146.159, Chateau Lake Louise, Banff, Alberta, Canada. ACM, 2001.

[HIL 00] Hill, J. *A software architecture to support network sensors.* Master's thesis, UC Berkeley, 2000.

[INT 00] Intanagonwiwat, C., Govindan, R., and Estrin, D. *Directed diffusion: A scalable and robust communication paradigm for sensor networks.* In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, pages 56.67, Boston, Massachusetts, USA, 2000.

[INT 02] Intanagonwiwat, C., Govindan, R., Estrin, D., Heidemann, J., and Silva, F. Directed diffusion for wireless sensor networking. *ACM/IEEE Transactions on Networking*, 11(1):2.16, 2002.

[JIE 02] Jie Liu, Patrick Cheung, Feng Zhao, and Leonidas Guibas. *A dual-space approach to tracking and sensor management in wireless sensor networks.* In Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, pages 131{139. ACM Press, 2002.

[KAN 99] Kanaian, A. N. (1999). *A wireless sensor network for smart roadbeds and intelligent transportation systems.* M. eng. thesis, MIT EECS Department and The MIT Media Lab, June 2000.

[KAR 00] Karp, B. and Kung, H. T. *Gpsr: Greedy perimeter stateless routing for wireless networks.* In Proceedings of the 6th annual international conference on Mobile computing and networking, pages 243.254. ACM Press, 2000.

[KAR 03] Chris Karlof e David Wagner – *Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures* – University of California at Berkeley – IEEE, 2003.

[KUR 06] James F. Kurose e Keith W. Ross – *Redes de Computadores, uma abordagem top-down* – Editora Pearson/Addison Wesley, 2006.

[LEA 05] LEACH, implementação para o NS2
http://www-mtl.mit.edu/researchgroups/icsystems/cad_tools.html (consultado em 08 de abril de 2006).

[LIN 02] Lindsey, S., Raghavendra, C., and Sivalingam, K. M. *Data gathering algorithms in sensor networks using energy metrics.* IEEE Transactions on Parallel and Distributed Systems, 13(9):924. 935, 2002.

[LIN 03] Linnyer Beatrys Ruiz – *Maná: Uma arquitetura para gerenciamento de redes de sensores sem fio* – tese de doutorado, Universidade Federal de Minas Gerais, 2003.

[LIN 04] Linnyer Beatrys Ruiz, Luiz Henrique A. Correia, Luiz Filipe M. Vieira, Daniel F. Macedo, Eduardo F. Nakamura, Carlos M. S. Figueiredo, Marcos Augusto M. Vieira, Eduardo Habib Bechelane, Daniel Camara, Antonio A.F. Loureiro, José Marcos S. Nogueira, Diógenes C. da Silva Jr. – *Arquitetura para redes de sensores sem fio* – Departamento de Computação da UFMG, mini-curso apresentado no Simpósio Brasileiro de Redes de Computadores, SBRC04, 2004.

[MAC 04] Macedo, D. F., Correia, L. H. A., Nogueira, J. M., and Loureiro, A. A. *Proc: Um protocolo pró-ativo com coordenação de rotas em redes de sensores sem fio.* In Simpósio Brasileiro de Redes de Computadores, Gramado - RS, 2004.

[MAN 01] Manjeshwar, A. and Agrawal, D. *Teen: A routing protocol for enhanced effeciency in wireless sensor networks.* In 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, 2001.

[MIL 05] *Millennial net: Wireless sensor mesh networking.* http://www.millennial.net (consultado em 08 de abril de 2006).

[MIN 04] Mini, Raquel Aparecida de Freitas, Loureiro, Antonio Alfredo Ferreira, Nath, Badri – *The Distinctive Design Characteristics of a Wireless Sensor Network: The Energy Map* - Computer Communications. , v. 27, n.10, p.935 – 945 - 2004.

[MIT 05] MIT - Massachussets Institute of Technology - http://web.mit.edu/ (consultado em 08 de abril de 2006).

[NEW 04] James Newsome, Elaine Shi, Dawn Song, Adrian Perrig – *The Sybil Attack in Sensor Networks: Analysis & Defenses* – IPSN´04, Berkeley California – USA, 2004.

[NS2 06] NS-2: The network Simulator ns-2. http://www.isi.edu/nsnam/ns/ (consultado em 08 de abril de 2006).

[PAU 05] Paula, Luciano B. de, Trevelin, Luis Carlos – *Detecção de intrusão em redes de sensores sem fio através da contagem de nós* – SSI´05 – Simpósio de Segurança em Informática – São José dos Campos – Brasil - 2005.

[POL 03] Polastre, J. *B-mac protocol. Technical report*, Universidade da California, Berkeley, 2003.

[POT 00] Pottie, G. J. and Kaiser, W. J. Wireless integrated network sensors. *Communications of theACM*, 43(5):51.58, 2000.

[RAJ 03] Rajendran, V., Obraczka, K., and Garcia-Luna-Aceves, J. J. *Energy-efficient collision-free medium access control for wireless sensor networks*. In Proceedings of the first international conference on Embedded networked sensor systems, pages 181.192. ACM Press, 2003.

[RIC 04] Richard W. N. Pazzi, Regina B. de Araújo, Azzedine Boukerche – *Especificação e implementação de um protocolo tolerante a falhas e de baixa latência para redes de sensores sem fio* – Universidade Federal de São Carlos, Centro de Ciências Exatas e de Tecnologia, Departamento de Computação, 2004.

[SAN 04] Serdan Sancak, Erdal Cayiri, Vedat Coskun, Albert Levi – *Sensor Wars: Detecting and Defending Against Spam Attacks in WSNs* – IEEE Communication Society, 2004.

[SOH 00] Sohrabi, K., Gao, J., Ailawadhi, V., and Pottie, G. *Protocols for self-organization of a wireless sensor network.* IEEE Personal Communications Magazine, 7(5):16.27, 2000.

[SOU 05] Souto, Eduardo et. al. - *Obtenção do Consumo de Energia em Redes de Sensores sem Fio Utilizando Amostragem Estratificada*- 23º. Simpósio Brasileiro de Redes de Computadores - SBRC2005 - 2005.

[TAN 03] Tanenbaum, A. S. *Computer networks*. Prentice Hall PTR, 4th edition edition, 2003.

[TCL 06] TCL–*Tool Command Language*– http://www.cis.rl.ac.uk/Publications/Cookbook/ (acessado em 08 de abril de 2006).

[TR1 04] TR 1000. ASH Tranceiver TR1000 data sheet. http://www.rfm.com, 2004 (consultado em 08 de abril de 2006).

[VIE 04] Vieira, M. A. M. Embedded system for wireless sensor network. Master's thesis, Departamento de Ciência da Computação, Universidade Federal de Minas Gerais, Belo Horizonte-MG, Brasil, 2004.

[GTA 04] Grupo de Teleinformática e Automação - Universidade Federal do Rio de Janeiro - http://www.gta.ufrj.br/wsns/ (consultado em 08 de abril de 2006).

[WIN 05] *Wireless Integrated Network Sensors.* http://www.janet.ucla.edu/WINS/ (consultado em 08 de abril de 2006).

[WOO 01] Woo, A. and Culler, D. E. *A transmission control scheme for media access in sensor networks.* In Mobile Computing and Networking, pages 221.235, 2001.

[WOO 02] Antony D. Wood, John A. Stankovic – *Denial of Service in Sensor Networks* – University of Virginia, IEEE, 2002.

[YE 02] Ye, W., Heidemann, J., and Estrin, D. *An energy-efficient mac protocol for wireless sensor networks.* In Proceedings of the IEEE Infocom, pages 1567.1576, New York, NY, USA. USC/Information Sciences Institute, IEEE, 2002.

[YU 01] Yu, Y., Govindan, R., and Estrin, D. *Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks.* Technical Report UCLA/CSD-TR-01-0023, UCLA Computer Science Department, 2001.