Segurança em Redes de Sensores sem Fio
Protocolos e Estratégias de Ataque

Giovanni Jacy Nicodemos Emerenciano

Rua Amintas Jacques de Morais, 833 – Ouro Branco – Minas Gerais
CEP 36420-000

Orientador: Gustavo Campos Menezes
Banca de Avaliação: Luís Augusto Mattos Mendes, Élio Lovisi Filho

Resumo. *Prover segurança em RSSFs[1] é uma tarefa árdua, pois os algoritmos de segurança implementados tem que ser funcionais e ao mesmo tempo utilizar o mínimo possível de recursos dos nós sensores. Isto acontece pelo fato de as RSSFs terem uma grande limitação de energia dos nós sensores. No decorrer deste artigo serão apresentados protocolos de segurança e diversos tipos de ataques existentes para as Redes de Sensores sem Fio, sempre levando em consideração a longevidade e as limitações da rede.*

1 Introdução

Conforme apresentado por *Loureiro et al* em [4], o crescente avanço da tecnologia, tem tornado a miniaturização de componentes algo muito comum, e com isso surgem novas tecnologias que necessitam da utilização de componentes menores, porém com desempenho elevado. Este é o caso das Redes de Sensores sem Fio.

As Redes de Sensores sem Fio podem ser compostas por milhares de nós e um nó sorvedouro, onde estes nós utilizam se de uma estrutura miniaturizada de componentes eletrônicos e computadorizados que são: memória, processador, dispositivos de comunicação sem fio, sensores para a monitoração do fenômeno desejado, bateria e outros diversos componentes. Sendo estes programados, organizados e mantidos de acordo com a aplicação da Rede de Sensores sem Fio em questão, ou até mesmo em relação a funcionalidade do sensor em questão.

As Redes de Sensores sem Fio se diferem das redes tradicionais pelo fato de poderem possuir milhares de nós – dependendo da aplicação, terem problema com relação à limitação de energia, e até mesmo pelo fato de serem auto-configuráveis. Posto de uma forma simplificada, o conceito de auto-configuração se refere a "sistemas que autonomamente se adaptam à dinâmica dos seus parâmetros ambientais, sem necessidade de pré-configuração ou re-configuração manual, de forma a permitir uma distribuição ad hoc e proporcionando robustez ao sistema".

O problema em relação à energia, vem do fato de que na maioria das vezes as Redes de Sensores sem Fio estarem em locais onde não existe fonte de energia e/ou acesso dificultado. A necessidade de serem auto-configuráveis vem do mesmo problema, e se por ventura ocorrer falha ou perda de sensor, invasão, falha de comunicação, é necessário que os nós restantes tenham capacidade de se auto-configurarem para que não

[1] RSSFs é a abreviação para Redes de Sensores sem Fio

comprometam o funcionamento e a vida-útil da Rede de Sensores sem fio como um todo.

A comunicação nas Redes de Sensores sem Fio se dá entre os nós, ou seja, os nós se comunicam entre si sem a necessidade de intermédio de nenhum tipo de base, e daí a grande similaridade das Redes de Sensores sem Fio com as redes móveis Ad Hoc no ponto de vista de comunicação. Em uma Rede de Sensores sem Fio os nós tendem a realizar tarefas colaborativas, ou seja, os nós tendem somente a capturar, filtrar e assim prover dados para que sejam processados por nós especiais chamados Sink Nodes ou nós sorvedouros.

Atualmente as Redes de Sensores sem Fio têm sido aplicadas nos mais diferentes ramos. Tais como, segurança civil e militar, meio ambiente, indústria, medicina e etc. Onde cada uma dessas aplicações utilizam nós sensores particulares como: câmeras, microfones, termômetros e etc.

Alguns exemplos de aplicações para as Redes de Sensores sem Fio extraídas de *Loureiro et al*:

Ambiente – Monitoração de variáveis ambientais em florestas, mares, áreas urbanas, casas, prédios.

Tráfego – Monitoração de tráfego de veículos em rodovias e vias urbanas.

Segurança – Prover segurança a ambientes diversos com utilização de câmeras, microfones, sensores de movimento e som.

Militar – Monitorar áreas de difícil acesso ou hostis, movimentação inimiga, presença de materiais perigosos.

Industrial – Monitoração de processos e áreas industriais com elevada periculosidade.

Mais aplicações para as Redes de Sensores sem Fio podem ser encontradas em [4] e [5].

Pelo fato de as Redes de Sensores sem Fio terem aplicações diversas e que envolve a segurança de cidadãos comuns – vamos tratar da segurança em Redes de Sensores sem Fio, daí a necessidade de prover segurança para que as Redes de Sensores sem Fio trabalhem corretamente, porém prover segurança nas Redes de Sensores sem Fio é uma tarefa que exige grande cautela e estudo para não comprometer a vida útil e a funcionalidade da mesma. Estes problemas ocorrem pelo fato de as Redes de Sensores sem Fio possuírem uma grande limitação de recursos. Portanto, para prover segurança nas Redes de Sensores sem Fio é necessário mensurar a implicação da implantação da segurança em toda a rede, para que não a comprometa.

Durante o restante do artigo serão apresentadas, características diversas das Redes de Sensores sem Fio (seção 2), considerações sobre segurança e protocolos (seção 3), alguns motivos de falha nas Redes de Sensores sem Fio (seção 4) e também algumas estratégias de ataque (seção 5).

2 Redes de Sensores sem Fio e Protocolo S-MAC

De acordo com *Pereira et al*, as Redes de Sensores sem Fio são redes compostas por milhares de nós que se comunicam entre si por meio de comunicação sem fio e um nó responsável pela agregação das informações, que é conhecido como nó sorvedouro ou sink node (Figura 1), esses nós possuem bateria como fonte de energia e essas redes são formadas por: sensores, observadores e fenômeno.

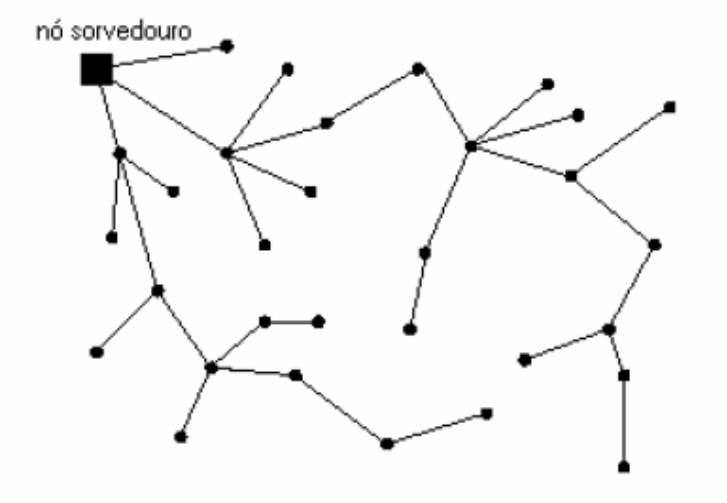

Figura 1. Redes de Sensores sem Fio, extraída de [7]

A figura 2 apresenta alguns modelos de micro-sensores resultantes de pesquisas de diversas instituições como, o SmartDust e COSTS Dust da Universidade da Califórnia - Berkeley, o WINS da Universidade da Califórnia, Los Angeles, o JPL Sensor Webs do Jet Propulsion Lab da NASA, todos extraídos de *Loureiro, A.*

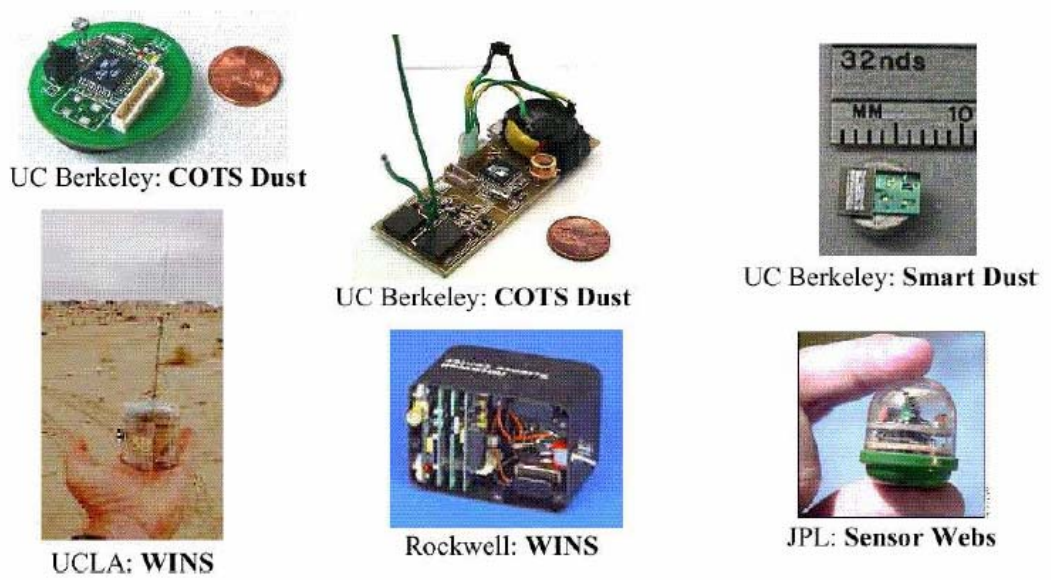

Figura 2. Modelos de Micro-Sensores, extraídos de [4]

O nó sensor é o dispositivo que faz a monitoração de um determinado fenômeno gerando diversos relatórios que são transmitidos através de comunicação sem fio. Os nós sensores podem ter características diferentes dependendo de sua aplicação, mas são compostos basicamente por: sensor, processador, bateria e rádio transmissor/receptor sem fio.

- Bateria: é a fonte de energia do nó sensor, possui capacidade finita e taxa de consumo.
- Rádio: representa todo o sistema de transmissão e recepção, amplificador e antena. O consumo de energia depende da tarefa que está sendo efetuada. A transmissão geralmente consome mais energia que a recepção.

- Processador: representa o elemento central de processamento do nó sensor. O consumo de energia depende do *clock* do processador do nó.
- Sensor: é o dispositivo responsável pelo sensoriamento do fenômeno.

Esses dispositivos utilizados nas Redes de Sensores sem Fio possuem escala e desempenho menor que os comumente usados e encontrados em equipamentos de grande porte, porém com o crescente avanço da tecnologia, esses dispositivos estão se aproximando cada vez mais dos dispositivos de grande escala quando se trata de processamento/desempenho. Como característica, na maioria dos modelos de sensores a sensibilidade ao fenômeno diminui com o aumento da distância do sensor ao fenômeno e aumenta de acordo com o tempo de exposição do sensor ao fenômeno.

Conforme apresentado por *Pereira et al*, o observador é o interessado final das informações coletadas e filtradas pela Rede de Sensores sem Fio é ele quem decide o que deve ou não coletar.

O fenômeno é de onde serão coletadas as informações para o observador. A Rede de Sensores sem Fio é construída de forma a estar próximo ao fenômeno e a partir de dado momento são coletadas e filtradas as informações de acordo com o interesse do observador.

Em uma Rede de Sensores sem Fio, os sensores coletam amostras locais de acordo com a informação, distribuem entre os outros nós e até mesmo para o observador.

Conforme apresentado por *Loureiro et al* em [4] e por *Pereira et al* em [5], pelo fato de as Redes de Sensores sem Fio utilizarem baterias e na maioria das vezes estarem dispostas em locais de difícil acesso, existe uma grande preocupação quanto ao consumo de energia da mesma. Com isso, os protocolos utilizados pelas Redes de Sensores sem Fio devem ser otimizados para serem eficientes na utilização da energia e assim elevar o tempo de vida útil do sistema.

A vida útil de uma Rede de Sensores sem Fio pode ser mensurada por parâmetros diversos, como tempo de envio e recebimento de dados, tempo de nós ativos e etc.

Considerando o problema de energia citado, foi desenvolvido o protocolo S-MAC (Sensor Medium Access Control) mostrado por *Silva et al* . Este protocolo é utilizado para controlar o acesso ao meio para as Redes de Sensores sem Fio, e para isso o S-MAC faz com que os nós tornem-se rapidamente ativos dada a ocorrência do fenômeno desejado. Para isso ele utiliza 3 técnicas:

1. Nós ficam inativos para economizar energia.
2. Formação de clusters entre nós para realizarem auto-sincronização.
3. Transmissão/Recepção sem fio ficam inativos durante transmissões para outros nós.

As Redes de Sensores sem Fio devem ainda possuir uma tolerância razoável a falha dos sensores, falhas estas que podem ser causadas por exaurimento de bateria ou condições físicas dos sensores. Estas falhas devem passar despercebido para os outros nós da Rede de Sensores sem Fio e uma maneira de se fazer isto é utilizar a replicação de informação.

Como exemplo de protocolo de replicação de dados, podemos utilizar os protocolos SPIN (Sensor Protocols for Information via Negotiation) conforme mostrado por *Pereira et al* em [5] e por *Campista et al* em [7]. Estes são protocolos adaptativos para disseminação de dados em Redes de Sensores sem Fio. Nós que utilizam os protocolos de comunicação SPIN, fazem a transmissão de meta-dados, que é uma espécie de dicionário de dados que contém um conjunto de informações para serem analisadas e a partir

da análise detectar se esses dados são necessários à aplicação em questão, e assim eliminam a redundância de informação na Rede de Sensores sem Fio.

Os protocolos SPIN são considerados os melhores quando se é levado em consideração o desempenho e o consumo de energia, tanto para Redes de Sensores sem Fio ponto-a-ponto quanto para Redes de Sensores sem Fio Broadcast.

Existem diversos tipos de protocolos SPIN, tais como:

SPIN-PP/SPIN-EC – Redes de Sensores sem Fio ponto-a-ponto

SPIN-BC/SPIN-RL – Redes de Sensores sem Fio broadcast

3 Segurança

Conforme apresentado por *Campista et al* em [7] e *Oliveira et al*em [3], as Redes de Sensores sem Fio empregam grande número de nós sensores comunicando e desenvolvendo padrões irregulares de processamento distribuído ad hoc, que por sua vez podem produzir informação de alta qualidade com consumo minimizado de recursos. Para prover confidencialidade, integridade e autenticação, esquemas de segurança deverão ser adotados, como por exemplo, mecanismos de criptografia e assinatura digital. Estas funcionalidades de segurança são difíceis de disponibilizar devido à natureza não estruturada da rede, a conectividade intermitente e a limitação de recursos.

Toda rede para ser considerada segura deve cumprir determinados requisitos. Cabe ao administrador da rede avaliar entre os objetivos da rede e sua funcionalidade quais dos objetivos apresentados, satisfarão a condição de seguridade da Rede de Sensores sem Fio. Este estudo deve ser levantado com muito cuidado para tentar obter o menor custo de usabilidade dos recursos de cada nó sensor, visando assim uma maior vitalidade da Rede de Sensores sem Fio.

A rede deve estar sempre disponível para usuários autorizados, portanto deve estar livre de ataques de negação de serviços (DoS – Denial of Service).

A rede deve prover um grau elevado de confidencialidade das informações que nela trafegam. Se houver invasão na rede o intruso poderá interceptar as informações, porém deve ser incapaz de compreendê-las. Isto pode ser feito através da implantação de algoritmos de criptografia na estrutura da rede.

A autenticidade apresentada por *Campista et al*, garante que todas as informações recebidas por um determinado nó são realmente de uma fonte segura, evitando assim que nós maliciosos façam injeção de dados. A autenticidade se faz necessária principalmente para proteger informações relevantes ao funcionamento correto da rede ou para evitar que invasores se passem por usuários autorizados e façam alterações nos dados da mesma. Para verificar se o dado foi realmente originado pelo nó indicado podem ser utilizados protocolos que fazem desafios aos nós transmissores. Estes enviam mensagens em texto claro para que os nós que estão sendo autenticados criptografem com sua chave. A autenticidade é confirmada através da decriptografia dos dados enviados ao mecanismo autenticador, que posteriormente ao recebimento do desafio verifica se a chave utilizada é realmente de quem diz ser e se a mensagem é a mesma que foi originada. Outro mecanismo seria a troca de uma chave secreta para computar um código de autenticação de mensagem, porém essa solução não é segura porque a propagação das mensagens é em broadcast sendo esta uma característica do meio e assim poderia ocorrer que nós invasores recebessem esta mensagem podendo assim ser autenticados na rede.

A atualização garante que informações não sejam disseminadas na rede mais de uma vez, isto pode ser feito através da atualização das chaves criptográficas, ou seja, as chaves criptográficas teriam um tempo de expiração e a partir daí seriam renovadas.

A integridade dos dados garante que uma determinada informação não foi manipulada durante o processo de envio de dados.

Com o crescente uso das Redes de Sensores sem Fio, gerou-se a necessidade de prover segurança nas mesmas, e para isto são usados os algoritmos de segurança a nível de roteamento. Esses algoritmos devem apresentar um alto nível de desempenho, ou seja, se falando de Redes de Sensores sem Fio eles devem desempenhar o papel de asseguradores da rede gastando o mínimo de energia possível. A seguir serão apresentados dois algoritmos de segurança em Redes de Sensores sem Fio.

3.1 SPINS

O SPINS (Security Protocols for Sensor Networks) [7] [3] é composto por dois protocolos. O µTESLA que é o responsável por prover autenticação quando há comunicação em broadcast e o SNEP que é o responsável pela confidencialidade, autenticação da comunicação ponto a ponto e atualização dos dados com baixo overhead.

O SNEP confia num contador compartilhado entre transmissor e receptor utilizando-o como um vetor de inicialização para que o algoritmo de criptografia utilizado possa criptografar e decriptografar os dados. Devido a limitação dos sensores tanto de energia como de processamento, os algoritmos utilizados para criptografia são menos robustos, porém não deixam de ser eficazes. Como ambos participantes possuem o contador e o incrementam após cada bloco de dados criptografados, o contador não precisa ser enviado a cada transmissão.

Para autenticar transmissor e receptor e manter a integridade dos dados é utilizado um código de autenticação de mensagem.

O µTESLA utiliza um método para autenticar comunicação em broadcast a partir de chaves simétricas emulando assimetria para que nenhum receptor não autorizado consiga obter a chave. Para isso o protocolo envia ponto a ponto a cada nó participante da rede, os parâmetros necessários para a comunicação ser segura e para o algoritmo poder funcionar. A autenticidade desses parâmetros é garantida por uma assinatura digital. Existem propostas que tentam otimizar esse processo de transmissão de parâmetros para que não seja ponto a ponto, pois em uma rede com muitos nós esse processo induziria um grande atraso.

A assimetria que o µTESLA introduz é devido à característica do protocolo de sempre atualizar a chave criptográfica simétrica e somente transmiti-las em broadcast no final de intervalos de tempo pelas ERBs[2]. A partir dessa chave, os receptores terão condição de construir cadeias de chaves e assim autenticar as chaves recebidas, pois ao receber a chave essa deve pertencer a cadeia de chaves computadas através de uma função aleatória.

Só então as mensagens poderão ser decriptografadas. Dentro desse intervalo de tempo, todos os nós utilizam a mesma chave. Essa cadeia de chaves é obtida a partir de um dos parâmetros que foi recebido no início processo. Ataques de repetição são evitados porque os nós têm como identificar a que intervalo pertence à chave recebida e, portanto, não a utilizam posteriormente.

[2] ERBs é a abreviação para Estações Rádio Base, ou somente Estações Base

A estação base ou nó sorvedouro novamente é considerado fora de risco de ataques e, portanto é confiável.

3.2 INSENS

O INSENS (Intrusion-Tolerant Routing Protocol for Wireless Sensor Networks) [7] [3] leva em consideração a possibilidade da existência de nós intrusos na rede, por isso é capaz de detectá-los. O INSENS parte do pressuposto que um nó malicioso só consegue prejudicar os nós da vizinhança e nunca a rede como um todo.

O INSENS tem o objetivo de evitar ataques do tipo DoS (Denial of Service), somente a estação rádio base tem autorização para realizar inundações na rede, e para que um nó malicioso não se passe pela ERB, a mesma possui uma autenticação junto à Rede de Sensores sem Fio.

Para eliminar a introdução de rotas falsas na Rede de Sensores sem Fio, a ERB faz a disseminação e o processamento de todas as rotas da rede e depois envia as tabelas de rotas autenticadas para os nós da rede, isto evita que um nó malicioso tente inserir uma rota de comunicação falsa na rede. Para atingir a confidencialidade e autenticidade das informações, são utilizados algoritmos de criptografia simétrica pois são funcionais e mais leves que os demais tipos de algoritmos de criptografia, e assim também efetuando uma grande economia de energia.

O fato de INSENS utilizar a transferência de dados em múltiplas rotas tem como objetivo permitir que se por ventura for detectado um nó intruso na rede, tenha assim a possibilidade de transmitir todos os pacotes para todos os nós sem passar pelo nó intruso, ou seja, utilizando caminhos alternativos na rede.

3.3 Segurança nas ERBs

Partindo do pressuposto que as ERBs possuem uma capacidade de processamento elevada e utilizam algoritmos de segurança mais poderosos, mesmo assim elas estão sujeitas a ataques.

Como forma de prover uma maior segurança nas ERBs, foi proposto por *Deng* no ano de 2003 conforme apresentado em [7], existem três formas para prover mais seguranças nas ERBs (figura 3):

1. Definir mais de uma ERB e assim possuir mais de um caminho para atingir as ERBs;
2. Esconder o endereço do destinatário nos pacotes que estão sendo transferidos, pois caso ocorra uma interceptação em um pacote o nó invasor pode descobrir o endereço de uma das ERBs, e isso possibilitará um grande estrago na rede; e
3. Fazer o deslocamento das ERBs dentro da rede, ou seja, as ERBs de tempos em tempos se movimentariam dentro da rede, se tornariam ERBs dinâmicas.

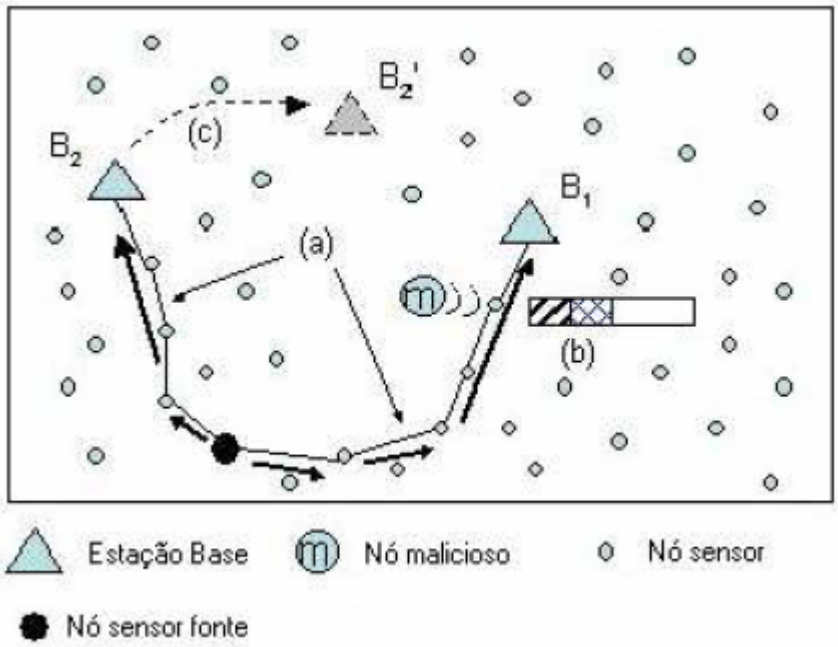

Figura 3. Segurança nas Estações Rádio Base extraída de [7]. (a) situação 1, (b) situação 2 e (c) situação 3

4 Falhas nos nós sensores

Existem dois casos distintos de falhas de acordo com *Silva et al,* o primeiro é quando somente um nó falha e o segundo é quando ocorrem falhas em diversos nós da Rede de Sensores sem Fio.

No primeiro, a correção se dá por meio da geração de uma nova topologia de roteamento contornando a rota em torno do nó inativo.

No segundo, é emitido um aviso sobre o mal funcionamento de muitos nós.

A distinção entre os dois casos se dá através de um controle existente na estação base que é um *trace* dos nós ativos ou inativos na Rede de Sensores sem Fio.

Como tentativa de permitirem a recuperação das possíveis falhas nas Redes de Sensores sem Fio, pode ser considerado o Roteamento de Múltiplas Rotas proposto por Ganessal et al. Para isso foi proposta a construção de dois tipos de rotas para a recuperação de falhas pela rota mais curta entre o nó fonte e o nó destino. E também algoritmos simples que fazem o roteamento de mensagens por todas as rotas possíveis entre o nó fonte e o nó destino.

5 Estratégias de ataques às RSSFs

De acordo com *Campista e Oliveira et al,* algumas características e ataques podem ser específicos de determinadas camadas do modelo OSI, que é o modelo desenvolvido pela ISO para padronizar os modelos de produtos para a comunicação de dados em redes de computadores. Os ataques são mais perigosos se forem sobre a camada de enlace e de rede.

É importante ser observado que um ataque pode ser mais perigoso e mais difícil de contornado se for combinado com outros, independente das camadas atingidas. A se-

guir serão apresentadas algumas formas de ataques separados pelas camadas de rede que eles afetam.

5.1 Camada Física

Conforme apresentado por *Campista et al* em [7], pelo fato de os nós sensores possuírem uma séria restrição quanto a energia, muitos ataques são feitos para exaurir a fonte de energia ou mesmo diminuir o tempo de vida dos nós sensores.

Como forma de ataque, temos como exemplo o DoS (Denial of Service) que tem como objetivo bloquear o serviço da rede visando impedir o funcionamento normal da rede. Para isso são feitas tentativas de exaurir a fonte de energia dos nós sensores sobrecarregando-os.

Outros ataques introduzem ruídos na mesma freqüência da comunicação dos nós sensores com o intuito de prejudicar a comunicação.

Como forma de evitar esses tipos de ataque pode-se usar as técnicas de espalhamento de espectro por salto de freqüência ou aumentar a potência de transmissão em relação ao sinal x ruído, porém esta última por enquanto é inviável visto que seu funcionamento demanda muito gasto de energia.

A técnica de espalhamento de espectro por salto de freqüência tem como objetivo dividir a banda passante total em vários canais de pequena banda e fazer com que o transmissor e o receptor fiquem em um desses canais por um certo tempo e depois salte para outro canal.

5.2 Camada de Enlace

Nas Redes de Sensores sem Fio prover segurança ao nível da camada de enlace é crítico pelo fato de estarem dispostas em meios abertos, porém há a possibilidade de limitação do alcance das transmissões e assim diminuindo a possibilidade de interceptação do sinal. [7]

Ataques à camada de enlace podem prejudicar a rede ao nível de pacote. Isso pode ser feito através de indução de colisões, danificação de pacotes de dados ou de controle. Porém esses ataques podem ser detectados através do *checksum*, ou seja, através da computação de um valor que depende dos índices de um bloco de dados que é transmitido juntamente com o pacote a fim de detectar a corrupção do pacote e assim poderem ser corrigidos. O que isso pode ocasionar é a repetição das mensagens até que elas consigam ser recebidas corretamente se for utilizado algum mecanismo de confiabilidade para transferência de dados. [7]

5.3 Camada de Rede

Pelo fato de as Redes de Sensores sem Fio terem a característica de transmissão por múltiplos saltos, a camada de rede é a camada mais afetada e a que pode gerar maiores danos quando invadidas. Os ataques na camada de rede tem o objetivo de prejudicar o roteamento e a transferência de dados. Nesta seção serão apresentados os mais conhecidos tipos de ataques às camadas de rede de acordo com *Campista et al* e *Oliveira et al*.

5.3.1 Spoofing

Esse tipo de ataque faz a disseminação de mensagens contendo rotas falsas na rede, causa *loops*, atraem ou repelem o tráfego, tendo como principais alvos as mensagens que contêm s informações de roteamento da rede.

5.3.2 Encaminhamento Seletivo

Esse tipo de ataque se dá quando um nó malicioso ao receber uma mensagem da rede não a encaminha para o próximo nó da rede, fazendo assim uma espécie de buraco negro na rede, o que pode proporcionar uma grande perda de informações. Esse tipo de ataque só é possível pelo fato de as Redes de Sensores sem Fio serem um tipo de rede salto por salto, onde se um nó não colaborar essa rede passa a ter uma falha.

Pelo fato de as Redes de Sensores sem Fio possuírem múltiplas rotas para chegar a um determinado destino, esse tipo de ataque somente é possível em uma rota e caso este nó malicioso estivesse participando da rota principal de transmissão de dados da rede, esse ataque seria mais perigoso.

Caso em determinada Rede de Sensores sem Fio fosse utilizada a métrica de roteamento baseada na justiça, a perda de dados seria maior pelo fato de a rede disseminar mais dados para o nó sensor que não está dando continuidade nas transmissões. Essa perda aconteceria até o momento que através de mecanismos detecção de intrusos (IDS) ou até a rede perceber que o nó em questão poderia estar com falha e assim refazer as rotas de transmissão, tirando o nó malicioso das rotas de transmissão da rede.

5.3.3 Worm Holes

Um *wormhole* é um túnel criado dentro da Rede de Sensores sem Fio pelos atacantes, esse túnel necessita que dois nós maliciosos estejam instalados na rede, onde cada um será uma das extremidades do túnel. Esse túnel geralmente possui um maior tempo de propagação da informação ao destino.

Os nós maliciosos após instalados na rede, utilizando a técnica da inundação tentam convencer seus nós vizinhos que utilizar o túnel é a forma mais rápida para a transmissão da informação pela rede e quanto mais próximos do nó sorvedouro, mais informações poderão passar pelo túnel, gerando assim diversos problemas em relação ao roteamento planejado para a rede (figura 4).

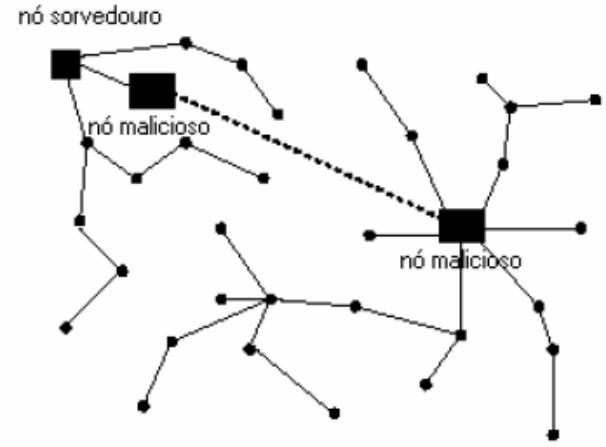

Figura 4. Representação de um WormHole em um RSSF extraída de [7]

5.3.4 Ataque de Inundação *HELLO*

Pelo fato de muitos protocolos de roteamento utilizarem a técnica de emissão de pacotes *HELLO* para a vizinhança afim de confirmar a conectividade dos nós vizinhos, nós maliciosos podem utilizar a mesma técnica para fazer com que os outros nós pensem que ele é seu vizinho e assim incluí-lo em sua rota de transmissão e aceitar as rotas de transmissão impostas pelo nó malicioso.

O tipo de inundação utilizado para esse fim é salto por salto, então a inundação de pacotes *HELLO* se dá num único salto pelo fato de serem feitas a partir de nós de maior porte.

5.3.5 Anel da Maldade

Esse tipo de ataque consiste em circundar qualquer nó da rede por nós maliciosos e assim esses nós maliciosos vão se recusar a encaminhar e vão injetar informações erradas no anel. Quando uma rede se encontra muito comprometida ou um nó está cercado por muitos nós maliciosos é muito difícil encontrar soluções.

5.3.6 Loop

Podem ser introduzidos na rede loops ou detours (desvios), que através de informações de roteamento transmitidas por nós comprometidos tendem a fazer com que informações fiquem circulando pela rede visando diminuir o tempo de vida da rede ou até exaurir todas as suas energias.

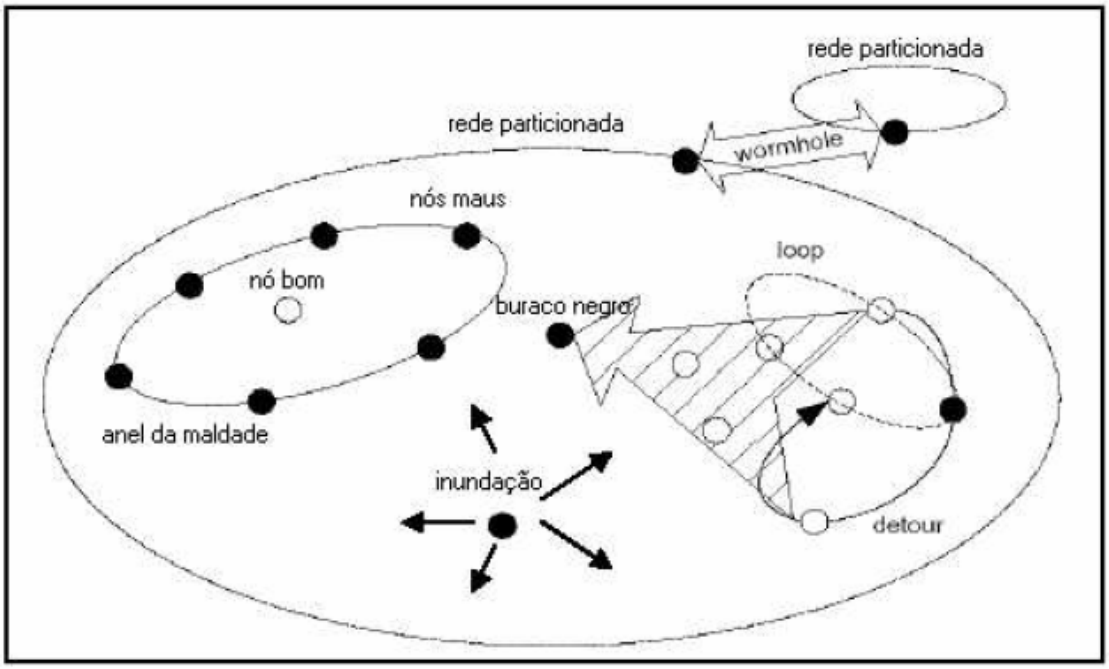

Figura 5. Representação das estratégias de ataque em uma RSSF extraída de [7]

6 Conclusão

Diante dos problemas relacionados às limitações dos nós sensores, prover segurança, confidencialidade, integridade e autenticidade em uma Rede de Sensores sem Fio demanda muito estudo e trabalho, visto que se tratando de uma tecnologia nova já existem diversas técnicas para invasão e também diversos algoritmos.

Ainda existe muito o que fazer visto que as práticas de invasão estão se tornando cada vez mais eficazes e os algoritmos obsoletos, portanto estudar algoritmos de implementação de segurança para Redes de Sensores sem Fio é uma prática importante porém não se deve jamais deixar de lado as questões de limitação dos nós que compõem as Redes de Sensores sem fio, ou seja, prover segurança deve ser de forma eficaz e também com baixos custos de processamento e energia.

Com relação a energia, já estão sendo feitos estudos sobre a implantação de energia solar, com isso num futuro bem próximo prover segurança será mais fácil e eficaz.

7 Referências Bibliográficas

[1] Ribeiro, W., Figueredo, T., Wong, H. e Loureiro, A. Detecção de nós maliciosos em Redes de Sensores sem Fio. Estudo do caso realizado na SensorNet - UFMG.

[2] Silva, A., Teixeira, F., Wong, H. e Nogueira, J. Aspectos de Detecção de Intrusos em Rede de Sensores sem Fio. Estudo do caso realizado na SensorNet - UFMG.

[3] Oliveira, S., Nogueira, J. e Wong, H. Segurança em Redes de Sensores sem Fio. Estudo do caso realizado na SensorNet - UFMG.

[4] Loureiro, A., Nogueira, J., Ruiz, L., Mini, R., Nakamura, E. e Figueiredo, C. Redes de Sensores sem Fio. Estudo do caso realizado na SensorNet - UFMG.

[5] Pereira, M., Amorim, C. e Castro, M. Tutorial sobre Redes de Sensores. Estudo do caso realizado por estudante das UFRJ.

[6] Guimarães, G., Souto, E. e Kelner, J. e Sadok, D. Avaliação de Mecanismos de Segurança em uma Plataforma de Redes de Sensores sem Fio.

[7] Campista, M. e Duarte, O. Segurança em Redes de Sensores sem Fio. Estudo do caso realizado pelo grupo de Teleinformática e Automação da UFRJ.

[8] Silva, F. Uso eficiente de energia em Redes de Sensores. Estudo do caso realizado na UERJ.