Segurança em Redes de Sensores

Miguel Elias Mitre Campista[1], Otto Carlos Muniz Bandeira Duarte[1]

[1]Grupo de Teleinformática e Automação – Universidade Federal do Rio de Janeiro (UFRJ)
Caixa Postal 68.504 – 21.945-970 – Rio de Janeiro – RJ – Brasil

{miguel,otto}@gta.ufrj.br

Abstract. *This paper has the objective to present the main challenges to provide safety to wireless sensor networks given its hardware constrains and its energy storage problems. It will be presented the main attacks that this kind of network is subjected and what are the main proposals to provide safety. Known its real importance and the uncountable applications that must come there still much to develop in this technology that is in wide expansion and opened to new ideas.*

Resumo. *Este artigo tem como objetivo apresentar os principais desafios para prover segurança às redes de sensores dadas as suas limitações de hardware e os seus problemas de armazenamento de energia. Serão apresentados os principais ataques aos quais esse tipo de rede está sujeito e quais as principais propostas para prover segurança. Visto sua real importância e as inúmeras aplicações que irão surgir ainda há muito que desenvolver nesse setor que está em plena expansão e em aberto a novas idéias.*

1. Introdução

Sensores são pequenos dispositivos que surgiram com o avanço da tecnologia de sistemas micro-eletro-mecânicos (MEMS), comunicações móveis e técnicas da eletrônica digital conhecidas como VLSI.

A técnica de fabricação VLSI (*Very large-scale integration*) permite a integração micro-mecânica, analógica e digital de dispositivos microeletrônicos em um mesmo chip produzindo sistemas multifuncionais.

Os MEMS são micromáquinas de silício construídas da mesma forma que um circuito integrado, porém ao final, o dispositivo é desprendido ou partes são deixadas livres para se moverem. A intenção é que esses dispositivos sejam fabricados em paralelo e em grande escala para que não sejam caros, porém o que é observado é que preço atual ainda não é satisfatório.

MEMS oferecem atributos desejáveis como pequeno tamanho, alta velocidade, baixa potência e um alto grau de funcionalidade. Esta nova tecnologia tem aplicações nas mais variadas áreas: moduladores de dados, atenuadores variáveis, nós ativos remotos (nós sensores), equalizadores, ADMs, comutadores ópticos, limitadores de potência, *crossconnects* ópticos. [Bishop 2002]

Os sensores foram concebidos com o principal objetivo de monitoração remota de ambientes hostis ou de difícil acesso. Esses dispositivos foram desenvolvidos e inicialmente utilizados em aplicações militares com o objetivo de monitorar o campo de batalha em busca de ameaças, como por exemplo, a detecção de radioatividade ou de movimentação inimiga.

Ao longo do tempo, novas aplicações vêm sendo desenvolvidas. Em grande parte delas a segurança se faz fundamental por se tratar de informações sigilosas e que não podem correr o risco de serem ouvidas por usuários maliciosos. O controle dos reatores de uma usina, a detecção de intrusos num ambiente de acesso restrito, o monitoramento de uma área de importância estratégica, os testes realizados num novo tipo de automóvel, dentre outros são possíveis exemplos onde a aplicação de segurança no tráfego de informações é fundamental.

Porém os sensores possuem grandes restrições ao nível de energia e de capacidade de processamento. Seu hardware é bastante restrito e suas baterias muito limitadas. Esses problemas impõem sérias barreiras para a aplicação de mecanismos de segurança, como algoritmos mais confiáveis. O *Smart Dust*, por exemplo, é um projeto da Universidade de Berkeley [Pister 1999] onde os sensores possuem uma CPU com processamento de 4MHz, memória RAM de 512 bytes e memória flash de 8kHz, onde só o sistema operacional ocupa 3,5kHz. O aumento da memória e do poder de processamento de cada sensor implicaria no aumento dos custos por unidade, havendo assim, a perda do seu princípio fundamental que é o baixo custo para que seja utilizado e produzido em grande quantidade.

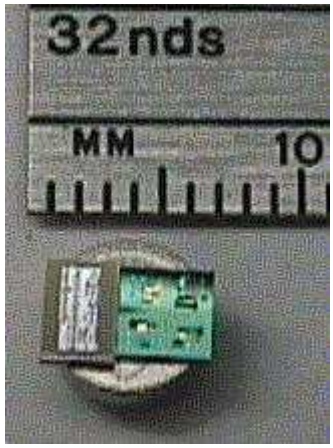

Figura 1. Nó sensor pertencente ao projeto Smart Dust.

As redes de sensores então, são compostas por nós sensores que são capazes de se comunicar e trocar informações, um nó de uma rede de sensores pode contêr mais de um sensor. Nesse cenário serão introduzidos os mecanismos de segurança, principalmente ao nível de camada de rede.

Esse tutorial tem como objetivo apresentar as principais ameaças que as redes de sensores são submetidas, os algoritmos de segurança propostos, em especial o SPINS [Perrig 2001], por ser o mais conhecido e o que apresentou a proposta mais completa e mais eficiente. Irá mostrar também que mecanismos de segurança em redes de sensores ainda têm muito que evoluir e ainda se mostra em aberto para pesquisa e desenvolvimento técnico.

Na seção número dois será descrito a arquitetura de uma rede de sensores e como eles trocam informação. Na seção número três, será descrito quais são os objetivos e principais obstáculos durante a adoção de algoritmos de segurança para as redes de sensores. Na seção número quatro, será descrito todos os principais ataques exercidos contra as redes de sensores por camada do modelo OSI (*Open System Interconnect*). Na seção número cinco será apresentado os principais algoritmos e protocolos que vem sendo utilizados para superar os problemas de segurança ao nível de roteamento. Na seção seis será apresentado as dificuldades existentes durante a escolha das chaves criptográficas. Na seção sete será apresentado uma proposta que garante segurança às estações rádio base.

2. Arquitetura de redes de sensores

As redes de sensores são compostas por nós responsáveis pelo sensoriamento e pelo envio das informações coletadas a um nó que agrega informações. Esse nó pode ser um outro nó comum da rede ou um nó de maior capacidade, em todo o caso a informação tende sempre a fluir na direção de um ponto centralizador que pode ser uma ERB ou um computador de maior porte. Esse nó é conhecido como nó sorvedouro. Como a informação atinge o nó sorvedouro depende do algoritmo sendo utilizado na camada de rede.

Figura 2. Rede de sensores. O nó quadrado é o nó sorvedouro e os nós que são ligados por mais de dois arcos são nós agregadores. [Karlof 2003]

A ERB ou o computador de maior porte será então responsável por conectar a rede de sensores a rede externa, para que o tráfego de dados então atinja o usuário da rede que pode estar monitorando-a remotamente. Percebe-se então, que esse ponto centralizador é de fundamental importância para a segurança da rede e a maioria das propostas parte do princípio que este ponto é seguro e confiável assim como a rede externa que conecta o usuário remoto à rede de sensores.

As redes de sensores são consideradas um tipo de rede ad hoc por muitos autores [Hu 2003][Karlof 2003][Law 2002] e assim são comparadas com as mesmas. Essa associação é devido às suas características de auto-configuração, resistência à falhas, dinamicidade, a capacidade de comunicação direta entre dois nós sem a necessidade da presença de um ponto de acesso e a não necessidade de infra-estrutura pré-estabelecida.

Essa última característica é contraditória, pois há sempre a presença de uma ERB ou de um outro elemento capaz de agregar as informações o que caracteriza uma infra-estrutura, como seria um ponto de acesso numa rede IEEE 802.11 infra-estruturada. Law em [Law 2003] diz que as redes de sensores combinam as características de uma rede ad hoc ao nível de sistema com características de sensores ao nível de componentes. As diferenças entre as redes de sensores e redes ad hoc são:

Aplicação de tipo específico: As redes de sensores têm a sua aplicação pré-definida no momento em que começam a ser utilizadas. Já as redes ad hoc possuem maior flexibilidade, por terem maior poder computacional e por não serem utilizadas em lugares de difícil acesso o que favorece possíveis reprogramações.

Encaminhamento de pacotes: As redes de sensores, na maioria das aplicações apenas enviam seus dados para um vizinho num único salto sem a capacidade de escolher melhores rotas. Já nas redes ad hoc cada nó tem capacidade de rotear o pacote e escolher o melhor caminho fazendo também comunicação nó a nó.

Limitação de energia: Os sensores têm geralmente uma quantidade de potência finita que quando acaba o torna sem utilidade. Os nós de uma rede ad hoc podem recarregar energia, além de possuir uma capacidade de armazenamento superior.

Limitação de memória e capacidade de processamento: A maioria dos algoritmos de segurança necessita de um poder de memória e processamento que os sensores não possuem para armazenar chaves criptográficas e processar algoritmos. Propostas que aproveitem algoritmos já aplicados em redes ad hoc ou até mesmo em redes cabeadas não são aplicáveis na maioria dos casos, pois estão além da capacidade dos sensores.

Grande número de nós: o número de nós numa rede de sensores é bem maior do que numa rede ad hoc comum, esse fator influencia na conectividade. A maioria dos sensores não possui identificação global, porque sempre se comunicam com um vizinho mais próximo evitando assim desperdício de energia. Além disso, a inclusão de endereços globais aumentaria o *overhead* das mensagens transferidas.

Facilidade de falhas: Os sensores estão susceptíveis a falhas que os nós ad hoc não estão, principalmente devido às suas restrições de energia e as aplicações as quais podem estar sendo submetidas. Por exemplo, em aplicações militares pode se encontrar um alto risco ao monitorar um território inimigo. Em vista disso, as redes de sensores devem ser mais robustas que as redes ad hoc.

Mobilidade: Na maioria das aplicações os nós sensores são fixos enquanto os nós em redes ad hoc devem levar em consideração a mobilidade como um fator de maior importância no desenvolvimento de aplicações e algoritmos.

Tipos de comunicação: Nas redes de sensores os tipos de comunicação são mais específicos que nas redes ad hoc que tem capacidade de rotear. Nas redes de sensores são realizadas comunicações nó a nó para reconhecer a direção dos vizinhos do nó emissor através de transmissão de sinais em *broadcast,* ou para reconhecer a direção dos nós agregadores dentro da própria rede. Pode ser realizada também comunicação de muitos nós para um único nó, para os nós enviarem informações ao nó agregador, ou ao nó sorvedouro. E finalmente o outro tipo de comunicação entre os nós de uma rede de sensores é a comunicação de um só nó para muitos, que é utilizada principalmente quando sinais de controle são úteis para mais de um nó, sendo transmitidos de um nó agregador para os que estão sob a sua área de influência. [Karlof 2003]

Em vista dessas diferenças percebe-se que a maior limitação e o maior obstáculo a ser superado para incluir mecanismos de segurança nas redes de sensores são as suas limitações de energia e processamento. Portanto todos os algoritmos propostos têm como principal objetivo otimizar esses parâmetros. Enquanto as redes ad hoc têm como principal objetivo fornecer QoS para que, principalmente aplicações multimídia, possam trafegar e superar as imprevisibilidades do meio de transmissão e a mobilidade dos nós, já que energia não é fator limitante.

3. Requisitos de Segurança

Toda a rede para ser considerada segura deve cumprir determinados requisitos. O importante é saber, diante da aplicação em questão, quais dos objetivos a seguir [Hu 2003] se fazem relevantes e que devem ser levados em consideração pelo administrador da rede durante a fase de escolha do algoritmo a ser utilizado para não sobrecarregar os sensores, dadas às suas limitações.

3.1.Objetivos

A rede deve estar sempre disponível para usuários autorizados, portanto deve estar livre de ataques de negação de serviço (DoS- Denial of Service). Este é um tipo de ataque que exaure os recursos da rede sobrecarregando-a. Deve-se ter cuidado também para que determinados serviços que consumam muita energia não sejam utilizados para que a rede não tenha um tempo de vida reduzido. A disponibilidade da rede pode ser prejudicada involuntariamente se houver a incidência de um espectro de freqüências por sinais espúrios que sejam iguais as utilizadas pela rede. As técnicas de espalhamento de sinais e de saltos de freqüências já tendem a contornar ou ao menos amenizar esse problema.

Outro objetivo é a confidencialidade dos dados onde um intruso que roube as informações trocadas pelos nós não tenha condição de compreender a informação obtida. Esse objetivo é alcançado a partir da criptografia dos dados, onde as chaves criptográficas devem ficar em poder dos nós. Quanto mais chaves cada nó tiver condição de utilizar e se cada nó tiver a sua própria chave mais confidencial será a informação. A questão é saber analisar qual o impacto que a inclusão de criptografia irá causar para rede devido as suas limitações.

A autenticidade 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. [Perrig 2001]

A atualização garante que determinadas informações não sejam copiadas e posteriormente sejam injetadas novamente na rede. Os dados copiados seriam autênticos, porém não seriam mais válidos. Dependendo da aplicação esse tipo de ação pode ser bastante danosa. A atualização pode ser alcançada através de renovações de chaves criptográficas, onde as chaves só são válidas por intervalos de tempo e os nós que se comunicam e pertençam a rede têm conhecimento dessas mudanças.

Já a integridade dos dados garante que os dados não foram alterados em trânsito por um adversário. Esse mecanismo é geralmente implementado por funções *hash*. Um determinado dado pode ser manipulado sem que o atacante nem ao menos saiba do que se tratava, por estar criptografado.

Os nós devem ser resistentes a manipulação, pois um usuário malicioso ao ter acesso a um nó, não pode obter informações sigilosas como, dados, código e até mesmo a chave criptográfica ou alguma pista que lhe leve a tal. Em posse de tais informações um nó falso pode ser incluído na rede comprometendo-a.

Todos os nós devem colaborar para o funcionamento da rede, ou seja, nenhum nó pode entrar na rede e se negar a encaminhar pacotes de dados ou de controle. Para detectar uma invasão desse tipo seria necessário algum mecanismo que detectasse anomalias na rede através de algum sistema de IDS, porém esse mecanismo ainda é muito sofisticado para sua inclusão nesse momento de desenvolvimento das redes de sensores por causar grande gasto de energia. [Law 2002]

3.2.Obstáculos

Num algoritmo de criptografia para redes de sensores existe um compromisso entre a segurança provida pelo algoritmo e a quantidade de energia que ele utiliza. Em vista disso já foram feitos testes comparativos por Law comparando o TEA e o RC5 em [Law 2002]. A escolha desses dois algoritmos foi feita por serem aplicáveis às redes de sensores.

Este tipo de estudo se faz importante porque é necessário energia para criptografar dados, decriptografar, enviar dados, receber, processar informações, verificar assinaturas etc e a quantidade de energia armazenada num sensor é o seu principal obstáculo ou limitação.

Outro fator relevante é o comportamento durante o processo em que o sensor fica em *standby* para economizar energias. Nesse momento, os sensores podem perder o sincronismo necessário para o funcionamento dos algoritmos de segurança, pois existe a troca de informações que são utilizadas durante o processo de atualização de chaves. Se um nó perder tais informações poderá ficar impedido de trocar informações com a rede. Além do que esse mecanismo de *standby* deve ser cuidadosamente utilizado, porque o fato do sensor entrar e sair desse estado muitas vezes pode gastar mais energia do que se estivesse ligado o tempo todo. [Akyildiz 2002]

Proteção contra manipulação aumenta o custo por nó. Deve ser assumido sempre que um ou dois nós estão comprometidos devido à falta de proteção dos nós contra esse tipo de ataque [Hu 2003]. Muitos algoritmos são criados levando em consideração tal possibilidade, como por exemplo, o INSENS [Deng 2002].

4. Segurança ao nível de camadas

Algumas características e ataques podem ser específicos de determinadas camadas do modelo OSI. Os ataques são mais incisivos se forem sobre a camada de enlace e de rede.

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

A divisão dos tipos de ataques por camadas pode ser realizada como será vista nas sub-seções a seguir.

4.1. Camada física

Uma das características mais importantes de ume rede de sensores é o seu tempo de vida. Sendo esse o parâmetro mais importante no projeto e no desenvolvimento de algoritmos que serão utilizados na mesma.

Atualmente, as propostas que vêm sendo feitas são tentativas de otimizar o consumo de energia por algoritmos mais enxutos ou que apresentem melhores resultados levando-se em conta essa métrica. Essas propostas não são somente na área de segurança, mas também em outras como roteamento. Falta ainda algo que realmente seja palpável e que possibilite o avanço dos sensores, esse fator será concebido quando forem encontrados materiais capazes de armazenar mais energia em pequenos dispositivos ou que sejam de alguma forma recarregáveis. Uma proposta poderia ser sensores que utilizassem luz do sol para recarregar energia.

Tendo isso em vista, muitos ataques visam justamente exaurir a energia da rede principalmente ataques de negação de serviço em que o objetivo é sobrecarregar de tal modo os nós que o seu tempo de vida seja reduzido.

Outros ataques introduzem ruídos com a mesma freqüência que o utilizado pelos sensores com o intuito de prejudicar a comunicação. As técnicas de espalhamento de espectro e salto de freqüência já tentam contornar esse problema. Outra solução seria aumentar a potência de transmissão para melhorar a relação sinal ruído, porém essa solução não seria viável, pois consumiria muita energia. Visto que é durante a transmissão que há o maior gasto de energia, mais do que na recepção e muito mais que durante o processamento.[Akyildiz 2002]

Existem, porém, aplicações em que é necessário e fundamental que a rede esteja disponível ao menos por um tempo previsível, para que não haja danos ou interrupções inesperadas danificando todos os resultados já atingidos ou evitando que se chegue a uma conclusão.

Existe uma proposta [Slijepcevic 2002] que tenta otimizar o consumo de energia dependendo da importância da aplicação em questão. Para tal, são feitos divisões por níveis que identifica qual o grau de segurança preciso e assim não haja desperdício de energia.

4.2. Camada de enlace

Em ambientes sem fio, segurança ao nível de enlace é mais crítico que nas redes cabeadas devido à característica do meio ser aberto. Haja vista, os exemplos de *war*

driving em que pessoas com latas iam andando pelas ruas de grandes cidades e captavam sinais das redes sem fio.

Essa vulnerabilidade também existe para a rede de sensores, porém há a possibilidade da limitação do alcance das transmissões, diminuindo a possibilidade de interceptação.

Ataques à camada de enlace, mais precisamente à sub-camada MAC, 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* e 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. Para roubar informações será necessário muito tempo de interceptação de mensagens para ser possível a extração de uma quantidade suficiente de dados úteis.[Hu 2003]

4.3.Camada de rede

As redes de sensores provêem segurança na camada de rede já que esta é a mais afetada e a que causa maiores danos. Isso se deve a sua característica de transmissão ser por múltiplos saltos, o que obriga que os dados passem por nós intermediários até atingir o seu destino podendo representar vulnerabilidades.

Nessa camada podem existir diversos tipos de ataques com características diferentes [Karlof 2003], mas que tem o mesmo intuito, o de prejudicar o roteamento e a transferência de dados.

4.3.1.*Spoofing*, alteração ou repetição de informações de roteamento

Esse tipo de ataque pode causar *loops* na rede, atrair ou repelir tráfego, gerar mensagens de erro de rota falsas, dividir a rede, dentre outros danos. Tudo por ter como alvo principal os pacotes de controle responsáveis pelas informações de roteamento, através de repetições ou modificações dos mesmos.

4.3.2.Encaminhamento seletivo

Encaminhamento seletivo acontece quando um nó malicioso se recusa a encaminhar determinados pacotes descartando-os, funcionando de forma não colaborativa com a rede. Esse tipo de ataque pode acontecer devido às características de transmissão da informação ser salto a salto, onde os nós têm responsabilidade de encaminhar pacotes vindo de seus vizinhos. Um nó malicioso pode funcionar como um buraco negro (*black hole*) ao não encaminhar os dados recebidos independente de quem recebeu.

Esse tipo de ataque pode ser realizado somente sobre algumas rotas selecionadas e pode ser mais incisivo se o nó malicioso estiver participando da rota principal de transmissão de dados. Outra forma em que haveria sérios danos seria se estivesse sendo utilizado alguma métrica de escolha de caminhos de roteamento baseados na justiça. Onde um nó que não encaminha os pacotes que recebe estaria se aproveitando mais da rede que contribuindo, logo o número de pacotes que seriam direcionados a ele seria cada vez maior.

Com o passar do tempo os pacotes não seriam mais encaminhados a ele, por esse nó não dar continuidade na transmissão dos dados. Isso poderia representar um defeito nesse nó ou através de algum mecanismo de detecção de intruso representaria uma anomalia, porém mecanismos de IDS ainda estão distantes das redes de sensores.

4.3.3.Ataque sorvedouro

Ataque sorvedouro acontece quando o tráfego é desviado para um determinado nó malicioso. Os nós vizinhos ou o próprio nó podem manipular os dados e fazer modificações. Esse tipo de ataque acontece porque os adversários podem alterar as mensagens de roteamento. Essa atitude faz com que um nó se torne atraente aos nós vizinhos fazendo parte de suas rotas, podendo inclusive atingir outros através de inundações da rede com rotas falsas.

Se a métrica utilizada for o número de saltos, um computador de maior poder e com uma maior potência de transmissão pode indicar apenas um salto ao destino, uma ERB, por exemplo, e assim atrair todo o tráfego para si. Nas redes de sensores esse tipo de ataque é mais drástico, pois na maioria das vezes o destino de todos os nós é o mesmo, o nó sorvedouro.

4.3.4.Ataque *Sybil*

Para resistir a determinadas ameaças alguns sistemas aplicam redundâncias ao nível de rotas, caso alguma seja comprometida. Um nó, conhecendo essas características, pode apresentar múltiplas identidades e assim se fazer passar por outros controlando grande parte da rede. Os nós afetados acham que um nó malicioso que esteja aplicando esse tipo de ataque representa nós disjuntos quando na verdade não o é.

Novamente, quanto maior o poder do nó mais efetivo pode ser o seu ataque por aumentar a sua área de influência. Para se defender desse ataque pode se introduzir um nó confiável ou mais de um que faça o papel de agência certificadora de identidades dos nós.[Douceur 2002]

4.3.5.*Wormholes*

Um *wormhole* é um túnel criado pelo atacante. As mensagens entram nesse túnel numa parte da rede e são propagadas até uma outra parte, normalmente esses túneis possuem uma latência superior.

Um *wormhole* é instanciado por dois nós maliciosos que ficam nas extremidades do túnel. Cada um deles irá convencer os nós vizinhos que o wormhole é o melhor caminho através de transmissão de pacotes de roteamento com métricas forjadas que façam o túnel mais atraente diante das outras possibilidades. Essa transmissão pode ser feita por inundação.

Quanto mais próximo do nó sorvedouro mais informação passará por dentro desse túnel.

Figura 3. Um *wormhole* entre dois nós maliciosos. [Karlof 2003]

4.3.6.Ataque de inundação de HELLO

Muitos protocolos de roteamento emitem pacotes especiais de HELLO para verificar conectividade. Esse tipo de pacote é trocado apenas por vizinhos.

Um nó mal intencionado pode enviar pacotes de HELLO para qualquer nó da rede desde que possua um transmissor capaz. Assim os sensores ao receber esses pacotes julgam esse nó como vizinho e começam a aceitar as rotas que são anunciadas por ele. Essas rotas anunciadas vão induzir os nós a encaminhar seus pacotes por onde o nó malicioso quiser.

A inundação que esse tipo de ataque menciona, não é feita em múltiplos saltos e sim num único salto. Portanto, a inundação de pacotes de HELLO, se dá num único salto por ser feito por um nó de maior porte.

4.3.7.*Spoofing* de reconhecimento positivo

Esse tipo de ataque pode ser utilizado para fazer parecer que um canal ruim ou um nó que já esteja fora da rede ainda está funcionando normalmente. Isso pode ser feito após um nó transmissor receber um reconhecimento positivo vindo de um nó malicioso.

Há então a transferência da mensagem pelo nó atacante. O reconhecimento positivo é característica de alguns algoritmos de transmissão de dados. Podendo inclusive ser ao nível MAC no caso de estar sendo usado o padrão IEEE 802.11, por exemplo.

4.3.8. Anel da maldade

Um nó normal ou um grupo podem ser cercados por nós maliciosos, formando o chamado anel da maldade (*the ring of evil*).

Esses nós então vão se recusar a encaminhar e vão injetar informações erradas no anel. Quando uma rede se encontra muito comprometida ou, como nesse caso, um nó está cercado por muitos nós maliciosos é muito difícil encontrar soluções.

4.3.9. *Loop*

Podem ser introduzidos na rede *loops* ou *detour*, que através de informações de roteamento transmitidas por nós comprometidos tendem a fazer com que informações fiquem circulando pela rede. Isso pode exaurir as energias dos sensores.

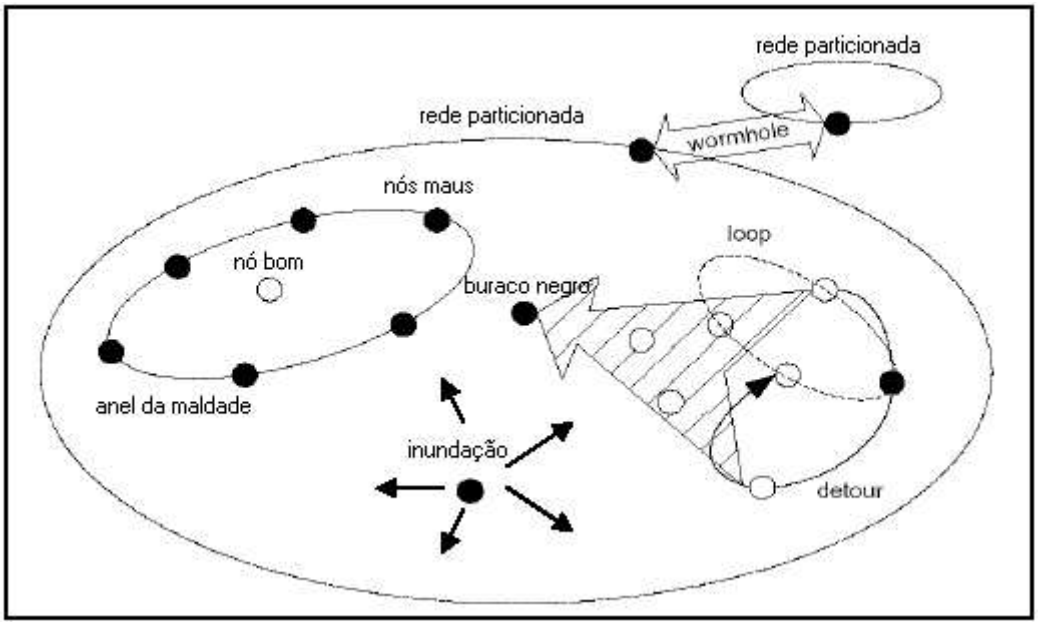

Figura 4. Ataques à camada de rede em redes de sensores.[Law 2002]

4.4.Camada de Transporte

Todas as medidas relativas à segurança são realizadas ao nível de rede e de enlace, portanto se fossem colocados também ao nível de transporte além de serem redundantes seriam dispendiosas energeticamente.

Ao nível de transporte são deixadas as suas atividades usuais como controle de fluxo, reordenamento de pacotes, recuperação de erro e controle de congestionamento.

5. Algoritmos de Segurança ao nível de roteamento

Os algoritmos que mostram melhor desempenho são aqueles que conseguem proteger da melhor forma a aplicação e ao mesmo tempo consumir o mínimo de energia possível.

Conforme foi se verificando a importância de se introduzir mecanismos de segurança em redes de sensores, mais houve a necessidade da elaboração de algoritmos capazes de prover tais funcionalidades. As primeiras soluções encontradas foram incluir mecanismos de segurança em protocolos de roteamento já existentes principalmente os que já eram utilizados em redes ad hoc. Após isso, começaram a surgir algoritmos que já foram concebidos levando-se em consideração a questão da segurança.

As soluções integradas são as mais eficientes que as que tentaram incluir segurança num segundo estágio. A maioria das propostas foi feita ao nível de camada de rede, pois é onde os ataques se fazem mais incisivos como já pôde ser observado.

Protocolos como o AODV [Perkins 1999] e o DSR [Maltz 2002] que são algoritmos de roteamento das redes ad hoc foram utilizados em redes de sensores e foram bem sucedidos, porém, no quesito segurança, não tiveram o mesmo sucesso, pois

este requisito não foi concebido com eles. Para contornar esse problema foram feitos os seguintes esforços [Law 2002]:

Watchdog e *pathrater* [Marti 2000] foram propostos por Marti. O *watchdog* tinha como objetivo o monitoramento das atividades dos outros nós durante o encaminhamento de pacotes. Isso é possível trabalhando em modo promíscuo, porém consome muita energia. Já o *pathrater* media taxas de confiabilidade de transmissão de todas as rotas alternativas a um mesmo destino baseado nos dados fornecido pelo *watchdog*. Essas propostas tinham alguns problemas que foram inclusive citados pelo próprio autor. Esses problemas eram referentes a sua ineficiência no caso de dois nós estarem de acordo e atacando a rede ao mesmo tempo.

No trabalho de Michiardi [Michiardi 2002] o mecanismo que media as taxas foi generalizado. Todos os nós vizinhos de qualquer nó colaboravam medindo o quão eficiente era esse nó ao desempenhar as tarefas solicitadas pelos vizinhos. O problema é que ao avaliar os nós são necessários dados fornecidos pelo próprio nó que está sendo avaliado abrindo espaço para informações forjadas e assim havendo dificuldade de se avaliar a veracidade dos dados recebidos. Ele definiu nó egoísta e nó malicioso, onde a diferença do nó egoísta do nó malicioso é que o egoísta não encaminha nenhum tipo de pacote para economizar recursos, sua intenção a princípio é não prejudicar a rede, porém seu comportamento o faz.

Buttyan [Buttyan 2001] e Blazevic [Blazevic 2001] introduziram um módulo de segurança que armazenasse identificadores, materiais de criptografia. Porém utilizava sistema de chaves assimétrica que consome muita energia.

Uma outra proposta foi feita por Yi [Yi 2001] que propôs níveis negociáveis de proteção como métricas de estabelecimento de rota durante a fase de descobrimento das melhores. A cada nível de proteção estaria associada uma métrica que seria levada em consideração para o estabelecimento de um caminho fim a fim mais seguro ou não dependendo da aplicação.

Alguns algoritmos foram desenvolvidos também no intuito de prover maior segurança para redes de sensores. O que obteve a maior aceitação foi o SPINS, conforme será visto adiante.

A maioria dos algoritmos propostos aplica criptografia de chave simétrica, pois a de chave pública consome muita energia. As variáveis necessárias para fazer os cálculos das chaves não caberiam na memória de um sensor [Perrig 2001]. A propagação em *broadcast* também é um importante obstáculo a ser contornado, principalmente na questão de distribuição de chaves por não representar um meio confiável.

Os algoritmos propostos são os que seguem nas sub-seções a seguir.

5.1.INSENS

O INSENS (INtrusion-tolerant routing protocol for wireless SEnsor NetworkS) [Deng 2002] já leva em consideração a possibilidade da existência de alguns nós maliciosos, por isso é capaz de detectá-los e não utilizá-los para as tarefas da rede. O INSENS parte do princípio que um nó malicioso consegue prejudicar a sua vizinhança apenas, mas não toda a rede.

O INSENS tem como objetivo prevenir ataques do tipo de negação de serviço realizados através de inundações da rede ao limitar o tipo de comunicação. Somente a estação rádio base tem permissão de fazer inundações. Para tal, a estação rádio base é autenticada para que nenhum nó malicioso se faça passar pela mesma. Para comunicação *unicast* todo o pacote deve passar pela ERB para que esta funcione como um filtro. Essa característica introduz infra-estrutura à rede de sensores.

Para prevenir o anúncio de rotas falsas a informação de controle de roteamento é autenticada. Para economizar energia, é utilizada criptografia simétrica para atingir confidencialidade e autenticação entre os nós comuns e a ERB. A ERB é utilizada para a disseminação e processamento das tabelas de roteamento, portanto os nós da rede apenas mantêm as tabelas recebidas e não as transmitem. Evitando assim, a injeção de tabelas de roteamento falsas na rede.

Essa atitude minimiza computação, comunicação, armazenamento, e largura de banda necessária pelos nós sensores. Em compensação o nó sorvedouro irá necessitar de aumento de computação, comunicação, armazenamento, e largura de banda. [Hu 2003]

O INSENS utiliza múltiplos caminhos para transferência de dados introduzindo redundância. Essa proposta tem como objetivo o aumento da robustez, pois se caso uma rota venha a ser comprometida devido à presença de um possível intruso outros caminhos poderão ser utilizados.

5.2.Ariadne

Ariadne [Hu 2002] é um protocolo de roteamento sob demanda para redes ad hoc seguro que pode ser utilizado também em redes de sensores. Esse protocolo previne atacantes de alterar rotas e nós que estejam livres de qualquer intenção maliciosa.

O Ariadne emprega chaves simétricas e previne contra ataques de negação de serviço. Cada nó deve gerar sua própria cadeia de sentido único de chaves. As suas restrições de memória impedem que sejam geradas cadeias de chaves muito longas o que pode proporcionar um gasto de tempo muito grande de cálculos de chaves. O Ariadne não é muito efetivo contra ataques de múltiplos nós em conluio.

5.3.SPINS

O SPINS [Perrig 2001] (Security Protocols for Sensor Networks) é composto por dois protocolos. O μTESLA é responsável por prover autenticação quando há comunicação em *broadcast* e o SNEP é 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 que é utilizado como um vetor de inicialização para o algoritmo usado criptografar e decriptografar os dados, no caso do SNEP a criptografia é realizada por um RC5 enxuto devido às limitações dos sensores. 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.

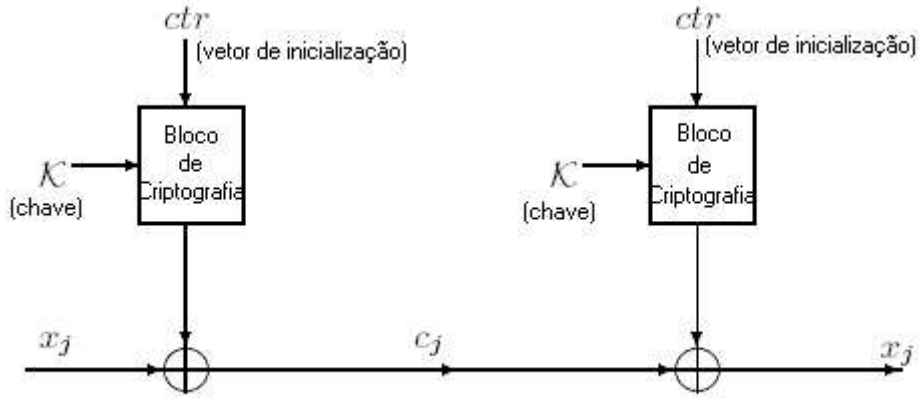

Figura 5. Contador utilizado para criptografar e decriptografar. A função de criptografia é aplicada a um contador com crescimento monótono para gerar uma única palavra que será multiplicada pelo texto plano num XOR. O processo de decriptografia é idêntico. [Perrig 2001]

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 ela envia em 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 numa rede com muitos nós esse processo induziria um grande atraso.[Liu 2003]

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. 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.

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

6. Gerenciamento de chaves

O gerenciamento de chaves é o processo em que as chaves criptográficas são geradas, armazenadas, protegidas, transferidas, carregadas, usadas e destruídas.

Esse gerenciamento é problemático em redes de sensores por serem vulneráveis a manipulações devido às suas limitações de custo, por não poderem armazenar muitas chaves devido às suas limitações de espaço em memória e por não poderem utilizar algoritmos de criptografia mais robustos devido às suas limitações de energia.

Para cumprir os requerimentos funcionais e de segurança da maioria das redes de sensores deve se levar em consideração os seguintes requisitos.[Law 2003]

Uma rede de sensores não deve trabalhar com uma única chave, pois devido a sua falta de proteção ter uma chave somente e não ter nenhuma faz o mesmo efeito.

Uma rede não deve ter um nó centralizador ou ponto de vulnerabilidade. O SPINS parte do princípio que o nó sorvedouro está livre de qualquer falha.

Devem ser respeitados critérios de escalabilidade para que a adição de novos nós possam ser feitos a qualquer momento sem causar aumentos excessivos ao nível de processamento por nó, de comunicação e de *overhead* administrativo na rede.

Existem dois tipos de esquemas para a distribuição de chaves em redes de sensores. Um tipo aberto a toda a rede e um tipo específico por nó . O tipo aberto à rede equipa todo o nó da rede com a mesma chave e iguala o comprometimento de um único sistema de chaves com o comprometimento de toda a rede. Se houver o roubo de informações, a rede estará completamente comprometida. O tipo específico por nó determina uma única chave para toda a combinação de nós que estão se comunicando. A segurança atingida por esse esquema é otimizada, entretanto o hardware necessário para armazenar está fora das possibilidades dos sensores.[Hu 2003]

O que se faz então é tentar encontrar soluções intermediárias que não sejam tão eficientes, mas que também não sejam tão vulneráveis.

Existem outras propostas para a distribuição segura de chaves. Dentre elas a feita por Chan [2003] que propõe três tipos métodos distintos, o *q-composite random key predistribution scheme* que atinge uma grande proteção sobre ataques de baixa escala enquanto troca um aumento da vulnerabilidade a ataques físicos em grande escala aos nós da rede. Essa vulnerabilidade ocorre porque o atacante tem condição de agregar muitas informações e não mais encontraria resistência da rede. Outro tipo é o *multi-path key reinforcement scheme*, que tem aumenta a segurança da rede ao transmitir a chave por múltiplos caminhos. Por último, há a proposta *random-pairwise keys scheme*, que garante que mesmo se alguns nós estiverem comprometidos, a rede continua completamente segura. Isso ocorre porque a comunicação entre dois nós é sempre feita baseado no reconhecimento da chave que está sendo utilizada pelo par, como uma forma de autenticação.

7. Segurança na estação rádio base

Durante a proposta de seus algoritmos muitos autores partem do princípio que a ERB é um ponto seguro. A justificativa é que a ERB por ter maior capacidade de processamento pode possuir um algoritmo mais eficiente que o provenha segurança. Porém, mesmo a ERB está sujeita a ataques.

Deng em [Deng 2003] propôs três métodos que podem aumentar a segurança das ERBs. O primeiro seria o estabelecimento de múltiplos caminhos que atingiriam múltiplas ERB. Com a introdução de ERBs redundantes haveria a proteção contra ataques a uma única ERB, essa estratégia pode ser considerada tanto para a fase de descobrimento de rota quanto para transferência de dados. A segunda solução é fazer com que o endereço do destino não fique claro nos pacotes transferidos. Assim, ao obter um pacote, um atacante não tem como identificar o destino, que poderia ser o endereço

da ERB. Finalmente, a última proposta é o deslocamento da ERB dentro da topologia da rede. A ERB não ficaria estática dificultando a sua localização.

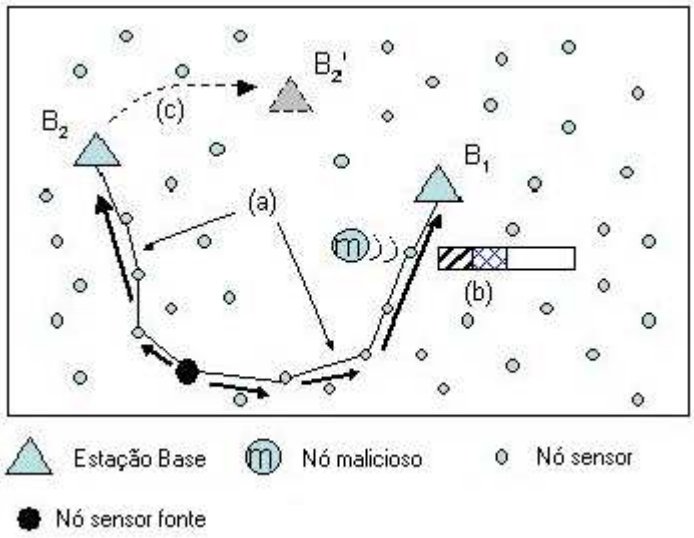

Figura 6. a) Múltiplos caminhos para múltiplas ERBs b) Disfarce dos campos de endereçamento c) Deslocamento da ERB.

8. Conclusão

Ainda existe muito que evoluir nessa área não só na área de segurança em particular, mas em todos os assuntos que dizem respeito às redes de sensores. O maior fator de limitação desse tipo de rede é a quantidade de energia que é armazenada e a capacidade de processamento dos nós que limitam as suas aplicações.

Poucos algoritmos foram desenvolvidos e foram implementados o que abre espaço ainda para muita pesquisa e desenvolvimento nessa área. O que vem sendo observado é que se deve buscar uma solução que consiga conciliar as limitações de energia com o máximo de segurança possível.

Referências

Akyildiz, I., Su, W., Sankarasubramaniam, Y., and Cayirci, E. (2002) “A Survey on Sensor Networks”, IEEE Communications Magazine, Agosto.

Blazevic, L., Buttyan, L., Capkun, S., Giordano, S., Hubaux, J. P. e Le Boudec, J. Y. (2001) ”Self-Organization in mobile ad hoc networks: the approach of terminodes”, IEEE Communication Magazine, p. 164-174, Junho.

Buttyan, L.e Hubaux, J. P. (2001) “Nuglets: A Virtual Currency to Stimulate Cooperation in Self-Organized mobile Ad-Hoc Networks”, Technical Report DSC/2001/001, Department of Communications Systems, Swiss Federal Institute of Technology.

Bishop, David J., Giles, C. Randy e Gary, P. Austin (2002) “The Lucent LambdaRouter: MEMS Technology of the Future Here Today”, IEEE Comunnications Magazine, Março.

Chan, H., Perrig, A. e Song, D. (2003) "Random Key Predistribution Schemes for Sensor Networks", IEEE Symposium on Security and Privacy, Maio.

Deng, J., Han, R. e Mishra, S. (2002) "INSENS: Intrution-Tolerant Routing in Wireless Sensor networks," TR CU-CS-939-02, Dept of Computer Science, University of Colorado.

Deng, J., Han, R. e Mishra, S. (2003) "Enhancing Base Station Security in Wireless Sensor Networks", Technical Report CU-CS 951-03, Department of Computer Science, University of Colorado, Abril.

Douceur, J. R. (2002) "Tha Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (IPTS`02), Março.

Hu, F., Tillett, J., Ziobro, J., Sharma, N. K. (2003) "A Survey on Securing Wireless Sensor Networks", Submetido ao IEEE Communications Surveys, Janeiro.

Hu, Y. C., Perrig A., Johnson, D. B. (2002) "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", MobiCOM 2002.

Karlof, C., Wagner, D. (2003) "Secure Routing in Sensor Networks: Attacks and Countermeasures", 1st IEEE International Workshop on Sensor Network Protocols and Applications, Maio.

Law, Y., W., Dulman, S., Etalle, S. e Havinga, P. (2002) "Assessing Security-Critical Energy-Eficcient Sensor Networks", 18th IFIP TC11 Int. Conf. on Information Security, Security and Privacy in the Age of Uncertainty (SEC), Maio.

Law, Y. W., Corin, R., Etalle, S. e Hartel, P. H. (2003) "A Formally Verified Decentralized Key Management Architecture for Wireless Sensor Networks", Personal Wireless Communications (PWC 2003), IFIP WG 6.8, Mobile and Wireless Communications, Setembro.

Liu, D. e Ning, P. (2003) "Efficient Distribution of Key Chain Commitments for Broadcast Authentication in Distributed Sensor Networks", In Proceedings of the 10th Annual Network and Distributed System Security Symposium, p. 263-276, Fevereiro.

Maltz, D. A., Johnson, D. B., Hu, Y. K. e Jetcheva, J. G. (2002) "The dynamic source routing protocol for mobile ad hoc networks", Internet Draft, draft-ietf-manet-dsr-06.txt.

Marti, S., Giuli, T. J., Lai, K. e Baker, M. (2000) "Mitigating routing misbehavior in mobile ad hoc networks", Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking", p.255-265.

Michiardi, M., e Molva, R. (2002) "Core: A COllaborative REputation mechanism to enforce node cooperation in Móbile Ad Hoc Networks", In Communications and Multimedia Security Conference.

Perkins, C. e Royer, E. (1999) "Ad Hoc On-Demand Distance Vector Routing", In 2nd IEEE Workshop on Mobile Computing Systems and Applications, p. 90-100.

Perrig, A., Szewczyk, R., Wen, V., Culler, D. e Tygar, J. D. (2001) "SPINS: Security Protocols for Sensor Networks", In Seventh Annual ACM International Conference on Mobile Computing and Networks(Mobicom 2001).

Pister, K. S. J., Kahn, J. M. e Boser, B. E. (1999) "Smart dust: Wireless networks of milimeter-scale sensor nodes.", Artigo técnico da U. C. Berkeley.

Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S., Srivastava, M. B. (2002) "On Communication Security in Wireless Ad-Hoc Sensor Networks", 11th IEEE

International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, Junho, p. 139-144.

Yi, S., Naldurg, P. e Kravets R. (2001) "Security-aware ad hoc routing for wireless networks", in Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking and Computing, ACM Press, p. 299-302.