Revista Gestão.Org, v. 13, Edição Especial, 2015. p. 402-411
ISSN 1679-1827
http://www.revista.ufpe.br/gestaoorg

Segurança em Redes de Sensores sem Fio – Desafios, Tendências e Orientações

Security in Wireless Sensor Networks - Challenges, Trends and Guidelines

Diego Assis Siqueira Gois[1], João Paulo Andrade Lima[1], Edward David Moreno Ordonez[1]

[1]Universidade Federal de Sergipe, UFS, Brasil

Correspondência: Diego Assis Siqueira Gois, Endereço: Av. Marechal Rondon, s/n Jardim Rosa Elze, São Cristóvão CEP 49.100-000, Aracajú, SE Brasil. Telefone: 55 79 2105-6600 E-mail: diego.se.ita@gmail.com

Recebido: 14 de outubro de 2015 Aceito: 26 de março de 2016 Publicado: 09 de maio de 2016

Resumo

Redes de sensores sem fio podem ser providas ou não de segurança, dependendo da aplicação, mas em grande parte das aplicações a segurança é necessária. A segurança em redes de sensores sem fio é um grande desafio devido às limitações de comunicação, processamento, memória e energia dos dispositivos presentes nas RSSF. O desafio em relação ao consumo energético ainda é agravado quando essas redes são submetidas a locais de difícil acesso, o que dificulta a substituição da bateria dos dispositivos ou dos próprios dispositivos. Este artigo apresenta um estudo quanto as principais questões de segurança em RSSF, levando a um direcionamento quanto à escolha de mecanismos de segurança apropriado para RSSF considerando confidencialidade, integridade e autenticação. Além disso, o dilema entre implantar segurança na rede e aumentar o consumo de energia é discutido, dando uma orientação sobre como diminuir o consumo energético através da utilização de ferramentas alternativas para compartilhamento de segredos, evitando o tradicional compartilhamento de chaves públicas. Ainda é apresentado um modelo de gerenciamento autonômico para segurança da rede, o qual nivela a quantidade de segurança implantada na rede a fim de reduzir o consumo de energia sempre que a rede não esteja em perigo. Por fim é mostrado um modelo de estimação de nível de segurança para um dado proveniente de um sensor, permitindo ao usuário do dado uma escolha em relação à aceitação ou não do dado.

Palavras-chave: Resumo; Segurança; Redes de Sensores sem Fio (RSSF); Avaliação de Desempenho; Modelo.

Abstract

Wireless sensor networks can be provided or not of security, depending on application, but in most applications safety is required. Security in wireless sensor networks is a major challenge due to the limitations of communication, processing, memory and power of devices present on wireless network sensor. The energy consumption challenge is further compounded when these networks are subjected to areas to difficult access, making it difficult to replace the battery of the devices or the devices themselves. This article presents a study as the main security issues in wireless network sensor, leading to a guidance as to the choice of appropriate security mechanisms for wireless sensor network considering confidentiality, integrity and authentication. Furthermore, the dilemma between deploying network security and increase energy consumption is discussed, giving guidance on how to reduce energy consumption through the use of alternative tools for sharing secrets, avoiding the traditional public key share. Already displayed an autonomic management model for safety of wireless sensor network, which levels the amount of security deployed on the network in order to reduce power consumption whenever the network is not in danger. Finally it is shown a level security estimation model for a date coming from a sensor, allowing the user data a choice about accepting or not of the data.

Keywords: Survey; security; Wireless Sensor Networks (WSN); Performance evaluation; Model.

1. Introdução

Os avanços recentes da microeletrônica estimularam o desenvolvimento de pequenos sensores, estes foram acoplados a pequenos dispositivos providos de comunicação sem fio, com pouca capacidade de processamento e limitados recursos de computação. O conjunto desses nós sensores trabalhando cooperativamente forma uma Rede de Sensores Sem Fio (RSSF) (Cavalcante et al, 2012). A esses nós, pode-se dar diversas funcionalidades

entre as quais estão o monitoramento, sensoriamento e até o controle de operações no mundo físico.

Um dos grandes desafios no RSSF está nas limitações de recursos de comunicação, processamento, memória e energia, que na maioria dos casos é oriunda de pequenas baterias. A depender da energia gasta nos nós sensores, estes podem passar dias ou anos em execução, porém levando em consideração que se a localização dos nós for de difícil acesso, a troca da bateria pode tornar-se inviável.

A segurança das informações tramitadas entre os nós é de relevante importância já que esses nós podem ser implantados nos mais diversos ambientes, como no monitoramento de um poço de petróleo. Por possuir comunicação sem fio, são abertos precedentes para os mais diversificados tipos de ataques às informações.

Assim um problema notável em RSSF é a forma de prover segurança de informação, sendo o foco de diversas pesquisas, já que algoritmos criptográficos exigem grande consumo de energia, processamento e memória. Os serviços de confidencialidade, integridade e autenticação, são providos em geral por algoritmos criptográficos e de autenticação, assim a escolha dos mecanismos apropriados é importante no fornecimento de segurança aos dados em RSSF.

Apenas a escolha do algoritmo correto de criptografia não resolveria totalmente o problema de consumo de energia, visto que qualquer algoritmo implementado impactará no consumo. Assim é interessante adicionar ao sistema um gerenciamento de segurança.

Um sistema de gerenciamento de segurança pode agir em uma rede ativando e desativando serviços e funções de segurança sempre que necessário em resposta a eventos ocorridos em uma rede. Este sistema pode economizar energia da rede se não houver indicação ou suspeita de presença de intrusos (Oliveira et al, 2008).

Entretanto apenas com o uso de algoritmo de criptografia e gerenciamento do nível de segurança, é difícil garantir que o dado seja realmente legítimo e não sofreu qualquer tipo de ataque, nesse contexto Ramos e Filho (2013) propõe um modelo para estimar o nível de segurança do dado que chega para o usuário, podendo este escolher se utilizará ou não este dado conforme o nível de segurança do mesmo.

Ainda assim pode-se melhorar o consumo de energia implantando na rede um mecanismo de compartilhamento de segredos alternativo às conhecidas chaves públicas. Esta é a ferramenta TinySharing, a qual demonstra a viabilidade de soluções colaborativas de segurança em dispositivos com capacidade limitada de processamento e armazenamento (Santos e Margi, 2011).

Este trabalho fornece uma visão geral dos principais desafios e tendências nas pesquisas sobre segurança em redes de sensores sem fio, mostrando soluções para os problemas e discutindo a viabilidade do uso das soluções em contraponto com o aumento no consumo de energia, processamento e memória. Assim é possível ter uma orientação sobre quais técnicas e mecanismos utilizar em trabalhos relacionados à segurança em RSSF.

O artigo está organizado em cinco seções, a seção 2 apresenta a fundamentação teórica, a seção 3 é dedicada aos trabalhos relacionados e análise dos mesmos, na seção 4 encontram-se as sugestões de trabalhos futuros, na seção 5 encontram-se as conclusões, e por fim a seção 6 apresenta as referências utilizadas para elaboração deste trabalho.

2. Fundamentação Teórica

2.1. Segurança em RSSF

A Segurança em redes de sensores sem fio (RSSF) precisa ser considerada em várias aplicações. Por exemplo, se colocarmos sensores em um poço de petróleo para detectar dados da perfuração a fim de executá-la da melhor forma possível. Os responsáveis por coletar os dados irão querer que os dados fossem confiáveis, não existindo nenhum tipo de interferência, alteração ou inclusão de dados falsos.

Assim é interessante que uma rede tenha capacidade de prover integridade dos dados, confidencialidade, autenticidade e disponibilidade, além de ser resistente a ataques. Este capítulo apresenta os principais conceitos de segurança em RSSF através de suas subseções.

2.2. Atributos Básicos

Nesta subseção iremos abordar uma visão geral dos atributos básicos necessários para prover segurança em um dado.

- ***Integridade dos dados*:** Visa garantir que todas as características originais dos dados geradas no sensoriamento do nó sejam mantidas durante todo o roteamento até a estação base em todo o ciclo de vida do dado;
- ***Confidencialidade:*** O direito de acessar a informação deve ser dado apenas ao nó que tem autorização para acessá-lo;

Revista Gestão.Org, v. 13, Edição Especial, 2015. p. 402-411
ISSN 1679-1827
http://www.revista.ufpe.br/gestaoorg

- ***Autenticidade:*** Visa garantir que o dado vem realmente do nó em que ela foi produzida, não sendo alvo de nenhum tipo de modificação ou mutação no caminho;
- ***Disponibilidade:*** A disponibilidade é fundamental, pois esta permite que o dado esteja sempre disponível para nós autorizados ao acesso da mesma;

2.3. Ataques Mais Comuns em RSSF

Todos os ataques nas redes de sensores sem fio têm como objetivo o mau funcionamento da rede ou até a interrupção do serviço. Assim os ataques são executados de diversas formas. Nesta subseção são mostrados os principais ataques relacionados às redes de sensores sem fio.

- ***Negação de serviço (Denial of Service – DOS)***

Muito utilizado contra servidores *Web*, a negação de serviço invalida a rede através de uma sobrecarga, tendo como objetivo consumir toda a memória e processamento da rede, a fim de fazer com que o serviço prestado pela rede seja interrompido.

O DOS se divide nos seguintes ataques: *Inundação:* inunda a rede com pacotes desnecessários gerando um grande volume de tráfico. *Amplificação:* Um nó malicioso forja o endereço da vítima e faz um grande número de requisições aos demais nós em nome do nó vitima, quando todos os demais nós começarem a responder as requisições o nó vítima irá ficar congestionado. E *exploração de protocolos:* Explora alguma falha de implementação no protocolo da vítima.

No caso de redes de sensores sem fio um ataque de negação de serviço interrompe facilmente o funcionamento da rede, já que os dispositivos da rede em questão são providos com pouca capacidade de memória e processamento.

- ***Nós irmãos (Sybil attack)***

Um nó malicioso assume a identidade de um ou mais nós legítimos podendo executar diversos tipos de ataques na rede, entre eles estão os ataques na agregação de dados, mecanismos de roteamento, alocação de recursos, armazenamento distribuído.

- ***Ataque do buraco da minhoca (Wormhole attack)***

É um ataque crítico na fase de descoberta de vizinhos da rede, pois este ataque cria um túnel entre dois nós em diferentes partições da rede, fazendo com que os nós pensem que são vizinhos, quando na verdade existem outros nós entre eles. Isto causa problema de convergência na rede.

- ***Inundação da rede (Hello flood attack)***

Um nó falso com alta capacidade de processamento e com alta potência de sinal inunda a rede com mensagens *HELLO*, isso causa congestionamentos em toda rede. Além disso, todos demais nós irão pensar que este nó falso é um vizinho, podendo também criar rotas falsas.

- ***Ataque do buraco negro (Black Hole attack ou Sinkhole attack)***

Um nó malicioso mostra rotas falsas para toda rede, fazendo com que os pacotes passem por este nó falso antes de chegar à estação base. Esse nó malicioso em posse dos pacotes pode descartar ou modificar os pacotes.

- ***Desvios e loops***

Como o nome do ataque sugere, o nó malicioso altera o roteamento, criando *loops* infinitos ou grandes desvios entre os nós.

- ***Sequestro de nós***

Um grupo de nós maliciosos cerca um nó legítimo e começam a inundar esse nó, além disso, o grupo altera o roteamento de forma que todas as mensagens que o nó emita, não cheguem ao destino.

- ***Interferência (Jamming)***

Um nó malicioso possui um transceptor potente configurado para utilizar a mesma frequência dos nós sensores, podendo ocupar o canal de comunicação com ruído e impedir que os nós sensores recebam qualquer tipo de mensagem.

- ***Alteração de dados***

Um nó malicioso captura uma mensagem e a retransmite de forma alterada.

- ***Negligência de dados e Selective Fowarding***

O nó intruso ignora mensagens que deveria enviar ou retransmitir.

- ***Repetição e Atraso***

O nó malicioso repete e atrasa, respectivamente, as mensagens que deveria retransmitir.

2.4. Componentes de Segurança

➢ ***Gerenciamento de segurança e energia***

O gerenciamento de energia consiste em ligar e desligar os componentes do dispositivo visando aumentar o tempo de vida da rede ao máximo através da economia de energia.

Como o uso de segurança aumenta o consumo de energia, o gerenciamento de segurança torna-se importante. Este consiste em habilitar ou desabilitar módulos de segurança implantados na rede seguindo os parâmetros definidos pelo projetista da rede.

➢ ***Criptografia***

De forma geral, criptografia consiste em aplicar um conjunto de técnicas, conceitos e métodos em uma informação tendo como objetivo transformá-la em uma informação codificada, de forma que apenas o receptor legítimo da informação consiga decifrar a mesma.

➢ ***Encriptação***

Consiste no processo de transformar uma informação comum em uma informação codificada usando-se de um algoritmo criptográfico.

No caso específico das RSSF, a encriptação dos dados pode ser feita por um processo fim-a-fim ou salto-a-salto. No processo salto-a-salto a encriptação é feita cada vez que a mensagem passa por um nó diferente até chegar à estação base, além disso, é necessário que todos os vizinhos compartilhem as chaves necessárias para o processo. Já no processo fim-a-fim a encriptação é feita uma vez por mensagem, ou seja, em uma transmissão apenas o nó em questão e a estação base precisam encriptar/decriptar a mensagem, fazendo com que esse processo seja menos dispendioso do que o processo salto-a-salto.

➢ ***Assinatura***

A assinatura de uma mensagem visa garantir ao nó destinatário que a mensagem realmente foi gerada pelo nó emissor. Em RSSF, a assinatura pode ser feita por processos fim-a-fim e também por processos salto-a-salto já citados.

➢ ***Gerenciamento de Chaves***

No que diz respeito às redes de sensores sem fio, o compartilhamento de chaves públicas, método comumente utilizado nos diversos tipos de redes, é inviável devido ao alto custo de processamento e consumo de energia. Compartilhar chaves privadas é um caminho, porém torna a rede bastante vulnerável, pois um nó da rede pode ser sequestrado e o sequestrador tomar posse da chave privada compartilhada.

➢ ***Sistema de detecção de intrusos (IDS)***

Um sistema de detecção de intrusão tem como objetivo detectar diversos tipos de comportamentos maliciosos na rede, gerando alertas a partir de eventos. Se alguma intrusão for detectada os alertas são enviados e podem existir dois tipos de resposta: ativa e passiva. Na ativa o comportamento malicioso é tratado pelo próprio sistema. Já na passiva, o sistema apenas gera relatórios para que o administrador da rede possa observar e tomar as providências cabíveis.

Os principais métodos de detecção de um IDS são baseados em assinatura e baseados em anomalias. E devido à natureza colaborativa e distribuída das redes de sensores sem fio, o ideal é que seja usado um IDS colaborativo e distribuído, existindo vários deles na literatura. Nestes mecanismos, cada nó sensor monitora seus vizinhos à procura de um comportamento suspeito. Assim que uma atividade maliciosa é detectada, nós vizinhos trocam informações sobre o nó suspeito. Neste processo de colaboração, cada sensor vizinho de um nó suspeito deve indicar seu ponto de vista em relação a esse nó para indicar se é malicioso ou legítimo (Ramos e Filho, 2013).

➢ ***Sistema de gerenciamento de confiança***

Mecanismos de gerenciamentos de segurança existem para avaliar a confiabilidade dos nós sensores, estes podem avaliar, manter e revogar a confiança entre os nós.

Normalmente no contexto de RSSF a noção de confiança é mostrada como um nó A confia no nó B para executar o processo Y. Essa confiança pode ser usada para o controle de acesso, roteamento seguro e detecção de intrusos.

Revista Gestão.Org, v. 13, Edição Especial, 2015. p. 402-411
ISSN 1679-1827
http://www.revista.ufpe.br/gestaoorg

3. Trabalhos Relacionados

Nesta sessão analisamos alguns trabalhos relacionados à segurança de redes de sensores sem fio, que foram divididos por área de atuação, observando as tendências e quais caminhos alternativos tomar em casos que nos deparamos com a falta de recursos nas RSSF.

3.1. Visão Geral

O trabalho de Amirthavalli e Sivakumar (2014) versa sobre as questões e desafios globais encontrados na conservação de energia e segurança de redes de sensores sem fio, os quais são agravados se o sensor é colocado em ambientes que a reposição de baterias ou dos próprios sensores é difícil, assim são apresentados os principais fatores que aumentam o consumo de energia como a escuta ociosa, colisões, *overhearing* e a sobrecarga de pacotes de controle.

Utilizando-se de uma metodologia de resumo, o autor explana técnicas de conservação de energia mais utilizadas atualmente como o *Duty cycling*, abordagens baseadas em mobilidade, clustering e teoria dos jogos, logo após faz uma comparação dessas técnicas mostrando qual tem maior ou menor escuta ociosa, colisões, *overhearing*, pacotes de controle, economia de energia e consumo de tempo, concluindo que a técnica baseada em prioridade é a melhor entre as mencionadas pelo autor.

As questões de segurança são tratadas separadamente das relacionadas à conservação de energia, dando mais foco ao aspecto arquitetônico das RSSF que as torna um alvo fácil de ataques. Discutir questões de segurança separado de conservação de energia não é interessante, já que impor segurança em RSSF significa maior consumo de energia. São discutidos como principais ataques: negação de serviço (DOS), *Sybil attack*, ataque do buraco da minhoca, ataque *Hello flood* e ataque do buraco negro, propondo alguns esquemas de segurança para esses ataques e mostrando seus principais recursos.

O artigo da um direcionamento sobre que mecanismo utilizar para conservação de energia, porém deixou a desejar quando o artigo não relacionou segurança ao consumo de energia, sendo isso um bom tema de trabalho futuro, já que são fatos diretamente relacionados. No entanto, descreve bem os principais problemas de conservação de energia e segurança, assim como as dificuldades em superar esses problemas, propondo então esquemas que possam resolver.

3.2. Criptografia Baseada em Algoritmos Criptográficos

O trabalho de Cavalcante et al (2012) demonstra uma avaliação de desempenho de mecanismos de segurança para redes de sensores sem fio, neste o autor analisa o desempenho dos algoritmos criptográficos AES, Skipjack, Klein, RC5, Present, utilizando os modos de operação CBC, CFB, OFB, CTR e OCB e os algoritmos de autenticação CBCMAC, CMAC, HMAC-MD5, HMAC-SHA1.

O experimento se deu com a utilização de uma plataforma MicaZ com auxílio de um osciloscópio digital e o sistema operacional TinyOS. Para avaliação de desempenho foi desenvolvida uma aplicação, a qual fornece condições para medição do tempo de execução das operações dos mecanismos, sendo validado por meio de vários testes de entradas e saídas conhecidas.

As métricas consideradas na avaliação de cada algoritmo foram a quantidade de memória RAM e ROM requeridos, obtidos através do próprio processo de compilação do código fonte no TinyOS. O consumo de energia foi obtido por meio da relação entre potência e tempo de execução.

Os resultados obtidos mostraram que em relação à memória ROM, o AES é consideravelmente mais dispendioso que os demais, seguido pelo *Present*, RC5, *Klein* e *Skipjack*, sendo este último o que requer menos ROM. Já em relação à memória RAM o que obteve melhor desempenho foi o RC5 seguido de perto pelo *Skipjack* e *Klein*, já o *Present* e AES apresentaram alto custo de RAM.

Em relação aos modos de operação, os resultados apontaram o menor gasto de ROM para o OFB obtendo pequena vantagem sobre CFB e CTR, os modos OBC e CBC apresentaram as maiores quantidades de ROM exigidas. O desempenho quanto à RAM foi bastante semelhante ao da ROM, com leve vantagem do modo CFB.

Na comparação de MACs, o CBCMAC foi o que consumiu menos ROM, logo após vieram CMAC, OCB, HMAC-MD5 e HMAC-SHA1, estes dois últimos consumiram uma quantidade consideravelmente maior que os demais. Já no consumo de RAM, os MACs se comportaram de forma contrária, sendo o HMAC-SHA1 e HMAC-MD5 os que obtiveram menor consumo.

Enquanto o RC5 e *Skipjack* apresentaram os menores consumos de energia, o AES foi o que apresentou o maior gasto, ficando o *Present* em uma faixa intermediária. Observando os modos de operação temos o CTR como mais eficiente, seguido de perto pelo CFB e OFB com OCB e CBC mais distantes. Na análise energética dos

MACs, o CBCMAC, CMAC, OCB e HMAC-MD5 obtiveram consumos próximos e foram nessa ordem os que menos gastaram energia, já o HMAC-SHA1 demonstrou um alto consumo comparado aos demais.

Contudo, a obtenção e análise de resultados aplicado em uma plataforma real MicaZ e uma discursão sobre os mesmos (levando em conta não apenas resultados numéricos, mas também se o algoritmo possui patente), é um dos principais pontos a ser absorvido por este trabalho. Assim, o leitor deste trabalho, pode obter uma orientação sobre quais algoritmos utilizar para prover segurança básica em RSSF.

3.3. Compartilhamento de Segredos

Os mecanismos de compartilhamento de segredos foram iniciados por Shamir (1979) com o objetivo de fornecer segurança para chaves criptográficas (Santos e Margi, 2011). Assim, o trabalho de Santos e Margi (2011) demonstra a ferramenta *TinySharing* para compartilhamento de segredos em redes de sensores sem fio sobre o modelo Shamir. Esta demonstra viabilidade de soluções colaborativas de segurança em dispositivos com capacidade limitada de processamento e armazenamento, e contribuiu para aplicações em que é necessária a colaboração entre nós da rede como um mecanismo de confiança (Santos e Margi, 2011).

A natureza colaborativa dos esquemas de compartilhamento de segredos faz com que os nós possam realizar cálculos de forma conjunta, isso sem mostrar elementos específicos da entrada para terceiros.

"Os exemplos mais comuns são aplicações de leilão, em que se deseja calcular a função f(x1, x2,..., xn) = max(x1, x2,..., xn) em que xi é um segredo conhecido apenas pelo i-ésimo usuário" (Santos e Margi, 2011).

Assim o autor desenvolveu a ferramenta *TinySharing*, uma ferramenta colaborativa de compartilhamento de segredos que está inserida na proposta de pesquisa de novos protocolos de segurança para redes de sensores sem fio. Esta pode ser usada em diversas aplicações visando melhorar o desempenho em relação aos métodos conhecidos de compartilhamento como a criptografia de chave pública.

Segundo Santos e Margi (2011) testes envolvendo criptografia de chave pública mostraram que esse método pode apresentar um alto custo para redes de sensores sem fio. Assim sendo, a ferramenta *TinySharing* pode ser usada para substituir esse método convencional.

A ferramenta é baseada na interpolação de polinômios e pode ser considerada uma extensão do modelo Shamir, porém o autor não implementou o serviço de renovação de compartilhamentos, mantendo o segredo e alterando os compartilhamentos.

O sistema conta com duas fases, a inicialização e reconstrução do segredo. Sendo que na primeira é feito o cálculo e distribuição do compartilhamento com base na identidade do usuário, a segunda requer agregação de uma quantidade mínima de compartilhamentos chamada *threshold* [5]. No caso da inicialização o sistema necessita de um canal seguro para comunicação.

O autor arquitetou a ferramenta dividindo-a em três módulos principais: *Módulo distribuidor de compartilhamentos:* Implementado em uma estação base que recebe uma solicitação de registro do cliente e fornece um compartilhamento ao mesmo. *Módulo reconstrutor de segredos:* Implementado em uma estação base que dá início a reconstrução dos segredos desde que um número mínimo de compartilhamentos seja recebido. E *Módulo cliente:* Clientes solicitam, armazenam e transmitem compartilhamentos para uma estação base, a qual pode reconstruir o segredo recebido.

Além disso, é definido um código de Leds para saber o funcionamento do sistema. Para testar o sistema foi proposta uma demonstração com dez dispositivos *TelosB* (Com processador 16bits MSP430 e 16kB de memória RAM), sendo sete clientes, um servidor de compartilhamento de segredos, um servidor de reconstrução de segredos e um *sniffer*.

3.4. Gerenciamento Autonômico

Gerenciar consiste em administrar algo de forma que obtenhamos o melhor desempenho possível em diversas áreas de atuação. Enquanto que autonômico consiste em fazer algo de forma independente no qual não se precisa uma ação concreta (Intervenção externa) para que haja as mudanças necessárias.

Nesse sentido, o gerenciamento autonômico em RSSF, dá-se de forma a economizar o máximo possível de energia, e para isso, pode-se desligar o rádio do dispositivo quando o mesmo estiver ocioso, pois o rádio é o componente que mais consome energia. Outra forma de melhorar o consumo energético é gerenciando autonomicamente níveis de segurança, pois ao adicionar ou diminuir a segurança através de um procedimento automático quando for necessário, o consumo será menor quando a rede se sentir segura e não existir a necessidade de segurança.

Como redes de sensores possuem pouco processamento e energia disponível, é de extrema importância que o consumo de processamento, memória e energia seja diminuído ao máximo, porém não deixando de prover

segurança entre os nós. Por isso, esse dilema nos leva a pensar em várias formas de manter uma rede de sensores sem fio segura. Uma das alternativas se dá através de um modelo de gerenciamento dos nós de forma autonômica, em que os nós aumentam o nível de segurança na rede (a depender do estado atual da rede). Caso não haja nenhuma ameaça, a rede pode se manter com o mínimo de segurança possível, e havendo algum ataque ou ameaça, o nível de segurança começa a crescer de acordo com níveis bem definidos.

Com o objetivo de estender ao máximo o tempo de vida dos nós na rede, o trabalho de Oliveira et al (2008) propõe um modelo de gerenciamento de segurança para RSSF, incluindo seleção de componentes de segurança, descrição de informação de gerenciamento, descrição de mensagens e definição de eventos em uma rede autonômica.

Entre os diversos problemas de segurança, o autor considerou para o trabalho a possibilidade de criptografia salto-a-salto e fim-a-fim, a utilização de técnicas de gerenciamento de chaves, a existência de mecanismos de detecção de intrusos, roteamento seguro, fusão e agregação segura de dados, bem como um esquema de revogação de nós (Oliveira et al, 2008).

As decisões autonômicas são tomadas através de uma extensão do MannaNMP, *Manna Network Management Protocol*, onde os componentes de segurança tem configuração dinâmica e orientado a mensagens, assim pode ser incluído, excluídos, ativados e desativados em tempo de execução através de mensagens de controle. Esses componentes de segurança são baseados em eventos de detecção de intrusos, assim o nível de segurança da rede aumenta toda vez que um intruso é percebido. Caso o mesmo seja percebido pela estação base, esta revoga o nó intruso, caso seja percebido por qualquer um dos demais nós, a estação base aumenta o nível de segurança. Esse nível foi divido pelo autor em baixo, médio, alto e crítico da seguinte forma:

- *Baixo:* Sem detecção de intrusos nos nós sensores, sem utilização de criptografia e com fusão de dados habilitada;
- *Médio:* 10% dos nós executam detecção de intrusos, atualização de rotas autenticadas fim-a-fim, criptografia salto-a-salto habilitada, fusão de dados habilitada, rotas alternativas;
- *Alto:* 20% dos nós executam detecção de intrusos, criptografia fim-a-fim habilitada, atualização de rotas autenticada salto-a-salto, rotas alternativas, sem fusão de dados;
- *Crítico:* 30% dos nós executam detecção de intrusos, sem fusão de dados, criptografia fim-a-fim e salto-a-salto habilitadas, atualização de rotas autenticadas salto-a-salto e fim-a-fim, rotas alternativas.

Vale lembrar que a cada vez que o nível de segurança cresce, existe um aumento significativo no consumo de energia e processamento, assim caso a rede tenha pouca energia disponível, os níveis de segurança podem ser diminuídos mesmo com intrusos detectados a fim de não fazer com que a rede pare de funcionar por falta de energia.

A fim de validar o modelo descrito, o autor fez simulações utilizando uma rede estacionária plana que se baseia no modelo conhecido como colmeia para disposição dos nós, os quais variam entre 50 e 1000. Cada nó possui seis vizinhos equidistantes conhecidos, sendo que todos possuem os mesmos recursos computacionais e funcionalidades, além disso, foi definida uma estação base, que é fonte ou destino de todos os pacotes de dados e controle, possui recursos ilimitados e não pode ser violado (Oliveira et al, 2008). O *mote* simulado foi o Berkeley Mica2 com 4Kbytes de RAM, 128Kbytes para memória de programas e CPU com 8Mhz. Sendo utilizado um simulador baseado em eventos discretos, desenvolvido no DCC-UFMG (Martins et al, 2005). Após a avaliação dos níveis de segurança seguindo o critério de consumo de energia, foram obtidas as seguintes diferenças médias: Do nível baixo para o médio aumentou 9,9%, do médio para o alto 18,7%, do alto para o crítico 8%, e considerando do nível baixo direto para o crítico o aumento foi de 40%.

Confirmando assim que o custo energético para utilização de segurança é alto, porém através de um gerenciamento autonômico pode ser melhorado.

Destaca-se neste trabalho a sua estrutura bem elaborada e a definição de uma nova forma de gerenciamento. Como também a avaliação do mesmo via simulação, dando ênfase ao maior problema em redes RSSF (eficiência energética) e a inclusão de mecanismos de segurança. Porém, um foco interessante seria avaliar o processamento e o consumo de memória RAM diante dos níveis sugeridos pelo autor.

Apesar de todo estudo que se tem feito sobre segurança em redes de sensores sem fio, não é possível garantir uma rede totalmente segura, já que o canal de comunicação não é confiável, além da exposição dos nós a ataques físicos. Diversos mecanismos de segurança podem ser utilizados em defesa da rede, porém se for necessário uma garantia de segurança, é interessante que o usuário saiba o quanto a rede é confiável. Diante disso, Ramos e Filho (2013) apresentou o *Sensor Data Security Estimator* (SDSE), um modelo para estimar o nível de segurança dos dados de redes de sensores com base nos mecanismos de segurança existentes nelas.

O nível de segurança auxilia o usuário na decisão de usar ou não o dado recebido, além disso, o cálculo do nível de segurança também pode ser usado para ajudar profissionais a tomar decisões sobre como avaliar diferentes mecanismos de segurança e modificar as configurações da rede a fim de aperfeiçoar a segurança (Ahmed et al, 2008).

Segundo o autor, o modelo SDSE demonstrado no artigo se diferencia dos demais trabalhos relacionados pelo fato que o SDSE define métricas que consideram resiliência e confiabilidade, além de ser baseado em informações que mostram o atual estado da rede.

O modelo SDSE utiliza como métricas os métodos estocásticos: probabilidade de força criptográfica, probabilidade de resiliência do gerenciamento de chave, probabilidade de legitimidade e probabilidade de entrega. Estes consideram quatro mecanismos de segurança sendo dois de prevenção, Criptografia e Gerenciamento de chave criptográfica, e dois de detecção, Sistema de detecção de intrusão e sistema de gerenciamento de confiança.

Com as probabilidades calculadas, pode-se chegar ao nível de segurança para um dado originado em um nó sensor que chega a estação base, isso é feito através do produto das métricas em cada nó. Cada nó em uma dada rota tem seu grau de segurança, e o nível de segurança do dado será o valor do menor grau de segurança encontrado na rota.

O autor testou as métricas de prevenção através do algoritmo conhecido RC5 e observou que quanto maior a força criptográfica do algoritmo, mais seguro ele é. Apesar de que quanto mais tempo é gasto, a probabilidade de força criptográfica diminui, visto que mais chaves podem ser testadas. No caso de resiliência, foi observado que quanto maior o número de nós capturados, menor a probabilidade de resiliência.

Na análise da probabilidade de legitimidade, o autor observou que a mesma diminui à medida que mais nós vizinhos são necessários para detectar o nó malicioso.

Por fim, foi analisada a probabilidade de entrega com o esquema de gerenciamento de segurança GTMS, este mostrou que à medida que fração de interações bem sucedida cresce a probabilidade de entrega também aumenta.

De forma geral o nível de segurança é afetado por todos os parâmetros utilizados nas métricas. A proposta mostrou-se viável, uma vez que foram mostrados exemplos de como extrair efetivamente os parâmetros dos mecanismos (Ramos e Filho, 2013). Assim é notável a importância do artigo, porém como o modelo não foi efetivamente testado em uma rede RSSF com diferentes mecanismos de segurança, não é possível estimar o comportamento do modelo.

3.5. Quadro Comparativo

O quadro 1 mostra um breve resumo dos trabalhos analisados.

Artigo	**Objetivo**	**Métricas**	**Metodologia**	**Resultados**
Power Conservation and security in wireless sensor network – A survey	-Descrever os principais problemas relacionados à RSSF no que diz respeito à conservação de energia e segurança.	-Técnicas de conservação de energia. -Principais ataques à RSSF.	-Resumo.	-Mostra as melhores técnicas de conservação de energia, apontando a que melhor se encaixa em RSSF; -Descreve os principais ataques e técnicas de como evita-los.
Avaliação de desempenho de mecanismos de segurança para redes de sensores sem fio	-Avaliação de desempenho de algoritmos criptográficos.	-Memória RAM; -Memória ROM; -Energia;	-Avaliação em uma plataforma real MicaZ.	-Orienta os leitores sobre qual melhor algoritmo para se usar em uma RSSF.

TinySharing: Uma Ferramenta para compartilhamento de segredos em redes de sensores sem fio	-Ferramenta para compartilhamento de segredos.	-Não foram definidas no trabalho.	-Modelagem.	-Uma ferramenta alternativa à criptografia de chaves públicas.
Um modelo de gerenciamento de segurança em redes de sensores sem fio	-Estender ao máximo o tempo de vida dos nós provendo segurança.	-Níveis de segurança; -Energia.	-Simulação.	-Análise do gasto de energia em cada nível proposto.
Estimando o nível de segurança de dados de redes de sensores sem fio	-Estimar o nível de segurança de um dado recebido.	-Probabilidade de força criptográfica, resiliência do gerenciamento de chave, legitimidade e entrega.	-Modelagem.	-É mostrado ao usuário a chance do dado recebido não ter sofrido nenhum tipo de interferência.

Quadro 1. Comparação dos trabalhos relacionados.

4. Trabalhos Futuros

Amirthavalli e Sivakumar (2014) não apresentam sugestões de trabalhos futuros, porém seria interessante adicionar alguns testes ou referenciar testes feitos por outros autores para mostrar como chegou à conclusão de quais técnicas seriam melhores na conservação de energia. Nesses testes poderiam ser adicionados os esquemas de segurança propostos e executar uma análise global envolvendo ambos os problemas e suas possíveis soluções.

Cavalcante et al (2012) apresenta como trabalhos futuros a avaliação de outros mecanismos de segurança e a avaliação de outras métricas, como a latência da rede em decorrência do uso de tais mecanismos. Seria interessante também, uma análise utilizando uma rede de vários nós e não somente uma plataforma, além de adicionar outras métricas e mais algoritmos.

Santos e Margi (2011) inclui como trabalho futuro um mecanismo de hierarquia entre os nós para possibilitar o papel de estação base para um nó cliente. Porém, seria interessante que fossem feitos testes reais para comparação com o método tradicional de chaves públicas, principalmente na questão de desempenho e consumo de energia.

Oliveira et al (2008) propôs a otimização das soluções de segurança, compartilhando algoritmos, chaves e código, para reduzir recursos de memória e processamento exigidos como trabalho futuro. Sugeriria também a avaliação de processamento e memória RAM.

"Para avaliar a dinâmica do modelo proposto, estamos atualmente com um trabalho em andamento que inclui uma simulação detalhada do SDSE em uma rede com diferentes mecanismos de segurança implementados" (Ramos e Filho, 2013). Como trabalho futuro é inerente à implantação em uma RSSF real, além disso, seria interessante uma avaliação do impacto que esse modelo iria causar em termos de consumo de energia, processamento e memória, visto que para ser viável em uma RSSF, precisamos de valores baixos nesses quesitos.

5. Conclusões

Como visto no decorrer do trabalho, aplicar segurança em uma RSSF é um desafio extremamente complicado devido às suas características.

Assim discutimos as principais questões de segurança, o impacto que a criptografia gera na rede através da aplicação de algoritmos criptográficos e orientando qual o algoritmo mais adequado para o caso.

Como é extremamente difícil garantir um sistema totalmente seguro, foi discutido um bom método estocástico de estimar o nível de segurança do dado, dando opção ao receptor do dado de utilizá-lo ou não. Ainda em relação à dificuldade de garantir um sistema seguro, discutimos a possibilidade de um gerenciamento eficaz de segurança, dando a possibilidade de a RSSF aumentar ou diminuir a segurança autonomicamente.

Além disso, também foi mostrado que são possíveis alternativas como o *TinySharing* para compartilhar segredos e fugir da dispendiosa criptografia de chave pública.

Referências

AHMED, M. S.; AL-SHAER, E.; KHAN, L. "A Novel Quantitative Approach For Measuring Network Security" In 2008 IEEE INFOCOM - **The 27th Conference on Computer Communications**, 2008, pages 1957–1965,IEEE.

AMIRTHAVALLI, K.; SIVAKUMAR, P., "Power conservation and security in Wireless Sensor Networks — A survey," **International Conference on Electronics and Communication Systems (ICECS)**, 2014, pp.1,7, 13-14 Feb. 2014

CAVALCANTE, M. T.; GARCIA, F. P.; ANDRADE, R. M. C. "Avaliação de Desempenho de Mecanismos de Segurança para Redes de Sensores Sem Fio" In **XXX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)**, 2012, pp. 277-290.

MARTINS, M. H. T.; SILVA, A. P. R. da; LOUREIRO, A. A. F.; RUIZ, L. B. "An IDS simulator for wireless sensor networks" Sensornet **Technical Report**, Comp Sci Dept, Federal University of Minas Gerais, May 2005.

OLIVEIRA, S.; OLIVEIRA, T. R.; NOGUEIRA, J. M. S. "Um Modelo de Gerenciamento de Segurança em Redes de Sensores Sem Fio" In **Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)**, 2008.

RAMOS, A. L.; FILHO, R. H. "Estimando o Nivel de Segurança de Dados de Redes de Sensores sem Fio" In **Anais** do Simpósio Brasileiro de Redes de computadores e Sistemas distribuídos (SBRC), 2013.

SANTOS, M. A. S; MARGI, C. B. "TinySharing: Uma ferramenta para compartilhamento de segredos em redes de sensores sem fio" In **Anais** do Simpsio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC), 2011, Salo de Ferramentas. , Campo Grande, MS, Brasil.

SHAMIR, A. "How to share a secret. Communications of the ACM", 1979, 22(11):612–613.