Universidade Estadual de Feira de Santana

Programa de Pós-Graduação em Computação Aplicada

Criptografia Adaptativa em Redes de Sensores Visuais sem Fio

Danilo de Oliveira Gonçalves

Feira de Santana

2015

Universidade Estadual de Feira de Santana

Programa de Pós-Graduação em Computação Aplicada

Danilo de Oliveira Gonçalves

Criptografia Adaptativa em Redes de Sensores Visuais sem Fio

Dissertação apresentada à Universidade Estadual de Feira de Santana como parte dos requisitos para a obtenção do título de Mestre em Computação Aplicada.

Orientador: Dr. Daniel Gouveia Costa

Feira de Santana

2015

Esta página deverá ser substituída por uma folha contendo as assinaturas dos membros da banca.

Esta página deverá ser substituída por uma folha contendo a ficha catalográfica.

Abstract

Recently Wireless Sensor Networks have gained attention of researchers and industry around the world, such that many projects and solutions have been developed for various scenarios and applications. Such networks are formed by small sensor nodes with low processing power, few memory and few energy. Thus, resources are scarce, particularly energy, where, in most cases these nodes are powered by batteries, which is a crucial point in the network design. A kind of sensor network in which camera-enabled sensors are inserted are call Wireless Visual Sensor Networks. Because of this, these networks become able to recover large quantities of environment information which may to be interesting for several applications. However, in general, sensor networks are very vulnerable due to the nature of the communication and due also to the sensor nodes are, sometimes, in remote, hostile and hard to reach areas. Moreover, the sensor nodes are potentially inexpensive devices that can be easily purchased or designed by others to attack the network. So to mitigate these vulnerabilities, research in security area for such networks are required. However, traditional security mechanisms lead to very overhead of computing and communication can compromise the network performance when they are adopted. Thinking about it, this master's thesis aims to propose a new paradigm to ensure security for wireless visual sensor networks, being presented through a theoretical mathematical model to perform differentiation of areas in the monitoring environment to then considering the particularities of the application monitoring to provide security at different levels. Called Adaptive Encryption, this theoretical model can be used for various applications requiring different security assurances for different network locations, implying providing security at acceptable levels while consuming less network resources, above all energy.

Keywords: Cryptography, Wireless Sensor Networks, Wireless Visual Sensor Networks.

Resumo

Recentemente as Redes de Sensores Sem Fio têm ganhado a atenção de pesquisadores, da indústria e do meio acadêmico ao redor do mundo todo, de modo que muitos projetos e soluções têm sido desenvolvidas para diversos cenários e aplicações. Essas redes são formadas por pequenos nós sensores com pouco poder de processamento, memória e energia. Sendo assim, os recursos são bastante escassos, principalmente energia, onde, na maioria das vezes estes nós são alimentados por baterias, sendo este um ponto crucial no projeto da rede. Um tipo de rede de sensores em que os nós possuem câmeras de vídeo embutidas são chamadas de Redes de Sensores Visuais Sem Fio. Devido a isso, tais redes se tornam capazes de recuperar grandes quantidades de informações do ambiente o que pode ser interessante para diversas aplicações. Todavia, de forma geral, as redes de sensores são muito vulneráveis devido a natureza da comunicação e devido também aos nós sensores estarem, algumas vezes, em locais remotos, hostis e de difícil acesso. Além disso, os nós sensores são dispositivos potencialmente baratos que podem ser facilmente adquiridos ou projetados por terceiros a fim de atacar a rede. Então, visando atenuar essas vulnerabilidades, pesquisas na área de segurança para tais redes são necessárias. Contudo, os mecanismos de segurança tradicionais geram muito sobrecarga de computação e comunicação podendo comprometer o desempenho da rede quando são adotados. Pensando nisso, este trabalho de mestrado tem como objetivo propor um novo paradigma para garantir segurança para redes de sensores visuais sem fio, sendo apresentado através um modelo matemático teórico para realizar diferenciação de áreas no ambiente de monitoramento para, então, considerando as particularidades da aplicação de monitoramento, prover segurança em diferentes níveis. Chamado de Criptografia Adaptativa, este modelo teórico pode ser utilizado por diversas aplicações que necessitem de garantias de segurança diferenciadas para diferentes locais da rede, o que implica em prover segurança em níveis aceitáveis consumindo menos recursos da rede, principalmente energia.

Palavras-chave: Criptografia, Rede de Sensores Sem Fio, Redes de Sensores Visuais Sem Fio.

Prefácio

Esta dissertação de mestrado foi submetida a Universidade Estadual de Feira de Santana (UEFS) como requisito parcial para obtenção do grau de Mestre em Computação Aplicada.

A dissertação foi desenvolvido dentro do Programa de Pós-Graduação em Computação Aplicada (PGCA) tendo como orientador o Dr. **Daniel Gouveia Costa**.

Esta pesquisa foi financiada pela CAPES.

Agradecimentos

O primeiro e merecido agradecimento é para André do Carmo, que pra mim é um "irmão", um amigo, um parceiro. Foi ele que soube da seleção para a primeira turma do PGCA em 2013, me falou e me incentivou a ingressar nessa jornada. Lembro que depois de uma longa discussão sobre o assunto numa mesa de bar, eu perguntei a ele na ocasião: "... *mas o que farei com um título de mestrado?*" e ele respondeu sem pestanejar: "*Pelo menos depois você pode bater na mesa do bar e dizer: - Eu sou mestre, nessa p...*". Então nada mais justo que ao fim desta jornada agradecer a André por me mostrar esse caminho, pelo incentivo, pelo apoio e pelo companheirismo mútuo que existe entre nós. Agora ao fim eu sei bem o que farei com o título de mestre. Em sequência, como de praxe, agradeço à Deus por estar vivo e pelas coisas e pessoas que cruzaram ou deixaram de cruzar o meu caminho. Sim, é a Deus que atribuo o acaso da minha vida. Agradeço por tudo e muito, aos meus pais, Gastão e Bárbara. À minha esposa Silvane que é a pessoa mais importante na minha vida e esta etapa cumprida é para e por ela. À minha "sobrinha" Vivi pela companhia na leitura dos artigos. À minha irmã Carol, por ser minha irmã sempre. O agradecimento mais importante é para meu orientador Prof. Dr. Daniel G. Costa, pelas dicas, pelos conselhos, pelos encaminhamentos e pela exemplar orientação durante o curso, valeu pela força! Deixo registrado também um agradecimento especial aos colegas Ivonete, Edcarlos e Fábio pelas experiências trocadas durante o curso, e pela amizade que se solidificou pra o resto da vida. Aos professores, Antônio Augusto, pela carta de recomendação, Iran Fernandes, pelos conselhos e amizade, Edgar Silva e Michele Fúlvia, pelas correções e dicas no projeto de dissertação e relatório de qualificação. Além disso, como sempre eu tenho que agradecer a pessoas e coisas lúdicas como às audíveis ondas sonoras traduzidas em músicas, que vão de Elis aos Rolling Stones, de Robert Jonson a Cartola, que eu ouço sempre e, nas horas difíceis, pra desafogar alguma angústia. Tenho que agradecer à Dell por montar um computador pessoal como o que tenho e que me ajuda muito. Agradeço também a Intel pelos processadores, ao Steve Jobs que é inspiração, ao Cleve Moler por inventar o MATLAB e ao Steven Sasson por inventar a câmera fotográfica digital e agradeço também a minha Nikon por me proporcionar um hobby saudável e prazeroso que comecei a praticar e estudar durante o curso PGCA e é algo que me leva meio que pra longe da realidade que se ver a olho nú. Agradeço também à James Naismith por inventar o basquete em 1891 e a Michael Jordan pelo exemplo de dedicação, perseverança e esforço, pois foi com ele que pude

perceber que não dá pra ser melhor em nada sem trabalho duro. E por fim, agradeço a minha magrela, como carinhosamente é chamada minha *mountain bike* aro 29, que me foi útil no transporte para a universidade no primeiro ano do curso, bem como ainda é até hoje nas trilhas de terra e lama longe da minha cidade natal.

Dedico este trabalho a minha amiga, namorada, mulher e esposa Silvane Santiago Souza.

Sumário

Lista de Publicações

Danilo de Oliveira Gonçalves & Daniel G. Costa (2015), A Survey of Image Security in Wireless Sensor Networks, Journal of Imaging 1(1), 4-30.

Lista de Tabelas

Lista de Figuras

Lista de Abreviações

Abreviação	**Descrição**
AC	Área de Confidencialidade
$AC_{N=0}$	Área de Confidencialidade com Nível de Confidencialidade igual a zero
$AC_{N=1}$	Área de Confidencialidade com Nível de Confidencialidade igual a um
$AC_{N=2}$	Área de Confidencialidade com Nível de Confidencialidade igual a dois
$AC_{N=3}$	Área de Confidencialidade com Nível de Confidencialidade igual a três
AC-ACK	Mensagem de Reconhecimento do Protocolo DACP
AC-Configure	Mensagem de Configuração do Protocolo DACP
AC-Request	Mensagem de Solicitação do Protocolo DACP
AES	*Advanced Encryption Standard*
AODV	*Ad hoc On-Demand Distance Vector*
BSD	*Berkeley Software Distribution*
CBC	*Cipher Block Chaining*
CFB	*Cipher Feedback*
CMOS	*Complementary Metal-Oxide-Semiconductor*
CRC	*Cyclic Redundant Check*
CSMA-CA	*Carrier Sense Multiple Access with Collision Avoidance*
DCAP	*Definition of Confidential Area Protocol*
DCT	*Discrete Cosine Transform*
DES	*Data Encryption Standard*
DFT	*Discrete Fourier Transform*
DoS	*Denial of Service*
DSR	*Dynamic Source Routing*
DVC	*Distributed Video Coding*
DWT	*Discrete Wavelet Transform*
ECB	*Electronic Code Book*
ECC	*Elliptic Curve Cryptography*
ECDH	*Elliptic Curve Diffie-Hellman*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
ECMV	*Elliptic Curve Menezes-Vanstone*
FoV	*Field of View*
GPS	*Global Positioning System*
IDEA	*International Data Encryption Algorithm*

ISM	*Industrial, Scientific and Medical*
LEAP	*Localized Encryption and Authentication Protocol*
LKHW	*Logical Key Hierarchy for Wireless sensor networks*
LR-WPAN	*Low-Rate Wireless Personal Area Networks*
MAC	*Media Access Control*
MD5	*Message-Digest Algorithm 5*
MDC	*Multiple Description Coding*
MENS	*Micro-Electro-Mechanical Systems*
mJ	*Micro Joules*
NC	Nível de Confidencialidade
OFB	*Output Feedback*
PAN	*Personal Area Networks*
PKC	*Public Key Cryptography*
QoE	*Quality of Experience*
QoS	*Quality of Service*
RAM	*Random Access Memory*
RISC	*Reduced Instruction Set Computer*
RSA	*Rivest Shamir Adleman Algorithm*
RSMSF	Rede de Sensores Multimídia Sem Fio
RSSF	Rede de Sensores Sem Fio
RSVSF	Rede de Sensores Visuais Sem Fio
SHA	*Secure Hash Algorithm*
SSL	*Secure Socket Layers*
TCP/IP	*Transmission Control Protocol/Internet Protocol*
TDMA	*Time Division Multiple Access*
TPGF	*Two Phase Geographic Forwarding Protocol*
WEP	*Wired Equivalent Privacy*
WPAN	*Wireless Personal Area Networks*
WSN	*Wireless Sensor Networks*
XOR	*Exclusive OR*

Lista de Símbolos

Símbolos	**Descrição**
α	Ângulo de orientação do nó sensor visual
Δ	Representação da área
θ	Ângulo de abertura do campo de visão da câmera

Capítulo 1

Introdução

As Redes de Sensores Sem Fio (RSSF) ou *Wireless Sensor Networks* (WSN), em inglês, são uma emergente tecnologia de baixo custo utilizada para monitoramento de ambientes remotos. Elas foram criadas e projetadas para coletar dados sobre algum tipo de evento em ambientes onde, por diversos motivos, o homem não pode interagir diretamente. Então, RSSF são compostas por centenas, até milhares, de pequenos dispositivos com capacidade de sensoriamento, processamento e comunicação [Akyildiz et al. 2002, Yick et al. 2008, Baronti et al. 2007, Min et al. 2001]. Atualmente, redes de sensores sem fio são utilizadas nas mais diversas aplicações, como rastreamento, automação industrial e residencial, agricultura, medicina e ecologia. De fato, esta é uma tecnologia barata e de baixa potência que exige que novos conceitos sejam considerados no projeto. As RSSF têm ganhado a atenção do mundo recentemente devido principalmente à proliferação dos *Micro-Electro-Mechanical Systems* (MEMS) que facilitaram o desenvolvimento de sensores menores e mais inteligentes [Yick et al. 2008]. Contudo, RSSF são redes que possuem muitas restrições de recursos como processamento, memória e energia, fazendo com que todo o projeto dependa significativamente das características da aplicação para que está sendo desenvolvida, sempre considerando fatores como o ambiente, os objetivos e o custo.

Um tipo diferente de redes de sensores são as Redes de Sensores Multimídia Sem Fio (RSMSF). As redes de sensores "tradicionais", são chamadas de redes de sensores escalares por coletar exatamente apenas dados escalares como temperatura, pressão e umidade. Já as RSMSF coletam dados multimídia como áudio, vídeo e imagens estáticas, e também dados escalares. Isso se torna possível com o surgimento de dispositivos como câmeras e microfones CMOS[1] mais baratos [Almalkawi et al. 2010]. Assim, uma rede de sensores multimídia pode capturar muito mais informação do ambiente que as redes de sensores tradicionais. Por outro lado, esse tipo de rede manipula dados massivos gerando muito fluxo na rede e, sendo assim, o projeto de

[1] *Complementary Metal-Oxide-Semiconductor*

redes de sensores multimídia tem desafios diferentes no que diz respeito à arquitetura, algoritmos e protocolos.

Tanto as redes de sensores escalares quanto as redes de sensores multimídia são muito vulneráveis a vários tipos de ameaças à segurança devido à sua natureza distribuída e ao seu uso, principalmente em áreas remotas. Além disso, a comunicação sem fio é mais sujeita a falhas e ataques à segurança que as redes cabeadas. A depender da aplicação, aspectos de segurança são muito importantes para garantir o funcionamento da rede, a sua vida útil e a preservação dos segredos que trafegam por ela. Assim, em RSSF, segurança é um aspecto muito relevante no projeto da rede, mas devido às restrições de recursos nos nós sensores, os mecanismos de segurança tradicionais com grande sobrecarga de computação e comunicação são muito dispendiosos para as RSSF [Sen 2009]. Em resumo, segurança em RSSF é uma tarefa desafiadora.

Dentro do âmbito das RSMSF, existe um tipo de rede chamada Redes de Sensores Visuais Sem Fio (RSVSF) que coleta apenas imagens estáticas e/ou vídeo. Prover segurança às RSVSF torna-se uma tarefa mais desafiadora e muito mais relevante que em redes de sensores escalares, devido à gama de aplicações possíveis existentes para as RSVSF. O problema de limitação de recursos é ainda maior quando se trabalha com dados multimídia, pois eles representam mais informações do ambiente. Sendo assim, tratá-los, compactá-los e criptografá-los, por exemplo, são tarefas muito mais degradantes aos recursos da rede do que quando se trabalha com dados escalares, então os mecanismos de segurança nas RSVSF devem ser mais atentos à economia de recursos.

O problema que motivou este trabalho relaciona a vulnerabilidade existente nas RSSF, concentrando-se nas RSVSF, com as restrições de recursos existentes nos elementos que compõem a rede. Em outras palavras, o problema emerge do contraponto existente entre o ambiente muito vulnerável a ataques e a escassez de recursos necessários para se garantir segurança utilizando os mecanismos conhecidos. Portanto, este trabalho tem como objetivo propor um novo paradigma de segurança para as RSVSF, que atenda aos requisitos de segurança das aplicações, porém minimizando o uso de recursos da rede, principalmente energia, para prover segurança.

A Criptografia Adaptativa surge como um novo paradigma que tem como premissa a adaptação de mecanismos de segurança para que sejam aplicados de forma mais energeticamente eficiente às redes de sensores sem fio. Sendo assim, este paradigma está baseado em fundamentos como criptografia seletiva, variação de tamanho de chaves, variação de algoritmos de criptografia e do tipo de criptografia (simétrica, assimétrica), entre outros fatores e mecanismos que podem ser agregados ao modelo a depender da necessidade da aplicação em questão. Além disso, a Criptografia Adaptativa visa criar conceitos que possibilitam prover segurança apenas no local da rede que se tem maior necessidade, fazendo isso da maneira mais eficiente para cada local da rede, proporcionando assim, de forma geral, uma maior economia de energia. Assim, este princípio delimita áreas para se prover segurança, onde

cada área poderá ter um nível de segurança diferente, onde cada nível executa os protocolos e medidas de segurança de forma diferenciada. Esta abordagem visa minimizar a utilização de recursos com segurança, principalmente em relação ao gasto energético, se comparado a aplicar um único mecanismo de segurança para a rede de sensores como um todo.

A criação deste modelo de segurança voltado para as RSVSF, como mencionado anteriormente, se dá pelo fato de que prover segurança em redes de sensores visuais é uma tarefa mais desafiadora devido à natureza dos dados coletados representarem mais informações do ambiente, necessitando, na maioria das vezes, de um tratamento diferenciado, fazendo com que o problema de limitação de recursos e restrição de energia seja um obstáculo ainda maior em comparação com as RSSF escalares. Além disso, o princípio da Criptografia Adaptativa não é genérico para os diversos tipos de rede de sensores, ou seja, existem diferenciações na aplicação do modelo em RSSF, RSVSF e RSMSF, e sendo assim, devido aos motivos citados anteriormente optou-se pelo foco nas redes de sensores visuais sem fio para elaboração, execução e validação do modelo apresentado.

1.1 Justificativa

Levando-se em consideração características como restrições de recursos, principalmente energia, a grande quantidade de informações necessárias para a representação de dados multimídia, como, por exemplo, imagens, e que os mecanismos de segurança tradicionais são dispendiosos para as redes de sensores, é sabido que prover segurança em RSVSF, assim como em RSSF, é algo desafiador. Contudo, é possível aplicar qualquer mecanismo de segurança numa rede de sensores como um todo, só que desta forma, garantir segurança se torna algo muito dispendioso aos recursos da rede, impactando principalmente na perda de nós sensores por falta de energia e consequentemente na perda da vida útil da rede como um todo. Partindo deste pressuposto, desenvolver uma maneira de se garantir segurança aos dados coletados numa rede de sensores sem que haja um grande desperdício dos recursos dos nós sensores, principalmente energia, torna-se algo vital para que se tenha uma rede de sensores segura e funcional. Assim, a proposta apresentada por este trabalho visa criar um novo paradigma de segurança para RSVSF chamado de Criptografia Adaptativa, que tem no seu princípio a diferenciação de nós sensores quanto à localidade, onde cada grupo de nós sensores pode ou não aplicar mecanismos de segurança aos seus dados coletados, a depender de onde estejam localizados e a depender das necessidades de segurança da aplicação em cada local da rede. Desta forma, a depender dos requisitos da aplicação, determinadas áreas do ambiente que a rede de sensores está operando podem ter mecanismos bastante seguros, menos seguros ou sem segurança alguma, levando a uma maior economia de energia nos nós sensores fonte em comparação a forma tradicional de se garantir segurança, onde um único mecanismo de segurança é aplicado à rede como um todo.

1.2 Relevância e Motivação

O modelo de criptografia adaptativa é relevante no aspecto da diferenciação dos nós sensores para a aplicação dos mecanismos de segurança. Em outras palavras, com a utilização deste modelo, não será necessário aplicar mecanismos de segurança à rede como um todo, se a necessidade da aplicação indica que apenas alguns nós sensores devem ter seus dados coletados seguros. Desta forma, economiza-se recursos nos nós sensores fonte, principalmente energia, pois apenas alguns nós sensores irão aplicar os mecanismos de segurança, garantindo sigilo aos dados coletados que são necessários mediante os requisitos da aplicação em questão. Como as redes de sensores sem fio, de forma geral, possuem limitações de comunicação, processamento, memória, armazenamento e energia, o modelo proposto pode ser válido para agregar segurança sem degradar severamente o desempenho da rede, consumindo menos recursos dos nós sensores, tendo como principal métrica de eficiência do modelo a energia gasta pelos nós sensores fontes para prover segurança. Em outras palavras, as verificações sobre como a criptografia adaptativa não degrada o desempenho de uma RSVSF é o consumo de energia, que implica em um maior *network lifetime*. Além disso, a solução proposta é uma nova forma de se prover segurança a redes de sensores visuais, que pode vir a contribuir com pesquisas futuras na área de segurança em RSVSF.

1.3 Objetivos

O objetivo geral deste trabalho é criar um modelo para prover segurança em rede de sensores visuais sem fio, intitulado de Criptografia Adaptativa. Desta forma, espera-se que com a utilização deste modelo seja possível prover um nível aceitável de segurança à RSVSF sem que seja necessário aplicar mecanismos ou aspectos de segurança à rede de sensores como um todo, porém somente a áreas onde haja necessidade de segurança, tendo o fator energia dos nós sensores fonte como métrica principal de eficiência no desempenho e economia de recurso. Como objetivos específicos pode-se listar:

- Elaborar o modelo para que se ofereça garantias de confidencialidade e integridade com impacto reduzido aos recursos da rede, principalmente energia;
- Desenvolver um protocolo de comunicação para aplicação do modelo;
- Fazer comparações do modelo proposto com a forma "tradicional" de se prover segurança à rede como um todo;
- Submeter um artigo para publicação em periódico conforme norma do Programa de Pós-Graduação em Computação Aplicada.

1.4 Organização da Dissertação

O restante desta dissertação está organizada da seguinte forma. No Capítulo Dois é apresentada uma revisão bibliográfica sobre rede de sensores sem fio, englobando temas relacionados ao desenvolvimento deste trabalho. No Capítulo Três é apresentada a especificação do modelo de criptografia adaptativa, expondo seus conceitos, definições e paradigmas. A metodologia de trabalho é descrita no Capítulo Quatro. No Capítulo Cinco são apresentados os resultados como forma de validação do modelo proposto através de verificações, simulações e gráficos. Por fim, no Capítulo Seis são apresentadas as considerações finais, seguidas das referências bibliográficas que são apresentadas no último capítulo.

Capítulo 2

Fundamentação Teórica

A necessidade de comunicação é algo crescente nas últimas décadas. Com o surgimento da Internet e das redes baseadas em pacotes a necessidade de comunicação tem se tornado muito comum ao redor do mundo. Por outro lado, existem aplicações que possuem a necessidade de comunicação e conectividade onde as redes de computadores tradicionais, como as redes TCP/IP, não são adequadas. Em aplicações para monitorar uma corrente marítima ou um vulcão, por exemplo, é necessário outro paradigma de rede para fazer com que qualquer informação deste evento chegue a um usuário final. A partir desta necessidade é que surgiram as redes de sensores sem fio (RSSF).

As redes de sensores multimídia sem fio (RSMSF) são muito parecidas com as redes de sensores tradicionais, destinadas a coleta de dados escalares. Contudo, o que diferencia estas redes é o tipo de dado que elas coletam e processam. Como as RSSF intrinsecamente possuem recursos limitados, trabalhar com dados de áudio, vídeo ou imagens é muito mais difícil, mesmo que estes dados sejam de muito baixa resolução e qualidade em relação aos arquivos multimídia que trafegam pela Internet. Como exemplo, uma medida de temperatura é representada com 10 Bytes ou menos, e um nó sensor numa RSSF transmite estes 10 Bytes com alguns acréscimos de informações de controle. Em contraponto, por exemplo, para transmitir uma imagem estática de resolução 128 pixels x 128 pixels, não comprimida, em escala de cinza e com codificação com 256 níveis, seriam necessários 16384 Bytes. Em outras palavras, transmitir uma imagem de baixa qualidade em escala de cinza é mais de 1600 vezes mais custoso que transmitir uma medição de temperatura. Portanto, aspectos como segurança em RSMSF devem ser pensados e projetados de forma que economizem recursos da rede sempre atentando para a característica do dado multimídia a ser transmitido.

Redes de sensores sem fio tradicionais e redes de sensores multimídia sem fio são um tipo especial de rede que compartilham características comuns às redes tradicionais de computadores [Sen 2009]. Contudo, essas redes possuem muitas características que são únicas e próprias a este novo tipo de rede. Os serviços de segurança numa

rede de sensores visa proteger os dados coletados contra acesso não autorizado e modificação, além de objetivar proteger os recursos da rede contra ataques e mal comportamento dos nós sensores, o que demanda recursos que podem levar à perda prematura da vida útil do nó sensor e da própria rede.

Levando em conta as características dos dados multimídia, foram desenvolvidos esquemas como criptografia seletiva [Podesser et al. 2002, Sadourny e Conan 2003, Pfarrhofer e Uhl 2005, Grangetto et al. 2006, Liu 2006] ou criptografia parcial [Cheng e Li 2000]. Este tipo de mecanismo de segurança pode ser aplicado em RSMSF, onde a imagem coletada é codificada e compactada para então suas partes principais serem criptografadas. Assim, um atacante quando se apropria das outras partes menos importantes da imagem não consegue reconstruí-la, uma vez que somente com a parte principal é possível reconstruir a imagem original. Em resumo, como a parte principal está criptografada, é garantido segurança ao dado por completo. As próximas seções apresentam os fundamentos relacionados ao desenvolvimento deste trabalho.

2.1 Rede de Sensores Sem Fio

O projeto de sistemas de sensores sem fio tem atraído a atenção e o interesse para diversas aplicações no âmbito civil e militar. Recentes avanços em sistemas micro eletromecânicos, minúsculos microprocessadores e tecnologias de rádio de baixa potência permitiram a criação e evolução de pequenos dispositivos sensores de baixo custo, de baixa potência e multi-funcionais capazes de observar e reagir a mudanças físicas no ambiente em que estão imersos [Baronti et al. 2007]. Portanto uma rede de sensores é uma nova tecnologia de redes que interconecta, ao invés de computadores, dispositivos embarcados bastante limitados, mas com capacidade de sensoriamento, chamados de nós sensores. Esses nós sensores são pequenos, com processamento, memória e recursos computacionais limitados e são baratos em relação a sensores tradicionais [Yick et al. 2008]. Segundo [Min et al. 2001], antes da proliferação dos MEMS a forma de sensoriamento era feita por *macrosensores* se comunicando diretamente com a estação base. Com o surgimento de sensores mais inteligentes e menores, o paradigma de sensoriamento mudou para a utilização de *microsensores* (nós sensores) se comunicando entre si, formando uma rede. Enquanto um nó sensor sozinho não tem a mesma precisão que um macrosensor, uma rede com uma larga quantidade de nós sensores tem uma alta qualidade de sensoriamento.

Na Figura 2.1 é apresentado um exemplo de disposição típica de uma rede de sensores sem fio genérica. Uma RSSF possui um nó especial chamado de *Sink Node* que é responsável por receber os dados coletados pelos outros nós sensores e enviá-los a uma estação base. A estação base é formada por um ou mais computadores convencionais sem restrições de processamento e armazenamento, possuindo softwares que interpretam e armazenam os dados coletados, realizam o gerenciamento e

configuração da rede e podem realizar tomadas de decisões. De fato, o *Sink Node* é quem faz a interface entre a RSSF e a estação base. Ele pode se conectar com outro tipo de rede para enviar as informações até o usuário e na maioria dos casos esta comunicação se dá pela Internet ou através de um gateway numa rede estruturada. Como não existe uma alta capacidade de armazenamento, os nós, na maioria das aplicações, enviam os dados coletados pela rede através da interface sem fio para o *Sink Node* a fim de que a informação alcance a estação base.

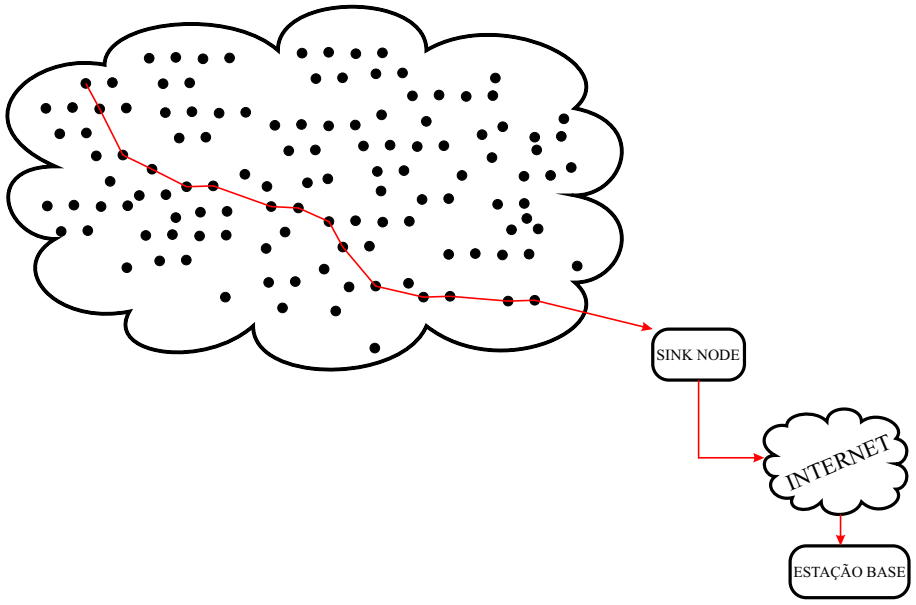


Figura 2.1: Exemplo conceitual de uma RSSF.

As RSSF são aplicadas na maioria das vezes em áreas extensas, ambientes hostis e/ou de difícil acesso. Mas também podem ser aplicadas em ambientes industriais e residenciais. Portanto, uma RSSF é projetada baseando-se principalmente na aplicação e no propósito para o qual ela vai operar. Além disso, uma RSSF é necessariamente centrada nos dados, ou seja, os dados coletados e as informações são mais importantes que a própria rede. Como o nó sensor pode sofrer danos ou falhas e também porque funciona com uma bateria como fonte de energia, muitas vezes ele não é recuperado ou a bateria é trocada, portanto a vida da rede (*network lifetime*) é também limitada. Na maioria dos casos os sensores são depositados em ambientes de difícil acesso, impossibilitando a troca ou recarga da fonte de energia. Desta forma, a principal preocupação no projeto de uma RSSF é com relação ao consumo de energia. Em algumas aplicações uma segunda fonte de energia, como painéis solares, pode ser utilizada, mas restrições de custos podem limitar o uso de tal recurso. Por isso aspectos como roteamento, localização, disponibilidade, cobertura, gerenciamento de dados e segurança devem estar sempre atentos à eficiência energética a fim de evitar o desperdício de energia e, consequentemente, aumentar o tempo de vida da rede.

Aplicações em larga escala requerem o uso de centenas ou milhares de nós sensores,

logo aumentando o custo. Por isso, os recursos em um nó sensor numa RSSF são limitados, a fim de diminuir o seu custo. Além disso, RSSF, devido às aplicações para que são utilizadas, são projetadas com a comunicação sem fio de maneira *ad hoc*[1] e com a ausência de uma comunicação estruturada. Assim, quando os nós sensores são depositados em largas quantidades em um ambiente, eles podem automaticamente auto organizar-se, formando a rede [Baronti et al. 2007].

2.1.1 Arquitetura do Nó Sensor

Os nós sensores podem sentir ou medir alguma grandeza física ou coletar alguma informação do ambiente que está monitorando e enviá-la pela rede até uma estação base. Assim, uma rede sensores é composta por nós sensores que estão tanto coletando ou medindo informações do ambiente quanto retransmitindo dados que outros sensores enviam. Portanto, os nós sensores são dispositivos inteligentes equipados com uma ou mais unidades de sensoriamento, um processador, memória, fonte de energia e um transmissor de rádio [Yick et al. 2008]. Opcionalmente, nós sensores podem incluir módulos de localização, geração de energia e atuadores. A Figura 2.2 apresenta um esquema geral para a organização interna dos nós sensores.

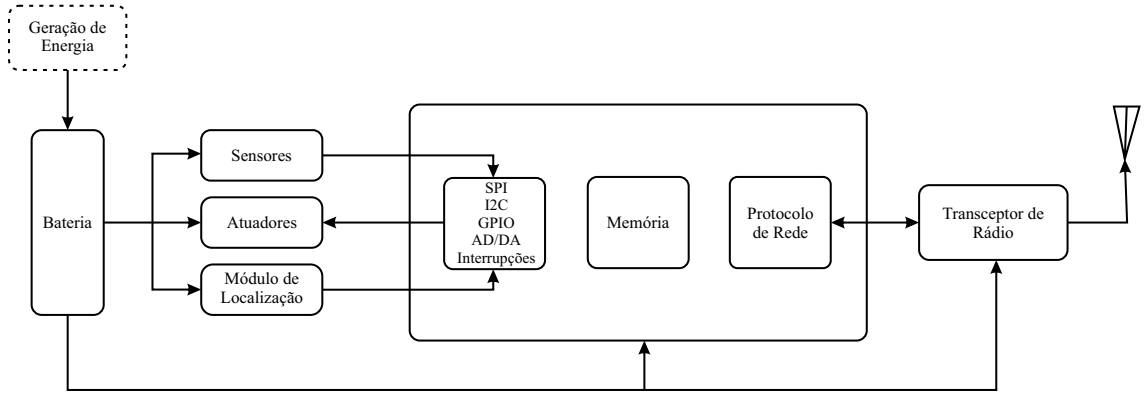


Figura 2.2: Descrição em alto nível de um nó sensor [Soares 2012, p.18].

Nós sensores empregam microcontroladores com um conjunto de instruções reduzidas de baixo custo (RISC - *Reduced Instruction Set Computer*), com um programa pequeno e tamanho da memória de dados de cerca de 100kB [Baronti et al. 2007]. Para aumentar a capacidade de memória e armazenamento do dispositivo, uma memória flash externa com tempo de acesso grande pode ser adicionada fornecendo armazenamento secundário. Como interfaces de entrada e saída existem as linhas seriais, conversores de analógico para digital e temporizadores.

[1]Redes *ad hoc* são redes sem fio que dispensam uma estrutura centralizada com pontos de acesso. Numa rede *ad hoc* os nós da rede funcionam tanto como *hosts* quanto como roteadores, encaminhando comunitariamente os pacotes dos nós vizinhos para que cheguem até o destino.

Segundo [Baronti et al. 2007], com relação à posição da unidade de sensoriamento, existem duas abordagens. Na primeira o sensor está em uma placa específica conectada à placa principal do microcontrolador através de uma interface de entrada e saída. A outra abordagem é ter a unidade de sensoriamento fixada diretamente na placa principal do microcontrolador. A unidade é soldada ou montada na placa, reduzindo os custos de produção dos nós sensores e fazendo com que eles se tornem mais robustos que a abordagem anterior.

Os nós sensores podem ser classificados ainda como dois tipos principais: sensores escalares e sensores multimídia. Os sensores escalares coletam apenas grandezas escalares que podem ser representados por um número em uma escala, por exemplo, temperatura, pressão, umidade, calor, abalos sísmicos, etc.. Os sensores multimídia podem recuperar dados multimídias como imagens, vídeo e/ou áudio, além de dados escalares [Almalkawi et al. 2010]. Na sessão 2.2 serão apresentadas as particularidades das Redes de Sensores Multimídia Sem Fio, que fazem parte do objeto de investigação desse trabalho.

2.1.2 Aplicações para RSSF

As aplicações em RSSF são divididas em duas categorias, sendo elas monitoramento e rastreamento, como pode ser visto na Figura 2.3. As aplicações de monitoramento incluem o monitoramento de estruturas como prédios, pontes e outras construções, monitoramento interno e externo de ambientes, aplicações de automação de processos, monitoramento da saúde de pessoas ou pacientes, monitoramento de níveis de energia ou substâncias químicas, monitoramento de animais ou máquinas, monitoramento do clima para auxiliar a agricultura, entre outras. As aplicações de rastreamento incluem rastreamento de animais, pessoas ou objetos [Yick et al. 2008].

Aplicações de monitoramento são aquelas que monitoram uma ou mais grandezas físicas em algum ambiente e reportam este dado para o usuário. Por outro lado, aplicações de rastreamento são utilizadas para localizar um determinado alvo e saber a sua exata localização. Este tipo de aplicação de rastreamento é muito utilizada em ambientes militares para rastrear inimigos. Contudo, existem aplicações onde podem-se rastrear veículos, o tráfego de ônibus no sistema público de transporte ou animais silvestres numa floresta. A seguir são elencados alguns exemplos de aplicações comuns em RSSF.

- **Monitoramento de animais**: coletar dados sobre o habitat, população, hábitos e localização são discutidas em [Szewczyk et al. 2004], [Čapkun et al. 2002], [Wang et al. 2003]. Os nós sensores são depositados no ambiente e continuamente enviam dados sobre estes fatores para uma estação base por um longo período de tempo. Este tipo de aplicação trouxe um avanço muito importante, pois ao invés dos seres humanos terem que entrar no ambiente natural do animal periodicamente para coletar os dados, os dados ficam disponíveis aos seres humanos através da RSSF, evitando que hajam

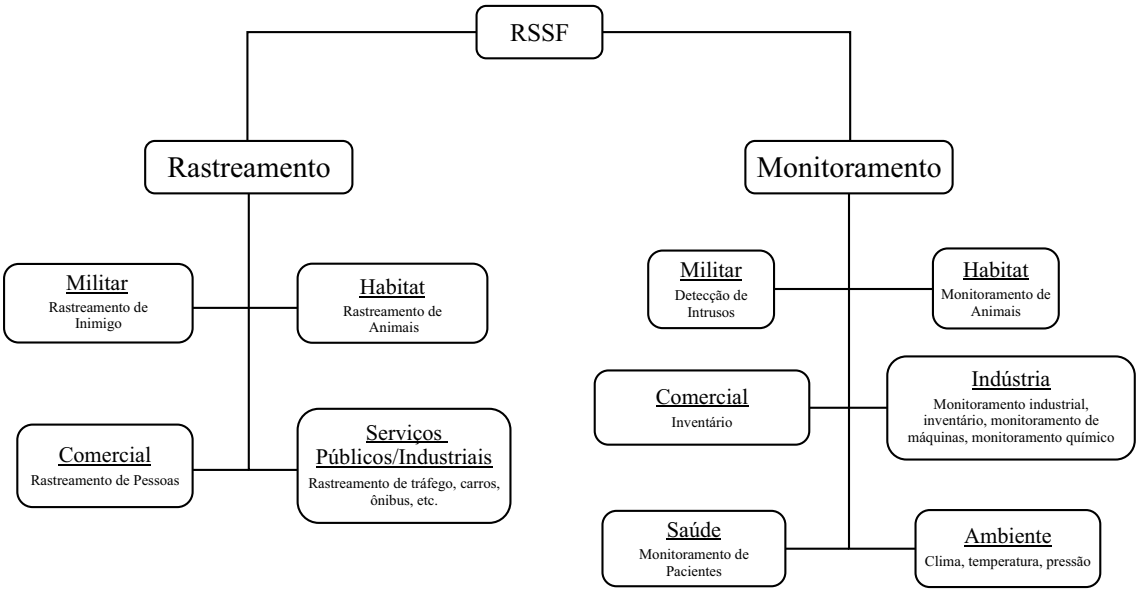


Figura 2.3: Aplicações para RSSF [Yick et al. 2008, p.2296].

erros de medição, barateando os custos e evitando que o meio ambiente sofra interferência do ser humano;

- **Área médica**: aplicações com redes de sensores são utilizadas para monitorar remota e continuamente parâmetros físicos de pacientes. O trabalho apresentado por [Gao et al. 2005] e o trabalho apresentado por [Malan et al. 2004a] exemplificam bem este tipo de aplicação e propõem uma estrutura apropriada. Então, parâmetros como pressão sanguínea, batimentos cardíacos e temperatura são monitorados e, havendo alguma alteração, um alerta é emitido;
- **Sistemas de detecção de poluição**: tipicamente, podem ser utilizados numa cidade, mar ou rio. Numa determinada região ou ambiente é possível espalhar nós sensores e formar uma RSSF para medir o nível de alguma substância química e detectar uma possível poluição no ambiente. Sistemas similares para detectar níveis de água em rios ou chuvas torrenciais, para prever inundações ou para detectar fogo e desastres naturais [Steere et al. 2000] são similares a aplicações de detecção de poluição e muito úteis para prever ou melhor se recuperar de problemas como este;
- **Localização**: uma aplicação de rastreamento interessante é a *PinPtr* [Simon et al. 2004]. Esta aplicação é um sistema para detectar e localizar atiradores, que utiliza uma densa rede de sensores na área a ser protegida para medir o tempo de chegada das ondas sonoras de um disparo de arma de fogo. Ocorrendo um tiro, os sensores enviam seus dados captados para um computador central ou laptop para ser calculada a localização do possível destino do disparo;
- **Monitoramento vulcânico**: é uma aplicação bastante interessante e eficaz,

além de ser um exemplo clássico do uso de RSSF. O projeto apresentado por [Werner-Allen et al. 2006] é um exemplo de monitoramento de abalos sísmicos em um vulcão, onde sensores são implantados ao redor de um vulcão para medir alguns parâmetros relacionados à erupção. Se alguns níveis pré-determinados forem atingidos, a RSSF consegue detectar muito mais rapidamente e precisamente que os equipamentos tradicionais e avisar a estação base de uma possível alteração na atividade do vulcão para que providências sejam tomadas;

- **Agricultura**: as RSSF podem ser usadas para monitorar fatores naturais, como condições climáticas de diferentes zonas numa larga área cultivada, para calcular mais precisamente a necessidade de água e/ou de substâncias químicas para cada zona, a depender da cultura cultivada [Baronti et al. 2007];
- **Segurança pública**: aplicações como monitoramento de tráfego de carros, monitoramento estrutural de pontes, construções ou prédios, sistemas de localização de criminosos e controle de incêndios em áreas públicas ou com aglomeração são alguns exemplos de aplicações para auxiliar a segurança pública. Pode-se destacar a aplicação *FireLine* que é um sistema de RSSF para monitorar os batimentos cardíacos de bombeiros em serviço [Yick et al. 2008]. Além disso, existem aplicações para auxiliar a segurança pública que utilizam nós sensores com câmeras para realizar vigilância ou detectar ações terroristas em grandes eventos, onde a quantidade de pessoas aglomeradas pode ser muito grande, evitando assim tragédias [Costa et al. 2013];
- **Automação residencial**: as RSSF podem ser utilizadas para monitorar o ambiente residencial, coletando fatores do ambiente e enviando ao usuário. Variáveis como temperatura, incidência de fogo, detecção de intrusos, entre outras, podem ser monitoradas;
- **Automação industrial**: existem aplicações de RSSF para controle de processos, controle e monitoramento de equipamentos e máquinas, monitoramento de substâncias químicas ou monitoramento de estruturas muito interessantes para o ambiente industrial [Yick et al. 2008]. O padrão WirelessHART foi desenvolvido exclusivamente para atender a demanda da industria [Song et al. 2008], sendo uma opção bastante viável para aplicações em ambientes industriais.

Outras aplicações de redes de sensores podem ser encontradas em [Yick et al. 2008][Baronti et al. 2007][Akyildiz et al. 2002] com vários detalhes e informações.

2.1.3 Restrições em RSSF

Devido às limitações energéticas dos nós sensores, as RSSF possuem muitas restrições a serem observadas durante o seu projeto. Pode-se dizer que redes de sensores sem fio possuem restrições inerentes de recursos. Algumas das principais restrições de recursos das RSSF são apresentadas a seguir.

- **Energia:** Energia é a principal restrição em RSSF. Os nós sensores são, na maioria das vezes, alimentados por bateria, que tem energia limitada. O tempo de vida útil da rede depende de quão bem aproveitada é esta fonte de energia. Segundo [Sen 2009], o consumo de energia nos nós sensores é realizado por três fatores: sensoriamento, comunicação e processamento. O estudo realizado por [Hill et al. 2000] afirma que transmitir um bit na rede em uma RSSF consome a mesma quantidade de energia que executar 800 a 1000 instruções no microprocessador. Assim, a comunicação é muito mais dispendiosa à RSSF que o processamento. Portanto, mensagens e dados desnecessários devem ser evitados para não reduzir o tempo de vida da rede;

- **Memória:** A memória e o armazenamento de um nó sensor é bastante limitado. Geralmente, a memória é disponibilizada como um bloco de *flash memory* ou memória RAM[2]. A *flash memory* é usada para armazenar o código da aplicação e a memória RAM é usada para armazenar o programa da aplicação, os dados do sensoriamento e resultados das computações [Sen 2009]. Assim, não existe espaço para executar algoritmos complicados (como por exemplo, uma criptografia robusta) depois de carregar na memória o sistema operacional e o código da aplicação;

- **Comunicação sem confiabilidade:** Normalmente, o roteamento em redes de sensores é baseado em protocolos sem conexão e, portanto, intrinsecamente não-confiáveis. Os pacotes podem ser danificados devido a erros de canal ou podem ser descartados em nós altamente congestionados. Além disso, a natureza do canal de comunicação sem fio também pode danificar ou corromper os pacotes. Altas taxas de erro exigem sistemas de tratamento de erros robustos a serem implementados, levando a uma maior sobrecarga. Em certas situações, mesmo que o canal seja de confiança, a comunicação pode não ser. Isto é devido à natureza da transmissão sem fio, que é mais propensa a erros e falhas, onde os pacotes podem colidir no canal de comunicação gerando retransmissões que degradam o desempenho e consomem energia [Akyildiz et al. 2002];

- **Alta latência:** Em RSSF, o roteamento *multi-hop*[3], o congestionamento do canal de comunicação e o processamento em nós intermediários podem ocasionar alta latência [Sen 2009];

- **Processamento:** O processamento também é uma restrição de recurso importante pois algoritmos tradicionais de roteamento e segurança, por exemplo, possuem muita sobrecarga de processamento o que degrada o tempo de vida da rede. Outro fator crítico é o processamento em nós intermediários, como compactação ou agregação de dados. Em resumo, qualquer aspecto de rede

[2]RAM - *Random Access Memory* ou em português, Memória de Acesso Aleatório.

[3]O raio de transmissão de uma RSSF é limitado, necessitando que o dado coletado seja roteado através de múltiplos nós intermediários. Como cada nó de uma rede *ad hoc* atua tanto como *host* quanto como roteador, cada nó intermediário participa da descoberta e manutenção das rotas para os outros nós sensores, por isso o termo roteamento *multi-hop*.

que se aborda em RSSF tem que se atentar para não gerar sobrecarga de processamento excessiva.

2.1.4 Serviços de Rede e Aspectos de Projeto

O projeto de uma RSSF deve ser planejado atentando para diversos aspectos para que seus serviços sejam oferecidos sem interrupção e de forma otimizada. Aspectos como tolerância a falhas, escalabilidade, custo, consumo de energia e roteamento, entre outros, devem estar bem definidos no projeto. A seguir são detalhados alguns aspectos de projeto, relacionando-os com os serviços de rede mais importantes:

- **Tolerância a falhas**: Os nós sensores podem falhar e/ou serem bloqueados devido à falta de energia, à danos físicos ao *hardware* ou à interferência do ambiente. Segundo [Akyildiz et al. 2002], a falha de nós não deve afetar a tarefa global da rede, estando esta afirmação ligada à confiabilidade da rede e à tolerância a falhas. Assim, tolerância a falhas é a capacidade da rede de manter suas funções independente da falha de alguns nós. De certa forma, este aspecto está ligado à confiabilidade e disponibilidade dos dados. Mecanismos como Direct Diffusion [Intanagonwiwat et al. 2000] podem ser empregados para realizar a comunicação com múltiplos caminhos para garantir a tolerância a falhas;

- **Escalabilidade**: Em algumas aplicações é necessária a utilização de nós redundantes, a fim de prolongar o tempo de vida da rede economizando bateria, e também a fim de prover tolerância a falhas. O número de nós sensores numa RSSF para monitorar ou rastrear um ambiente pode ser da ordem de centenas ou milhares. Dependendo da aplicação, este número pode chegar a milhões. Portanto, o fator da escalabilidade deve ser sempre considerado no projeto de uma RSSF, pois redes deste tipo devem ser utilizadas, com resultados positivos, tanto com alguns poucos nós sensores quanto com grande quantidades de nós sensores;

- **Custo de produção**: Como as RSSF podem utilizar uma grande quantidades de nós sensores, o custo de um único nó sensor tem que ser muito baixo para justificar a utilização de uma RSSF. Se o custo da rede é maior que um projeto tradicional de sensoriamento com *macrosensores*, a utilização de RSSF não é justificada [Akyildiz et al. 2002]. Portanto, o custo de um nó sensor tem que ser muito inferior que outras tecnologias, para justificar a adoção de uma RSSF com inúmeros nós para monitorar um ambiente;

- **Topologia**: A topologia numa RSSF geralmente é classificada como *mesh networking*. Segundo [Akyildiz et al. 2002], questões relacionadas com a manutenção e a mudança da topologia podem ser dividas em três fases:

    1. *Fase de implantação:* Nós sensores podem tanto ser jogados aleatoriamente no ambiente em largas quantidades, por exemplo de um avião, ou

colocados um a um no ambiente por um ser humano ou um robô;

2. *Fase de pós-implantação:* Após a implantação, mudanças podem ocorrer devido a mudanças de posição, danos, perda de acessibilidade devido a interferências, ruídos ou obstáculos, falta de energia, mal funcionamento ou mudanças no projeto;

3. *Redistribuição de fase adicional:* Nós sensores adicionais podem ser redistribuídos a qualquer momento para substituir os nós com defeito ou devido a mudanças na dinâmica de tarefas.

- **Ambiente**: Na maioria dos casos, os nós sensores são jogados em um ambiente remoto, de difícil acesso ou perigoso. Em resumo, numa RSSF os nós são colocados ou muito perto ou diretamente dentro do fenômeno físico a ser observado [Akyildiz et al. 2002]. A probabilidade desses nós sensores sofrerem danos ou ataques físicos em tais ambientes é muito grande, e o gerenciamento remoto virtual pode não ser suficiente para detectar uma alteração física do nó sensor. Os nós podem estar em ambientes como o interior de máquinas, no fundo do oceano, contaminados por agentes biológicos ou químicos ou numa guerra atrás das linhas inimigas;

- **Consumo de energia**: Um nó sensor numa RSSF é sempre equipado com uma fonte de energia limitada. Em alguns casos, a troca da bateria não é possível e o tempo de vida do sensor depende do tempo de vida da bateria. Numa RSSF, por realizar transmissão *multi-hop* e a comunicação ser baseada no princípio *ad hoc*, cada nó tem a função de coletar dados e retransmitir pacotes de outros nós. Como dito anteriormente, o mal funcionamento de poucos nós pode alterar significantemente a topologia da rede. Então o consumo de energia deve ser minimizado e gerido pela própria rede. Segundo [Akyildiz et al. 2002], por estas razões, os pesquisadores tem atualmente concentrado esforços para projetar protocolos e algoritmos conscientes em relação à energia para as RSSF;

- **Localização**: Algumas aplicações em RSSF necessitam de algum sistema de localização. O propósito da localização é localizar os nós sensores no ambiente em questão. Ela pode ser usada para auxiliar o roteamento ou para identificar o local de origem ou destino de determinados dados. Em aplicações onde os nós sensores são colocados de forma abundante e aleatória no ambiente, é muito difícil determinar a localização dos nós. Existem alguns métodos para se obter localização em uma RSSF. O primeiro deles são coordenadas físicas utilizando módulos de GPS (*Global Positioning System*). A desvantagem da localização via GPS é que os módulos GPS são muito caros, o que encareceria o projeto da rede. Outra forma de prover localização a uma RSSF é através de coordenadas virtuais baseadas em conectividade e proximidade dos nós da rede, onde os nós calculariam sua localização mediante as distâncias que estão dos outros nós e de um marco zero predefinido. A desvantagem de coordenadas virtuais é a complexidade da computação, sobrecarga de mensagens e memória para

armazenar a localização dos nós próximos. Mais informações sobre localização podem ser encontradas em [Baronti et al. 2007];

- **Sincronização**: A sincronização em RSSF é útil para o roteamento e para a economia de energia. Um sistema de sincronização possibilita que os nós sensores se comuniquem de forma planejada e programada. O consumo de energia é reduzido, pois quando os nós sensores estão sincronizados as colisões são reduzidas e, em consequência disso, as retransmissões também. Além disso, com sincronização os nós sensores se tornam *duty-cycled*[4] [Yick et al. 2008] economizando ainda mais energia, pois só transmitem dados no período de tempo preestabelecido;

- **Cobertura de monitoramento**: A cobertura é uma aspecto muito importante porque impacta na efetividade da rede [Yick et al. 2008]. Algumas aplicações toleram um baixo grau de cobertura, como por exemplo no monitoramento de um habitat natural de um determinado animal. Por outro lado aplicações na área militar necessitam de um alto grau de cobertura. Em RSSF para obter um alto grau de cobertura é requerido que vários nós sensores redundantes estejam na mesma região do ambiente monitorado. Contudo em redes de sensores multimídia isso não é regra, pois cada nó sensor captura uma informação diferente mesmo estando no mesmo local. Uma grande questão levantada com relação à cobertura é a sua ligação com o consumo energético. De acordo com [Yick et al. 2008], existem pesquisas focadas em estudar a cobertura voltada para a economia de energia;

- **Roteamento**: O roteamento em RSSF é um pouco diferente do roteamento em redes tradicionais. Nas redes tradicionais o roteamento é feito de forma hierárquica entre os componentes da rede, com tomadas de decisão, encaminhamento de pacotes, tabelas de roteamento e dispositivos roteadores. Segundo [Baronti et al. 2007], numa RSSF, onde os nós sensores são depositados aleatoriamente e em abundância, e a topologia da rede pode variar devido a falhas por dano ou falta de energia, a estrutura tradicional de roteamento é impraticável. Portanto, mensagens para manter as tabelas de roteamento geram sobrecarga de processamento e memória sendo inviável em RSSF. O roteamento em RSSF deve ser leve em processamento e memória, com o mínimo de mensagens de sobrecarga [Baronti et al. 2007], capaz de rotear os pacotes baseado nas informações trocadas com os nós vizinhos e resiliente a falhas e mudanças de topologia. Protocolos reativos como *Ad hoc On-Demand Distance Vector* (AODV) [Dubois-Ferriere et al. 2005] e *Dynamic Source Routing* (DSR) [Werner-Allen et al. 2005] tratam alguns desses problemas, mas com ressalvas com relação à escalabilidade da rede. Segundo [Baronti et al. 2007] existem basicamente três maneiras, baseadas em localização, de realizar o roteamento em RSSF: *Roteamento por árvore* onde cada nó memoriza seu antecessor (nó

[4]Os nós sensores são *duty-cycled* para salvar energia, onde o nó sensor periodicamente desliga o transmissor de rádio para economizar energia, ligando-o para participar da comunicação.

pai). Quando necessitar retransmitir um pacote ou transmitir um dado coletado, ele encaminhará para este. *Roteamento geográfico* ("guloso") onde, utilizando algum mecanismo de localização, é definida a distância de cada nó para com os seus vizinhos, para que, com base na localização do destino do pacote, os nós o encaminhem para o vizinho que minimiza a distância restante. E, por fim, *Roteamento hierárquico*, que divide o ambiente em questão em sub áreas e aplica o roteamento guloso nelas, transformando o nó destino no nó de hierarquia maior na sub área.

2.1.5 Padrões

Existem muitos padrões de comunicação disponíveis para RSSF de baixa potência. Para um padrão ser utilizado em redes de sensores ele tem que funcionar com baixa potência e com baixa vazão, impondo baixo consumo de energia. Os padrões definem as funções e protocolos necessários para que haja comunicação entre os nós sensores numa RSSF. A seguir são apresentados brevemente alguns padrões de comunicação para RSSF.

- **IEEE 802.15.4** [IEEE 2003a]: foi projetado para *Low-Rate Wireless Personal Area Networks* (LR-WPAN) e tem como seus principais objetivos o baixo custo, baixa complexidade de implementação e baixo consumo de energia. O IEEE 802.15.4 é bem adaptado para RSSF porque requer comunicação em faixas curtas para minimizar o consumo de energia [Yick et al. 2008]. Este padrão dá suporte a protocolos apenas das camadas física e camada MAC e permite dois tipos de topologia: estrela[5] e *peer-to-peer*[6]. Segundo [Yick et al. 2008], na camada física o padrão IEEE 802.15.4 utiliza frequências de 868/915 MHz ISM (*Industrial, Scientific and Medical*) *radio band* para bandas baixas e 2.4 GHz ISM *radio band* para bandas altas. A camada MAC utiliza *Carrier Sense Multiple Access with Collision Avoidance* (CSMA-CA) para controlar o acesso ao meio [Baronti et al. 2007].

- **ZigBee** [ZigBee 2004]: define camadas lógicas superiores de comunicação para RSSF, sendo construído tomando como base a camada física e MAC do padrão IEEE 802.15.4. Desta forma, o ZigBee opera na frequência de 2.4GHz e agrega as mesmas características e protocolos nas camadas física e camada MAC [Baronti et al. 2007]. ZigBee é bastante simples e barato, permitindo a formação de redes na topologia *mesh* conectando centenas ou milhares de dispositivos. Além disso, dispositivos ZigBee consomem pouca energia, podendo funcionar ao longo de anos com a mesma célula de bateria [Yick et al. 2008]. Por estes fatores o ZigBee é muito utilizado em RSSF.

[5]Os nós da rede se comunicam com um dispositivo central. Este dispositivo central tem a função de controlar toda a comunicação da rede.

[6]Na topologia peer-to-peer redes *ad hoc* e auto configuráveis são formadas sem a necessidade de uma entidade central.

- **WirelessHART**: é um padrão desenvolvido para RSSF com o foco em aplicações industriais. Ele é definido na camada física pelo padrão IEEE 802.15.4, porém ao contrário do ZigBee ele define sua própria camada MAC agregando aspectos importantes ao desempenho como *Channel Hopping*[7], *TDMA*[8] e *Channel Blacklisting*[9] [Song et al. 2008]. Além disso, pode-se dizer que WirelessHART é seguro e confiável, pois apesar das limitações de implementação e especificação ele possui bons esquemas de segurança com o uso de criptografia simétrica para autenticar dispositivos e trocar mensagens de forma segura. Diferentemente de padrões para RSSF como ZigBee e o próprio 802.15.4, WirelessHART forma uma rede necessariamente centralizada. Fazem parte da rede entidades como gateway, Network Manager e Security Manager. A entidade que centraliza o controle da rede é o Network Manager e a especificação da rede prevê uma parte núcleo cabeada onde estão localizados o controle de processos e o *host* de aplicação.

- **ISA100.11a** [ISA100.11a 2009]: diferentemente do WirelessHART que foi baseado no HART, o ISA100.11a foi criado baseado nas exigências dos usuários finais [Silva et al. 2013]. Este padrão é voltado para aplicações de monitoramento de controle de processos, sendo também muito aplicado na indústria. O objetivo do ISA100.11a é realizar a comunicação sem fio de forma confiável e segura estabelecendo conexões com *links* de latência de até 100ms.

- **IEEE 802.15.3** [IEEE 2003b]: é um padrão projetado para *Wireless Personal Area Networks* (WPAN) que necessitam de altas taxas de transferências, como, por exemplo, aplicações de tempo real e aplicações multimídia baseadas em vídeo. Este padrão define as camadas física e camada MAC, operando com 2.4GHz ISM *radio band*. Ele proporciona uma taxa de dados de 11Mbps a 55Mbps, usa TDMA para garantir qualidade da comunicação, realiza transferência de dados de forma síncrona e assíncrona e aborda aspectos com relação ao consumo de energia [Yick et al. 2008].

- **Bluetooth**: opera com uma frequência de 2.4GHz ISM *radio band*, suporta *time slots* (TDMA) e *channel hopping*. O Bluetooth foi projetado para o uso em *Personal Area Networks* (PAN), tendo o alcance de cerca de 10 metros. Implementa apenas a topologia em estrela e não tem nenhuma preocupação com eficiência energética [Bluetooth 1998].

- **Wibree** [Wibree 2007]: também opera com 2.4GHz ISM *radio band*, mas a taxa de transferência pode chegar a 1Mbps. A distância entre os dispositivos

[7] Mecanismo que permite a troca automática do canal de comunicação. No WirelessHART são definidos 15 canais de frequência e o *Channel Hopping* é responsável por mudar o canal de frequência quando necessário.

[8] *Time Division Multiple Access* é o mecanismo que define a fatia de tempo que um dispositivo possui para se comunicar, ou seja, é um mecanismo de controle de acesso ao meio baseado em *time slots*, onde cada dispositivo realiza a transmissão em um tempo pré-definido.

[9] Este mecanismo é utilizado para bloquear um canal de frequência que está tendo algum tipo de interferência ou mal funcionamento.

é de 5 a 10 metros. O Wibree foi projetado para funcionar em conjunto com o Bluetooth, onde dispositivos menores e mais energicamente eficientes podem ser construídos [Yick et al. 2008]. Por isso, o Wibree permite a conexão com outros dispositivos Bluetooth como teclado, relógios, celulares e dispositivos sensores.

2.2 Redes de Sensores Multimídia Sem Fio

As redes de sensores multimídia sem fio compartilham aspectos muito parecidos com as RSSF tradicionais. Entretanto, as RSMSF têm chamado a atenção da comunidade acadêmica pela riqueza de desafios teóricos e práticos [Akyildiz et al. 2007], possuindo características adicionais em relação as RSSF. Em resumo, pode-se citar a natureza de tempo real do dado multimídia, demanda por alta largura de banda, baixo atraso fim-a-fim, *jitter*[10] e taxa de perda de pacote toleráveis. Além disso, existem muitas diferenças nas restrições de recursos em RSMSF que envolvem energia, largura de banda (vazão), taxa de transferência de dados, memória, o tamanho de buffer e a capacidade de processamento [Almalkawi et al. 2010]. Em resumo, o tamanho físico do nó sensor é muito pequeno e suas capacidades são limitadas em contra ponto à natureza da aplicação multimídia que normalmente produz grandes quantidades de dados.

Para reunir qualidade de serviço (QoS, do inglês, *Quality of Service*) de forma eficiente sobre os recursos limitados da rede, uma RSMSF deve relacionar tais limitações e demandas dos dados multimídia com aspectos como cobertura e segurança. Além disso, de acordo com [Almalkawi et al. 2010], devido a alta redundância nos nós sensores visuais, RSMSF reúnem requisitos adicionais como técnicas de processamento nos nós fonte (como por exemplo, codificação e compressão de dados), QoS, técnicas de processamento nos nós intermediários, chamadas de processamento *in-network* (como por exemplo, gestão de armazenamento, fusão de dados e agregação), entre outros.

Assim, as limitações de recursos inerentes às RSSF somadas aos requisitos, características e desafios agregados pelas redes de sensores multimídia abrem muitas áreas de pesquisa para o desenvolvimento de melhores e mais adaptados protocolos, algoritmos, mecanismos, arquiteturas e dispositivos visando melhorar o uso dos recursos, aumentar o desempenho e principalmente aumentar o tempo de vida dos nós sensores e da rede como um todo.

2.2.1 Aplicações para RSMSF

As redes de sensores multimídia sem fio proporcionam um maior e melhor entendimento do mundo físico de um determinado ambiente [Costa e Guedes 2011]. As

[10] Variação do atraso

RSMSF não só melhoram as aplicações conhecidas em RSSF como controle, automação, monitoramento e rastreamento, mas também permitem o surgimento de muitas outras novas aplicações [Akyildiz et al. 2007], tais como:

- **Vigilância**: Esse tipo de aplicação visa complementar os sistemas de vigilância contra o crime ou ataques terroristas. As RSMSF podem ser utilizadas para monitorar grandes áreas, eventos públicos, propriedades particulares e fronteiras de países;
- **Observação de animais selvagens**: O registro da vida selvagem pode ser feito utilizando redes de sensores multimídia através de imagens e vídeo, onde registros do habitat, dos hábitos, locomoção e localização podem ser obtidos com mais precisão;
- **Monitoramento de atividades relevantes**: Sensores com câmeras podem monitorar e registrar atividades em áreas urbanas, como, por exemplo, acidentes de trânsitos;
- **Telemedicina**: Além do monitoramento de parâmetros médicos dos pacientes através das RSSF tradicionais, como dito anteriormente, pode-se realizar com o auxílio de sensores multimídia o monitoramento remoto mais avançado e intervenções médicas através de imagens e vídeo;
- **Assistência automatizada para idosos ou pessoas com deficiência física**: RSMSF podem auxiliar o monitoramento e o estudo do comportamento de pessoas idosas a fim de identificar as causas de doenças que os afetam, como, por exemplo, a demência. Além disso, as redes de sensores multimídia podem reagir a incidentes relacionados a saúde de pessoas idosas ou deficientes em situações de emergência, realizando uma comunicação remota com o centro de tratamento;
- **Monitoramento ambiental**: O monitoramento de ambientes como prédios, condomínios, residências, *shopping*, entre outros, pode ser feito com redes de sensores multimídia coletando vídeo e áudio para detectar invasões, eventos críticos ou outros incidentes;
- **Serviços de localização**: O conteúdo multimídia combinado com técnicas de processamento digital de sinais pode ser útil para aplicações de reconhecimento de pessoas desaparecidas ou para identificar terroristas foragidos;
- **Controle de processos industriais**: RSMSF podem ser usadas para o controle de processos industriais de tempo crítico. Combinada com aplicações de processamento de imagens, uma RSMSF pode auxiliar na extração e análise de informações e parâmetros de uma linha de produção automatizada, por exemplo. Este esquema pode ajudar a detectar problemas em máquinas, no processo ou nos produtos, realizando até o controle de qualidade de ambos;
- **Auxílio ao tráfego de carros**: Com RSMSF é possível monitorar o trânsito nas grandes cidades e rodovias a fim de informar aos condutores as melhores

rotas para se tomar no momento.

Existem outras aplicações para redes de sensores multimídia sem fio e outras tantas podem surgir mediante a necessidade. Algumas destas aplicações possuem projetos promissores conforme descritos na literatura. [Akyildiz et al. 2007] [Almalkawi et al. 2010].

2.2.2 Rede de Sensores Visuais Sem Fio

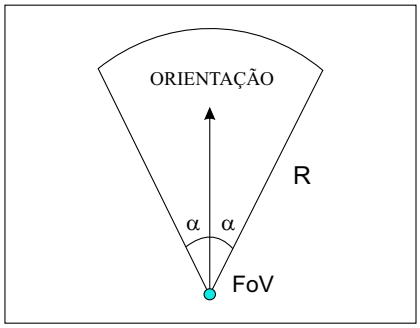
As redes de sensores multimídia sem fio que coletam apenas dados visuais, ou seja, imagens e vídeo, podem ser classificadas como Redes de Sensores Visuais Sem Fio (RSVSF). Este tipo especial de rede possui inúmeras aplicações, sendo o objeto de estudo deste trabalho. Os sensores nestas redes coletam dados de forma diferente das RSSF tradicionais [Costa e Guedes 2011]. As cameras geralmente não captam informação em 360 ° graus, ou seja, não são *ominidirecionais*[11]. Assim, as câmeras passam a ter um campo de visão (FoV, do inglês *Field of View*), como pode ser visto na Figura 2.4(a). Além disso, segundo [Costa e Guedes 2011], o ângulo de visão, a qualidade das lentes, a capacidade de aproximação e o tipo das câmeras influenciam o FoV e a forma como os dados são coletados.

Na Figura 2.4(b) e Figura 2.4(c) pode ser visto que, realizando o posicionamento correto das câmeras, pode-se obter melhores resultados na captura da informação visual desejada. O posicionamento das câmeras e a característica do FoV de cada câmera influencia diretamente na cobertura da rede, ressaltando que os nós coletam informações únicas, não sendo as mesmas que o nó vizinho.

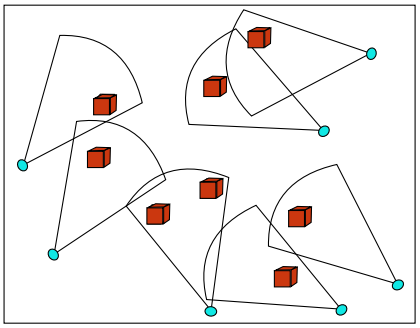
Além disso, vale ressaltar que em redes de sensores visuais a proximidade entre os nós vizinhos só tem relevância no que diz respeito à conectividade, e a capacidade de sensoriamento de um nó sensor em uma RSSF é substituída pelo campo de visão (FoV) em nós sensores em RSVSF [Costa e Guedes 2010]. Assim, o mesmo objeto pode estar no campo de visão de dois nós sensores vizinhos e as imagens capturadas serem diferentes (ver Figura 2.5(b)), ou em nós muito próximos, um objeto estar no campo de visão de apenas um deles, algo que não acontece numa RSSF tradicional. [Costa e Guedes 2010] discutem questões como *overlapping*, *occlusion* e redundância relacionados com a cobertura em RSVSF. A Figura 2.5 apresenta uma comparação entre a cobertura em redes de sensores tradicionais e em redes de sensores com câmeras.

A Figura 2.5(c) exemplifica questões como *overlapping* e *occlusion*. O primeiro é quando dois sensores tem seus campos de visão sobrepostos. Alguns sistemas toleram essas sobreposição até um determinado limite; a partir disso deve-se reposicionar os nós sensores. *Occlusion* é quando o objeto alvo a ser monitorado não consegue aparecer no campo de visão de um nó sensor devido a um obstáculo. Mais detalhes sobre *overlapping* e *occlusion* podem ser encontrados em [Costa e Guedes 2010].

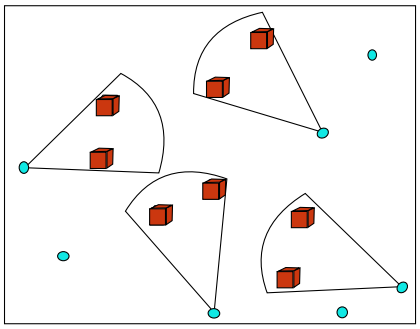
[11] Que tem as mesmas propriedades em todas as direções.



(a) Campo de Visão (FoV) de uma câmera



(b) Sete sensores cobrindo oito alvos



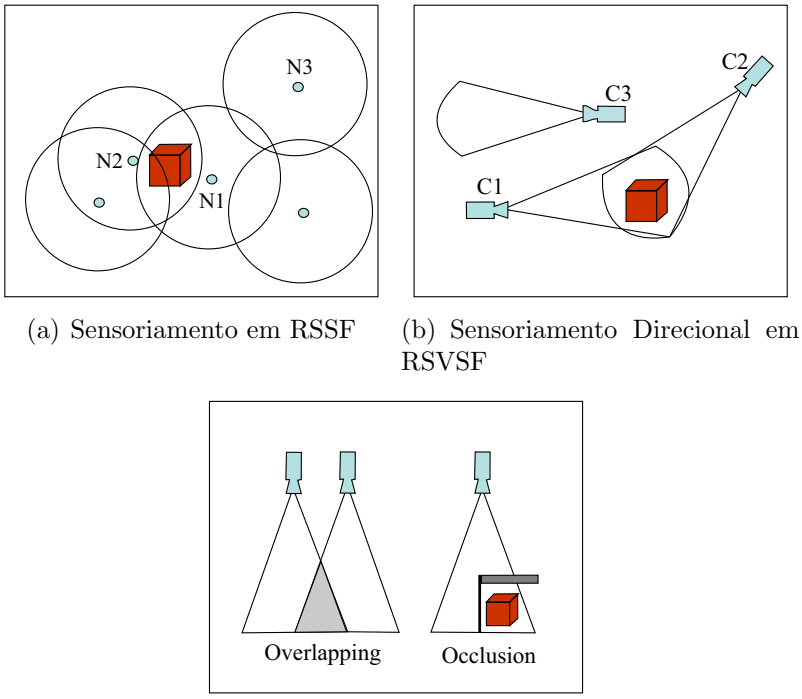
(c) Mudando a orientação das câmeras para maior eficiência na cobertura

Figura 2.4: *Directional sensing model* [Costa e Guedes 2010, p.8220].

Em resumo, assim como as RSSF, redes de sensores visuais devem ser projetas estando atentas às restrições de recursos. Contudo, em RSVSF é inevitável a utilização de técnicas de codificação de imagens para modificar como os dados são processados, reduzir a taxa de transmissão, reduzir o atraso fim-a-fim, reduzir o tamanho dos pacotes e da memória gasta. Existem técnicas de codificação de imagem disponíveis, como por exemplo *Codificação Progressiva*, *Codificação baseada em Wavelet*, e de vídeo, tais como *Codificação Preditiva*, *Codificação de Descrição Múltipla* (MDC, do inglês, *Multiple Description Coding*) e *Codificação Distribuída de Vídeo* (DVC, do inglês, *Distributed Video Coding*) [Costa e Guedes 2011] que possuem níveis de complexidade diferentes em termos de consumo de energia, tempo de processamento e consumo de recursos computacionais. Em resumo, em redes de sensores visuais é aconselhada a utilização de técnicas de codificação para melhorar o desempenho da rede, gerando dados mais compactos e melhorando a transmissão deles na rede.

2.2.3 Otimização Cross-Layer

A abordagem *cross-layer* é uma forma de propor que as camadas de rede operem de maneira cooperativa, quebrando o fluxo normal da hierarquia de camadas que atua



(a) Sensoriamento em RSSF (b) Sensoriamento Direcional em RSVSF

(c) *Overlapping* e *Occlusion*

Figura 2.5: Sensoriamento [Costa e Guedes 2010, p.8220].

nas redes de computadores tradicionais, com o objetivo de otimizar o funcionamento da rede atingindo alta eficiência, reduzindo potencialmente o atraso e economizando energia nos nós sensores [Costa e Guedes 2011]. Na Figura 2.6 é apresentado em diagramas como seria o funcionamento desta abordagem. Por exemplo, caso ocorra um congestionamento, numa abordagem tradicional, geralmente, a camada de transporte irá reduzir o tráfego para diminuir os efeitos do congestionamento. Contudo, esta ação degrada a qualidade da transmissão de mídia na rede com perdas de pacotes e aumento do atraso. Numa abordagem *cross-layer* as camadas podem cooperar para que os pacotes que possuem prioridade não tenham diminuição de tráfego ou vazão, garantindo que o dado chegue com qualidade e sem atraso ao destino, em detrimento de outros pacotes que não possuem prioridade.

Otimizações *cross-layer* são frequentemente utilizadas em combinação com técnicas de codificação. Segundo [Almalkawi et al. 2010], uma otimização *cross-layer* relacionando técnicas de codificação na camada de aplicação e protocolos de roteamento na camada de rede pode explorar melhor o roteamento *multipath*[12] e o processamento *in-network*.

Em resumo, protocolos que seguem a otimização *cross-layer* são projetados para quebrar o conceito linear das camadas de rede, visando reduzir a sobrecarga e oti-

[12]Em comunicações sem fio, é quando o sinal de rádio alcança o destino por dois ou mais caminhos.

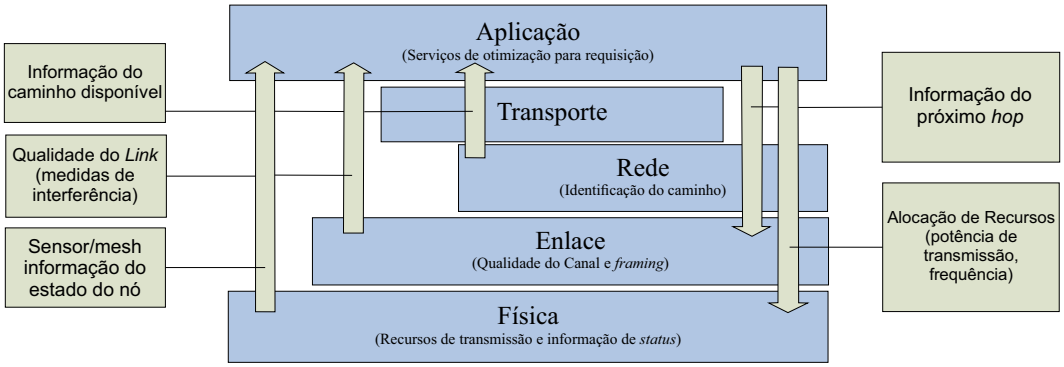


Figura 2.6: Abordagem *cross-layer* em diagrama de camadas de rede [Sheikh e Mahmoud 2012].

mizar o funcionamento dos protocolos a fim de atender os requisitos e necessidades das RSVSF. Segundo [Costa e Guedes 2011], muitos pesquisadores afirmam que a otimização *cross-layer* é a melhor opção quando se trabalha com redes de sensores visuais sem fio.

2.2.4 QoS em Redes de Sensores Visuais Sem Fio

Qualidade de Serviço (QoS) é um conceito utilizado em muitos âmbitos com significados diferentes. Contudo, no contexto de telecomunicações, é a probabilidade de uma ligação entre origem e destino ser estabelecida com sucesso. Já no âmbito das redes de computadores, QoS implica na garantia de recursos da rede para fazer com que um pacote tenha mais probabilidade de trafegar entre dois pontos da rede. Em outras palavras, QoS pode ser definido como uma diferenciação do tráfego de uma determinada rede, garantido por exemplo maior largura de banda ou níveis aceitáveis de atraso e *jitter* à um determinado tipo de tráfego, garantindo assim uma maior probabilidade destes pacotes alcançarem o destino. Sendo assim, qualidade de serviço implica também em priorização de pacotes em relação aos demais pacotes que trafegam na rede, garantindo não somente que os pacotes atinjam o destino, mas também que cheguem em tempo hábil, atendendo aos requisitos da aplicação.

Assim como em outras redes de computadores, em redes de sensores sem fio QoS pode ser muito importante para o desempenho e eficácia de várias aplicações. Em RSSF, o QoS pode ser aplicado em nível local ou global, o que diferencia a forma de priorização. Para QoS em um nível local a rede de sensores é configurada para que a priorização ocorra internamente no nó sensor fonte dos pacotes, ou seja, o nó sensor é configurado para definir qual pacote é mais relevante e deve ser priorizado ou não. Desta forma, o tráfego de um único nó pode ser priorizado para um tipo de pacote e não ser priorizado para outro tipo de pacote. Por outro lado, QoS em um nível global é quando toda a rede é configurada para que alguns nós sensores fontes tenham uma significância global e, sendo assim, tenham seu tráfego priorizado

a depender de alguns fatores como a configuração deseja, a proximidade de algum alvo ou objeto, ou após a detecção de um evento. Assim, no QoS global, todo tráfego de alguns nós sensores fonte é priorizado a depender de um evento crítico, proximidade ou configuração da própria rede.

Parâmetros de QoS podem ser associados à criptografia seletiva de imagens para prover segurança em RSVSF na transmissão de imagens ou vídeo. [Costa e Guedes 2012a] apresentam um conceito de QoS local combinado com *Discrete Wavelet Transform* (DWT), onde os pacotes gerados nos nós sensores fonte que possuem maior relevância são priorizados. Assim, utilizando criptografia seletiva de imagens associada à transformada DWT, os pacotes encriptados que contém as partes mais relevantes da imagem podem ter uma maior prioridade de tráfego sobre os outros pacotes. Pode-se notar que desta forma o QoS é aplicado em nível local, ou seja, os pacotes contendo informações relevantes da imagem coletada em um nó sensor fonte são criptografados e terão seu tráfego priorizado em relação aos outros pacotes menos relevantes da mesma imagem no mesmo sensor fonte. Fazendo isso, os pacotes com as informações mais relevantes têm mais chance de alcançar o destino, e como contém a informação vital para a reconstrução da imagem original, o QoS em nível local garante um melhor funcionamento da aplicação e da rede de sensores como um todo.

O QoS em nível global pode otimizar o tráfego de uma rede de sensores baseado em relevância de sensoriamento. [Costa e Guedes 2013] apresentam um novo índice de relevância de sensoriamento para ser explorado por mecanismos de otimização *cross-layer* objetivando eficiência energética, controle de fluxo, confiabilidade e segurança para RSVSF. Neste modelo, o QoS global é baseado na relevância de sensoriamento de cada nó sensor que é calculado de forma centralizada de acordo com os requisitos da aplicação. Pode-se classificar esta abordagem como sendo uma abordagem de priorização baseada em *Quality of Experience* (QoE), que expressa a satisfação do usuário ou da aplicação[13] em relação ao serviço. Neste caso, o QoS global é um QoE pois a medida que a rede está operando, as necessidades da aplicação ditam o ritmo de quais tráfegos devem ser priorizados, ou seja, a experiência é quem determina o cálculo da relevância do sensoriamento.

Outros trabalhos semelhantes propõem diferentes otimizações baseadas em relevâncias de sensoriamento e QoS global para reduzir o consumo de energia, tais como adaptar as frequências de transmissão dos nós sensores fonte [Costa e Guedes 2012b], a proposta de algoritmos de roteamento para transmissões de tempo crítico [Costa et al. 2012a] e realizar retransmissão de pacotes corrompidos de forma otimizada baseado em relevâncias dos nós sensores fonte [Costa et al. 2012b].

Por outro lado, como mencionado anteriormente, o QoS em nível global pode ser aplicado para priorizar o tráfego de dados coletados por sensores próximos a eventos críticos. Algumas aplicações necessitam que câmeras monitorem ambientes ou grupo de alvos, mas que algum evento seja observado para funcionar como um gatilho de

[13]Em RSSF, o usuário para esta definição é exatamente a aplicação para qual a rede foi projetada.

nível crítico para o monitoramento visual. Tais aplicações de vigilância crítica, como para segurança pública, automação industrial, monitoramento de trânsito ou de resposta a desastres naturais podem necessitar de que eventos como uma explosão, uma erupção vulcânica, um incêndio ou um acidente sejam monitorados para que quando ocorrerem, o monitoramento visual seja considerado com alta relevância podendo auxiliar na identificação de possíveis responsáveis e contra medidas. [Costa et al. 2013] apresentam uma proposta de novos níveis de relevância que podem refletir em uma alta qualidade das imagens ou vídeo transmitidos ou mesmo numa maior prioridade durante a transmissão destas imagens na rede que, de forma dinâmica, são atribuídos aos nós sensores visuais que monitoram tal evento crítico. Assim, neste caso, o QoS aplicado é a nível global, mas com o agravante de que está associado a um elemento crítico aleatório. A proposta apresentada por [Costa e Guedes 2013] fornece um certo nível de diferenciação de tráfego dos nós sensores de acordo com suas relevâncias, mas não é tão eficiente para aplicações de vigilância crítica, por ter as relevâncias calculadas de maneira centralizada o que pode ocasionar em um maior atraso no processo de atribuição das relevâncias. Além disso, a identificação das relevâncias baseadas em decisões humanas, em computação de cobertura ou processamento de padrões visuais podem ser muito lentas quando uma rápida resposta a um evento crítico é desejada.

Portanto, frequentemente têm-se a necessidade de que situações críticas sejam monitoradas com uma alta qualidade de imagem e que esta informação seja transmitida com um atraso fim-a-fim muito baixo. Um exemplo recente foi a Maratona de Boston em 2013, onde um ataque terrorista através de uma bomba próximo à linha de chegada ocorreu. Como mencionado por [Costa et al. 2013], uma rede com câmeras poderia estar monitorando todo o trajeto da prova e ligados a ela nós sensores escalares estariam monitorando os eventos críticos através de grandezas escalares como pressão, calor, intensidade sonora, abalos sísmicos, fumaça, umidade, entre outros. Assim, quando a bomba explodisse o evento seria detectado e as câmeras próximas ao local da explosão seriam dinamicamente configuradas para capturarem em uma qualidade mais alta de imagem e vídeo e teriam seu tráfego priorizado em relação aos outros nós sensores que não estivessem próximos ao local do evento.

Em resumo, QoS global pode ter a abordagem da proximidade de alvos, pode estar relacionado a eventos críticos ou simplesmente pela configuração, enquanto o QoS em nível local está relacionado com a diferenciação de pacotes em um mesmo nó sensor. Além disso, tanto QoS local quanto QoS global também podem ser relacionados com segurança onde o tráfego priorizado pode ter garantias de sigilo através de mecanismos de segurança, contudo, não é a regra.

2.3 Aspectos de Segurança em RSSF

Prover segurança em rede de sensores sem fio, sendo elas multimídia ou não, é sempre uma tarefa desafiadora. Devido à natureza desestruturada da rede, ao meio

sem fio ser mais propenso a falhas e ataques, aos nós sensores muitas vezes estarem em ambientes remotos, hostis, de difícil acesso ou desassistidos, as RSSF são muito vulneráveis a vários tipos de ataques. Segundo [Sen 2009], os mecanismos de segurança tradicionais, como criptografia, não são viáveis para rede de sensores devido à alta sobrecarga de processamento e comunicação. Os pesquisadores em segurança para RSSF têm proposto vários esquemas de segurança que são otimizados para as restrições deste tipo de rede.

Segurança em RSSF visa proteger o dado coletado contra o acesso não autorizado e contra a adulteração [Guerrero-Zapata et al. 2010]. Além disso, os serviços de segurança visam garantir, entre outros fatores, a disponibilidade da rede de sensores, garantindo os serviços e permitindo que os nós sensores se comuniquem mesmo quando existem atividades maliciosas.

Em RSSF, um adversário pode comprometer um nó sensor, alterar a integridade dos dados, escutar mensagens, analisar mensagens, injetar falsas mensagens e gastar os recursos da rede [Yick et al. 2008]. Além disso, as ameaças de segurança em RSSF podem ser de dois tipos: ameças externas (*outsider attacks*), onde o oponente não possui conhecimento das chaves de segurança, ou ameaças internas (*insider attacks*), onde o oponente possui conhecimento das chaves de segurança [Kundur et al. 2008].

Os requisitos de segurança em RSSF são, em sua maioria, os mesmos que em todas as redes que pretendem ser seguras. Entretanto, devido às restrições já mencionadas, estes requisitos devem ser observados por outra ótica. Os quatro pilares da segurança que devem ser bem observados são: confidencialidade, autenticidade, integridade e disponibilidade. Outros requisitos, não menos importantes, devem ser sempre bem observados nos projetos de segurança para RSSF, como *data Freshness*, *self-organization*, localização segura e sincronização de tempo. A seguir são detalhados tais requisitos de segurança para RSSF:

- **Confidencialidade:** É o mesmo que privacidade. Os mecanismos de segurança devem garantir que nenhuma mensagem da rede seja entendida por quem não tem autorização [Sen 2009]. Também os nós sensores não podem permitir que seus dados coletados sejam acessados por seus vizinhos, a menos que eles tenham autorização;

- **Integridade:** É quando um sistema não pode ser modificado por uma entidade indevida. Perda de dados ou danos podem ocorrer sem a necessidade de uma ação maliciosa devido à natureza do ambiente e da comunicação sem fio [Mahmoud et al. 2013]. Ainda assim, uma informação em trânsito não deve poder ser alterada por um adversário. Frequentemente, integridade estará relacionada à garantia de que a informação não será alterada durante o trânsito pela rede devido a uma ação maliciosa;

- **Autenticidade:** Em algumas aplicações os dados coletados ajudam em tomadas de decisão. A autenticidade é quando um receptor pode garantir que o dado recebido que será usado em qualquer decisão é da correta fonte

[Mahmoud et al. 2013]. Um adversário pode inserir um nó falso, que se passa por um nó da rede, não apenas para modificar pacotes de outros nós, mas também para enviar pacotes falsos criados por ele;

- **Disponibilidade:** É a garantia de que os serviços da RSSF estarão sempre disponíveis mesmo quando a rede sofre problemas como ataques ou interferências [Sen 2009];
- ***Data Freshness:*** Significa a "idade" da informação. Em outras palavras, este requisito deve garantir que o dado enviado é recente, impedindo que um atacante replique na rede dados antigos. Para garantir que nenhuma mensagem velha é replicada na rede, um carimbo de tempo (*Time Stamp*) pode ser adicionado ao pacote [Mahmoud et al. 2013];
- ***Self-organization:*** Numa RSSF é requerido que os nós se auto organizem e se auto consertem. Um vez que centenas ou milhares de nós sensores são densamente espalhados no ambiente, a rede, através da camada MAC, deve estabilizar os links de comunicação a fim de formar uma estrutura básica para fornecer à RSSF a capacidade de auto organização [Yick et al. 2008]. Como os nós sensores são depositados, muitas vezes, em ambientes de difícil acesso e de forma aleatória, a capacidade de se auto organizar e se auto consertar é de suma importância para o funcionamento da rede, pois os nós sensores podem sofrer danos e a comunicação não pode ser interrompida. Além disso, como os nós sensores são alimentados por uma fonte de energia limitada, eles podem falhar, sendo esta capacidade de se auto organizar fundamental para a reestruturação da rede. Entretanto, essa característica dificulta muito os mecanismos de segurança devido à natureza dinâmica.
- **Localização Segura:** Algumas aplicações requerem que seja informada a localização precisa de um determinado dado coletado. Assim, um adversário pode facilmente manipular ou fornecer uma falsa informação de localização dos nós sensores. Logo esta informação deve, em alguns casos, ser tratada de forma segura.
- **Sincronização de Tempo:** Muitas aplicações em RSSF são sincronizadas. Os mecanismos de segurança devem também ser sincronizados e proteger o esquema de sincronização dos nós sensores.
- **Resiliência a Erros:** É a capacidade de se recuperar de um erro, podendo ser este ocasionado por um ataque ou não. Segundo [Kundur et al. 2008] a maioria das abordagens para prover resiliência a erros utiliza processamento de sinal resiliente em que redundância de dados é explorada para superar falsos conjuntos de dados inseridos por um nó comprometido [Wagner 2004].

Para garantir integridade e confidencialidade aos dados coletados numa RSSF é comum o uso de algoritmos de criptografia. Por isso, numa RSSF, aspectos como distribuição e gerenciamento de chaves de segurança é fundamental para um bom

nível de segurança da rede. Basicamente existem dois tipos de algoritmos de criptografia: os simétricos e os assimétricos. Na criptografia simétrica existe apenas uma mesma chave para encriptar e desencriptar os dados. A criptografia assimétrica funciona no esquema de chave pública e chave privada, onde uma chave pública encripta os dados e a chave privada desencripta-os, necessitando sempre desse par de chaves para realizar a criptografia [Simmons 1979]. A tendência dos esquemas de segurança para RSMSF são que eles devem ser mais leves e conscientes energeticamente que os esquemas para RSSF tradicionais. Segundo [Almalkawi et al. 2010], para prover segurança em RSMSF, a criptografia assimétrica é uma melhor escolha em relação à criptografia simétrica.

2.3.1 Análise de Ameaças

Como dito anteriormente, as RSSF são vulneráveis por vários motivos. [Sen 2009] separa as ameças e ataques às redes de sensores em três vertentes: (i) ataques aos segredos da rede, passando pela autenticação e confidencialidade, onde o atacante tenta descobrir como a rede funciona e o que trafega sobre ela; (ii) ataques contra a disponibilidade, onde o ataque foca somente em tornar a rede indisponível para realizar sua função e prover os serviços para o qual ela foi projetada e (iii) ataques contra a integridade, que é quando o ataque visa atrapalhar o funcionamento da rede inserindo dados falsos ou adulterando dados na rede. Esses três grupos de ameaças são materializados em diferentes tipos de ataques, como descrito a seguir.

- **Interference:** Não é bem um ataque propriamente dito, porém é uma ameaça ao funcionamento normal da rede wireless podendo interromper o sinal de rádio causando indisponibilidade. Interferência é uma ameaça não intencional.
- **Jamming:** É uma interferência intencional, ou seja, causada por um atacante a uma rede sem fio. O *jamming* é um tipo de ataque de *Denial of Service* (DoS) realizado na camada física [Sarma e Kar 2008]. Um adversário causa a interrupção ou o mal funcionamento do sinal de rádio da rede introduzindo um ruído ou sinal na mesma frequência e modulação usada pela rede sem fio. Isso pode afetar parte da rede ou a rede inteira. Mesmo com um sinal de ruído fraco um atacante pode desconectar uma rede inteira, bastando espalhar as fontes de *jamming* por toda a rede [Sen 2009]. Além disso, um *jamming* intermitente pode atrapalhar a rede corrompendo os pacotes, o que pode ser danoso tanto para redes sensíveis ao tempo, quanto para RSSF tradicionais, onde muitas retransmissões podem ser danosas.
- **Tampering:** É um ataque onde o adversário modifica dados secretos, como chaves de segurança, ou dados coletados que estão em trânsito. Em uma RSSF, os nós não são projetados para ser *tampering-resistant* porque devem ser baratos e simples. Como o nó sensor é muito simples e de baixo custo, qualquer adversário pode projetar um nó sensor semelhante para acessar a rede. Em resumo, em um ataque de tampering, o adversário geralmente pode modificar

uma informação a fim de causar ou um mal funcionamento da rede ou a não detecção de um evento ou ainda apagar informações críticas [Chang et al. 2004]. Além disso, os nós em RSSF geralmente são implantados em ambientes desassistidos, sendo monitorados apenas remotamente, tornando a rede suscetível a ataques físicos, onde atacantes podem modificar o circuito, trocar as unidades de sensoriamento ou alterar o código do programa [Sen 2009].

- **Collision:** A colisão ocorre quando dois ou mais nós sensores tentam acessar o meio ao mesmo tempo, podendo ser intencional ou não. Um atacante pode induzir uma colisão em uma pequena porção da rede ou na rede toda [Sarma e Kar 2008]. Este ataque pode inserir erros em pacotes, devido a colisão com outros pacotes na rede, e gerar muitas retransmissões, o que consome os recursos da rede pelo gasto desnecessário de energia nos nós sensores.

- **Exhaustion:** Esta ameça ocorre quando um dispositivo falso realiza inúmeras solicitações tentando se comunicar com os nós sensores da rede, o que provoca respostas. Isto pode esgotar os recursos de energia dos nós sensores.

- **Flooding:** Neste ataque os adversários enviam vários pedidos de estabelecimento de conexão, fazendo com que os sensores aloquem memória para manter estas conexões. Protocolos que mantém informação de estado da comunicação tanto na fonte quanto no destino são vulneráveis a *flooding attacks*. Uma forma de evitar ataques deste tipo é limitar o número de conexões de um nó sensor.

- **De-synchronization:** A comunicação entre dois nós sensores pode ser interrompida pela introdução de uma falsa informação de tempo da rede (*timing information*), levando os dispositivos a gastar seus recursos na sincronização de tempo desnecessariamente [Raza et al. 2009]. Este problema é resolvido com o uso de um forte mecanismo de autenticação. A rede pode ser projetada para autenticar todos os pacotes trocados, inclusive os campos de controle no cabeçalho do pacote da camada de rede, assumindo que a autenticação seja robusta e que o atacante não possa quebrá-la. Os nós sensores podem detectar os pacotes maliciosos e descartá-los [Sarma e Kar 2008].

- **Traffic Analysis:** A natureza do meio sem fio é favorável a este tipo de ataque, pois o componente da rede não está ligado fisicamente a rede, como acontece em redes cabeadas. Numa RSSF sem o uso de criptografia será possível um atacante analisar os pacotes de rede e descobrir como a rede funciona, a localização de dispositivos, entre outros segredos. Estas informações podem ser úteis para auxiliar outros ataques mais perigosos ao funcionamento da rede. A solução neste caso é a utilização de criptografia para garantir confidencialidade aos dados.

- **Sybil:** Homônimo ao popular livro da década de setenta, *Sybil*, sobre o distúrbio de múltiplas personalidades. Num *Sybil Attack* um adversário pode assumir múltiplas identidades na rede introduzindo um ou mais nós sensores,

ou um software malicioso, com o objetivo de confundir os esquemas de roteamento [Kundur et al. 2008]. As RSSF, pela forma de comunicação empregada ser *ad hoc* e descentralizada, são mais propensas a este tipo de ataque.

- **Sinkhole:** Neste ataque um adversário compromete um nó e faz com ele seja mais atrativo para seus vizinhos forjando as informações de roteamento [Sen 2009]. O resultado é que os nós irão escolher este nó comprometido como próximo destino (*next-hop node*) para rotear seus dados através dele. Este tipo de ataque é geralmente utilizado para auxiliar outros ataques.

- **Wormhole:** é um poderoso tipo de ataque do tipo *Sinkhole* envolvendo um conluio de mais de um nó [Kundur et al. 2008]. Neste tipo de ataque, um adversário cria um túnel de mensagens de uma parte da rede para outra. O atacante utiliza nós maliciosos ou comprometidos para criar links de baixa latência com a finalidade de atrair o tráfego, se aproveitando da característica *multi-hop* dos mecanismos de roteamento empregados em redes de sensores sem fio, bem como a diversidade de caminhos. Assim, todo o tráfego é atraído por estes links de baixa latência até o *Wormhole*, não chegando ao seu destino, o *Sink Node*. Uma das soluções recomendadas para prevenir *wormhole attacks* é *packet leashes* [Hu et al. 2006][Hu et al. 2003]. *Leash* é uma informação adicionada ao pacote com o objetivo de limitar a distância de transmissão máxima permitida. Existem dois tipos de *packet leashes*: geográfico e temporal. A abordagem geográfica garante que o destinatário do pacote está dentro de uma certa distância da fonte do pacote. Na abordagem temporal, é definido para o pacote um tempo de vida relacionado com a distância que o pacote tem que percorrer. Isto é possível uma vez que o pacote pode viajar no máximo na velocidade da luz [Hu et al. 2003]. Desta forma, é possível o nó fonte identificar se o pacote foi atraído por *wormhole attacks*.

- **Eavesdropping:** Este ataque consiste na escuta de mensagens privadas. O atacante compromete a segurança fazendo com que um nó malicioso consiga receber os pacotes e retransmiti-los à rede. Assim, este ataque muitas vezes não é detectado e afeta a confidencialidade da comunicação. O uso de criptografia evita que as mensagens sejam escutadas livremente pelo atacante.

- **Selective Forwarding Attack:** Na operação normal de uma RSSF, nós sensores intermediários sempre encaminham os pacotes recebidos para o próximo *hop* [Chang et al. 2004], para que então eles atinjam o preterido destino. Entretanto, num *selective forwarding attack*, um nó malicioso ou comprometido pode seletivamente encaminhar alguns pacotes e descartar outros [Sen 2009]. Naturalmente nós vizinhos podem entender que este nó, neste caminho, está falhando e procurar outro caminho.

- **Neglect and Greed:** Literalmente, este ataque pode ser descrito como negligência e ganância. Ocorre quando um nó malicioso negligencia rotear alguns pacotes ou todos pacotes que passam por ele. Este nó pode apenas participar de protocolos de baixo nível como manutenção de rotas, mas ele descarta as

mensagens de forma aleatória e arbitrária, podendo dar indevida prioridade para seus próprios pacotes [Kundur et al. 2008].

- **Homing Attack:** É baseado em análise de tráfego. Atacantes farejam (*sniff*[14]) os cabeçalhos dos pacotes a fim de descobrir de onde os pacotes vieram e pra onde os pacotes vão [Kundur et al. 2008]. O objetivo é conhecer a topologia da rede observando os pacotes roteados para a partir desta informação lançar e auxiliar outros ataques prejudiciais à rede.
- **Misdirection Attacks:** Tem o efeito similar a ataques como *Sinkhole* ou *Wormhole* em que o atacante encaminha as mensagens para caminhos mais difíceis a fim de inundar o *link* e prejudicar a entrega de pacotes [Kundur et al. 2008]. Como o próprio nome diz, este é um ataques que tem como o princípio central a desorientação para alcançar a negação de serviço (DoS). Aqui, o atacante induz o pacote para um destino diferente, em vez de o destino atual. Desta forma, atraso fim-a-fim do sistema de rede aumentará aleatoriamente, algumas vezes tornando-se infinito, o que resulta na degradação do desempenho geral da rede [Joseph e Vijayan 2014]. Portanto, *misdirection attacks*, devido à presença de nós egoístas, levará à diminuição da eficiência na entrega de pacotes do sistema de rede, pois, alguns nós se comportam de maneira inesperada e não encaminham os pacotes de mensagens e para o nó de destino correto. Uma maneira de conseguir isso, é quando o atacante forja respostas aos pedidos de descoberta de rota, incluindo ID do nó corrompido nas rotas falsificados. Segundo [Kundur et al. 2008], OPSENET *guards* atua contra este ataque e outros ataques de falsificação de rota (*spoofing*), exigindo que todos os nós anexem seu ID juntamente com seus endereços MAC, criptografado com as chaves individuais, utilizando-se de uma noção de frescura das informações (*freshness*).

A Tabela 2.1 sumariza as ameças mais comuns que uma RSSF pode sofrer ao longo do seu tempo de vida.

2.3.2 Criptografia em RSSF

Criptografia é o recurso de segurança que objetiva manter as mensagens seguras, sendo comumente empregada para garantir integridade, confidencialidade e autenticidade. A criptografia é usada como base para muitos mecanismos de segurança, onde os dados encriptados garantem confidencialidade uma vez que somente podem ser acessados pelos destinatários adequados. Além disso, garante também integridade já que as mensagens não podem ser acessadas por agentes externos. Por fim, é garantido também um certo nível de autenticidade com a distribuição e gerenciamento das chaves usadas na criptografia dos dados aos seus devidos proprietários,

[14] Em redes de computadores *sniffer* é um software ou hardware com capacidade de interceptar e registrar o tráfego de dados da rede. Em RSSF ocorre o mesmo princípio só que feito por um nó sensor malicioso ou comprometido.

Tabela 2.1: Resumo: Ameaças vs Aspectos de segurança afetados.

Ameaça	**Aspecto afetado**
Denial of Service (DoS)	Disponibilidade
Jamming	Disponibilidade
Tampering	Integridade e Localização
Collision	Disponibilidade
Exhaustion	Disponibilidade
Flooding	Disponibilidade
De-synchronization	Disponibilidade e Sincronização do Tempo
Traffic Analysis	Confidencialidade
Sybil Attack	Autenticidade e *Data Freshness*
Sinkhole	Disponibilidade
Wormhole	Disponibilidade
Eavesdropping	Autenticidade e Confidencialidade
Selective Forwarding Attack	Autenticidade e Confidencialidade
Neglect and Greed	Disponibilidade e Autenticidade
Homing attack	Confidencialidade
Misdirection attack	Autenticidade e Confidencialidade

tanto na fonte quanto no destino da comunicação. O processo de estudar os algoritmos e sua quebra é chamado de criptoanálise. Numa comunicação de rede, a mensagem original é chamada de *plaintext* e a mensagem cifrada é chamada de *ciphertext* [Cheng e Li 2000].

A escolha do método de criptografia apropriado é vital para prover a segurança adequada a qualquer tipo de rede. Contudo, alguns aspectos devem ser atentados no momento de optar por um método ou outro de criptografia. Os métodos de criptografia quando usados em RSSF devem estar de acordo com as restrições dos nós sensores, já mencionadas anteriormente, e devem ser avaliados pelo tamanho do código, tamanho do dado após a encriptação, tempo de processamento e consumo de energia [Sen 2009]. A seguir são descritos os dois tipos de criptografia para RSSF mais comumente utilizados.

Criptografia Simétrica

O mecanismo de criptografia simétrica utiliza uma única chave compartilhada para ambas funções de criptografar e descriptografar o dado. Contudo, o maior desafio é como distribuir de forma segura a chave compartilhada entre os envolvidos na comunicação, não sendo uma tarefa trivial porque nem sempre é possível pré-implantar ou pré-distribuir as chaves nos nós sensores [Sen 2009].

O gerenciamento de chave é o núcleo do mecanismo de segurança baseado em criptografia de dados. O objetivo principal do gerenciamento de chave é estabelecer a

troca de chaves entre os nós sensores e entre os nós e a estação base de forma segura e confiável [Sen 2009]. Estes esquemas devem suportar a adição e a revogação de nós da rede e devem ser extremamente leves, devido às restrições de memória, processamento e energia das RSSF. A maioria dos protocolos existentes para RSSF para efetuar o gerenciamento de chave são baseados na criptografia simétrica, isso devido à criptografia simétrica possuir apenas uma chave para encriptar e decriptar os dados. Alguns algoritmos de criptografia simétrica descritos na literatura são:

- ***Advanced Encryption Standard* (AES):** é um dos mais populares algoritmos de criptografia simétrica [Rijmen e Daemen 2001]. Também conhecido como Rijndael, é um esquema de criptografia por bloco utilizado em larga escala internacionalmente. Em RSSF, este é o principal mecanismo de criptografia adotado pelo padrão WirelessHART [Raza et al. 2009]. [Mahmoud et al. 2013] propõe um esquema de segurança energicamente eficiente para RSSF que utiliza o algoritmo AES como principal algoritmo de criptografia;
- ***Data Encryption Standard* (DES):** utiliza um chave pequena de 56 bits e demonstra falhas, por isso foi substituído pelo AES [Coppersmith 1994]. Apesar das falhas e suspeitas de mal funcionamento, o DES foi estudado mais a fundo na academia e motivou os sistemas modernos de criptoanálise;
- **RC4:** é um algoritmo de criptografia de fluxo. É utilizado em protocolos bem conhecidos, como *Secure Socket Layers* (SSL), que tem a função de proteger o tráfego Internet, e WEP, que é utilizado para prover autenticação de acesso em redes sem fio [Fluhrer et al. 2001];
- ***International Data Encryption Algorithm* (IDEA):** este é um algoritmo de cifra de bloco criado para ser o substituto do DES [Lai e Massey 1991]. Ele usa a confusão e a difusão para produzir o texto cifrado, com chaves de 128 bits e com o uso de portas XOR, adição e multiplicação de 16 bits (como as operações são feitas com blocos de 16 bits, o algoritmo é eficiente em microprocessadores de 16 bits).

Todos estes algoritmos podem ser utilizados em RSSF, cada um com seus prós e contras. Além deles, existem os algoritmos de criptografia chamados de *Hash Functions*, tais como *Message-Digest Algorithm 5* (MD5) e *Secure Hash Algorithm* (SHA-1), só que eles além de possuírem maior sobrecarga que os algoritmos citados acima, não permitem a descriptografia dos dados.

Alguns autores, como apresentado por [Guerrero-Zapata et al. 2010], defendem o uso de criptografia simétrica em RSSF ao invés da criptografia assimétrica devido à grande sobrecarga de computação que os algoritmos assimétricos possuem, tendo como principal argumento a limitação de recursos das RSSF. Este argumento é baseado no fato de que algumas RSSF são tão restritas em recursos nos nós sensores que o gasto com computação é bastante limitante para o uso de criptografia assimétrica. Entretanto, recentes estudos mostram que é viável a utilização de criptografia

assimétrica em RSSF [Sen 2009, Guerrero-Zapata et al. 2010].

Criptografia Assimétrica

Criptografia assimétrica, também conhecida como criptografia de chave pública (em inglês, *public key cryptography* ou algoritmos PKC), utiliza um par de chaves para realizar a encriptação dos dados. Uma chave pública que é conhecida por todos os nós da rede é utilizada para encriptar os dados e outra chave privada somente conhecida pelo nó destino é utilizada para descriptografar os dados. Geralmente os algoritmos de criptografia assimétrica tradicionais possuem alta sobrecarga de computação e demandam mais tempo de processamento. Partindo deste pressuposto, segundo [Gaubatz et al. 2005], de início, a maioria das publicações parecem afirmar que a criptografia de chave pública não é viável para RSSF. Contudo, ainda segundo [Gaubatz et al. 2005], com o passar dos anos, análises como a proposta por [Lenstra e Verheul 2001], [Malan et al. 2004b] e [Wander et al. 2005] foram comprovando o contrário, onde a criptoanálise sobre custo computacional e tamanhos de chave apontam a viabilidade dos algoritmos assimétricos para RSSF.

A seguir são apresentados brevemente três algoritmos de chave pública largamente utilizados em redes de computadores e viáveis para o uso em RSSF:

- **RSA:** criado pela empresa *RSA Data Security* e, até 2008 era a implementação de sistemas de chaves assimétricas mais bem sucedida [Rivest et al. 1978]. Baseado em teorias clássicas dos números, foi também o primeiro a prover criptografia e assinatura digital, se tornando uma das grandes inovações em criptografia de chave pública;
- **Rabin's Scheme:** introduzido em 1979 [Rabin 1979], é um algoritmo baseado em fatorização de problema, sendo por isso similar ao RSA. O processo de codificação é mais rápido que o processo de decodificação se comparado com RSA nos mesmos parâmetros [Gaubatz et al. 2005];
- ***Elliptic Curve Cryptography* (ECC)**: é um termo coletivo para múltiplos algoritmos de troca de chave e protocolos de acordo [Koblitz 1987, Miller 1986], por exemplo, ECDH, ECDSA e ECMV [Gaubatz et al. 2005]. ECC oferece uma segurança equivalente ao RSA só que com chaves muito menores, se tornando mais atrativo para RSSF, pois chaves menores geram menos uso de memória, economia de largura de banda e menos sobrecarga de computação [Raju e Akbani 2003]. Por exemplo, segundo [Hankerson et al. 2004] o algoritmo RSA com 1024 bits provê a mesma segurança que o ECC com 160 bits.

Uma análise energética é proposta por [Wander et al. 2005], comparando RSA com ECC para o uso em RSSF, como apresentada na Tabela 2.2.

Tabela 2.2: Análise do custo energético de assinatura e troca de chave dos algoritmos RSA e ECC [mJ] [Wander et al. 2005, p.3].

Algoritmo	Assinatura		Troca de Chave	
-	Assinatura	Verificação	Cliente	Servidor
RSA-1024	304	11.9	15.4	304
ECC-160	22.82	45.09	22.3	22.3
RSA-2048	2302.7	53.7	57.2	2302.7
ECC-224	61.54	121.98	60.4	60.4

2.4 Protegendo Imagens em Redes de Sensores

Nós sensores com câmeras embutidas podem recuperar informações muito valiosas do ambiente monitorado. Muitas aplicações para redes de sensores visuais sem fio podem requerer níveis de segurança aceitáveis para a proteção e manutenção do sigilo das imagens capturadas pelos nós da rede. Entretanto, como os mecanismos de segurança tradicionais não são adaptáveis para este tipo de rede, prover segurança em RSVSF demanda a investigação de novos conceitos e paradigmas mais apropriados a este tipo de rede. Muitos trabalhos tem como característica central explorar a estrutura da imagem codificada. A seguir são apresentados alguns mecanismos e paradigmas para proteger imagens em RSVSF, que fazem parte do objeto de investigação deste trabalho.

2.4.1 Criptografia Seletiva de Imagens

Qualquer comunicação, principalmente sobre *links* sem fio, pode ser interceptada por nós maliciosos e por isso necessita de segurança. Como visto anteriormente, o processo de criptografar e descriptografar dados é muito custoso em tempo e poder computacional, muitas vezes não sendo possível aplicar tais métodos de segurança para algumas aplicações, como por exemplo, aplicações de tempo real, aplicações multimídia e também aplicações com restrições de recursos tais como as aplicações para redes de sensores sem fio, particularmente as RSVSF. Para redes de sensores sem fio, eficiência energética lidera a maior parte dos esforços de otimização. Todavia, existem métodos que combinam compressão (ou codificação) e encriptação para reduzir o tempo de processamento, mas eles não são tão melhores pois se tornam inseguros ou computacionalmente mais intensos. Ambas abordagens, notadamente, somente criptografia ou a combinação de compressão e criptografia resultam em um *trade-off*[15] entre segurança e complexidade computacional.

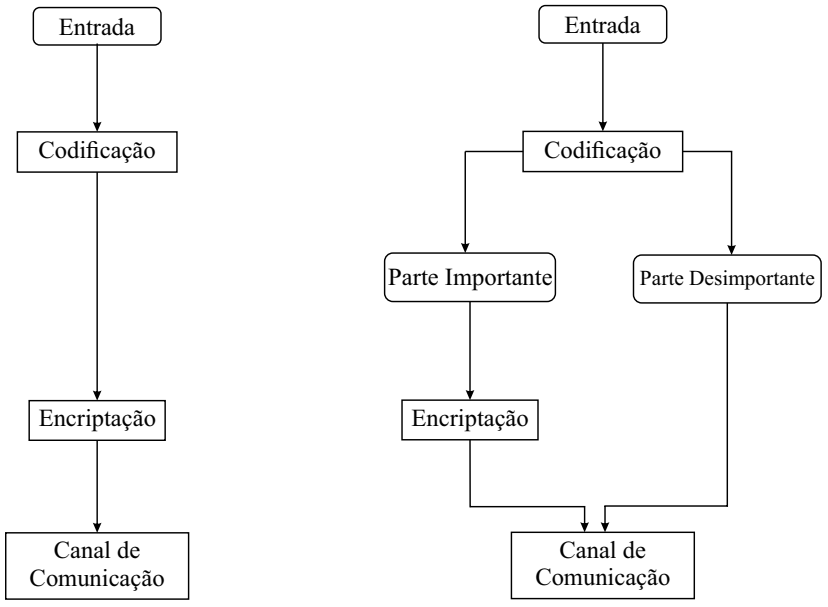
Em um processo de encriptação de dados toda a informação do dado é encriptada. Entretanto, isso não é obrigatório quando se trata de conteúdo mul-

[15]Conflito de escolhas. A escolha de garantir um aspecto é sempre em detrimento de outro e vice-versa.

timídia. *Criptografia Seletiva* ou *Parcial* é um método recente que tem sido ponto chave de vários trabalhos de criptografia de dados multimídia tais como [Sadourny e Conan 2003, Pfarrhofer e Uhl 2005, Liu 2006], que sugere que apenas parte do conteúdo seja encriptado e não o dado por completo. O objetivo é impor sigilo numa imagem (ou vídeo) reduzindo a complexidade computacional [Grangetto et al. 2006]. Em resumo, esse princípio explora as características do algoritmo de codificação da mídia para fornecer sigilo enquanto reduz a complexidade computacional. Em outras palavras, criptografia seletiva propõe que seja usado algum mecanismo ou algoritmo de criptografia de dados em apenas parte da mídia codificada. Assim, por exemplo, em uma imagem ou em um vídeo, a compressão é efetuada sobre a estrutura dos dados para que a partir desta compressão a estrutura seja explorada, onde apenas partes significantes são encriptadas criando-se assim sistemas de criptografia bem mais eficientes que os tradicionais [Podesser et al. 2002].

Na criptografia seletiva o objetivo é codificar apenas um conjunto de blocos de uma imagem, por exemplo. Alguns algoritmos de compressão são baseados em decomposição de dados e permitem que partes do dado comprimido tenham uma relevância maior, pois nestas partes são concentradas uma quantidade mais significante da informação sobre o dado original [Cheng e Li 2000].

Na Figura 2.7 é apresentado um diagrama comparando a criptografia tradicional com a criptografia seletiva.



(a) Criptografia Tradicional (b) Criptografia Seletiva

Figura 2.7: Comparação entre princípios para realizar criptografia em um dado de entrada [Cheng e Li 2000, p.2440].

Dois princípios de compressão de imagens que decompõem dados que são bem adaptados à criptografia seletiva são: *Compressão Quadtree* e *Compressão Wavelet*. Os

algoritmos baseados em *Quadtree* são mais simples e superam o JPEG em performance em baixas taxas de bits, enquanto que os baseados em *Wavelet* tem boa performance de compressão. Ambos são adaptados para criptografia seletiva e o tamanho da parte relevante e a complexidade computacional de cada esquema foi analisado por [Cheng e Li 2000], sendo que o tamanho da parte relevante é diretamente proporcional ao tempo requerido no processo de encriptação e desencriptação.

Nas sessões a seguir são apresentados brevemente os métodos de compressão citados acima.

Compressão *Quadtree*

Embora existam algoritmos de compressão mais poderosos, a complexidade do *Quadtree* é bem baixa em comparação aos outros algoritmos mais robustos, por exemplo o JPEG, sendo bem adaptável para RSVSF. O *Quadtree* [Strobach 1991] é uma árvore enraizada em que todo nó tem zero ou quatro filhos como pode ser visto na Figura 2.8. Nós com filhos são chamados de *Nós Internos* e nós sem filhos são chamados de *Folhas*. Assim como em toda árvore computacional, os nós possuem um nível que é o número de arestas no caminho mais curto até a raiz da árvore. A altura da árvore é definida pelo número máximo de níveis e um nó é dito como nível mais baixo quando está mais perto da raiz da árvore.

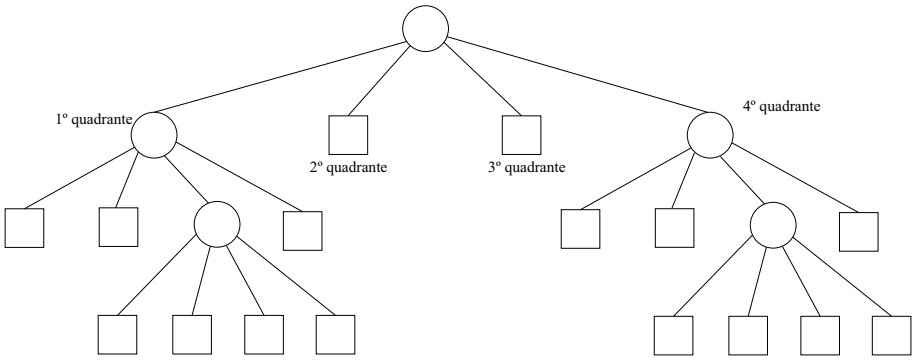


Figura 2.8: Exemplo de árvore *Quadtree* [Cheng e Li 2000, p.2445].

O esquema de compressão *Quadtree* pode ser com ou sem perda. Na compressão sem perda o valor de cada folha da árvore é representada pelo mesmo número de bits, enquanto que na compressão com perda o número de bits para representar a folhas da árvore são diferentes.

Segundo [Cheng e Li 2000], na compressão sem perda, inicialmente a árvore começa com um nó e realiza um teste para verificar se a imagem inteira é homogênea. Sendo homogênea o nó raiz recebe a informação dos tons de cinza da imagem. A partir daí, a imagem é particionada em quatro quadrantes e quatro correspondentes filhos são adicionados à raiz da árvore. O algoritmo recursivamente examina cada quadrante usando cada uma das quatro folhas como nó raiz para uma nova sub

árvore. Na compressão com perda o processo é similar só que ao invés de um teste de homogeneidade é feito um teste de similaridade de *pixels*. No teste de similaridade, um bloco da imagem pode ser mensurado pela variância dos valores dos pixels e textura, enquanto que no teste de homogeneidade os valores são reais e não estatísticos.

(a) Imagem Original (b) Imagem decomposta

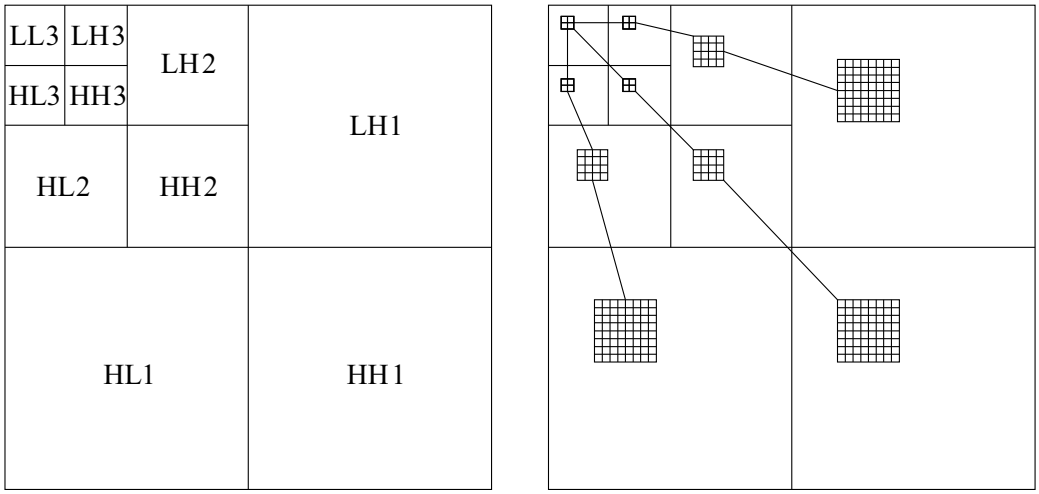
Figura 2.9: Decomposição de uma imagem com *Quadtree* [Cheng e Li 2000, p.2444].

A decomposição *Quadtree* pode delimitar os objetos na imagem original, como mostrado na Figura 2.9(b). Desta forma, a criptografia seletiva propõe criptografar apenas os objetos delimitados na estrutura *Quadtree*. Outro ponto relevante é que este método de compressão pode ser implementado tanto na forma *top-down*, apresentada previamente, ou na forma *bottom-up*. Nesta segunda forma, a árvore começa completa com tamanho n. O nível mais alto é examinado antes da execução, e os quatro nós folhas irmãos são somados para construir o nó pai. O algoritmo repete até não existir mais folhas ou atingir o nó raiz da árvore. Segundo [Cheng e Li 2000], na prática, a implementação *bottom-up* é mais eficiente.

Compressão Baseada em *Wavelet*

Neste método é criada uma hierarquia dos coeficientes das bandas de frequência chamada de *Pirâmide de Decomposição*. A Figura 2.10(a) apresenta a pirâmide de sub-bandas da imagem, onde o número do rótulo indica o nível da pirâmide. A Figura 2.10(b) apresenta a árvore de coeficientes. Geralmente os algoritmos baseados em *Wavelet* são baseados em *zerotrees*, tendo a vantagem de agrupar os coeficientes insignificantes dentro das *zerotrees* e indicar sua insignificância muito eficientemente [Cheng e Li 2000].

Numa compressão baseada em *Wavelet*, a banda de mais alto nível da compressão contém as informações visuais mais importantes [Grangetto et al. 2006,



(a) Hierarquia dos coeficientes (Pirâmide de Decomposição)

(b) Arvores de Coeficientes *Wavelet*

Figura 2.10: Compressão *Wavelet* [Cheng e Li 2000, p.2442].

Chew et al. 2008]. O mais alto nível da pirâmide é chamado de banda LL, sendo esta a raiz da árvore. Desta forma, encriptando o bloco raiz da árvore e deixando os níveis abaixo sem criptografia é garantida uma criptografia seletiva de imagens, uma vez que somente as partes relevantes da imagem comprimida ficam seguras, deixando o restante sem criptografia, reduzindo a complexidade e o tempo computacional e garantindo segurança nos dados. Sem a parte relevante da imagem, ou seja, a parte que contém as informações visuais mais importantes, não será possível reconstruir a imagem original.

Este método de compressão é bastante similar ao *Quadtree* só que ao invés de homogeneidade ser o ponto chave, o ponto chave é o fator de significância que decide se o conjunto é particionado ou não. Quando o conjunto não mais for particionado esta será a sub-banda relevante da imagem.

Um algoritmo eficiente para este tipo de compressão é o *Discrete Wavelet Transform* (DWT). Em resumo, DWT decompõe a imagem coletada em partes menores chamadas de sub-bandas ou sub-camadas, tendo cada sub-banda da imagem relevâncias diferentes no processo de reconstrução da imagem original [Costa e Guedes 2012a]. Desta forma cada sub-banda pode ser colocada em pacotes de dados, onde a sub-banda de maior relevância terá sempre maior prioridade de tráfego que as outras. Vale ressaltar que, ao utilizar DWT, a sub-banda de maior relevância é primordial para a reconstrução da imagem original, e sem ela a imagem não é reconstruída com nitidez. Entretanto, somente com apenas a sub-banda de maior relevância é possível reconstruir a imagem numa qualidade aceitável, a depender da aplicação.

A Figura 2.11 apresenta um exemplo de codificação DWT em um e dois níveis utilizando a transformada de onda numa imagem de 128x128 *pixels* de resolução.

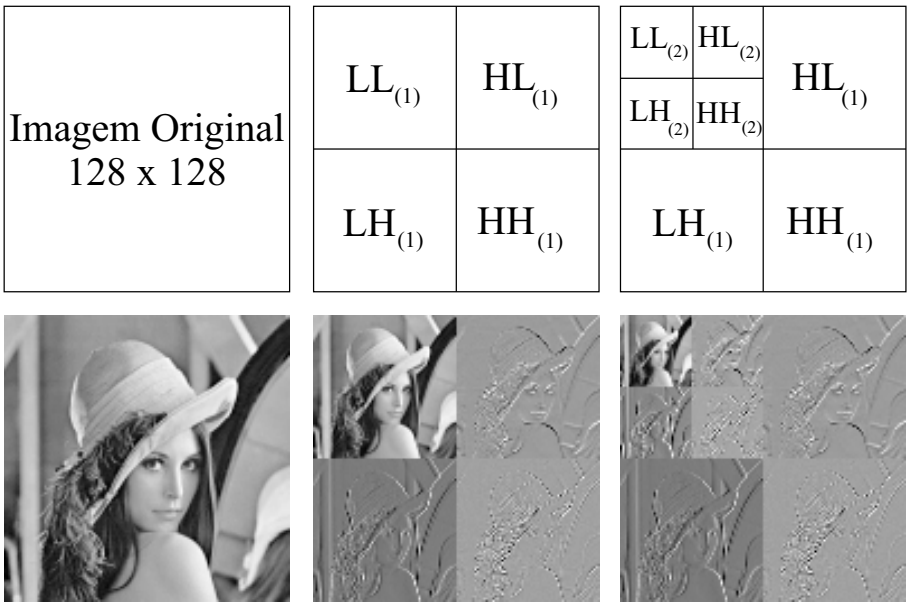


Figura 2.11: Compressão DWT gerando um e dois níveis de resolução [Costa e Guedes 2012a, p.15].

Desta forma, significa que a transformada DWT foi aplicada uma e duas vezes respectivamente, como mostrado na Figura 2.11.

Capítulo 3

Criptografia Adaptativa

Nas redes de sensores sem fio o aspecto segurança é muito relevante e, a depender da aplicação, torna-se um aspecto central para o funcionamento da rede. Como dito anteriormente, devido às restrições de recursos dos nós sensores, prover segurança em RSSF é uma tarefa muito difícil e desafiadora. Nas RSVSF devido ao dado coletado representar uma maior quantidade de informações do ambiente, garantir segurança passa a ser ainda mais desafiador. Além disso, os mecanismos de segurança conhecidos e utilizados nas redes de computadores tradicionais não são benéficos para redes de sensores devido à alta sobrecarga de computação e comunicação que esses mecanismos possuem. Partindo desses pressupostos, este trabalho vem propor um novo paradigma de segurança para RSVSF, chamado de Criptografia Adaptativa. Este conceito é inédito e tem como objetivo garantir segurança às RSVSF sem que isso seja degradante aos recursos dos nós sensores da rede.

Criptografia adaptativa visa prover segurança para redes de sensores sem fio sem que os recursos da rede, ou seja, dos nós sensores, como memória, processamento e, principalmente, energia, sejam severamente degradados, levando à economia desses recursos em relação à mecanismos de criptografia que sejam aplicados a todos os dados coletados na rede. Em outras palavras, a criptografia adaptativa tem como objetivo garantir segurança apenas aos dados coletados pelos nós sensores que tenham maior necessidade de confidencialidade. Sendo assim, apenas alguns nós sensores despendem energia para garantir segurança, economizando energia de modo global.

Portanto, para alcançar estes objetivos, o modelo de criptografia adaptativa, proposto por este trabalho, tem como ideia central a criação do conceito chamado *Área de Confidencialidade* (AC). Além disso, foram definidos outros conceitos relacionados à área de confidencialidade, chamados de *Níveis de Confidencialidade* e *Esquemas de Segurança*. Estes três conceitos juntos irão reger o funcionamento do modelo proposto de criptografia adaptativa de forma centralizada, fundamentado na figura do *Sink Node*. Para isso, foi definido um protocolo de comunicação a ser utilizado apenas entre o *Sink Node* e os nós sensores, chamado de Protocolo de Definição da Área de Confidencialidade, em inglês, *Definition of Confidential Area Protocol*

(DCAP), que tem a função de configurar e informar aos nós sensores qual configuração cada um deles deve adotar durante a execução do modelo de criptografia adaptativa.

As aplicações desenvolvidas para RSSF podem requerer níveis de confidencialidade diferentes para determinadas partes da área monitorada. Assim, empregando o paradigma de criptografia adaptativa, a rede de sensores é subdividida em áreas menores, onde estas áreas poderão ter níveis de segurança diferentes que podem ser refletidos em mecanismos de segurança particulares. Sendo assim, os nós sensores garantem segurança aos dados coletados de forma diferenciada a depender da área de confidencialidade a qual fazem parte. Desta forma, pode-se prover segurança a áreas com altos requisitos de segurança sem que seja aplicado um mecanismo de segurança completamente seguro à rede como um todo. Portanto, aplicando o modelo de criptografia adaptativa pode-se garantir segurança aos dados coletados apenas no local do ambiente onde existe esta necessidade, evitando assim que a RSSF tenha que aplicar algum mecanismo de segurança em todo o ambiente, o que consumiria muito mais os recursos da rede.

Um ponto importante a se ressaltar é que todos os aspectos e características que envolvem a solução de criptografia adaptativa são definidos pelos requisitos da aplicação, ou seja, é a aplicação que dita as definições do modelo proposto mediante às suas necessidades. Além disso, não se deve confundir uma área segura com uma área que necessita de priorização de tráfego. O que o modelo de criptografia adaptativa propõe é empregar segurança aos dados coletados dentro das áreas de confidencialidade, sem garantir priorização. Contudo, aplicando o conceito defendido por este trabalho em conjunto com algoritmos baseados em QoS (*Quality of Service*) e QoE (*Quality of Experience*), pode-se alcançar este objetivo de se prover ambos, tanto segurança quanto priorização de tráfego.

O princípio da criptografia adaptativa pode ser aplicado em todos os tipos de RSSF. Contudo, o foco inicial deste trabalho é a utilização deste modelo de segurança em redes de sensores visuais sem fio. Prover segurança em RSVSF é algo mais desafiador que em RSSF comuns, devido, entre outros fatores, à natureza da informação captada. Por estas razões optou-se por aplicar o modelo de criptografia adaptativa em RSVSF. Contudo trabalhos futuros podem surgir tendo o foco em RSSF tradicionais.

3.1 Área de Confidencialidade

A Área de Confidencialidade (AC) é um conceito que define uma área delimitada que recebe um nível de segurança seguindo um determinado esquema proposto, para prover segurança aos dados coletados pelos nós sensores compreendidos nessa área. As aplicações das AC dependem dos requerimentos de segurança de cada aplicação, ou seja, cada aplicação para RSSF é que determina qual esquema de

segurança será aplicado, em quais níveis e onde será aplicado. *Grosso modo*, área de confidencialidade é onde será aplicado o mecanismo de segurança no ambiente monitorado pela rede de sensores.

Uma RSSF pode possuir mais de uma AC com níveis de confidencialidade diferentes. A quantidade pode ser definida pelo projeto da rede de sensores, atendendo sempre aos requisitos da aplicação para a qual foi projetada. Na esquematização proposta por este trabalho, foram definidos quatro níveis de confidencialidade, descritos na seção 3.1.1. Assim, cada uma das áreas poderá possuir um nível de confidencialidade diferente que, a depender do esquema de segurança escolhido, terá uma forma diferenciada de garantir segurança aos dados coletados pelos sensores que estão dentro da mesma.

Desta forma, o conceito de AC define que cada área delimitada possui um nível de confidencialidade particular, e que a forma de prover segurança aos dados coletados dentro da área varia de acordo com o esquema de segurança adotado. Além disso, o conceito de AC possui algumas outras características e definições:

- A criação das AC e a inclusão dos nós sensores nelas é feita de forma centralizada. Sendo assim, o *Sink Node* é quem calcula e informa aos nós sensores qual AC cada um deles pertence, e realiza as devidas adaptações de funcionamento;
- As AC não se sobrepõem. Ou seja, não existe intersecção entre áreas de confidencialidade diferentes, nem tão pouco entre áreas com o mesmo nível de confidencialidade;
- Pode mudar ao longo do tempo. As AC podem se mover, ou seja, variando sua posição ao longo do tempo, ou ainda, podem variar o seu nível de confidencialidade ao longo do tempo;
- Uma AC sempre será um quadrilátero convexo. A figura geométrica escolhida para delimitar uma AC, por simplicidade, foi o quadrilátero. Sendo assim, para delimitar cada área de confidencialidade, são necessários quatro pontos cartesianos. Desta forma a AC é definida por uma quíntupla: AC(N,P,Q,R,S), onde N é seu nível de confidencialidade e P, Q, R e S são os pares ordenados dos vértices do quadrilátero. Na modelagem proposta inicialmente as AC são em duas dimensões, porém é possível adaptar o modelo de criptografia adaptativa para trabalhar com áreas de confidencialidade em três dimensões;
- É necessário algum serviço de localização, podendo ser ele a partir de coordenadas físicas reais fornecidas por um GPS [Čapkun et al. 2002, Moore et al. 2004, Caruso et al. 2005], por exemplo, ou a partir de algum mecanismo de coordenadas virtuais [Cao e Abdelzaher 2006, Fonseca et al. 2005], para poder delimitar e posicionar corretamente as AC;
- O tamanho da área de confidencialidade pode variar;

- A localização, o tamanho e a variação das AC são definidos estritamente pelos requisitos da aplicação, que é um conceito abstrato;
- Não é definido nenhum conceito ou aspecto para priorizar o tráfego de dados gerados dentro de uma AC. Em outras palavras, o tráfego dos dados não é necessariamente priorizado. O conceito de área de confidencialidade, uma contribuição para essa área de pesquisa, não deve ser confundido com priorização de tráfego.

A Figura 3.1 apresenta um exemplo de uma rede de sensores com diversas áreas de confidencialidade.

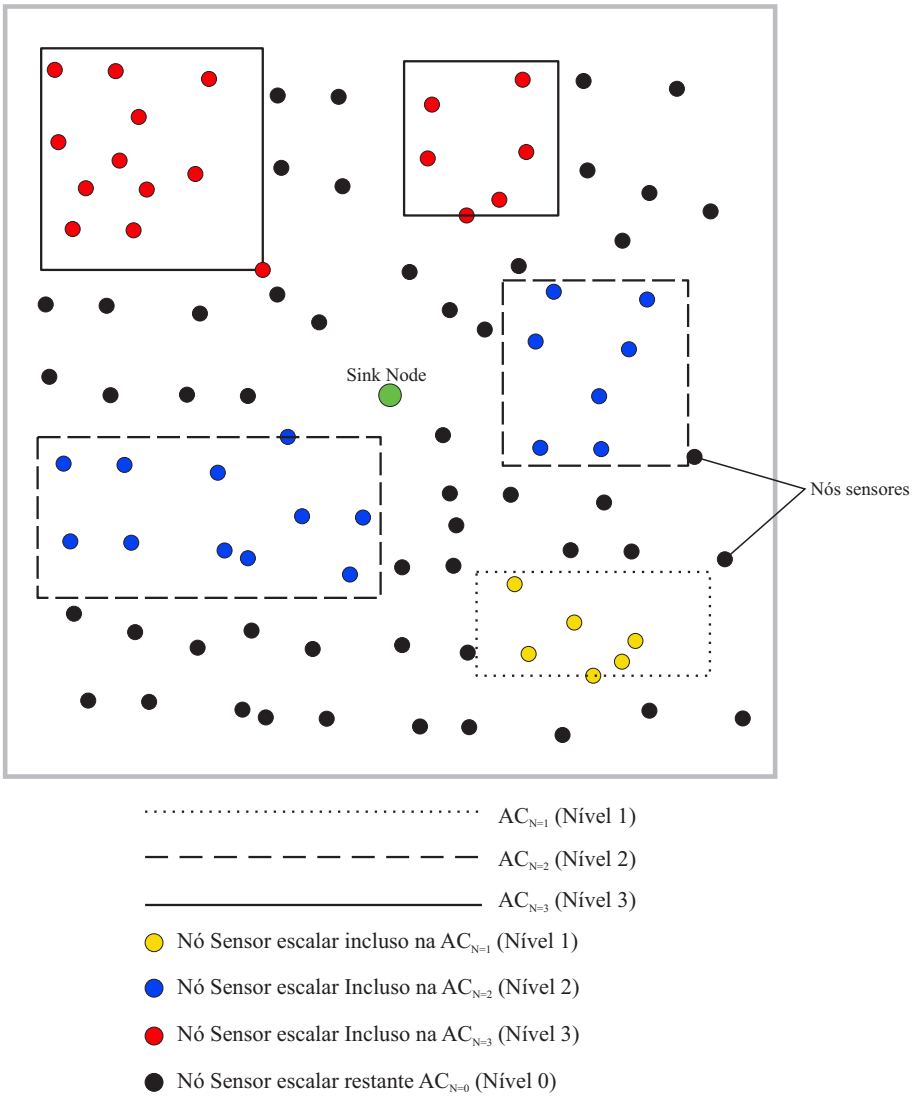


Figura 3.1: Exemplificação dos conceitos de Área de Confidencialidade e Nível de Confidencialidade.

As seções a seguir apresentam conceitos que complementam a definição de área de confidencialidade, sendo eles os *Níveis de Confidencialidade* e os *Esquemas de Segu-*

rança. São estes conceitos que fundamentam a criptografia adaptativa na garantia e manutenção da segurança, definindo como e de que forma se pode prover segurança dentro de uma área de confidencialidade numa RSSF.

3.1.1 Níveis de Confidencialidade

O conceito de Nível de Confidencialidade (NC) irá rotular cada AC com relação à necessidade de confidencialidade e segurança de cada área. Como forma de ilustrar foram propostos quatro níveis de confidencialidade, porém este conceito pode variar de acordo com os requisitos da aplicação:

- **Nível 0:** Área sem criptografia ou qualquer mecanismo de segurança, sendo o nível mais baixo. Este nível não está associado à nenhuma AC, já que ele existe apenas para configurar os nós que não estão em nenhuma AC. A notação $AC_{N=0}$, em outras palavras, representa as áreas da rede de sensores onde não houver qualquer área de confidencialidade;
- **Nível 1:** AC pouco segura. Nesta área estão os nós sensores que requerem pouca segurança, mas ainda assim algum mecanismo será aplicado. Notação $AC_{N=1}$;
- **Nível 2:** AC com segurança moderada. A segurança neste nível é um pouco maior que do nível anterior, mas com aspectos que garantem a economia de recursos. Notação $AC_{N=2}$;
- **Nível 3:** AC com segurança máxima. Neste nível todos os dados coletados na área de confidencialidade são protegidos no nível máximo mesmo com maior uso dos recursos dos nós sensores. Notação $AC_{N=3}$.

Frequentemente, pode existir a necessidade de mais de uma área de confidencialidade ser rotulada com o mesmo nível. Um exemplo desta necessidade é a aplicação deste modelo numa solução de detecção de intrusão, onde as portas de um prédio podem ser monitoradas por nós sensores em uma $AC_{N=3}$ (Área de Confidencialidade nível 3). Sendo assim, existirão várias AC nível 3, uma em cada entrada e saída do local.

A Figura 3.1 apresenta um exemplo de rede de sensores contendo cinco AC: duas no nível 3, duas no nível 2 e uma no nível 1. Vale ressaltar que, o nível de confidencialidade 0, que não recebe nenhum mecanismo de segurança, corresponde ao restante da rede, ou melhor, aos nós sensores que não estão em nenhuma AC delimitada. O nível 0 é importante para definir quais são estes nós sensores que não estão em nenhuma AC.

3.1.2 Esquemas de Segurança

Esquema de segurança é o conceito que vai definir qual mecanismo, aspecto ou medida de segurança será aplicado em cada AC a depender do seu nível de confi-

dencialidade. Em outras palavras, um determinado esquema pode variar o tipo de criptografia, o tamanho da chave, a forma como o dado coletado é criptografado ou ainda que tipo de dado coletado é criptografado em cada nível, entre outros.

Vale lembrar que os esquemas podem variar de acordo com os requisitos de segurança da aplicação e com as necessidades do projeto. O modelo de criptografia adaptativa proposto por este trabalho define alguns esquemas de segurança (listados a seguir), onde apenas um esquema é aplicado por vez no modelo proposto. Na prática, outros esquemas poderão ser propostos a depender do projeto e das necessidades da aplicação:

- **Esquema 1 - Codificação**:
  - Nível 0: Sem criptografia;
  - Nível 1: Criptografia seletiva de imagens (DWT em dois níveis[1]);
  - Nível 2: Criptografia seletiva de imagens (DWT em um nível[2]);
  - Nível 3: Criptografia integral de imagens;
- **Esquema 2 - Tamanho da chave de criptografia**:
  - Nível 0: Sem criptografia;
  - Nível 1: Chave de 128 bits;
  - Nível 2: Chave de 192 bits;
  - Nível 3: Chave de 256 bits;
- **Esquema 3 - Tipo de dado coletado**:
  - Nível 0: Sem criptografia;
  - Nível 1: Criptografia apenas em dados escalares;
  - Nível 2: Criptografia em dados escalares e imagem;
  - Nível 3: Criptografia em dados escalares, imagem e vídeo;

Portanto, o esquema de segurança vai definir qual medida será tomada ao aplicar o modelo de criptografia adaptativa. Além disso, vale ressaltar que os dados coletados dentro de uma AC no nível 1 possui confidencialidade, mesmo que de forma minimizada, logo possuindo proteção.

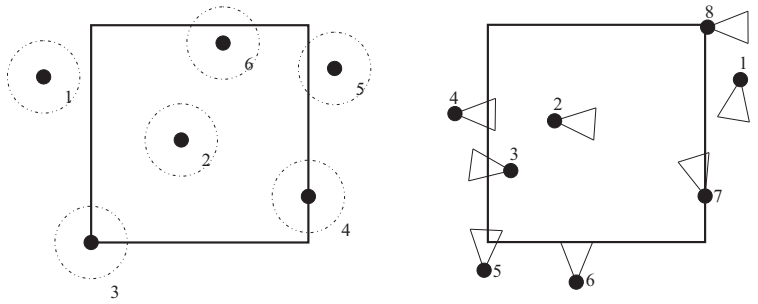
O conceito de Esquemas de Segurança deixa claro que a ideia geral do modelo de criptografia adaptativa é degradar menos os recursos da rede quando comparado com modelos onde seja aplicado o mesmo mecanismo de segurança para todos os dados coletados em todos os nós sensores da rede. Assim, como toda e qualquer forma de se garantir segurança numa RSSF por completo exige grande dispêndio de energia, aplicando o modelo de criptografia adaptativa objetiva-se reduzir o gasto de energia com mecanismos de segurança.

[1] Encriptando $LL_{(2)}$
[2] Encriptando $LL_{(1)}$

3.1.3 Inclusão de nós sensores numa Área de Confidencialidade

Um dos problemas relacionados ao paradigma proposto é a inclusão de nós sensores numa AC. Assim, a questão a ser respondida é: *como saber se um nó sensor pertence ou não à área de confidencialidade delimitada?* Numa RSVSF, tem-se o campo de visão (FoV - *Field of View*) da câmera do nó sensor [Costa e Guedes 2011] definindo o alcance de sensoriamento do nó, porém um mesmo sensor pode ver regiões de mais de uma AC diferente. Isso torna essa identificação potencialmente complexa, demandando modelagem matemática apropriada.

A Figura 3.2 apresenta exemplos de posicionamento de nós sensores tanto numa RSSF quanto numa RSVSF nas proximidades de uma AC. Esses dois tipos de rede exigem modelagens próprias, com problemáticas particulares a serem tratadas. Também por esta razão, essa análise é voltada apenas para as RSVSF.



(a) Inclusão numa RSSF tradicional

(b) Inclusão numa RSVSF

Figura 3.2: Inclusão de nós sensores em AC.

Numa RSSF tradicional, o alcance de sensoriamento de cada sensor é definido como uma circunferência. Por outro lado, sensores visuais possuem cobertura de monitoramento que pode ser simplificada para um triângulo isósceles [Costa et al. 2014]. Em ambos os casos, pode-se notar as situações listadas a seguir, cada uma necessitando de tratamento apropriado

1. Nó sensor e alcance de sensoriamento fora da AC;
2. Nó sensor e alcance de sensoriamento dentro da AC;
3. Nó sensor posicionado em cima de um dos vértices da AC;
4. Nó sensor posicionado em cima de uma das laterais da AC;
5. Nó sensor fora da AC, mas com o alcance de sensoriamento com uma parte dentro da AC;
6. Nó sensor dentro da AC, mas com o alcance de sensoriamento parcialmente fora da AC.

As situações 2, 3, 4 e 6 na Figura 3.2(a) podem ser resolvidas pela posição do sensor, onde se o sensor está dentro ou sobreposto aos limites da AC, então significa que uma parte ou todo o alcance de sensoriamento do mesmo está dentro da AC. Contudo, podem existir situações como exemplificado por 1 e 5, na Figura 3.2(a), que têm-se que avaliar a circunferência do alcance de sensoriamento em relação ao quadrilátero da AC para definir se o nó está incluso na AC, mesmo estando fora dela, já que seu alcance de sensoriamento pode estar monitorando informações dentro da AC. Numa abordagem mais simples, considerando apenas a posição dos nós sensores escalares, basta saber as coordenadas do nó sensor dentro de algum sistema de localização e compará-las com as coordenadas dos vértices do quadrilátero que delimita a AC em questão, traçando as retas laterais do quadrilátero.

Nas RSVSF, ao invés de um alcance de sensoriamento radial em torno do nó sensor, ele será definido pelo posicionamento da câmera, o tipo da câmera, o alcance e o campo de visão (FoV), sendo estes parâmetros que serão considerados para determinar se o nó sensor pertence ou não a uma determinada AC. Assim, a configuração apresentada na Figura 3.1 sofre algumas modificações quando se trata de uma rede de sensores visuais. A Figura 3.3 apresenta a definição de campo de visão em um nó sensor visual. Para efeitos de simplificação, é considerado FoV como um triângulo isósceles, logo, tendo conhecimento do tamanho do raio (R) e do ângulo de abertura do FoV (θ), ambos definidos pelo tipo de câmera, pode-se determinar os pontos B e C mostrados na Figura 3.3, considerando que o sensor visual possui orientação, representada pelo ângulo α nesta mesma Figura 3.3. A Equação 3.1[3] apresenta como encontrar os vértices B e C, em um sistema 2D, conhecendo previamente a posição do nó sensor (vértice A) [Costa et al. 2014]. Portanto, A_x e A_y representam o par ordenado do vértice A, B_x e B_y o par ordenado do vértice B, C_x e C_y o par ordenado do vértice C, R o raio, θ o ângulo de abertura e α o ângulo de orientação.

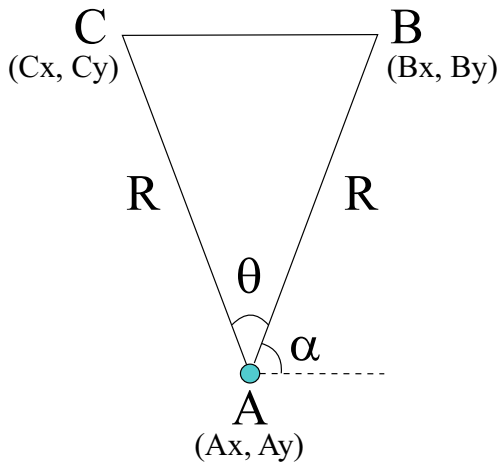


Figura 3.3: Campo de visão (FoV) de um nó sensor visual [Costa et al. 2014].

[3]A parte da expressão $mod 2\pi$ foi inserida para que seja considerada apenas o resto da divisão inteira por 2π.

$$
\begin{aligned}
B_x &= A_x + R.cos(\alpha) \\
B_y &= A_y + R.sen(\alpha) \\
C_x &= A_x + R.cos((\alpha + \theta) mod 2\pi) \\
C_y &= A_y + R.sen((\alpha + \theta) mod 2\pi)
\end{aligned} \tag{3.1}
$$

A Figura 3.4 apresenta um exemplo de uma RSVSF com áreas de confidencialidade delimitadas. Pode-se notar nesta figura que alguns nós sensores estão fora de uma AC, porém o FoV faz com que ele colete informações dentro da área em questão. Desta forma, o nó sensor deve ser considerado incluso à AC.

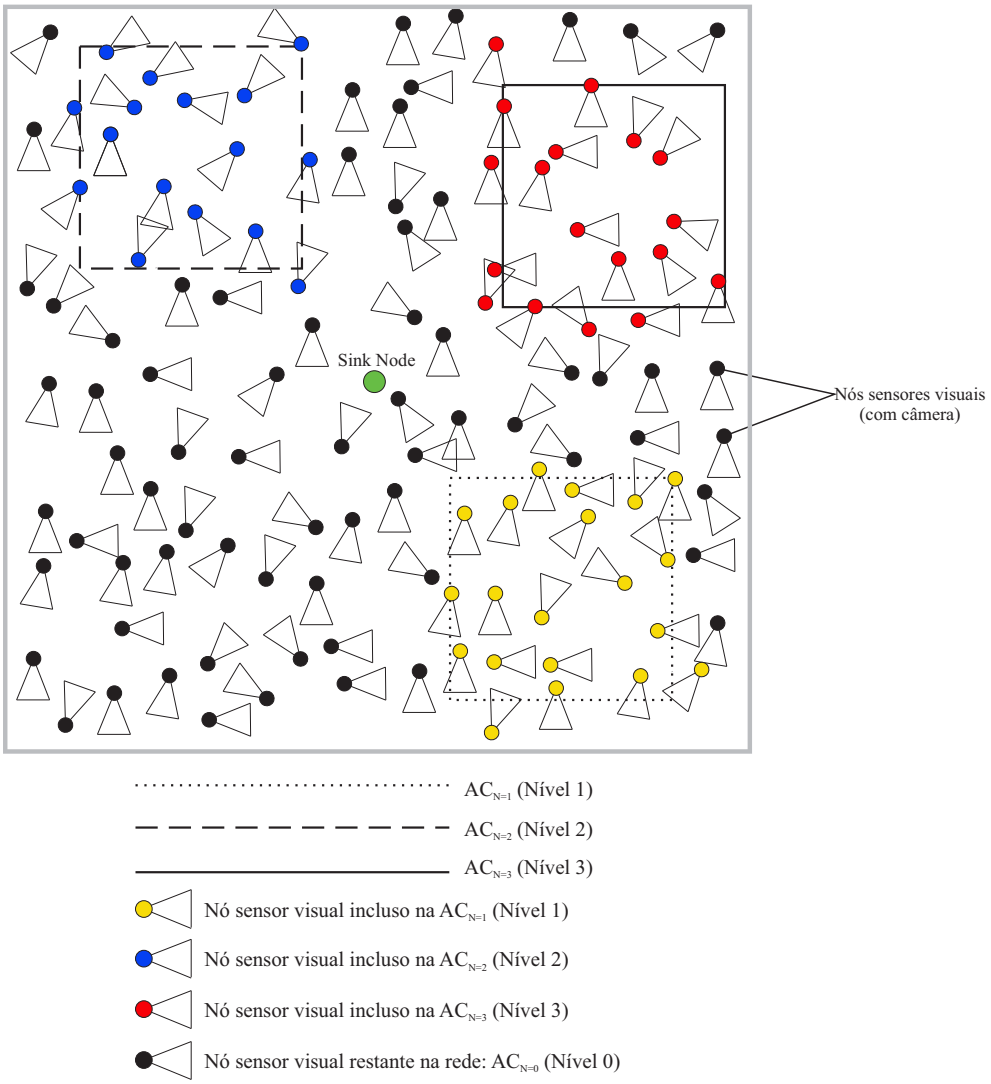


Figura 3.4: Áreas de Confidencialidade em RSVSF.

Numa RSVSF existem também situações em relação à posição do nó sensor que

devem ser consideradas e requerem atenção especial. A Figura 3.2(b) apresenta oito possíveis opções de posicionamento que devem ser consideradas:

1. Nó sensor e campo de visão fora da AC;
2. Nó sensor e campo de visão dentro da AC;
3. Nó sensor dentro da AC, mas com uma parte do campo de visão para fora;
4. Nó sensor fora da AC, mas com o campo de visão com dois pontos para dentro;
5. Nó sensor fora da AC, mas com o campo de visão com um ponto para dentro;
6. Nó sensor fora da AC, mas com o campo de visão com um ou dois pontos em cima dos limites da área;
7. Nó sensor posicionado em cima dos limites da AC;
8. Nó sensor posicionado em cima de um dos vértices da AC.

Então, somente na posição onde o nó sensor e o campo de visão estão fora da AC é que o nó sensor é considerado fora da área. Em todas as outras hipóteses o nó sensor é considerado incluso à área de confidencialidade em questão.

Para que o nó sensor visual seja considerado dentro de uma AC, um dos vértices do triângulo delimitado pelo nó sensor e seu campo de visão deve estar dentro da AC. Sendo assim, se pelo menos um vértice estiver dentro da AC, ele será considerado incluso na AC em questão. Portanto, para saber se algum destes vértices do nó sensor está dentro ou não de uma AC, cada vértice deve ser submetido a um teste definido pelo modelo geométrico descrito a seguir. Este modelo geométrico será utilizado pelo algoritmo que inclui um nó sensor em uma AC.

Modelo geométrico para determinar posição de vértices

O nó sensor e seu campo de visão (FoV) formam um triângulo hipotético, chamado aqui de *Triângulo do Nó Sensor*, onde a posição dos vértices deste triângulo são conhecidas devido às pré-disposições mencionadas anteriormente. Sendo assim, como a posição dos vértices do quadrilátero que delimita cada AC é conhecida também, pode-se, através do modelo geométrico apresentado nesta seção, descobrir se os vértices deste triângulo formado pelo nó sensor e seu FoV estão ou não dentro dos limites de uma AC em questão. A Figura 3.5(a) apresenta um nó sensor visual e uma AC, onde pode-se visualizar esta configuração.

O modelo geométrico analisa um vértice de cada vez, ou seja, este modelo foi projetado para avaliar a inclusão de um vértice do triângulo do nó sensor cuja a posição é conhecida e, a partir dessa avaliação, sinalizar se o nó sensor está ou não dentro de uma AC em questão. Se pelo menos um dos vértices deste triângulo estiver dentro da AC em questão, o nó sensor como um todo será considerado incluso à AC assumindo suas políticas e esquemas de segurança pré-configurados. Um ponto

importante a ser lembrado é que todo este cálculo do modelo para inclusão de nós sensores nas AC é feita de forma centralizada pelo *Sink Node*, que deve conhecer a topologia e localização dos sensores e das AC.

Para saber se um dos vértices do triângulo está dentro de uma AC será realizado um procedimento geométrico que formará um triângulo entre o vértice em questão e outros dois vértices adjacentes do quadrilátero que delimita a AC, formando assim outros quatro triângulos. As Figuras 3.5(b) e 3.5(c) apresentam graficamente como seria este processo. Então, assumindo um quadrilátero PQRS que delimita uma AC e um vértice V, conforme a Figura 3.5(b), o modelo geométrico irá formar os seguintes triângulos: VPQ, VQR, VRS, VPS. Feito isso o modelo irá calcular a área destes quatro triângulos, somá-las e comparar o resultado com a área do quadrilátero, como apresentado na Equação 3.2. Se o resultado for igual, o vértice está dentro da AC. Se o resultado for maior o vértice está fora da AC. Desta forma é possível saber se um ponto qualquer está ou não dentro de uma determinada AC.

$$\begin{aligned} &X = \Delta_{VPQ} + \Delta_{VQR} + \Delta_{VRS} + \Delta_{VPS} \\ &Se\ X = \Delta_{PQRS}\ \ (Vértice\ dentro\ da\ AC) \\ &Se\ X > \Delta_{PQRS}\ \ (Vértice\ fora\ da\ AC) \end{aligned} \tag{3.2}$$

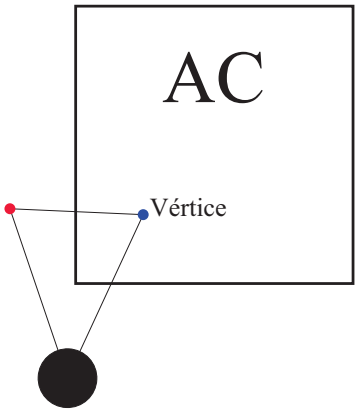
Como não se tem conhecimento dos lados, nem altura, nem qualquer outra informação destes triângulos formados por um vértice em questão e outros dois vértices da AC, a área destes triângulos deve ser calculada utilizando-se apenas as coordenadas dos vértices, pois esta é a única informação conhecida do triângulo formado. Então, a área de um triângulo pode ser calculada conforme definido na Equação 3.3.

$$Área_{(triângulo)} = \frac{1}{2}.\,|D| \tag{3.3}$$

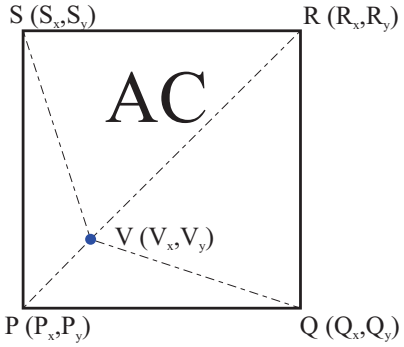
onde D é o determinante da matrix 3x3 formada pelas coordenadas dos vértices, conforme a Equação 3.4.

$$D = \begin{vmatrix} v1_x & v1_y & 1 \\ v2_x & v2_y & 1 \\ v3_x & v3_y & 1 \end{vmatrix} \tag{3.4}$$

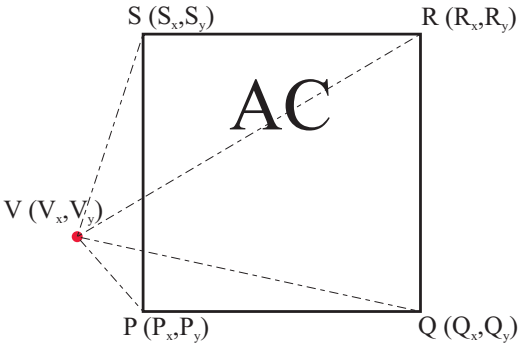
Desta forma, resolvendo o determinante para os quatro triângulos, as suas respectivas áreas serão definidas pela Equação 3.5 apresentada a seguir:



(a) Nó sensor com um dos vértices dentro da AC



(b) Exemplo de vértice incluso



(c) Exemplo de vértice não incluso

Figura 3.5: Modelo Geométrico: Exemplo 1.

$$
\begin{aligned}
\Delta_{VPQ} &= \frac{V_x.(P_y - Q_y) + P_x.(Q_y - V_y) + Q_x.(V_y - P_y)}{2} \\
\Delta_{VQR} &= \frac{V_x.(Q_y - R_y) + Q_x.(R_y - V_y) + R_x.(V_y - Q_y)}{2} \\
\Delta_{VRS} &= \frac{V_x.(Q_y - S_y) + R_x.(S_y - V_y) + S_x.(V_y - R_y)}{2} \\
\Delta_{VPS} &= \frac{V_x.(P_y - S_y) + P_x.(S_y - V_y) + S_x.(V_y - P_y)}{2}
\end{aligned} \tag{3.5}
$$

Além destas posições de vértice do triângulo formado pelo nó sensor e seu FoV apresentadas anteriormente, existem outras situações que devem ser tratadas. Caso o vértice em questão esteja em cima de uma das laterais da AC ou em cima da reta prolongada de uma das laterais da AC, somente será possível formar três triângulos,

como apresentado nas Figuras 3.6(a) e 3.6(b). Estas situações acontecem se um dos determinantes resultar em zero, significando que os três vértices não formam um triângulo, ou seja, estão na mesma reta, o que permite concluir que o vértice em questão não está dentro da AC, mas em cima de um dos lados ou em cima da reta prolongada de um dos seus lados. Desta forma, mesmo quando uma das áreas dos quatro triângulos formados é zero, se a soma das outras três áreas for igual à área da AC, significa que o vértice está em cima de uma das laterais da AC, conforme mostrado na Figura 3.6(a). Caso a soma das outras três áreas dos triângulos for maior que a área da AC, significa que o vértice está em cima da reta prolongada de uma das laterais da AC e, portanto, fora da AC, conforme a Figura 3.6(b).

Sendo assim, estas duas posições especiais não alteram o funcionamento do modelo, pois considerando as outras três áreas dos triângulos formados entre o vértice em questão e os vértices da AC é possível determinar, da mesma forma, se aquele vértice está ou não em cima de uma das laterais do quadrilátero, e portanto dentro ou fora da AC.

Outra situação é se um dos vértices do triângulo formado pelo nó sensor e pelo seu FoV for coincidente à um dos vertices do quadrilátero que delimita a AC, como apresenta a Figura 3.6(c). Neste caso, antes da execução do modelo será testado se os vértices são coincidentes, e assim sendo, o vértice é considerado incluso à AC.

Além disso, existe a possibilidade do triângulo do nó sensor ter seus vértices inclusos em duas ou mais AC diferentes. Neste caso, propõe-se que o nó sensor assuma o esquema de segurança da AC que possua o maior nível de confidencialidade, a fim de não comprometer os requisitos da aplicação. As Figuras 3.7 e 3.8 apresentam exemplos de como seriam estas situações.

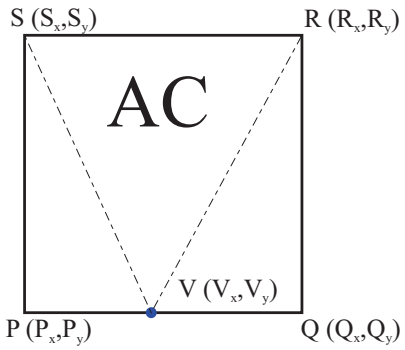
Por fim, uma consideração a ser feita é sobre a área do quadrilátero que delimita a AC. Por simplicidade os quadriláteros que serão considerados na implementação deste modelo são o quadrado e o retângulo, como apresentado pelas equações 3.6 e 3.7 respectivamente. Todavia, este modelo geométrico suporta a utilização de qualquer quadrilátero desde que seja calculada de forma correta a área do mesmo.

$$Área_{(quadrado)} = L^2 \tag{3.6}$$

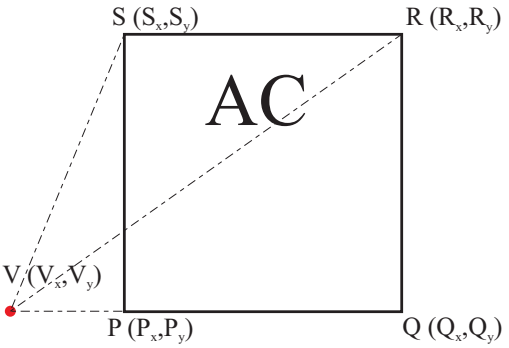
$$Área_{(retângulo)} = B.H \tag{3.7}$$

Algoritmo para incluir um nó sensor visual em uma AC

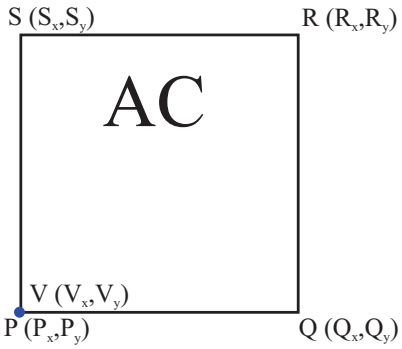
Foi proposto um algoritmo para incluir automaticamente os nós sensores visuais nas AC definidas pela aplicação. O Algoritmo 1 é um código auxiliar que descreve a



(a) Vértice em uma das laterais da AC



(b) Vértice na reta prolongada de uma das laterais da AC



(c) Vértice coincidente à um dos vértices da AC

Figura 3.6: Modelo Geométrico: Exemplo 2.

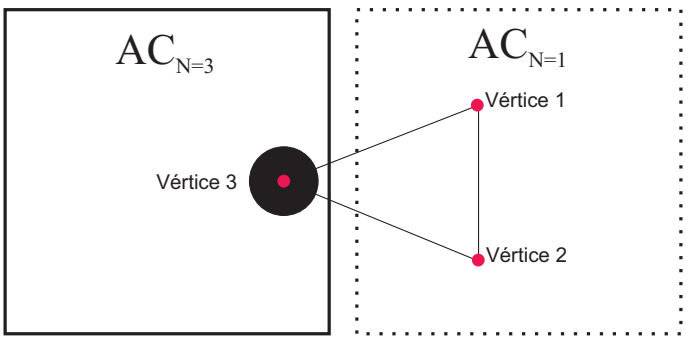


Figura 3.7: Nó sensor com dois vértices em AC diferentes.

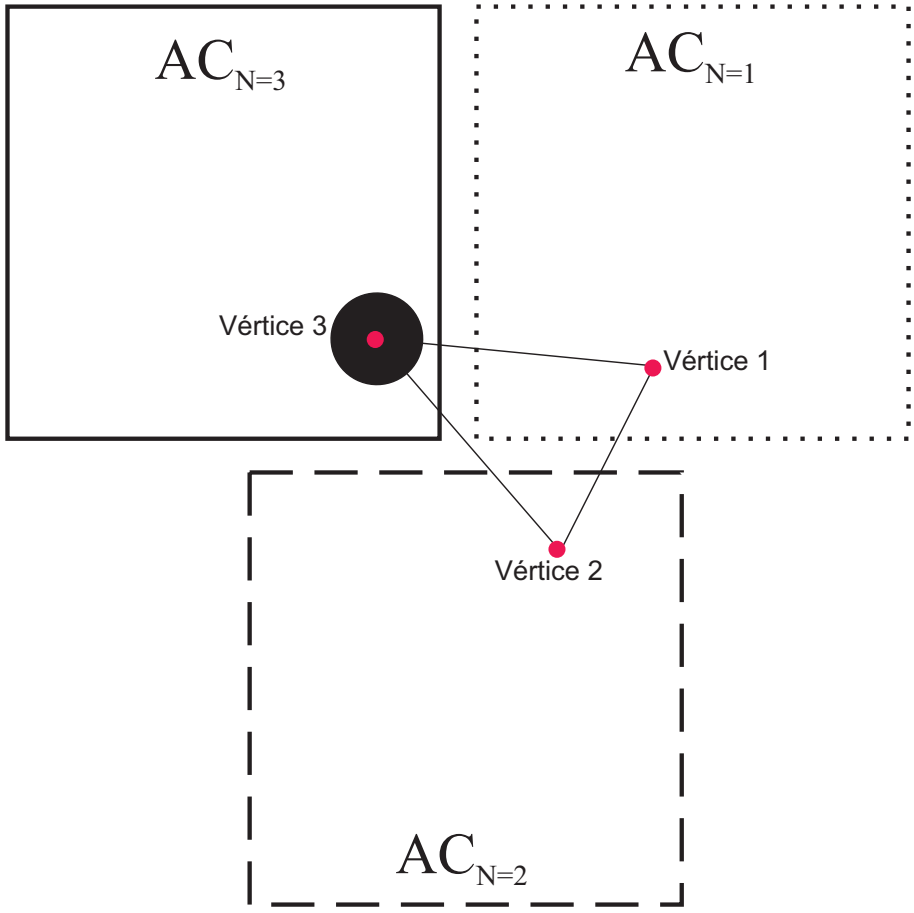


Figura 3.8: Nó sensor com três vértices em AC diferentes.

sequência de passos do modelo geométrico descrito na seção anterior que tem como finalidade descobrir se um vértice, ou melhor, um ponto qualquer, está dentro do quadrilátero que delimita uma AC. As entradas deste algoritmo são o vértice a ser analizado, ou seja, o ponto que se deseja saber se está ou não dentro de uma AC, e os vértices do quadrilátero que delimita a AC.

Em seguida foi definido o algoritmo principal, como apresentado no Algoritmo 2. Este pseudo-código utiliza o Algoritmo 1 para saber se um ponto está ou não dentro da AC. As entradas do Algoritmo 2 são todas as AC, os seus respectivos níveis de confidencialidade e as coordenadas do nó sensor. Inicialmente, é realizado um procedimento para descobrir os outros dois vértices que formam o triângulo do nó sensor, formado por cada nó e seu respectivo FoV. Este procedimento é baseado na Equação 3.1. Sendo assim, passa-se a ter três coordenadas para definir cada nó sensor.

O próximo passo é analisar todas as AC para descobrir se pelo menos um dos vértices do triângulo do nó sensor pertence a uma AC. Quando se detecta que o ponto está dentro da AC o nó sensor como um todo recebe o nível da AC analisada, se este for

maior que o nível atual do nó sensor.

Algoritmo 1: Algoritmo do Modelo Geométrico

Entrada: Vértice do Triângulo, Vértices da AC
Saída: VERDADEIRO ou FALSO
início
  V_x,V_y = Vértice do triângulo;
  P_x, P_y = Primeiro Vértice da AC;
  Q_x,Q_y = Segundo Vértice da AC;
  R_x,R_y = Terceiro Vértice da AC;
  S_x,S_y = Quarto Vértice da AC;
  se *(V_x=P_x e V_y=P_y) ou (V_x=Q_x e V_y=Q_y) ou (V_x=R_x e V_y=R_y) ou (V_x=S_x e V_y=S_y)* **então**
    Retorna VERDADEIRO;
  senão
    Δ_{t1}=Área do triângulo VPQ;
    Δ_{t2}=Área do triângulo VQR;
    Δ_{t3}=Área do triângulo VRS;
    Δ_{t4}=Área do triângulo VPS;
    Δ_{quad}=Área do Quadrilátero PQRS;
    Soma=$\Delta_{t1} + \Delta_{t2} + \Delta_{t3} + \Delta_{t4}$;
    se Δ_{quad}=*Soma* **então**
      Retorna VERDADEIRO;
    senão
      Retorna Falso
    fim
  fim
fim

3.1.4 Protocolo de Definição de Área de Confidencialidade

O Protocolo de Definição da Área de Confidencialidade, em inglês, *Definition of Confidential Area Protocol* (DCAP) é uma "ferramenta" para que o *Sink Node* possa configurar cada nó sensor atribuindo um nível de confidencialidade de AC para cada um. Este protocolo foi definido com o objetivo de estabelecer a comunicação necessária entre os nós sensores e o *Sink Node* a fim de realizar a configuração dos nós sensores de uma RSVSF seguindo as definições do modelo de criptografia adaptativa. Como o modelo prevê que a etapa de criação das AC e inclusão dos nós sensores nas AC é feita de forma centralizada pelo *Sink Node*, este protocolo é necessário, fazendo com que tanto o *Sink Node* como os demais nós sensores da rede se comuniquem durante o processo de configuração.

O protocolo DCAP foi especificado em nível de aplicação seguindo diretivas para atender aos propósitos do modelo de criptografia adaptativa. Inicialmente, os nós

Algoritmo 2: Algoritmo para inclusão de Nós Sensores em AC

Entrada: Nó Sensor, Vértices de todas AC, Nível de cada AC
Saída: Nó Sensor em uma AC
início
    Descobrir Vértices do Triângulo do Nó Sensor (Nó Sensor);
    A_x,A_y = Posição do nó sensor;
    B_x,B_y = Vértice 1;
    C_x,C_y = Vértice 2;
    Nível do Nó Sensor = 0;
    NS = Nível do Nó Sensor;
    AS = AC do nó sensor;
    AC atual = Primeira AC;
    repita
        P_x, P_y = Primeiro Vértice da AC atual;
        Q_x,Q_y = Segundo Vértice da AC atual;
        R_x,R_y = Terceiro Vértice da AC atual;
        S_x,S_y = Quarto Vértice da AC atual;
        N = Nível da AC atual;
        se *Algoritmo do Modelo Geométrico(A_x,A_y, P_x, P_y, Q_x,Q_y, R_x,R_y, S_x,S_y)*
        então
            se $NS < N$ **então**
                NS = N;
            senão
                Não Altera NS
            fim
        senão
            Continua;
            se *Algoritmo do Modelo Geométrico(B_x,B_y, P_x, P_y, Q_x,Q_y, R_x,R_y, S_x,S_y)* **então**
                se $NS < N$ **então**
                    NS = N;
                senão
                    Não Altera NS
                fim
            senão
                Continua;
                se *Algoritmo do Modelo Geométrico(C_x,C_y, P_x, P_y, Q_x,Q_y, R_x,R_y, S_x,S_y)* **então**
                    se $NS < N$ **então**
                        NS = N;
                    senão
                        Não Altera NS
                    fim
                senão
                    Não pertence à AC atual;
                fim
            fim
        fim
        AC atual = Próxima AC;
    até *Última AC*;
fim

sensores estarão pré-configurados com relação ao nível e esquemas de segurança, garantindo aspectos iniciais para todos os nós sensores de forma que a RSVSF possa ter seu início de funcionamento. Estas pré-configurações estão de acordo com o modelo de criptografia adaptativa e são pré-implantadas nos nós sensores, como o nível de confidencialidade $AC_{N=0}$ e os esquemas de segurança prévios. Sendo assim, pode-se afirmar que todos os nós sensores possuem inicialmente as mesmas configurações.

Este protocolo irá permitir que o *Sink Node*, através de mensagens, re-configure cada nó sensor da rede incluindo-os nas devidas AC, de acordo com o modelo de inclusão de nós sensores descrito anteriormente. Assim, o DCAP é uma forma que o modelo de criptografia adaptativa possui para que o *Sink Node* se comunique com cada nó sensor e informe a eles a qual AC pertencem.

O protocolo DCAP tem seu funcionamento composto por três tipos de mensagens diferentes. Uma mensagem de solicitação/identificação do nó sensor (AC-Request), uma mensagem de configuração (AC-Configure) e uma mensagem de reconhecimento (AC-ACK). AC-Request é uma mensagem que somente é enviada pelo *Sink Node* para um nó sensor. Esta mensagem visa solicitar dados do nó sensor, como por exemplo, nível AC atual e localização. Num cenário ideal onde os nós sensores não mudam de posição, esta mensagem pode se tornar desnecessária caso o *Sink Node* seja pre-configurado com uma tabela contendo estas informações de todos os nós sensores. Contudo, prevendo que a posição dos nós sensores pode mudar ao longo do tempo, antes de incluir um nó numa AC ou mudar o nó de uma AC, o *Sink Node* deve através da mensagem AC-Request solicitar a localização do nó sensor e seu nível atual. Desta forma, evita-se que o *Sink Node* tenha que demandar memória interna para armazenar informações do nó. Após receber um AC-Request, o nó sensor responde a esta mensagem enviando para o *Sink Node* uma mensagem do tipo AC-ACK para fins de reconhecimento e também informando dentro da mensagem as informações de localização e nível de confidencialidade atual. A mensagem AC-Configure é uma mensagem de retorno, enviada somente pelo *Sink Node* para o nó sensor fornecendo a configuração após a execução do algoritmo proposto para descobrir tal configuração para cada nó sensor. Por fim, uma outra mensagem AC-ACK é utilizada também para o reconhecimento da mensagem AC-Configure encerrando a comunicação. A Tabela 3.1 resume as mensagens do protocolo DCAP.

Tabela 3.1: Resumo das Mensagens do protocolo DCAP.

Mensagem	**Descrição**	**Enviada por**
AC-Request	Requisição de informações do nó sensor	*Sink Node*
AC-Configure	Informa ao nó sensor a configuração	*Sink Node*
AC-ACK	Mensagem de reconhecimento e para informar dados em resposta à AC-Request	Nós Sensores

Como a maior parte do consumo de energia de uma RSSF, como um todo, resulta da transmissão e recepção de pacotes, é esperado que o protocolo DCAP seja o mais

energeticamente eficiente possível, ou seja, que evite o desperdício de energia com mensagens desnecessárias e com informações desnecessárias nas mensagens. Assim, pode-se dizer que o protocolo DCAP se propõe a garantir que a transmissão de suas mensagens seja confiável, mas com eficiência de energia. Além disso, como as transmissões sem fio são muito suscetíveis a erros de transmissão e perda de pacotes e a configuração dos nós sensores não pode deixar de ser feita, segundo o modelo de criptografia adaptativa, o protocolo DCAP prevê as retransmissões de mensagens para o caso de erros deste tipo.

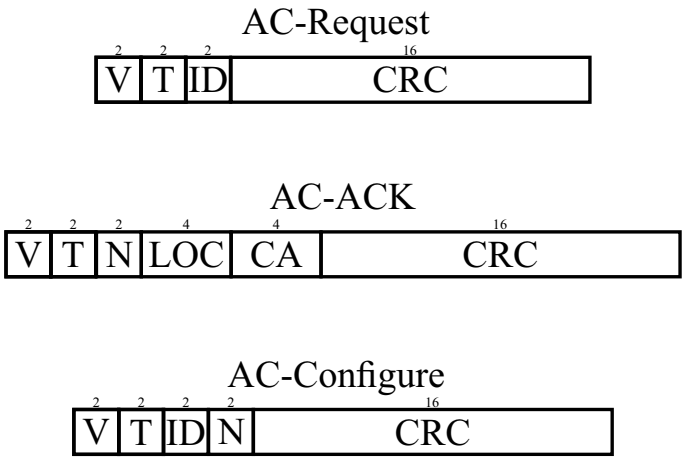


Figura 3.9: Mensagens do Protocolo DCAP.

A Figura 3.9 apresenta as três mensagens do protocolo DCAP. O campo "V" (Versão) tem tamanho 2 bits e indica a versão do protocolo, que inicialmente foi estabelecida como "00". O campo "T" (Tipo) tem tamanho 2 bits e é utilizado para diferenciar as mensagens umas das outras, sendo "00" para AC-Request, "01" para AC-Configure e os valores "10" e "11" para AC-ACK. A mensagem AC-ACK pode ser de dois tipos: ou para reconhecer a mensagem AC-Request ou para reconhecer a mensagem AC-Configure. Desta forma, o funcionamento da mensagem AC-ACK é diferente para estes dois casos. Se o campo "T" da mensagem AC-ACK for "10" significa que é uma resposta à mensagem AC-Request, logo os campos seguintes "N" e "LOC" da mensagem AC-ACK devem ser considerados e interpretados pelo *Sink Node*. Caso o campo "T" da mensagem AC-ACK tenha o valor "11" significa que é apenas uma mensagem de reconhecimento da mensagem AC-Configure, não necessitando interpretar os campos "N" e "LOC" da mensagem AC-ACK. O Campo "ID" é um identificador de cada mensagem, existente apenas nas mensagens AC-Request e AC-Configure. Ele inicia em "00" e deve ser sempre incrementado a cada nova mensagem. A retransmissão de uma mensagem deve possuir o mesmo valor para "ID", associando assim mensagens em um mesmo escopo. Apenas a mensagem AC-ACK possui o campo "CA" (Código ACK) usado para manter uma relação temporal entre as mensagens de requisição e resposta e as mensagens de reconhecimento. Composto por 4 bits, o campo "CA" contém nos dois primeiros bits o valor de "T" e nos dois últimos bits o valor do campo "ID", ambos da mensagem que está sendo reconhecida. O campo "N"

da mensagem AC-ACK é o nível de confidencialidade atual do nó sensor em questão e o campo "LOC" são as coordenadas cartesianas ou geográficas da sua localização. Estes campos são usados para enviar ao *Sink Node* estas informações através da própria mensagem de reconhecimento AC-ACK em resposta à mensagem AC-Request. O campo "N" da mensagem AC-Configure é o novo nível de confidencialidade que o *Sink Node* calculou para o nó sensor em questão. Assim, o nó sensor irá assumir esse nível, entrando na AC correspondente e aplicando o esquema de segurança pré-configurado referente ao nível informado. A Tabela 3.2 apresenta os possíveis valores de "N" associando aos níveis de confidencialidade. Por fim, o campo "CRC" (*Cyclic Redundant Check*), de tamanho 16 bits, é utilizado para verificar se a mensagem foi corrompida durante a transmissão, aplicando uma soma de verificação baseada em complemento de 2.

Tabela 3.2: Valor do campo N.

Valor de N	**Nível de Confidencialidade**	**Descrição**
00	Nível 0	Sem Confidencialidade
01	Nível 1	Pouca Confidencialidade
10	Nível 2	Confidencialidade Média
11	Nível 3	Máxima Confidencialidade

A mensagem AC-ACK é enviada apenas pelo nó sensor em resposta e reconhecimento das outras mensagens. Além disso, a mensagem AC-ACK não é confirmada pelo seu receptor, ou seja, ela é utilizada para reconhecimento das outras duas mensagens, mas quem envia uma AC-ACK não recebe nenhuma confirmação de recebimento. O protocolo DCAP é baseado no protocolo genérico proposto por [Costa et al. 2015], e da mesma forma o tempo de resposta não é restrito, pois a economia de energia é mais importante. Assim, a mudança dos estados do protocolo é controlada por dois contadores: t_m e t_{ack}. O contador t_m é o tempo que o *Sink Node* deve esperar por uma mensagem AC-ACK em retorno às mensagens AC-Request e AC-Configure. Em outras palavras, t_m é o tempo que o *Sink Node* deve esperar pela mensagem de reconhecimento. O contador t_{ack} é o tempo necessário para assegurar que uma mensagem AC-ACK foi recebida pelo *Sink Node*, assim, t_{ack} é utilizado pelos nós sensores para controlar se deve assumir ou não que a mensagem AC-ACK enviada por ele foi corretamente recebida pelo destino.

Então, se nenhuma mensagem AC-ACK for recebida pelo *Sink Node* antes de t_m a mensagem correspondente deve ser retransmitida. De fato a retransmissão será necessária nos casos a seguir, pois a mensagem AC-ACK não será recebida a tempo pelo *Sink Node*:

- Se uma mensagem AC-request ou AC-Configure for perdida (descartada ou corrompida) durante a transmissão;
- Se a mensagem AC-ACK correspondente for perdida;
- Se a mensagem AC-ACK esperada for recebida após t_m.

Baseando-se no protocolo proposto em [Costa et al. 2015], a fim de garantir que a solução seja escalonável e com alguma resistência a erros de transmissão e congestionamento, no protocolo DCAP, o tempo t_m deve dobrar se uma mensagem AC-request ou AC-Configure precisar ser retransmitida e o número máximo de retransmissões de uma mesma mensagem é 4, para evitar que se tente retransmitir quando as rotas estiverem congestionadas ou inativas, fazendo com que o nó sensor de destino fique inalcançavel. Assim, assumindo como a tentativa de retransmissão sendo r, $r = 1$, ..., 4, e o tempo fim a fim de referência para a transmissão, processamento e reconhecimento definido como t_r, pode-se definir t_m como $t_m = 2^{(r-1)}.t_r$. O valor de t_m é reiniciado para o valor de referência t_r após cada transmissão bem sucedida.

O outro contador t_{ack} funciona da forma que, após o envio de uma mensagem AC-ACK, o nó sensor que enviou essa mensagem espera um tempo t_{ack}, desta forma:

- Se uma mensagem AC-request ou AC-Configure for recebida antes de t_{ack}, será considerado que a AC-ACK foi perdido;
- Se uma mensagem AC-request ou AC-Configure for recebida após t_{ack}, deve-se assumir que a AC-ACK foi recebido corretamente e que se trata de uma nova mensagem.

Portanto, desta forma, espera-se que $t_{ack} > t_m$, mesmo no caso de retransmissão quando t_m dobra. A Figura 3.10 define a modelagem da operação do protocolo no *Sink Node* e a Figura 3.11 define a modelagem da operação do protocolo nos demais nós sensores, ambos através de uma Rede de Petri.

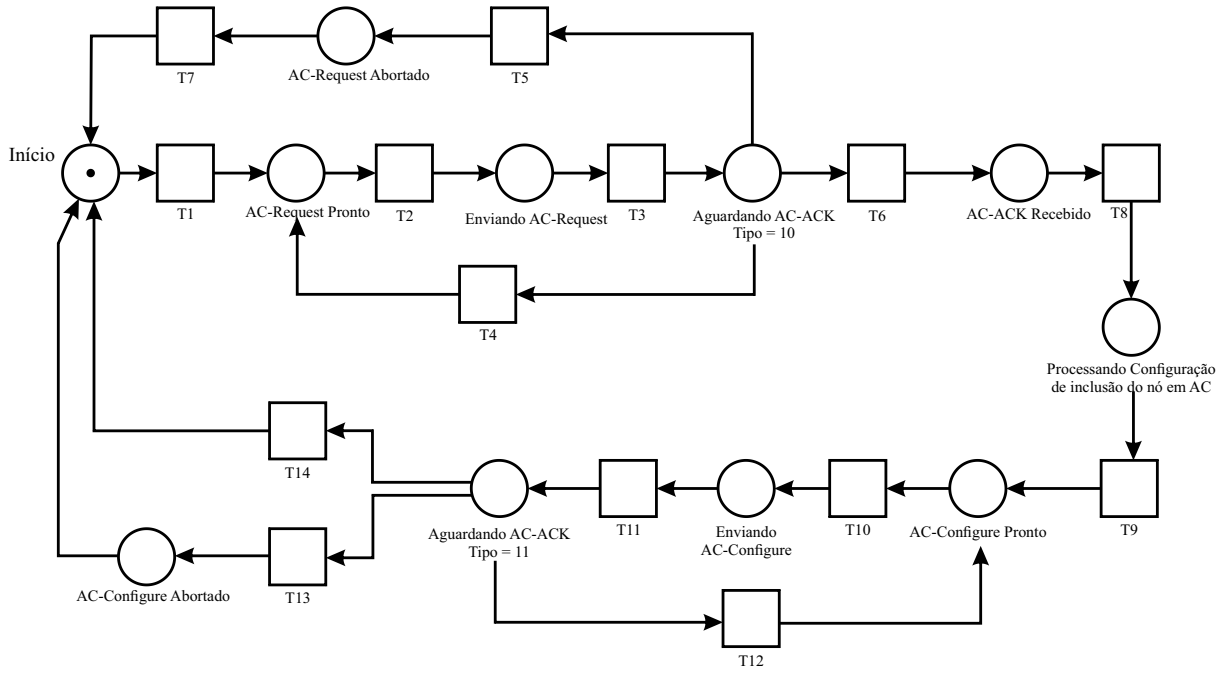


Figura 3.10: Rede de Petri para *Sink Node*.

Em ambos modelos de operação, quando o *Sink Node* está aguardando uma AC-ACK para reconhecimento de uma mensagem, se o tempo de espera for maior que t_m e nenhuma AC-ACK for recebida, é necessária a retransmissão da mensagem em questão. Transições como esta são representadas na Figura 3.10 pelas transições T4 e T12 no modelo de operação no *Sink Node*. Se ocorrerem quatro retransmissões e nenhuma AC-ACK for recebida a operação é abortada, conforme apresentado na Figura 3.10 pelas transições T5 e T13 para as mensagens AC-Request e AC-Configure, respectivamente.

Após um envio de uma AC-ACK, as transições T4 e T9 na Figura 3.11 representam um ciclo voltando para o estado anterior de recebimento da mensagem. Isso significa que antes do tempo t_{ack} uma nova mensagem chegou, significando que a mensagem AC-ACK não chegou ao seu destino e aconteceu uma retransmissão.

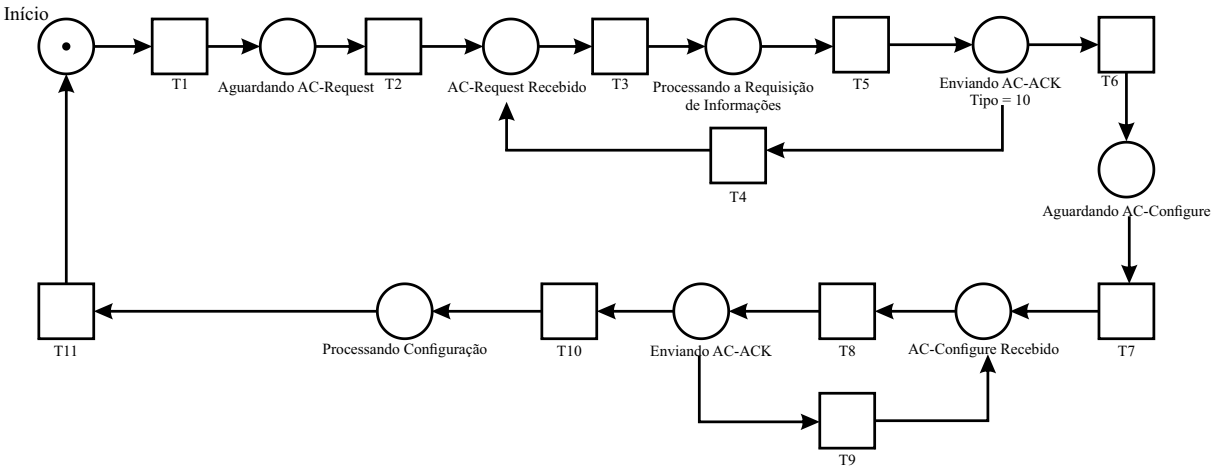


Figura 3.11: Rede de Petri para os demais nós sensores.

As Figuras 3.12 e 3.13 exemplificam a operação do protocolo DCAP, mostrando o funcionamento ideal, onde não existe perda de mensagens e uma situação onde mensagens AC-ACK não são entregues. Vale lembrar que o tempo entre o recebimento de uma AC-Request e o envio de uma AC-ACK é indefinido no nó sensor, assim como o tempo entre o recebimento de uma AC-ACK (Tipo "10") e o envio de uma AC-Configure é também indefinido.

3.2 Exemplos de Aplicações

Como dito anteriormente, são os requisitos da aplicação para a qual foi projetada a rede de sensores que define como será o funcionamento geral do modelo de segurança proposto. Em outras palavras, a quantidade de AC, o posicionamento das AC, bem como a variação do posicionamento delas, quais níveis de confidencialidade existirão e qual será o esquema de segurança adotado são definidos no projeto da aplicação.

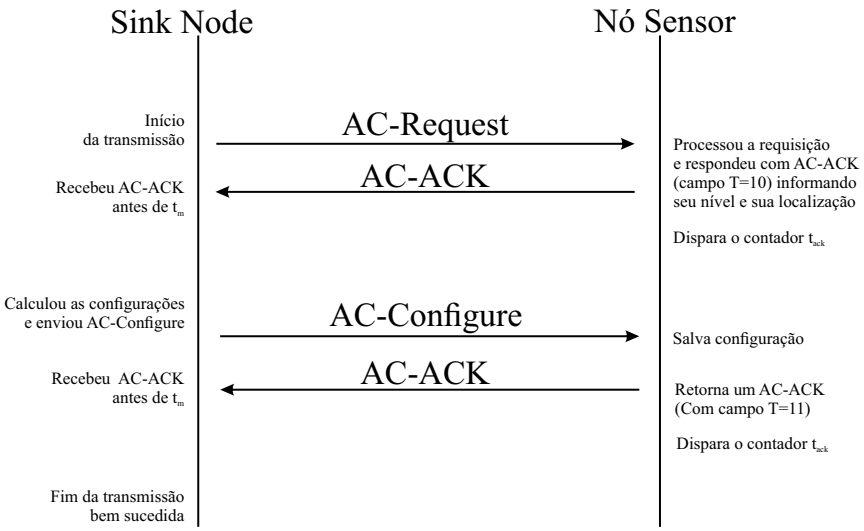


Figura 3.12: Exemplo de operação do protocolo DCAP em uma situação ideal.

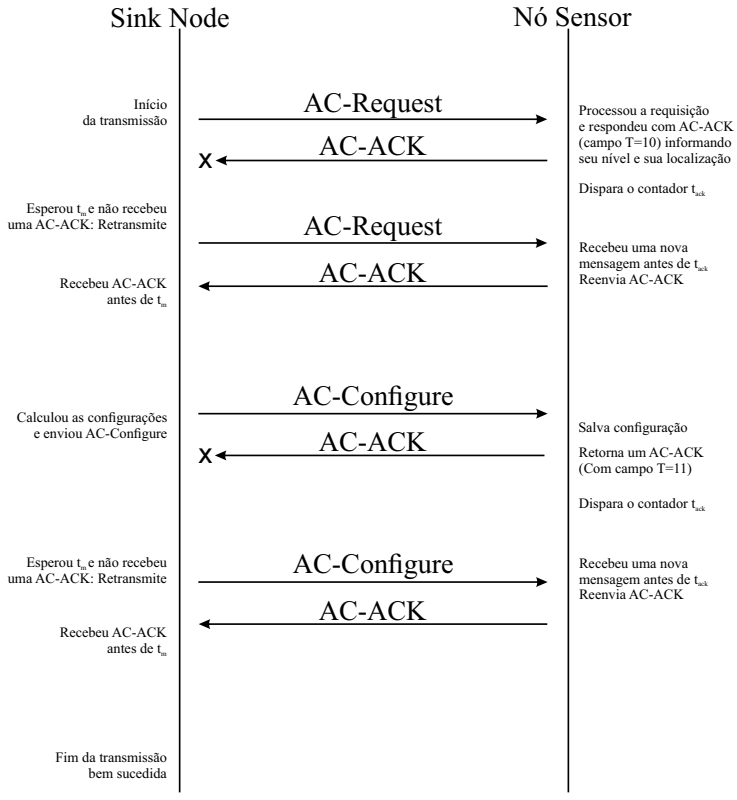


Figura 3.13: Exemplo de operação do protocolo DCAP em uma situação com perdas de AC-ACK.

Assim, pode-se ter vários cenários diferentes para cada tipo de aplicação, existindo uma gama imensa de possíveis configurações do modelo.

Pode-se citar, inicialmente, uma RSVSF que monitora um ambiente industrial. O monitoramento de linhas de produção, maquinários, caldeiras e outros ambientes numa indústria não requerem necessariamente um alto grau de segurança dos dados monitorados. Contudo, pode ser requerido que a RSVSF monitore o acesso à determinadas áreas da indústria para detectar intrusos, invasões ou acesso não autorizado. Esta parte da rede de sensores pode requerer um grau de segurança maior, logo, a aplicação do modelo de criptografia adaptativa pode ser útil para garantir segurança apenas a determinados acessos da indústria, sem necessariamente prover segurança aos demais sensores que monitoram os equipamentos. Assim, obtém-se economia de recursos, pois apenas os nós sensores que necessitam de segurança terão gastos energéticos com criptografia e mecanismos de segurança.

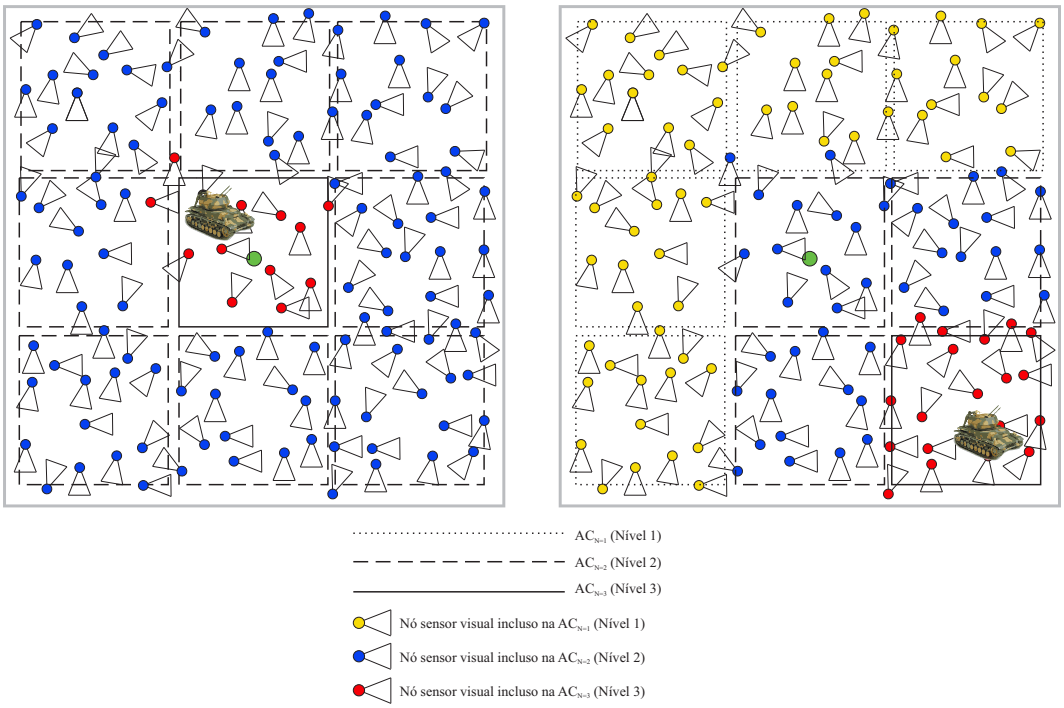


Figura 3.14: Aplicação de RSVSF para monitorar um tanque em um ambiente militar utilizando o modelo de criptografia adaptativa empregando o conceito de área de confidencialidade fixa.

Outro exemplo de aplicação é o monitoramento militar. Um aplicação pode requerer que uma rede de sensores monitore visualmente um ou mais tanques de guerra dentro de um ambiente militar. Assim, todos os dados de imagem dos tanques devem ser criptografados antes de serem enviados na rede. Pode-se concluir que o uso do modelo de criptografia adaptativa pode ser útil para garantir confidencialidade à imagens captadas dos tanques, fazendo com que onde o tanque estiver, em um certo perímetro definido, os nós sensores estejam numa área de confidencialidade nível 3,

e nas proximidades uma área de confidencialidade nível 2. Assim garante-se alta segurança às imagens dos tanques e uma segurança mediana às imagens próximas dele. O restante da rede não executa nenhum mecanismo de segurança, economizando energia de forma global na RSVSF. Contudo, o tanque pode se movimentar dentro de um trajeto conhecido ou não, fazendo com que as áreas de confidencialidade sejam alteradas de posição ao longo do tempo, ou tenham seus níveis de confidencialidade alterados, sendo de forma dinâmica estas alterações, fazendo com que novos sensores passem a criptografar suas imagens coletadas e outros deixem de fazer isso.

A Figura 3.14 apresenta como pode se dar esta mudança do nível de confidencialidade das áreas delimitadas ao decorrer do movimento do tanque no ambiente. Em outras palavras, o conceito de área de confidencialidade permite que exista essa mudança ao longo do tempo ou ao longo do movimento do objeto monitorado, como é o caso do exemplo em questão. A configuração do cenário pode ter áreas de confidencialidade fixas que vão alterando o seu nível ao longo do movimento do tanque, por exemplo, como mostrado na Figura 3.14, ou pode ter áreas de confidencialidade com localização variável ao longo do movimento do objeto.

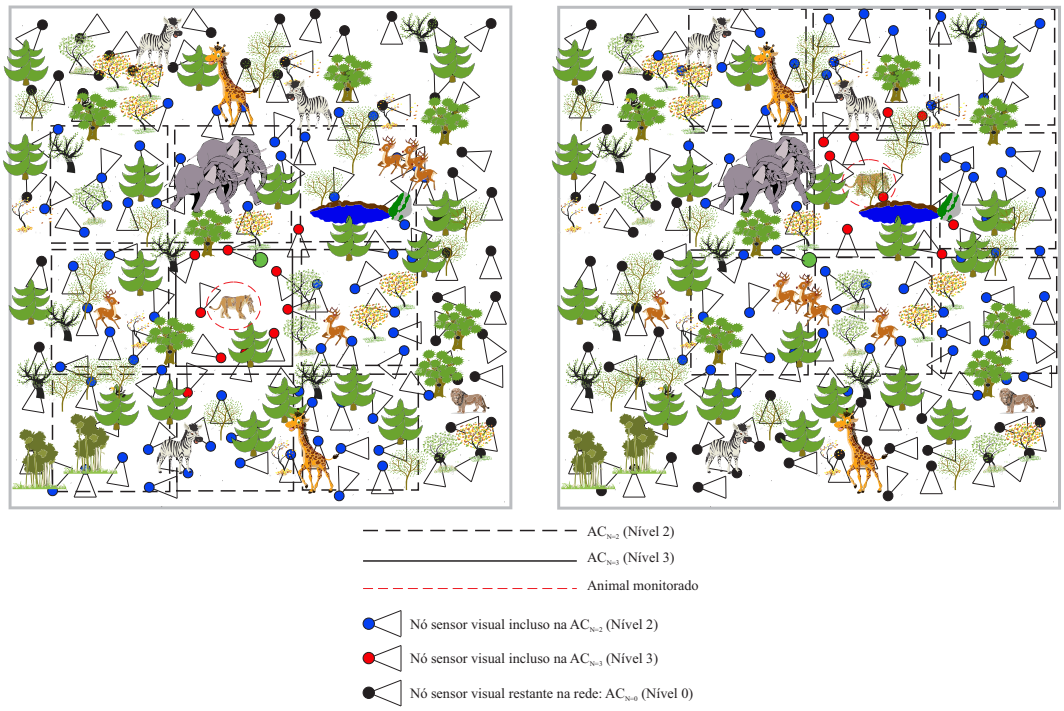


Figura 3.15: Aplicação de RSVSF para monitorar o comportamento de um animal selvagem em seu habitat natural utilizando o modelo de criptografia adaptativa empregando o conceito de área de confidencialidade variável.

Um exemplo similar ao dos tanques numa área militar é o monitoramento de animais selvagens, onde o animal a ser monitorado no seu habitat natural irá se movimentar

aleatoriamente e a área de confidencialidade de mais alto nível terá que ser alterada dinamicamente ao longo do tempo para garantir segurança apenas a dados ou imagens do monitoramento do animal em questão. Neste exemplo, a posição área de confidencialidade poderá ser variável de acordo com o movimento do animal pelo ambiente. A Figura 3.15 apresenta um exemplo de configuração deste cenário.

Vale ressaltar que, a definição de quantidade de níveis e como cada nível se comporta vai depender do projeto da RSVSF e necessariamente dos requisitos da aplicação. Sendo assim, pode-se imaginar uma necessidade de apenas uma AC com nível 3, como por exemplo, no monitoramento de algum objeto, pessoa ou animal no ambiente. Partindo deste pressuposto, pode-se haver a necessidade de segurança máxima dos dados coletados apenas para os nós sensores que estão a volta do objeto monitorado, não existindo a necessidade de prover segurança alguma ao restante da rede. Neste cenário, tem-se apenas uma AC em um nível alto de confidencialidade que pode ter sua posição alterada ao longo do tempo.

Capítulo 4

Resultados

O modelo de criptografia adaptativa visa garantir segurança em diferentes níveis às redes de sensores visuais sem fio (RSVSF) o que pode implicar diretamente em um menor consumo de energia. Partindo deste pressuposto, espera-se que o modelo de criptografia adaptativa seja energeticamente mais eficiente que aplicar um único mecanismo de segurança a todos os nós de uma determinada RSVSF. Em outras palavras, espera-se que ao aplicar o modelo de criptografia adaptativa se garanta segurança diferenciadamente a determinadas áreas, que foram chamadas de áreas de confidencialidade (AC), obtendo-se, assim, uma economia de recursos em relação à forma tradicional de se prover segurança, em que todos os nós sensores da rede aplicam o mesmo mecanismo de segurança aos seus dados coletados.

Nesse trabalho foi definido um modelo matemático cujo objetivo é verificar o comportamento de uma rede de sensores sem fio ao aplicar mecanismos de segurança, visando mensurar o consumo energético ao aplicar tais mecanismos. Na implementação foi utilizado o algoritmo AES [Rijmen e Daemen 2001] para realizar a criptografia e também foram empregados os conceitos da criptografia adaptativa, apresentados no Capítulo 3, para simular o comportamento do modelo ao se tentar prover segurança à rede de sensores proposta na implementação. A seguir são descritos os aspectos da implementação e os critérios utilizados para validação do modelo.

4.1 Ambiente de Validação

Para a validação da solução proposta, foi definido um ambiente para a verificação matemática do modelo de criptografia adaptativa. O objetivo inicial é provar que aplicando os conceitos da solução apresentada no Capítulo 3 obtém-se um consumo energético menor que aplicar um único mecanismo de segurança à rede de sensores como um todo. Optou-se por utilizar o algoritmo de criptografia AES que, por ser

um algoritmo de criptografia simétrico, possui uma baixa sobrecarga de computação. Além disso, os conceitos do modelo teórico de criptografia adaptativa foram simulados, juntamente com as métricas de consumo de energia do algoritmo AES, possibilitando mensurar a economia energética ao aplicar a solução proposta.

4.1.1 AES

O Algoritmo de criptografia AES, do inglês, *Advanced Encryption Standard*, foi criado para ser o sucessor do DES (*Data Encryption Standard*), solucionando algumas falhas que este possui. Assim, o NIST (National Institute of Standard and Technology) realizou um processo de escolha que deu início em 1997 e teve o algoritmo de Rijndael como vencedor em 2000, sendo posteriormente anunciado em 2001 como o algoritmo sucessor do DES, sendo chamado de AES pelo NIST [NIST 2001]. O algoritmo AES funciona com uma entrada de dados de 128 *bits* gerando uma saída de dados também de 128 *bits*, onde essas sequências de 128 *bits* são denominadas blocos. Desde modo, tem-se 16 *bytes*, do *byte* 00 ao *byte* 15, que para facilitar a representação são divididos em quatro partes de 4 *bytes* conforme a figura 4.1 que passa a ser chamada de matriz de estado [Rinaldi 2012]. Diferentemente da entrada e saída o algoritmo AES aceita três tamanhos de chaves 128, 192 e 256 *bits*.

	coluna 0	coluna 1	coluna 2	coluna 3
linha 0	00	04	08	12
linha 1	01	05	09	13
linha 2	02	06	10	14
linha 3	03	07	11	15

Figura 4.1: Representação da matriz estado do algoritmo AES [Rinaldi 2012].

Sobre a matriz de estado são aplicadas quatro operações:

- **Adição de chave de rodada (*AddRoundKey*)**: Realiza um XOR *byte* a *byte* da matriz de estado com a subchave em questão. A subchave é também uma matriz de 16 *bytes*, onde o conjunto de bytes é selecionado a cada rodada a partir da chave expandida;

- **Substituição de bytes (*SubBytes*)**: É a única transformação não-linear do AES. Ela consiste em aplicar uma caixa de substituição em cada *byte* da matriz de estado, onde esta caixa de substituição é uma tabela fixa bidimensional de valores e igual para todas as rodadas [NIST 2001];
- **Deslocamento de linhas (*ShiftRows*)**: Consiste em um deslocamento cíclico dos *bytes* da matriz de estado, sendo cada linha deslocada por um número fixo;
- **Mistura de Colunas (*MixColumns*)**: Consiste numa permutação linear que opera sobre as colunas da matriz de estado. Cada coluna é vista como um polinômio de quatro termos, e então multiplicado em módulo $x^4 + 1$ com um polinômio fixo definido pelos autores do algoritmo: $c(x) = 0x03 * x^3 + 0x01 * x^2 + 0x01 * x + 0x02$. Segundo [Daemen e Rijmen] a escolha foi devido a este polinômio ser coprimo do polinômio $x^4 + 1$, possuindo assim inverso.

O tamanho da chave defini a quantidade de rodadas que o AES efetuará sobre o bloco de entrada, sendo 10, 12 e 14 respectivamente para as chaves de 128, 192, e 256 *bits*. Por isso, a chave necessita passar por um processo de escalonamento que expande sua quantidade de bits para suportar o número de máximo de rodadas. Ao final do processo de expansão a chave expandida resulta em 1408, 1664 e 1920 *bits*, para os respectivos tamanho de chaves 128, 192, e 256 *bits*. O processo matemático da expansão das chaves AES é descrito em detalhes por [Rinaldi 2012].

Por fim, o processo de cifragem do AES, consiste em após expandir a chave AES e montar a matriz de estado com os dados de entrada, realizar as operações de transformação sobre esta matriz por um número de rodadas que varia com o tamanho da chave.

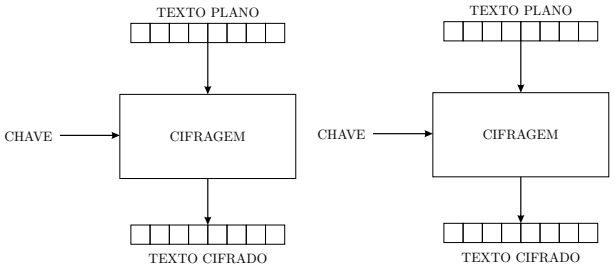
Além disso o AES possui alguns modos de operação. Os quatro modos de operação utilizados na implementação das métricas de consumo são:

- **ECB (*Electronic Code Book*)**: A mensagem é dividida em blocos de texto plano e cada bloco é criptografado separadamente [Rinaldi 2012, Ribeiro e Roiha 2010]. Apesar de ser o mais simples e eficiente tanto em computação quanto em consumo de energia, o modo ECB não é tão seguro, pois para duas entradas de texto plano idênticas é gerada a mesma saída, se utilizada a mesma chave, o que pode ocasionar problemas quanto à confidencialidade;
- **CBC (*Cipher Block Chaining*)**: É o modo de operação mais utilizado pelos algoritmos de cifragem que consistem em combinar textos planos com textos cifrados anteriormente, através de um XOR *byte* a *byte*;
- **CFB (*Cipher Feedback*)**: Este modo utiliza a operação de cifragem para gerar uma saída pseudo randômica de dados. A pós a cifragem é realizado um XOR entre o texto plano e o texto cifrado e este resultado é utilizado como entrada na próxima rodada, por isso o nome de realimentação por cifragem.

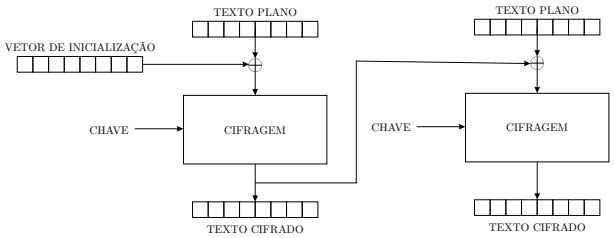
No primeiro momento um vetor de inicialização passa pela cifragem para gerar o texto cifrado que fará o primeiro XOR com o primeiro bloco de texto plano;

- **OFB (*Output Feedback*)**: Este modo é semelhante ao CFB, apenas com uma diferença, ao invés de realimentar a cifragem com o resultado do XOR entre o texto plano e o saída da cifragem, a cifragem é realimentada apenas com a própria saída da cifragem.

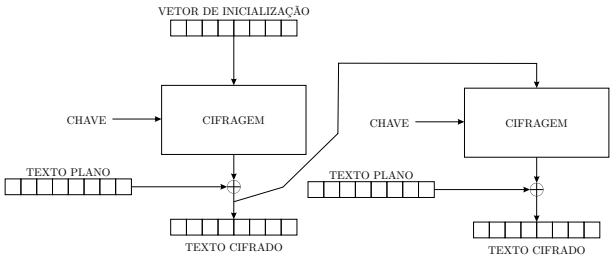
A figura 4.2 resume graficamente os quatro modos de operação.



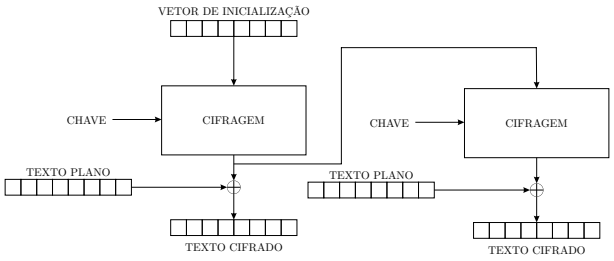
(a) ECB



(b) CBC



(c) CFB



(d) OFB

Figura 4.2: Diagrama de Blocos dos modos AES. Adaptado de [Rinaldi 2012]

4.1.2 Esquemas de Segurança Implementados

Para simular a criptografia adaptativa foram escolhidos dois esquemas de segurança para que seja mostrado que esquemas diferentes podem gerar efeitos diferentes no consumo de energia. Assim, foi adotado um esquema de segurança que varia os níveis da codificação DWT de uma imagem coletada e outro esquema de segurança que varia o tamanho da chave de criptografia do algoritmo AES, conforme listado a seguir:

- **Esquema 1 - Variação de Níveis da Codificação DWT**:
  - Nível 0: Sem criptografia;
  - Nível 1: Criptografia seletiva da imagem (DWT em dois níveis[1]);
  - Nível 2: Criptografia seletiva da imagem (DWT em um nível[2]);
  - Nível 3: Criptografia integral da imagem;
- **Esquema 2 - Tamanho da chave de criptografia AES**:
  - Nível 0: Sem criptografia;
  - Nível 1: Chave de 128 bits;
  - Nível 2: Chave de 192 bits;
  - Nível 3: Chave de 256 bits;

A Figura 4.3 apresenta através de diagramas o primeiro esquema de segurança verificado que varia os níveis de codificação DWT. Assim, os nós sensores localizados na $\mathrm{AC}_{N=3}$ não irão realizar a codificação DWT na imagem, fazendo com que a imagem seja totalmente encriptada, garantindo assim uma segurança maior. Os nós sensores localizados na $\mathrm{AC}_{N=2}$ irão realizar a codificação DWT em um nível e encriptar apenas a sub-camada $LL_{(1)}$, garantindo assim um nível de segurança inferior à $\mathrm{AC}_{N=3}$. Por fim, os nós sensores localizados na $\mathrm{AC}_{N=1}$ irão realizar a codificação DWT em dois níveis e encriptar a sub-camada $LL_{(2)}$, garantindo assim uma segurança inferior às outras duas AC. Os restantes dos nós sensores da rede que não estão em nenhuma AC não realizam nem codificação, nem criptografia.

Com relação ao Esquema 2, em que se varia o tamanho das chaves de criptografia, a Figura 4.4 apresenta o diagrama deste esquema. Sendo assim, pode ser visto na Figura 4.4 que os nós sensores localizados na $\mathrm{AC}_{N=3}$ utilizam o tamanho de chave de 256 *bits* para encriptar as imagens coletadas por eles. Já os nós sensores nas $\mathrm{AC}_{N=2}$ e $\mathrm{AC}_{N=1}$ utilizam o tamanho de chave de 192 e 128 *bits*, respectivamente, para encriptar suas imagens coletadas. Vale lembrar que os nós sensores que não estão localizados em nenhuma AC não realizam criptografia nas imagens coletadas. Além

[1] encriptando $LL_{(2)}$
[2] encriptando $LL_{(1)}$

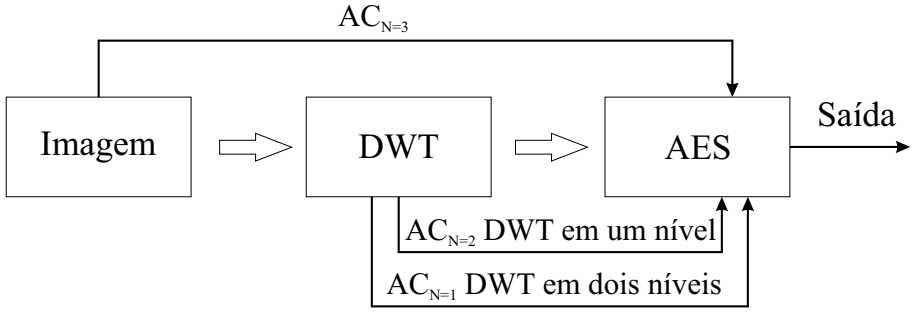


Figura 4.3: Diagrama de implementação do esquema de variação de níveis de codificação DWT.

disso, neste esquema a imagem é criptografada pelos nós pertencentes às AC sem a realização da codificação DWT para gerar sub-camadas, sendo assim, o que varia é apenas o tamanho da chave de criptografia e não o tamanho do dado, como acontece no esquema anterior. Em outras palavras, as imagens coletadas são criptografadas integralmente não havendo nenhum tipo de codificação.

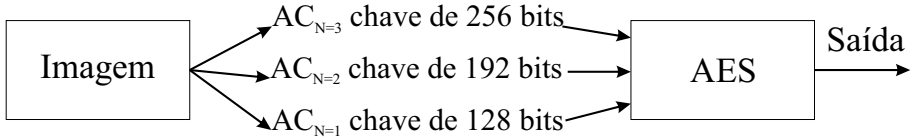


Figura 4.4: Diagrama de implementação do esquema de variação de tamanho de chaves de criptografia.

4.1.3 Consumo Energético

No software MATLAB [MATLAB 2015] foram implementados os conceitos do modelo matemático para que fosse possível verificar seu comportamento. Desta forma, foram criadas funções para mensurar o consumo energético dos nós sensores ao realizar a criptografia de imagens coletadas. Em relação às áreas de confidencialidade somente é informada a quantidade de sensores em cada área. Sendo assim, não é diferenciada a posição, quantidade e local das determinadas AC. Além disso, as especificações das imagens coletadas são inseridas como parâmetros para as funções relacionando a resolução da imagem e profundidade de cor em *bits* para definir o tamanho de cada imagem.

Da mesma forma, vale ressaltar que não foi implementado o algoritmo AES, e sim o seu comportamento quanto ao consumo, tomando como parâmetros o tamanho do dado a ser encriptado e o tamanho das chaves. Segundo [Potlapally et al. 2006], o consumo energético de um algoritmo simétrico pode ser dado pela Equação 4.1 mostrada a seguir:

$$CustoEnergia_{(Si)} = EChave_{(Si)} + (EByte_{(Si)} * Tamanho_{(Dado)}), \quad (4.1)$$

Na Equação 4.1, $EChave_{(Si)}$ representa o custo de energia para expandir a chave simétrica para o algoritmo Si. A energia gasta por *byte* na encriptação/decriptação usando o algoritmo Si é dada por $EByte_{(Si)}$, e $Tamanho_{(Dado)}$ é o tamanho total do dado a ser encriptado pelo algoritmo Si. Utilizando esta equação é possível, conhecendo as variantes de consumo, mensurar o consumo energético de qualquer algoritmo de criptografia simétrico. Sendo assim, é possível modelar o consumo energético do algoritmo AES, como mostrado na Equação 4.2:

$$CustoEnergia_{(AES)} = EChave_{(AES)} + (EByte_{(AES)} * Tamanho_{(Dado)}) \quad (4.2)$$

Como na implementação dos cenários de validação só existe a necessidade de mensurar o consumo nos nós sensores fontes, o valor de $EByte_{(AES)}$ somente tem a necessidade de representar o processo de encriptação, sendo assim, o $CustoEnergia_{(AES)}$ representa apenas o gasto energético nesse processo.

Os valores referentes às variantes $EChave_{(AES)}$ e $EByte_{(AES)}$ são descritos por [Potlapally et al. 2006] e foram tomados como base para a implementação da função de consumo energético de encriptação do algoritmo AES, como mostrado na Tabela 4.1, levando em conta os modos de operação do algoritmo AES.

Tabela 4.1: Custo energético das variantes AES [Potlapally et al. 2006].

Tamanho da Chave (bits)	$EChave_{(AES)}$ (μJ)	$EByte_{(AES)}$ em modo ECB (μJ/B)	$EByte_{(AES)}$ em modo CBC (μJ/B)	$EByte_{(AES)}$ em modo CFB (μJ/B)	$EByte_{(AES)}$ em modo OFB (μJ/B)
128	7.83	1.21	1.62	1.91	1.62
192	7.87	1.42	2.08	2.30	1.83
256	9.92	1.64	2.29	2.31	2.05

Os parâmetros que foram necessários para implementação e validação do modelo de criptografia adaptativa são descritos a seguir:

- **Quantidade de Sensores:** é a quantidade total de sensores da rede;
- **Tempo de execução:** tempo total em que a rede está executando, ou seja, coletando dados e encriptando mediante os demais parâmetros;
- **Intervalo de tempo:** é o intervalo de tempo utilizado para desenhar o gráfico;
- **Frequência de Transmissão:** é a quantidade de imagens que são coletadas, criptografadas e transmitidas por cada nó sensor fonte;
- **Esquema de Segurança:** esquema de segurança adotado pelo modelo de criptografia para realizar a diferenciação. As opções implementadas para teste e validação foram *Variação de Níveis da Codificação DWT* (Esquema 1) e *Variação do Tamanho de Chaves de Criptografia* (Esquema 2);

- **Quantidade de sensores na $AC_{N=1}$:** é a quantidade de sensores localizados em alguma AC com o nível de confidencialidade igual a 1 realizando criptografia;
- **Quantidade de sensores na $AC_{N=2}$:** é a quantidade de sensores localizados em alguma AC com o nível de confidencialidade igual a 2 realizando criptografia;
- **Quantidade de sensores na $AC_{N=3}$:** é a quantidade de sensores localizados em alguma AC com o nível de confidencialidade igual a 3 realizando criptografia;
- **Resolução da imagem coletada:** significa a resolução da imagem a ser criptografada e é utilizada para saber o tamanho do dado a ser encriptado;
- **Profundidade de cor da imagem coletada:** significa o esquema de cor da imagem a ser criptografada e juntamente com a resolução é utilizado para saber o tamanho do dado a ser encriptado;
- **Algoritmo de Criptografia:** variação dos modos de operação AES. Opções implementadas:
  1. Modo ECB (*Electronic Code Book*);
  2. Modo CBC (*Cipher Block Chaining*);
  3. Modo CFB (*Cipher Feedback*);
  4. Modo OFB (*Output Feedback*);
- **Tamanho da Chave:** tamanho da chave de criptografia AES que é utilizado ao escolher o esquema de variação de níveis da codificação DWT. Ao escolher o esquema de variação de chave de criptografia este campo não é utilizado;
- **Esquema de medição:** é a forma como o gráfico será desenhado, ou seja, se deve plotar a comparação entre as AC ou de modo geral considerando a rede como um todo sem aplicação do modelo e com a aplicação do modelo de criptografia adaptativa.

4.2 Resultados Numéricos

Como forma de validar o modelo de criptografia adaptativa proposto, foram montados alguns cenários que exemplificam possíveis configurações para RSVSF. Os parâmetros apresentados na seção 4.1 foram alterados de cenário para cenário com o propósito de criar situações para que seja mensurado o consumo energético. Os quatro primeiros cenários têm seus gráficos relacionando consumo energético dentro de cada área de confidencialidade em função do tempo. Além disso, no primeiro e no segundo cenário foi aplicado o esquema de segurança de variação de níveis de

codificação DWT, enquanto no terceiro e no quarto cenário foi aplicado o esquema de segurança de variação de tamanho de chaves de criptografia, que no caso como foi aplicado o algoritmo AES essas chaves variaram em 128, 192 e 256 *bits*. Os três últimos cenários têm seus gráficos comparando o consumo total da RSVSF com e sem a aplicação do modelo proposto em relação ao tempo, sendo possível perceber a economia energética alcançada com a criptografia adaptativa.

Vale ressaltar que, o tempo de execução das medidas de consumo em todos os cenários foi estabelecido em 100 horas e o intervalo de tempo de cada análise realizada para construir o gráfico foi fixado em 10 horas. Além disso, a frequência de transmissão foi fixada em uma imagem por segundo para todos os cenários, ou seja, cada nó sensor fonte coleta, encripta e transmite apenas uma imagem a cada segundo da execução da aplicação. Desta forma, o consumo medido nos cenários de validação é referente ao consumo nos nós sensores fonte pelo processo de encriptação. Nas próximas subseções são detalhados os cenários de validação e os resultados obtidos.

4.2.1 Cenário 1

O primeiro cenário define uma configuração de uma RSVSF contendo 500 nós sensores. As imagens coletadas tiveram a resolução de 128x128 *pixels* num esquema de cor de 8 *bits*. Desta forma, é possível calcular o tamanho em *bytes* das imagens, que na situação seria de 16384 *Bytes* cada. Além disso, foi utilizado o algoritmo AES no modo ECB para realizar a criptografia com o tamanho de chave de 128 *bits*. Cada AC teve sua quantidade de nós sensores estabelecida em 125, cada uma. Para fins de uma melhor representação e significância dos resultados as AC foram configuradas com o mesmo número de nós, ressaltando que todos os nós de cada AC foram considerados nós sensores fonte ativos, ou seja, todos eles coletam, criptografam e transmitem imagens a todo o tempo, não ficando nenhum deles em estado de dormência.

A Figura 4.5 apresenta um gráfico de consumo de energia nas fontes em função do tempo, comparando os resultados para AC com níveis diferentes de confidencialidade. A Tabela 4.2 apresenta um resumo de toda a configuração deste primeiro cenário.

Pode-se notar na Figura 4.5 que o consumo de energia na $AC_{N=3}$ foi superior a 600 Joules, sendo muito superior ao das outras duas AC. A linha traçada em vermelho mostra o consumo de energia na $AC_{N=3}$, a linha em azul o consumo de energia na $AC_{N=2}$ e a linha em verde o consumo de energia na $AC_{N=1}$. Vale ressaltar que, as $AC_{N=2}$ e $AC_{N=1}$, ou seja, as AC que empregam os níveis de confidencialidade igual a 2 e 1, realizaram a codificação das imagens coletadas em DWT, em um e dois níveis, respectivamente, enquanto a $AC_{N=3}$ não realizou a codificação DWT para criptografá-las.

Tabela 4.2: Parâmetros utilizados no Cenário 1.

Parâmetro	**Valor**
Quantidade total de nós sensores	500
Quantidade de nós sensores na $AC_{N=1}$	125
Quantidade de nós sensores na $AC_{N=2}$	125
Quantidade de nós sensores na $AC_{N=3}$	125
Frequência de Transmissão	1 imagem/s
Resolução das imagens coletadas	128x128 *pixels*
Profundidade de Cor das imagens coletadas	8 *bits*
Algoritmo de criptografia	AES no modo ECB
Tamanho da chave de criptografia	128 *bits*
Esquema de Segurança	Variação de níveis de codificação DWT

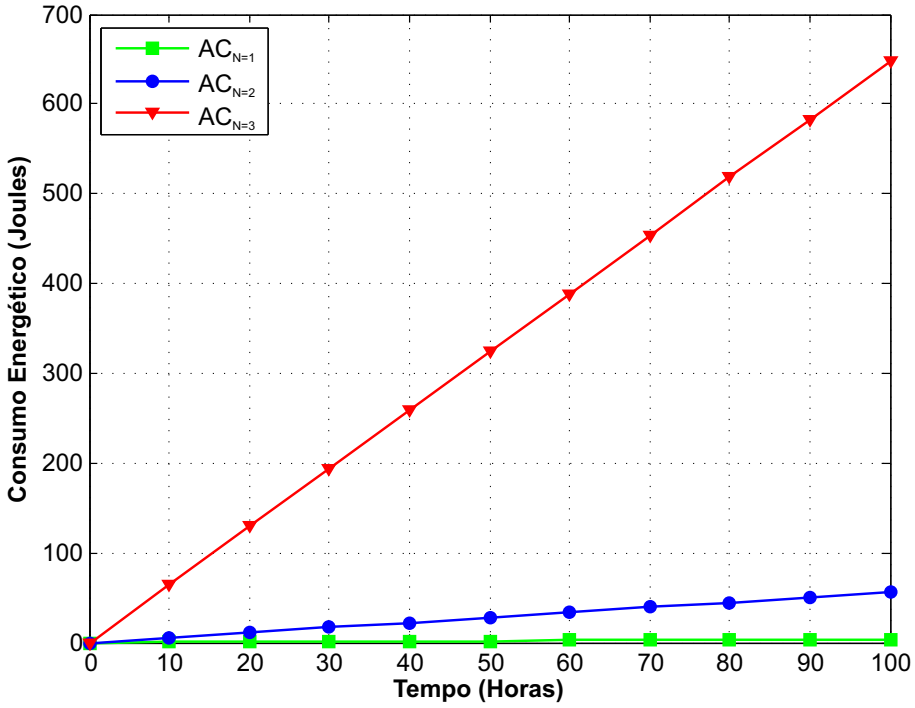


Figura 4.5: Validação: Gráfico do Cenário 1.

4.2.2 Cenário 2

O segundo cenário é bem semelhante ao primeiro cenário, somente com uma variação das imagens coletadas e do tamanho da chave de criptografia. Assim como no primeiro cenário foi aplicado o esquema de segurança de variação de níveis de codificação DWT, onde $AC_{N=2}$ e $AC_{N=1}$ aplicam DWT nas imagens coletadas em um e dois níveis, respectivamente. O cenário foi configurado também com 500 nós sensores, a criptografia sendo realizada pelo algoritmo AES no modo ECB, só que com o tamanho de chave sendo agora 256 *bits*. As imagens coletadas possuem uma resolução de 256x256 *pixels* em um esquema de cor de 4 *bits*, formando assim imagens de 32768 *bytes* de tamanho cada. A quantidade de nós sensores fonte ativos

nas AC foram as mesmas do primeiro cenário, igual e fixada em 125. A Figura 4.6 apresenta o gráfico de consumo de energia nas fontes em função do tempo, com esta configuração, comparando os resultados para AC com níveis diferentes de confidencialidade. A seguir, na Tabela 4.3, é apresentado um resumo de toda a configuração do segundo cenário:

Tabela 4.3: Parâmetros utilizados no Cenário 2.

Parâmetro	**Valor**
Quantidade total de nós sensores	500
Quantidade de nós sensores na $AC_{N=1}$	125
Quantidade de nós sensores na $AC_{N=2}$	125
Quantidade de nós sensores na $AC_{N=3}$	125
Frequência de Transmissão	1 imagem/s
Resolução das imagens coletadas	256x256 *pixels*
Profundidade de Cor das imagens coletadas	4 *bits*
Algoritmo de criptografia	AES no modo ECB
Tamanho da chave de criptografia	256 *bits*
Esquema de Segurança	Variação de níveis de codificação DWT

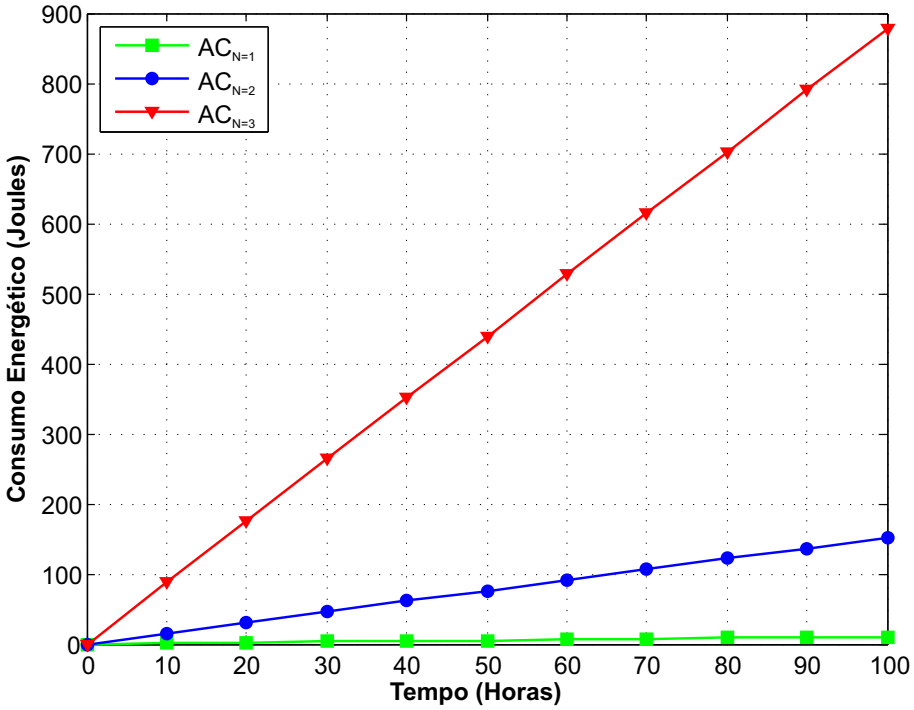


Figura 4.6: Validação: Gráfico do Cenário 2.

O consumo de energia na $AC_{N=3}$ aumentou em relação ao primeiro cenário, passando agora para quase 900 Joules. Isso é devido ao aumento do tamanho da chave de criptografia e do tamanho das imagens a serem criptografadas. O consumo das outras AC também aumentou em relação ao primeiro cenário. Todavia, realizando uma breve análise do gráfico apresentado na Figura 4.6, pode ser visto que a diferença

de consumo entre as AC existe, ou seja, é garantida a segurança em níveis diferentes com economia de energia mediante os requisitos da aplicação. No gráfico mostrado nesta mesma figura, a linha vermelha representa o consumo de energia da $AC_{N=3}$, a linha azul da $AC_{N=2}$ e a linha verde da $AC_{N=1}$.

4.2.3 Cenário 3

No terceiro cenário foi aplicado o segundo esquema de segurança implementado que varia as chaves de criptografia. A rede de sensores foi configurada com 600 nós sensores, sendo que 90 deles estão localizados na $AC_{N=1}$, outros 90 na $AC_{N=2}$ e outros 90 na $AC_{N=3}$, todos nós sensores ativos. As imagens coletadas possuíram uma resolução de 128x128 *pixels* em um esquema de cor de 4 *bits*, tendo um tamanho de 8192 *bytes* cada. Novamente, vale ressaltar, que a frequência de transmissão dos nós sensores fonte é uma imagem por segundo. O algoritmo de criptografia foi o AES no modo ECB. A variação de chaves, assim como foi descrita na Seção 4.1, foi de 128 *bits* na $AC_{N=1}$, 192 *bits* na $AC_{N=2}$ e 256 *bits* na $AC_{N=3}$. Além disso, vale ressaltar, que as imagens são criptografadas integralmente não havendo nenhum tipo de codificação. A Figura 4.7 apresenta um gráfico de consumo de energia nas fontes em função do tempo, comparando os resultados para AC com níveis diferentes de confidencialidade. A seguir, na Tabela 4.4, é apresentado um resumo de toda a configuração do terceiro cenário:

Tabela 4.4: Parâmetros utilizados no Cenário 3.

Parâmetro	**Valor**
Quantidade total de nós sensores	600
Quantidade de nós sensores na $AC_{N=1}$	90
Quantidade de nós sensores na $AC_{N=2}$	90
Quantidade de nós sensores na $AC_{N=3}$	90
Frequência de Transmissão	1 imagem/s
Resolução das imagens coletadas	128x128 *pixels*
Profundidade de Cor das imagens coletadas	4 *bits*
Algoritmo de criptografia	AES no modo ECB
Esquema de Segurança	Variação de Tamanho de Chaves

Novamente foi possível perceber que houve um maior consumo de energia na $AC_{N=3}$, por aplicar um nível maior de segurança. No gráfico apresentado na Figura 4.7 é possível perceber que o consumo de energia na $AC_{N=3}$ foi de quase 450 Joules sendo representado pela linha vermelha, na $AC_{N=2}$ foi superior a 350 Joules sendo representado pela linha azul e na $AC_{N=1}$ foi superior a 300 Joules sendo representado pela linha verde. Desta forma, é possível afirmar que também neste esquema de segurança houve uma redução de consumo de energia com a aplicação de níveis de segurança diferenciados.

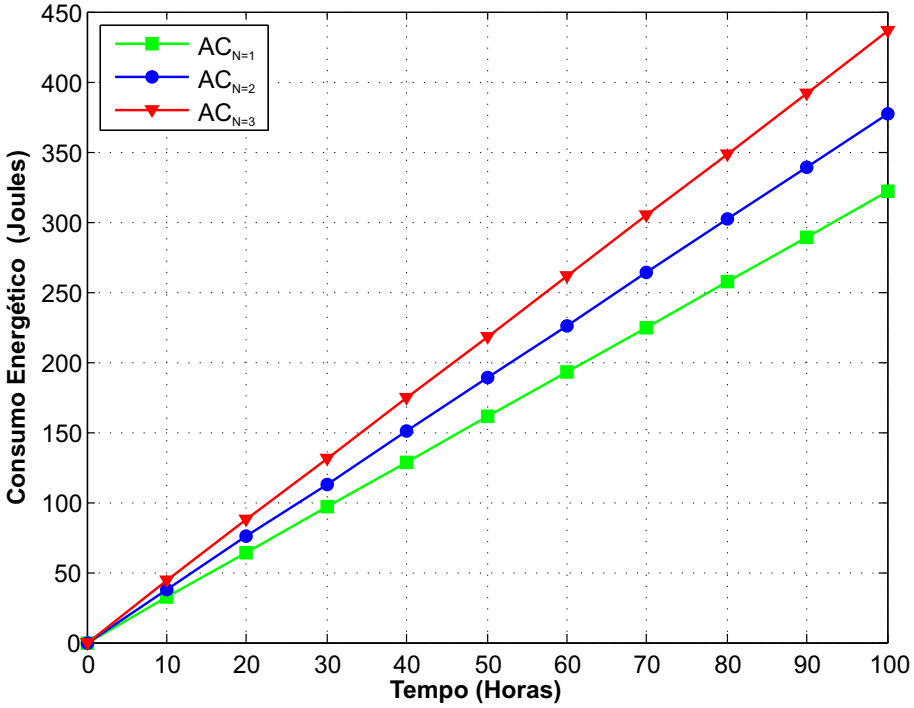


Figura 4.7: Validação: Gráfico do Cenário 3.

4.2.4 Cenário 4

O quarto cenário também emprega o esquema de segurança de variação de chaves de criptografia, apenas com algumas mudanças de configuração em relação ao cenário anterior. Apenas foi diferenciado o modo do algoritmo AES que foi alterado para operar no modo CBC. A Figura 4.8 apresenta um gráfico de consumo de energia nas fontes em função do tempo, comparando os resultados para AC com níveis diferentes de confidencialidade. A seguir, na Tabela 4.5, é apresentado um resumo de toda a configuração deste quarto cenário:

Tabela 4.5: Parâmetros utilizados no Cenário 4.

Parâmetro	**Valor**
Quantidade total de nós sensores	600
Quantidade de nós sensores na $AC_{N=1}$	90
Quantidade de nós sensores na $AC_{N=2}$	90
Quantidade de nós sensores na $AC_{N=3}$	90
Frequência de Transmissão	1 imagem/s
Resolução das imagens coletadas	128x128 *pixels*
Profundidade de Cor das imagens coletadas	4 *bits*
Algoritmo de criptografia	AES no modo CBC
Esquema de Segurança	Variação de Tamanho de Chaves

Desta forma, foi possível concluir que o algoritmo AES no modo ECB é mais eficiente energeticamente que no modo CBC. Além disso, segundo [Potlapally et al. 2006], o

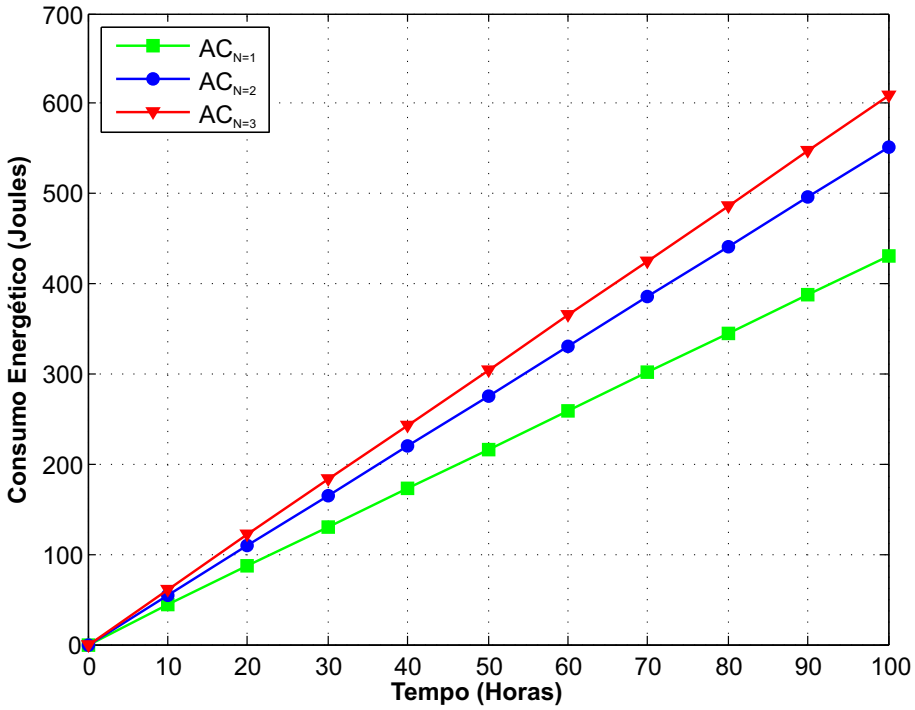


Figura 4.8: Validação: Gráfico do Cenário 4.

algoritmo AES no modo ECB é mais eficiente que os outros quatro modos mais comuns do algoritmo AES. Contudo o algoritmo AES no modo ECB é mais vulnerável, em relação à segurança, que nos demais modos que empregam a forma de encriptação por cadeia de bloco [Dworkin 2001]. A maior desvantagem do AES no modo ECB é que para dois textos planos idênticos é gerada uma mesma saída da cifragem, o que pode ocasionar problemas na segurança e por isso este modo não é aconselhável. Como não é objetivo da pesquisa a análise dos modos de operação do AES, nem quanto à eficiência nem quanto à vulnerabilidade, o modo ECB foi utilizado em alguns cenários.

Mesmo assim, é possível comparar a eficiência dos modos de encriptação do algoritmo AES com este cenário. O consumo de energia na $AC_{N=3}$ neste quarto cenário foi em torno de 600 Joules, já no terceiro cenário com a mesma configuração a $AC_{N=3}$ consumiu pouco menos que 450 Joules. No gráfico apresentado na Figura 4.8, a linha vermelha representa o consumo de energia da $AC_{N=3}$, a linha azul o consumo de energia da $AC_{N=2}$ e a linha verde o consumo de energia da $AC_{N=1}$.

4.2.5 Cenário 5

O quinto cenário foi configurado com as AC com quantidade de nós sensores ativos diferentes, as imagens coletadas tiveram a resolução de 128x128 *pixels* em um esquema de cor de 8 *bits*, gerando imagens de 16384 *bytes* de tamanho cada. A

criptografia foi realizada pelo algoritmo AES no modo CBC com tamanho de chave de 128 *bits*. Além disso, o esquema de segurança foi a variação de níveis de codificação DWT. O objetivo deste cenário é comparar o consumo total da RSVSF com e sem a utilização da criptografia adaptativa. A Figura 4.9 apresenta um exemplo de disposição das AC na configuração realizada neste quinto cenário.

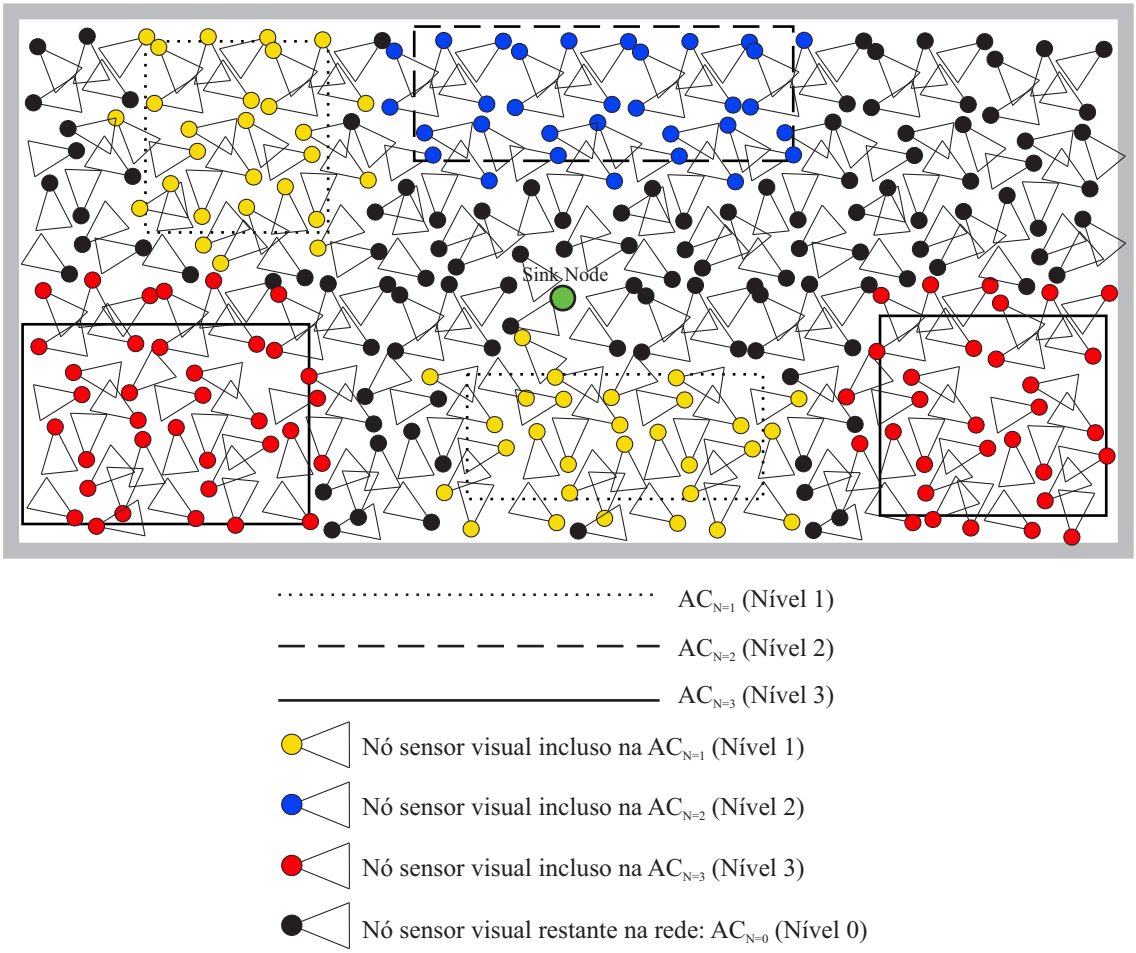


Figura 4.9: Exemplo de configuração das AC em uma RSVSF no Cenário 5.

Desta forma, a Figura 4.10 apresenta um gráfico de consumo de energia nas fontes em função do tempo, comparando agora o consumo de energia total dos nós sensores fonte da rede sem aplicação da criptografia adaptativa com o consumo de energia total dos nós sensores fonte da rede aplicando a criptografia adaptativa, para o exemplo de configuração apresentado na Figura 4.9. Vale ressaltar que, a verificação do consumo de energia da RSVSF sem a criptografia adaptativa foi realizada aplicando o nível máximo de segurança do esquema a todos os nós sensores da rede. A Tabela 4.6 apresenta um resumo de toda a configuração deste quinto cenário.

É possível perceber no gráfico apresentado na Figura 4.10 que o consumo de energia na simulação da rede de sensores com aplicação da criptografia adaptativa é bem

Tabela 4.6: Parâmetros utilizados no Cenário 5.

Parâmetro	**Valor**
Quantidade total de nós sensores	270
Quantidade de nós sensores na $AC_{N=1}$	46
Quantidade de nós sensores na $AC_{N=2}$	32
Quantidade de nós sensores na $AC_{N=3}$	67
Frequência de Transmissão	1 imagem/s
Resolução das imagens coletadas	128x128 *pixels*
Profundidade de Cor das imagens coletadas	8 *bits*
Algoritmo de criptografia	AES no modo CBC
Tamanho da chave de criptografia	128 *bits*
Esquema de Segurança	Variação de níveis de codificação DWT

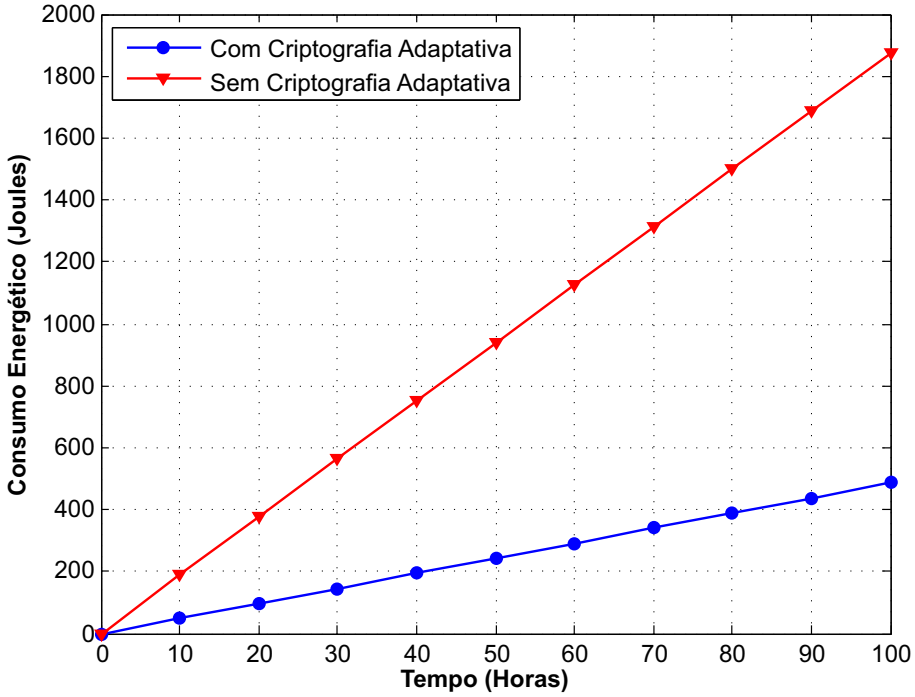


Figura 4.10: Validação: Gráfico do Cenário 5.

inferior à configuração em que não foi aplicada. A diferença neste cenário foi de cerca de 1400 Joules de economia. A linha vermelha representa a configuração sem a criptografia adaptativa e a linha azul representa a configuração aplicando a criptografia adaptativa nos parâmetros citados anteriormente.

4.2.6 Cenário 6

O sexto cenário é uma comparação ao quinto cenário. Apenas foram alteradas as quantidades de nós sensores nas AC, com o mesmo tamanho das imagens coletadas, o mesmo algoritmo de criptografia no mesmo modo, o mesmo tamanho de chave e o

mesmo esquema de segurança. A Figura 4.11 apresenta uma RSVSF com uma possível disposição das AC com os parâmetros deste sexto cenário. É possível perceber que em relação ao quinto cenário a quantidade de AC, a localização e disposição das AC mudaram. Contudo para o cálculo do consumo o que tem maior relevância é a quantidade de nós sensores em cada AC, pois o consumo é medido na fonte.

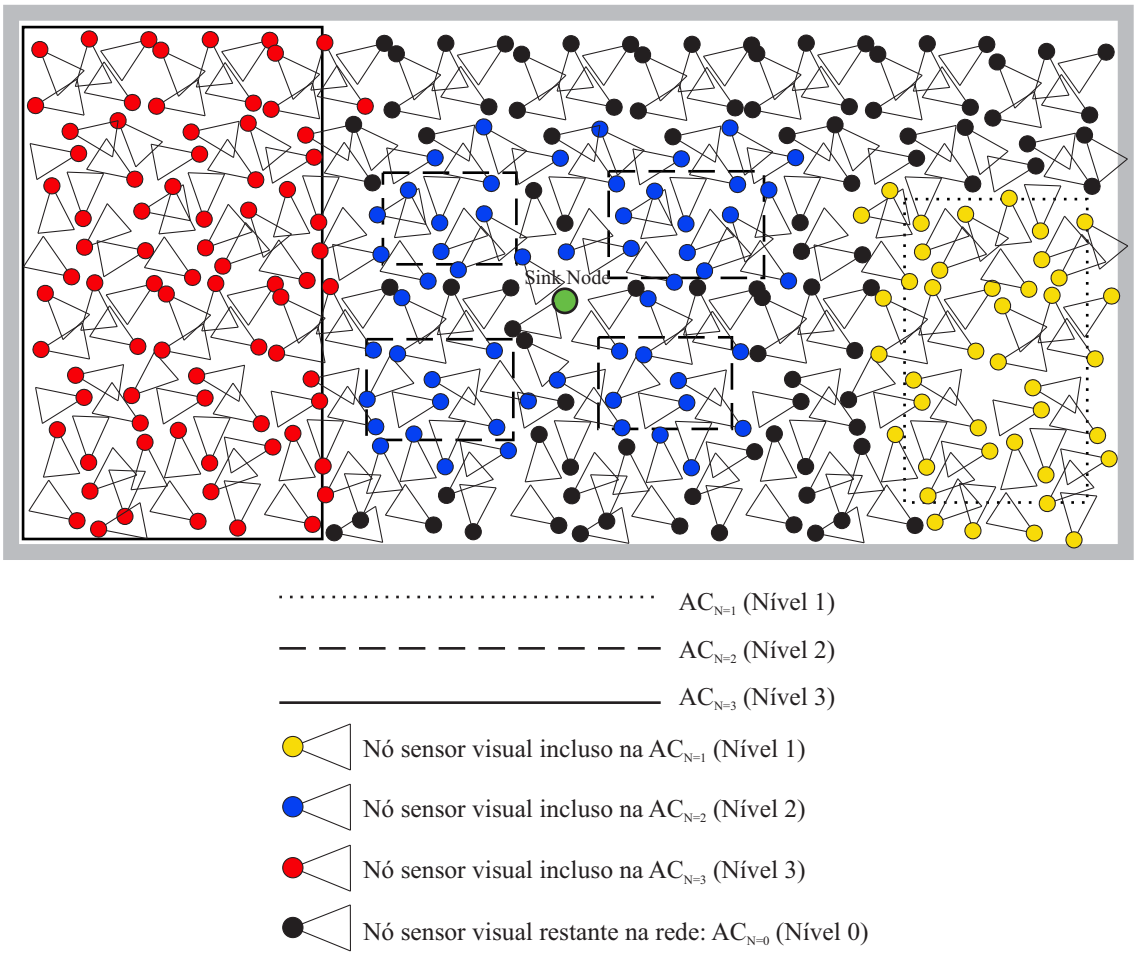


Figura 4.11: Exemplo de configuração das AC em uma RSVSF no sexto cenário.

A Figura 4.12 apresenta um gráfico de consumo de energia nas fontes em função do tempo, comparando novamente o consumo de energia total da rede sem aplicação da criptografia adaptativa com o consumo de energia total da rede aplicando a criptografia adaptativa. É possível perceber novamente que ao aplicar a criptografia adaptativa o consumo de energia total da rede é reduzido substancialmente em relação ao consumo de energia total da rede sem a criptografia adaptativa. Nota-se que o consumo de energia total sem a criptografia adaptativa é o mesmo que no quinto cenário cerca de 1900 Joules. Com a mudança da configuração das AC, como pode ser reparado nas Figuras 4.9 e 4.11, o consumo de energia da solução com a criptografia adaptativa neste sexto cenário é um pouco maior que no quinto cenário, exatamente devido a esta mudança. A seguir, na Tabela 4.7, é apresentado um

resumo de toda a configuração deste sexto cenário:

Tabela 4.7: Parâmetros utilizados no Cenário 6.

Parâmetro	**Valor**
Quantidade total de nós sensores	270
Quantidade de nós sensores na $AC_{N=1}$	41
Quantidade de nós sensores na $AC_{N=2}$	56
Quantidade de nós sensores na $AC_{N=3}$	79
Frequência de Transmissão	1 imagem/s
Resolução das imagens coletadas	128x128 *pixels*
Profundidade de Cor das imagens coletadas	8 *bits*
Algoritmo de criptografia	AES no modo CBC
Tamanho da chave de criptografia	128 *bits*
Esquema de Segurança	Variação de níveis de codificação DWT

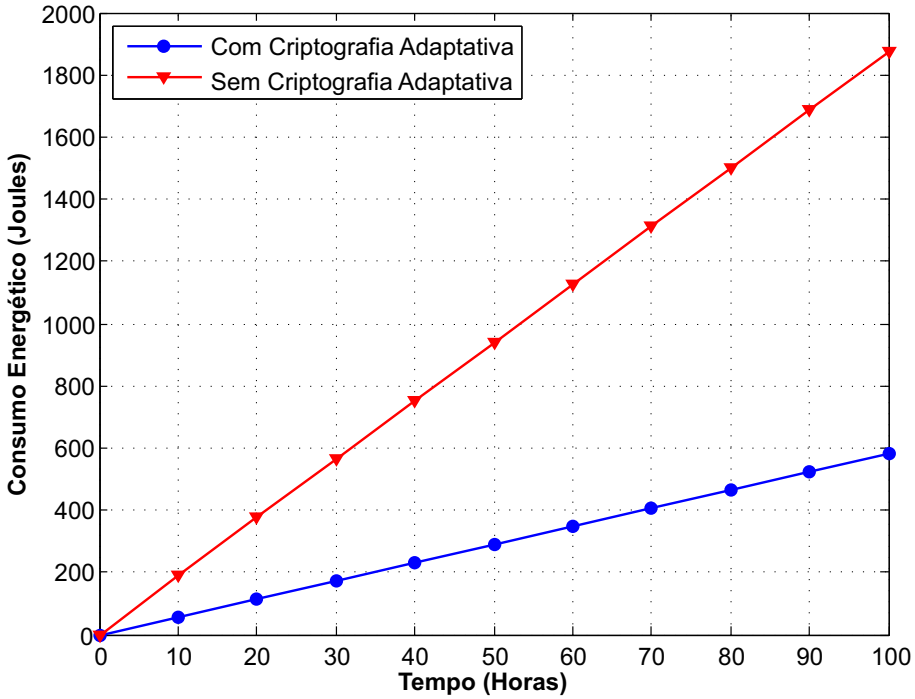


Figura 4.12: Validação: Gráfico do Cenário 6.

4.3 Cenário 7

Este sétimo cenário foi realizado em nível de comparação com o cenário anterior, sendo apenas alterado o esquema de segurança para o Esquema 2, que varia o tamanho de chaves para cada nível de confidencialidade diferente. Sendo assim, o restante da configuração deste sétimo cenário é igual à do cenário anterior, a mesma

quantidade de nós sensores ativos em cada AC, o mesmo tamanho das imagens coletadas e o mesmo algoritmo de criptografia no mesmo modo. Vale ressaltar, que as imagens coletadas são criptografadas integralmente não havendo nenhum tipo de codificação. A Figura 4.11 ilustra também uma possível disposição dos nós sensores numa RSVSF igualmente ao sexto cenário. A seguir, na Tabela 4.8, é apresentado um resumo de toda a configuração deste sétimo cenário:

Tabela 4.8: Parâmetros utilizados no Cenário 7.

Parâmetro	**Valor**
Quantidade total de nós sensores	270
Quantidade de nós sensores na $AC_{N=1}$	41
Quantidade de nós sensores na $AC_{N=2}$	56
Quantidade de nós sensores na $AC_{N=3}$	79
Frequência de Transmissão	1 imagem/s
Resolução das imagens coletadas	128x128 *pixels*
Profundidade de Cor das imagens coletadas	8 *bits*
Algoritmo de criptografia	AES no modo CBC
Esquema de Segurança	Variação de Tamanho de Chaves

Na Figura 4.13, é possível perceber que o consumo de energia total da rede aumentou tanto aplicando a criptografia adaptativa quanto aplicando um mesmo mecanismo de segurança para a rede como um todo, em relação ao cenário anterior. Este aumento é em parte pelo fato das chaves de criptografia serem variadas e ao aplicar segurança sem a criptografia adaptativa ser empregado o algoritmo AES com a maior chave possível para ele, 256 *bits*. Além disso, em toda criptografia realizada neste Cenário 7, foram utilizas as imagens coletadas com tamanho integral, e no cenário anterior houve a aplicação do DWT que reduz o tamanho das imagens, gerando uma menor sobrecarga no processo de criptografia e consequentemente um menor consumo.

Entretanto, é possível perceber que variando também o esquema de segurança pode-se obter uma economia de recursos e energia significante para a RSVSF. A Figura 4.13 apresenta um gráfico de consumo de energia nas fontes em função do tempo, comparando o consumo de energia total da rede sem aplicação da criptografia adaptativa com o consumo de energia total da rede aplicando a criptografia adaptativa, para este cenário. Assim, neste caso, a economia foi em torno de 1000 Joules.

4.3.1 Análise dos Resultados

Após a verificação dos cenários é possível concluir, inicialmente, que ao aplicar o modelo de criptografia adaptativa a uma RSVSF conseguiu-se obter segurança em diferentes níveis para diferentes áreas da rede de sensores o que pode ser útil para diversas aplicações. Além disso, provendo segurança desta maneira obteve-se uma economia de recursos da rede implicando principalmente em energia, em relação à aplicação de um único mecanismo de segurança à RSVSF como um todo.

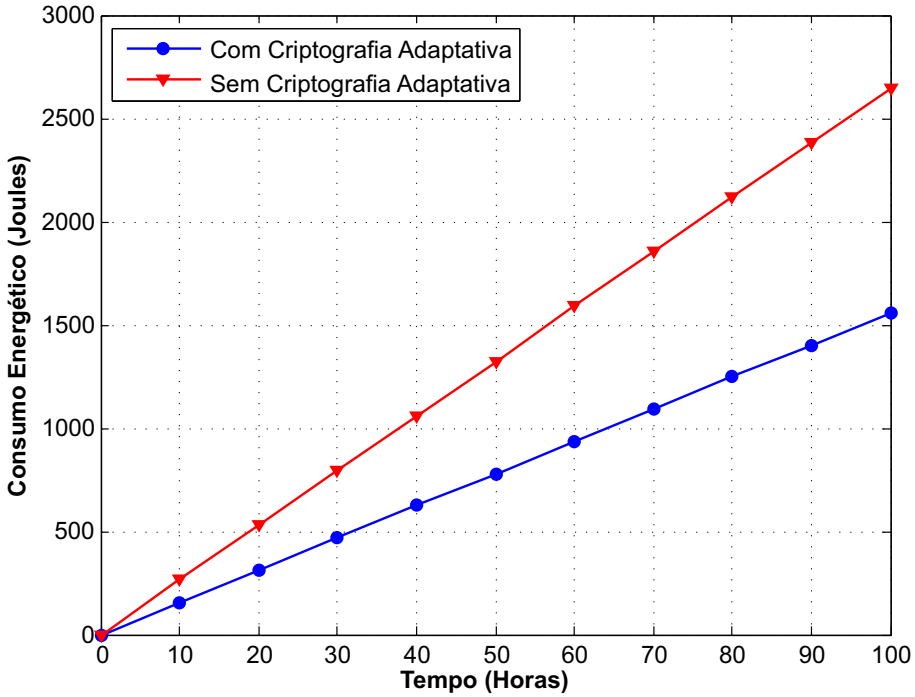


Figura 4.13: Validação: Gráfico do Cenário 7.

Nos quatro primeiros cenários foi realizada uma comparação da energia consumida dentro das AC, podendo provar que o consumo é diferenciado de uma AC para outra a depender do nível de confidencialidade empregado. Sendo assim, estes cenários, apesar de terem variáveis diferentes, tiveram aspectos em comum, como por exemplo, a quantidade de nós sensores ativos dentro de cada AC com nível de confidencialidade diferentes. Esta premissa foi adicionada para validar melhor os cenários, onde $AC_{N=3}$, $AC_{N=2}$ e $AC_{N=1}$ tendo o mesmo número de nós sensores ativos têm o comparativo do consumo voltado para o aspecto de segurança empregado, não sendo deturpado pela diferença da quantidade de sensores em cada tipo de AC. É possível notar também, que em cada cenário isoladamente, o tamanho das imagens coletadas e criptografadas pelos sensores também é o mesmo. Então, pode-se afirmar que os resultados de cada um destes quatro primeiros cenários são referentes ao consumo energético variando apenas a forma como cada tipo de AC emprega o mecanismo de segurança.

Por outro lado, os cenários 5 e 6 tentam empregar uma situação mais real, onde a quantidade de nós sensores ativos em cada tipo de AC é diferente. Assim, é possível perceber o ganho em economia de energia total da rede de sensores simulando situações mais comuns de acontecer. Vale ressaltar também que, o tamanho das imagens coletadas, o tamanho da chave de criptografia, o algoritmo de criptografia utilizado e o esquema de segurança empregado foi o mesmo para os dois cenários, variando apenas as quantidades de nós sensores ativos em cada tipo de AC. Desta forma, o comparativo entre a aplicação da criptografia adaptativa para uma RSVSF utili-

zando o Esquema 1 proposto e a aplicação de um único mecanismo para a RSVSF como um todo, apresenta claramente, no Cenário 5 e no Cenário 6, que houve um menor consumo de energia total da rede ao aplicar o modelo de criptografia adaptativa.

Por fim, o Cenário 7 apenas realiza um comparativo com o Cenário 6, onde alterou-se o esquema de segurança, sendo nesse sétimo cenário o Esquema 2, onde varia-se o tamanho das chaves de criptografia para cada nível de confidencialidade, para uma mesma configuração das AC. Assim, é possível perceber que aplicando a criptografia adaptativa em esquemas diferentes obtém-se sempre uma economia de recursos e energia. O objetivo deste último cenário é comprovar que assim como o consumo energético varia em relação à disposição das AC, referente à quantidade de nós sensores ativos criptografando e transmitindo dentro de cada Área com o nível de confidencialidade diferente, o consumo energético também varia a depender do esquema de segurança adotado.

Em resumo, é possível afirmar, de forma geral, que os resultados apresentados nesta seção são válidos e comprovam a redução de consumo energético pelo modelo de criptografia adaptativa proposto.

Capítulo 5

Considerações Finais

Redes de sensores sem fio ainda são um tema bastante relevante e emergente que vem ganhando a atenção do mundo todo cada vez mais devido à vasta gama de aplicações possíveis e do surgimento de novas necessidades tecnológicas e de novas soluções. Pesquisas nesta área têm sido cada vez mais corriqueiras e têm agregado a cada dia mais pessoas, instituições e ramos da indústria interessados em desenvolver e criar soluções para projetos de RSSF. Nós sensores com câmeras embutidas aumentam significantemente a complexidade dos projetos, aumentando também a necessidade de novas soluções para problemas até então simples e para outros problemas que surgem devido a natureza do dado coletado. As RSVSF são capazes de coletar muito mais informações do ambiente em que os nós sensores estão inseridos para monitoramento ou rastreamento, elevando assim a complexidade para quaisquer tipo de aplicações e de projeto.

Prover segurança tanto em RSSF quanto em RSVSF é algo muito desafiador devido às vulnerabilidades intrinsecamente existentes nessas redes e devido também à escassez de recursos nos nós sensores da rede. Desta forma, aspectos de segurança são bastante importantes e relevantes no projeto de uma rede de sensores onde, a restrição de recursos torna inadequada a utilização de mecanismos de segurança conhecidos, devido a alta sobrecarga de computação e comunicação, o que abre uma margem para o surgimento de novos paradigmas e mecanismos de segurança específicos para redes de sensores.

O modelo proposto por esta dissertação de mestrado explora exatamente esta lacuna existente entre garantir segurança às redes de sensores e as restrições de recursos existentes nestas redes. Como as RSVSF apresentam um aspecto mais desafiador devido à existência de nós sensores com câmeras e uma maior representatividade do ambiente monitorado, o modelo matemático, chamado de Criptografia Adaptativa, foi inicialmente proposto para este tipo de rede com o foco em imagens estáticas como dado coletado. Entretanto, apesar de não ser necessariamente genérico, este modelo pode ser adequado a qualquer tipo de RSSF, atingindo os mesmos objetivos, que se concentram em prover segurança economizando os recursos da rede, necessitando

apenas de adequações e ajustes para cada tipo de rede de sensores, o que pode ser considerado uma linha de trabalhos futuros desta pesquisa.

Partindo do presuposto que aplicações diferentes podem ter necessidades de segurança diferentes, o trabalho apresentado por esta dissertação explora a diferenciação de áreas como conceito principal para, então, empregar medidas de segurança diversificadas para áreas diferentes de uma mesma RSVSF. Estas áreas de confidencialidade foram definidas pelo modelo, onde são empregadas as medidas de segurança apenas pelos nós sensores pertencentes a tais áreas, seguindo a lógica de níveis. Foram estabelecidos inicialmente três níveis de confidencialidade que geram esta diversidade entre as áreas mencionadas anteriormente. Por fim, o modelo prevê que sejam adotados e propostos pelo projetista esquemas de segurança onde serão definidos os mecanismos ou medidas de seguranças adotados em cada nível de confidencialidade e, sucessivamente, adotados pelos sensores inclusos em cada área de confidencialidade que possuir tal nível. Como forma de exemplificar, alguns esquemas de segurança foram propostos neste trabalho, no entanto outros podem ser adaptados pelo projetista a depender da necessidade da aplicação.

Como dito anteriormente, adaptações a este modelo poderão ser realizadas a fim de abranger o âmbito das RSSF e RSMSF, assim como redes de sensores móveis. Além disso, os conceitos apresentados por esta dissertação independem da topologia da rede e do padrão de comunicação, onde estes conceitos podem ser adaptados em pesquisas futuras às mais diversas situações, sendo uma característica importante para ser abordada. Ainda como trabalhos futuros, a implementação e teste da criptografia adaptativa em redes de sensores em ambientes reais é algo necessário para o futuro e completa verificação do modelo.

Por fim, é possível concluir que os resultados apresentados pelo trabalho foram bastante satisfatórios, comprovando que o modelo de criptografia adaptativa pode ser uma opção viável para garantir segurança de forma energeticamente eficiente, sempre a depender das necessidades da aplicação.

Referências Bibliográficas

[Akyildiz et al. 2007] Akyildiz, I. F., Melodia, T., e Chowdhury, K. R. (2007). A survey on wireless multimedia sensor networks. *Computer networks*, 51(4):921–960.

[Akyildiz et al. 2002] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., e Cayirci, E. (2002). A survey on sensor networks. *Communications magazine, IEEE*, 40(8):102–114.

[Almalkawi et al. 2010] Almalkawi, I. T., Zapata, M. G., Al-Karaki, J. N., e Morillo-Pozo, J. (2010). Wireless multimedia sensor networks: current trends and future directions. *Sensors*, 10(7):6662–6717.

[Baronti et al. 2007] Baronti, P., Pillai, P., Chook, V. W., Chessa, S., Gotta, A., e Hu, Y. F. (2007). Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and zigbee standards. *Computer communications*, 30(7):1655–1695.

[Bluetooth 1998] Bluetooth (1998). Bluetooth special interest group.

[Cao e Abdelzaher 2006] Cao, Q. e Abdelzaher, T. (2006). Scalable logical coordinates framework for routing in wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 2(4):557–593.

[Čapkun et al. 2002] Čapkun, S., Hamdi, M., e Hubaux, J.-P. (2002). Gps-free positioning in mobile ad hoc networks. *Cluster Computing*, 5(2):157–167.

[Caruso et al. 2005] Caruso, A., Chessa, S., De, S., e Urpi, A. (2005). Gps free coordinate assignment and routing in wireless sensor networks. In *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, volume 1, pp. 150–160. IEEE.

[Chang et al. 2004] Chang, J., Kolla, A., e Kapoor, S. (2004). Security threats in wireless sensor network.

[Cheng e Li 2000] Cheng, H. e Li, X. (2000). Partial encryption of compressed images and videos. *Signal Processing, IEEE Transactions on*, 48(8):2439–2451.

[Chew et al. 2008] Chew, L. W., Ang, L.-M., e Seng, K. P. (2008). Survey of image compression algorithms in wireless sensor networks. In *Information Technology, 2008. ITSim 2008. International Symposium on*, volume 4, pp. 1–9. IEEE.

[Coppersmith 1994] Coppersmith, D. (1994). The data encryption standard (des) and its strength against attacks. *IBM journal of research and development*, 38(3):243–250.

[Costa e Guedes 2010] Costa, D. G. e Guedes, L. A. (2010). The coverage problem in video-based wireless sensor networks: A survey. *Sensors*, 10(9):8215–8247.

[Costa e Guedes 2011] Costa, D. G. e Guedes, L. A. (2011). A survey on multimedia-based cross-layer optimization in visual sensor networks. *Sensors*, 11(5):5439–5468.

[Costa e Guedes 2012a] Costa, D. G. e Guedes, L. A. (2012a). A discrete wavelet transform (dwt)-based energy-efficient selective retransmission mechanism for wireless image sensor networks. *Journal of Sensor and Actuator Networks*, 1(1):3–35.

[Costa e Guedes 2012b] Costa, D. G. e Guedes, L. A. (2012b). Energy-efficient visual monitoring based on the sensing relevancies of source nodes for wireless image sensor networks. In *Sensors Applications Symposium (SAS), 2012 IEEE*, pp. 1–6. IEEE.

[Costa e Guedes 2013] Costa, D. G. e Guedes, L. A. (2013). Exploiting the sensing relevancies of source nodes for optimizations in visual sensor networks. *Multimedia tools and applications*, 64(3):549–579.

[Costa et al. 2012a] Costa, D. G., Guedes, L. A., Vasques, F., e Portugal, P. (2012a). A routing mechanism based on the sensing relevancies of source nodes for time-critical applications in visual sensor networks. In *Wireless Days (WD), 2012 IFIP*, pp. 1–6. IEEE.

[Costa et al. 2013] Costa, D. G., Guedes, L. A., Vasques, F., e Portugal, P. (2013). Adaptive monitoring relevance in camera networks for critical surveillance applications. *International Journal of Distributed Sensor Networks*, 2013:1–14.

[Costa et al. 2015] Costa, D. G., Guedes, L. A., Vasques, F., e Portugal, P. (2015). A generic energy-efficient protocol for wireless sensor network applications without response time constraints. *RTIC - Revista de Tecnologia da Informação e Comunicação*, 5(1):1–6.

[Costa et al. 2012b] Costa, D. G., Guedes, L. A., Vasques, F., Portugal, P., e Valle, O. T. (2012b). A semi-reliable energy-efficient retransmission mechanism based on the sensing relevancies of source nodes for wireless image sensor networks. In *Wireless Communication Systems (ISWCS), 2012 International Symposium on*, pp. 506–510. IEEE.

[Costa et al. 2014] Costa, D. G., Silva, I., Guedes, L. A., Portugal, P., e Vasques, F. (2014). Selecting redundant nodes when addressing availability in wireless visual sensor networks. In *Industrial Informatics (INDIN), 2014 12th IEEE International Conference on*, pp. 130–135. IEEE.

[Daemen e Rijmen] Daemen, J. e Rijmen, V. The design of rijndael: Aes the advanced encryption standard. *Static Instruction Count (NIOS) Static Instruction Count (this work) Dynamic Instr. Count (NIOS) Dynamic Instr. Count (this work) Percentage of Instr. w/true predicates*.

[Dubois-Ferriere et al. 2005] Dubois-Ferriere, H., Estrin, D., e Vetterli, M. (2005). Packet combining in sensor networks. In *Proceedings of the 3rd international conference on Embedded networked sensor systems*, pp. 102–115. ACM.

[Dworkin 2001] Dworkin, M. (2001). Special publication 800-38a: Recommendation for block cipher modes of operation. *National Institute of Standards, US Department of Commerce*.

[Fluhrer et al. 2001] Fluhrer, S., Mantin, I., e Shamir, A. (2001). Weaknesses in the key scheduling algorithm of rc4. In *Selected areas in cryptography*, pp. 1–24. Springer.

[Fonseca et al. 2005] Fonseca, R., Ratnasamy, S., Zhao, J., Ee, C. T., Culler, D., Shenker, S., e Stoica, I. (2005). Beacon vector routing: Scalable point-to-point routing in wireless sensornets. In *Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2*, pp. 329–342. USENIX Association.

[Gao et al. 2005] Gao, T., Greenspan, D., e Welsh, M. (2005). Improving patient monitoring and tracking in emergency response. In *Proceedings of the International Conference on Information Communication Technologies in Health*.

[Gaubatz et al. 2005] Gaubatz, G., Kaps, J.-P., Ozturk, E., e Sunar, B. (2005). State of the art in ultra-low power public key cryptography for wireless sensor networks. In *Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on*, pp. 146–150. IEEE.

[Grangetto et al. 2006] Grangetto, M., Magli, E., e Olmo, G. (2006). Multimedia selective encryption by means of randomized arithmetic coding. *Multimedia, IEEE Transactions on*, 8(5):905–917.

[Guerrero-Zapata et al. 2010] Guerrero-Zapata, M., Zilan, R., Barceló-Ordinas, J. M., Bicakci, K., e Tavli, B. (2010). The future of security in wireless multimedia sensor networks. *Telecommunication Systems*, 45(1):77–91.

[Hankerson et al. 2004] Hankerson, D., Vanstone, S., e Menezes, A. J. (2004). *Guide to elliptic curve cryptography*. Springer.

[Hill et al. 2000] Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D., e Pister, K. (2000). System architecture directions for networked sensors. In *ACM SIGOPS operating systems review*, volume 34, pp. 93–104. ACM.

[Hu et al. 2003] Hu, Y.-C., Perrig, A., e Johnson, D. B. (2003). Packet leashes: a defense against wormhole attacks in wireless networks. In *INFOCOM 2003.*

Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, volume 3, pp. 1976–1986. IEEE.

[Hu et al. 2006] Hu, Y.-C., Perrig, A., e Johnson, D. B. (2006). Wormhole attacks in wireless networks. *Selected Areas in Communications, IEEE Journal on*, 24(2):370–380.

[IEEE 2003a] IEEE (2003a). Institute of electrical and electronics engineers, inc., ieee std. 802.15.4-2003, wireless medium access control (mac) and physical layer (phy) specifications for low rate wireless personal area networks (lr-wpans). In *IEEE Press*, New York.

[IEEE 2003b] IEEE (2003b). Standard 802.15.3, wireless medium access control (mac) and physical layer (phy) specifications for high rate wireless person area networks (wpans).

[Intanagonwiwat et al. 2000] Intanagonwiwat, C., Govindan, R., e Estrin, D. (2000). Directed diffusion: a scalable and robust communication paradigm for sensor networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pp. 56–67. ACM.

[ISA100.11a 2009] ISA100.11a (2009). Isa100.11a standard.

[Joseph e Vijayan 2014] Joseph, J. e Vijayan, V. P. (2014). Misdirection attack in wsn due to selfish nodes; detection and suppression using longer path protocol. *International Journal of Advanced Research in Computer Science and Software Engineering*, 4(7):825–829.

[Koblitz 1987] Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209.

[Kundur et al. 2008] Kundur, D., Luh, W., Okorafor, U. N., e Zourntos, T. (2008). Security and privacy for distributed multimedia sensor networks. *Proceedings of the IEEE*, 96(1):112–130.

[Lai e Massey 1991] Lai, X. e Massey, J. L. (1991). A proposal for a new block encryption standard. In *Advances in Cryptology-EUROCRYPT'90*, pp. 389–404. Springer.

[Lenstra e Verheul 2001] Lenstra, A. K. e Verheul, E. R. (2001). Selecting cryptographic key sizes. *Journal of cryptology*, 14(4):255–293.

[Liu 2006] Liu, J.-L. (2006). Efficient selective encryption for jpeg 2000 images using private initial table. *Pattern Recognition*, 39(8):1509–1517.

[Mahmoud et al. 2013] Mahmoud, N. E., Taha, M. H., Saroit, I. A., et al. (2013). A secure energy efficient schema for wireless multimedia sensor networks. *CiiT International Journal of Wireless Communication*, 5(6).

[Malan et al. 2004a] Malan, D., Fulford-Jones, T., Welsh, M., e Moulton, S. (2004a). Codeblue: An ad hoc sensor network infrastructure for emergency medical care.

In *International workshop on wearable and implantable body sensor networks*, volume 5.

[Malan et al. 2004b] Malan, D. J., Welsh, M., e Smith, M. D. (2004b). A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography. In *Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on*, pp. 71–80. IEEE.

[MATLAB 2015] MATLAB (1984-2015). The mathworks, inc.

[Miller 1986] Miller, V. (1986). Use of elliptic curves in cryptography. In *Advances in Cryptology-CRYPTO'85 Proceedings*, pp. 417–426. Springer.

[Min et al. 2001] Min, R., Bhardwaj, M., Cho, S.-H., Shih, E., Sinha, A., Wang, A., e Chandrakasan, A. (2001). Low-power wireless sensor networks. In *VLSI Design, 2001. Fourteenth International Conference on*, pp. 205–210. IEEE.

[Moore et al. 2004] Moore, D., Leonard, J., Rus, D., e Teller, S. (2004). Robust distributed network localization with noisy range measurements. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pp. 50–61. ACM.

[NIST 2001] NIST (2001). Federal information process standard publication 197: Announcing the advanced encryption standard (aes).

[Pfarrhofer e Uhl 2005] Pfarrhofer, R. e Uhl, A. (2005). Selective image encryption using jbig. In *Communications and Multimedia Security*, pp. 98–107. Springer.

[Podesser et al. 2002] Podesser, M., Schmidt, H.-P., e Uhl, A. (2002). Selective bit-plane encryption for secure transmission of image data in mobile environments. In *Proceedings of the 5th IEEE Nordic Signal Processing Symposium (NORSIG'02)*, pp. 4–6.

[Potlapally et al. 2006] Potlapally, N. R., Ravi, S., Raghunathan, A., e Jha, N. K. (2006). A study of the energy consumption characteristics of cryptographic algorithms and security protocols. *Mobile Computing, IEEE Transactions on*, 5(2):128–143.

[Rabin 1979] Rabin, M. O. (1979). Digitalized signatures and public key functions as intractable as factorization. Massachusetts Institute of Technology.

[Raju e Akbani 2003] Raju, G. e Akbani, R. (2003). Elliptic curve cryptosystem and its applications. In *Systems, Man and Cybernetics, 2003. IEEE International Conference on*, volume 2, pp. 1540–1543. IEEE.

[Raza et al. 2009] Raza, S., Slabbert, A., Voigt, T., e Landernas, K. (2009). Security considerations for the wirelesshart protocol. In *Emerging Technologies & Factory Automation, 2009. ETFA 2009. IEEE Conference on*, pp. 1–8. IEEE.

[Ribeiro e Roiha 2010] Ribeiro, C. H. C. e Roiha, L. H. (2010). Estudo comparativo dos modos de operação de confidencialidade: um overview para iniciantes. *Revista Ciência e Tecnologia*, 8(13).

[Rijmen e Daemen 2001] Rijmen, V. e Daemen, J. (2001). Advanced encryption standard. *Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology*, pp. 19–22.

[Rinaldi 2012] Rinaldi, G. D. (2012). Análise do aes e sua criptoanálise diferencial.

[Rivest et al. 1978] Rivest, R. L., Shamir, A., e Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126.

[Sadourny e Conan 2003] Sadourny, Y. e Conan, V. (2003). A proposal for supporting selective encryption in jpsec. *Consumer Electronics, IEEE Transactions on*, 49(4):846–849.

[Sarma e Kar 2008] Sarma, H. K. D. e Kar, A. (2008). Security threats in wireless sensor networks. *Aerospace and Electronic Systems Magazine, IEEE*, 23(6):39–45.

[Sen 2009] Sen, J. (2009). A survey on wireless sensor network security. *International Journal of Communication Networks & Information Security*, 1(2).

[Sheikh e Mahmoud 2012] Sheikh, O. M. e Mahmoud, S. A. (2012). *Wireless Sensor Networks - Technology and Protocols*, chapter Cross-Layer Design for Smart Routing in Wireless Sensor Networks. InTech.

[Silva et al. 2013] Silva, D. L. I., Duarte, A., Guedes, L. A., Aquino, L., e Saito, K. (2013). Tecnologias emergentes para redes industriais sem fio: Wirelesshart vs isa100. 11a.

[Simmons 1979] Simmons, G. J. (1979). Symmetric and asymmetric encryption. *ACM Computing Surveys (CSUR)*, 11(4):305–330.

[Simon et al. 2004] Simon, G., Maróti, M., Lédeczi, Á., Balogh, G., Kusy, B., Nádas, A., Pap, G., Sallai, J., e Frampton, K. (2004). Sensor network-based countersniper system. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pp. 1–12. ACM.

[Soares 2012] Soares, S. A. F. (2012). Rede de sensores sem fio para localização e monitoramento de pequenos ruminantes.

[Song et al. 2008] Song, J., Han, S., Mok, A. K., Chen, D., Lucas, M., e Nixon, M. (2008). Wirelesshart: Applying wireless technology in real-time industrial process control. In *Real-Time and Embedded Technology and Applications Symposium, 2008. RTAS'08. IEEE*, pp. 377–386. IEEE.

[Steere et al. 2000] Steere, D. C., Baptista, A., McNamee, D., Pu, C., e Walpole, J. (2000). Research challenges in environmental observation and forecasting systems.

In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pp. 292–299. ACM.

[Strobach 1991] Strobach, P. (1991). Quadtree-structured recursive plane decomposition coding of images. *Signal Processing, IEEE Transactions on*, 39(6):1380–1397.

[Szewczyk et al. 2004] Szewczyk, R., Mainwaring, A., Polastre, J., Anderson, J., e Culler, D. (2004). An analysis of a large scale habitat monitoring application. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pp. 214–226. ACM.

[Wagner 2004] Wagner, D. (2004). Resilient aggregation in sensor networks. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pp. 78–87. ACM.

[Wander et al. 2005] Wander, A. S., Gura, N., Eberle, H., Gupta, V., e Shantz, S. C. (2005). Energy analysis of public-key cryptography for wireless sensor networks. In *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*, pp. 324–328. IEEE.

[Wang et al. 2003] Wang, H., Elson, J., Girod, L., Estrin, D., e Yao, K. (2003). Target classification and localization in habitat monitoring. In *Acoustics, Speech, and Signal Processing, 2003. Proceedings.(ICASSP'03). 2003 IEEE International Conference on*, volume 4, pp. IV–844. IEEE.

[Werner-Allen et al. 2006] Werner-Allen, G., Lorincz, K., Ruiz, M., Marcillo, O., Johnson, J., Lees, J., e Welsh, M. (2006). Deploying a wireless sensor network on an active volcano. *Internet Computing, IEEE*, 10(2):18–25.

[Werner-Allen et al. 2005] Werner-Allen, G., Swieskowski, P., e Welsh, M. (2005). Motelab: A wireless sensor network testbed. In *Proceedings of the 4th international symposium on Information processing in sensor networks*, pp. 68. IEEE Press.

[Wibree 2007] Wibree (2007). Wibree standard.

[Yick et al. 2008] Yick, J., Mukherjee, B., e Ghosal, D. (2008). Wireless sensor network survey. *Computer networks*, 52(12):2292–2330.

[ZigBee 2004] ZigBee (2004). Zigbee alliance.