Pós-Graduação em Ciência da Computação

FRANCISCO FERREIRA DE MENDONÇA JÚNIOR

UM SERVIÇO DE SEGURANÇA ADAPTÁVEL PARA APLICAÇÕES DA INTERNET DAS COISAS BASEADAS NO PADRÃO 802.15.4

Universidade Federal de Pernambuco
posgraduacao@cin.ufpe.br
www.cin.ufpe.br/~posgraduacao

RECIFE
2016

Francisco Ferreira de Mendonça Júnior

Um Serviço de Segurança Adaptável Para Aplicações da Internet das Coisas Baseadas no Padrão 802.15.4

Este trabalho foi apresentado à Pós-Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre Profissional em Ciência da Computação.

ORIENTADOR: **Prof. Dr. Paulo Roberto Freire Cunha**
CO-ORIENTADOR: **Prof. Dr. Obionor de Oliveira Nóbrega**

RECIFE

Catalogação na fonte
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

M539s Mendonça Júnior, Francisco Ferreira de
Um serviço de segurança adaptável para aplicações da Internet das coisas baseadas no padrão 802.15.4 / Francisco Ferreira de Mendonça Júnior. – 2016.
83 f.: il., fig., tab.

Orientador: Paulo Roberto Freire Cunha.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2016.
Inclui referências.

1. Redes de computadores. 2. Internet das coisas. I. Cunha, Paulo Roberto Freire (orientador). II. Título.

004.6 CDD (23. ed.) UFPE- MEI 2017-36

Francisco Ferreira de Mendonça Júnior

Um Serviço de Segurança Adaptável Para Aplicações da Internet das Coisas Baseadas no Padrão 802.15.4

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

Aprovado em: 22/08/2016

BANCA EXAMINADORA

_____

Prof. Dr. Kelvin Lopes Dias
Centro de Informática / UFPE

_____

Profa. Dra. Jeísa Pereira de Oliveira Domingues
Departamento de Estatística e Informática/ UFRPE

_____

Prof. Dr. Paulo Roberto Freire Cunha
Centro de Informática / UFPE
(**Orientador**)

Eu dedico esta dissertação à minha família, aos meus amigos, e a todos os professores, que deram condições e suporte para que eu chegasse até aqui.

AGRADECIMENTOS

Gostaria de agradecer a todas as pessoas que estiveram envolvidas, direta ou indiretamente, com a construção deste trabalho.

Inicialmente, agradeço toda compreensão e apoio dado por minha família todo esse tempo que estive longe. Agradeço as orações e palavras de incentivo que recebi de minha mãe e meu pai. Agradeço todo o carinho, atenção e compreensão despendidos por Lívia: foram momentos difíceis.

Agradeço as contribuições dadas direta ou indiretamente por meus professores. A Obionor, pelo acompanhamento e liberdade, que resultaram em grande crescimento. A Paulo Cunha, pelo apoio e críticas nos momentos mais essenciais. Aos professores das disciplinas que deram contribuições mais importantes e precisas do que podem imaginar.

Por fim, agradeço aos colegas que tive e aos amigos que fiz durante esse período, eles proporcionaram momentos de distração e companhia e ajudaram a fazer esse tempo valer a pena.

A emoção mais antiga e mais forte da humanidade é o medo, e o mais antigo e mais forte de todos os medos é o medo do desconhecido.

—H. P. LOVECRAFT

RESUMO

A Internet das Coisas - *Internet of Things (IoT)* - é uma arquitetura que pretende ser dinâmica e global, buscando prover autoconfiguração e interoperabilidade, principalmente através de tecnologias padronizadas. A consolidação da arquitetura passa pelo amadurecimento de tecnologias como as Redes de Sensores sem Fio (RSSF). Essas redes, formadas por dispositivos com limitações de recursos computacionais, podem apresentar restrições na comunicação quando são conectados diretamente à Internet. A coexistência entre dispositivos com limitações e dispositivos robustos faz com que as RSASF precisem receber ou transmitir dados cujo comprimento excede a carga útil disponível nos quadros em sua camada de enlace. Essa característica resulta em fragmentação da carga útil transmitida, causando degradação no desempenho e na carga útil destas redes. Nesse contexto, verifica-se a necessidade da busca de alternativas que possam adequar os dispositivos limitados à utilização mais eficiente da IoT. Este trabalho apresenta a proposta de um Serviço de Segurança Adaptável - *Tunable Security Service* (TSS) - para aplicações da Internet das Coisas baseadas no padrão 802.15.4. A manipulação do nível de segurança, através do TSS, é utilizada para reduzir a fragmentação e seus efeitos. O TSS é avaliado em relação ao atraso e ao consumo energético das redes, proporcionando uma redução de até 5% no consumo energético e de até 20% no atraso.

Palavras-chave: Internet das Coisas. 6loWPAN. 802.15.4. Qualidade de Proteção. Serviços de Segurança Adaptáveis.

ABSTRACT

The Internet of Things (IoT) is an architecture that is intended to be dynamic and global. The IoT is intended to provide autoconfiguration and interoperability, primarily through standardized technologies. The consolidation of IoT depends on the maturing of technologies such as Wireless Sensor Networks (WSN). These networks are composed by devices with limited computing resources and may have restrictions on communication when they are connected directly to the Internet. The coexistence between devices with such limitations and devices withouth such limitations makes WSN need to receive or transmit data whose length exceeds the available payload in the frames of link layer. This kind of traffic may generate fragmentation, that leads to degradation in overall performance. In this context, there is the need to search for alternatives that might suit the limited devices to efficiently fit the IoT. This paper proposes a Tunable Security Service (TSS) for applications based on the 802.15.4 standard in the Internet of Things. The TSS manipulates the security level and reduces fragmentation and its effects. The evaluation of the TSS indicates a reduction up to 5% in energy consumption and up to 20% in the delay.

Keywords:

Internet of Things. 6loWPAN. 802.15.4. Quality of Protection. Tunable Security Services.

LISTA DE FIGURAS

2.1 Camadas padronizadas para Redes de Sensores sem Fio na Internet das Coisas Fonte: (GRANJAL; MONTEIRO; SILVA, 2015) (KEOH; KUMAR; TSCHOFENIG, 2014) 24
2.2 Endereço Unicast de Enlace Fonte: (SHELBY; BORMANN, 2011) 26
2.3 Endereço Unicast Global Fonte: (SHELBY; BORMANN, 2011) 26
2.4 Endereço Multicast Fonte: (SHELBY; BORMANN, 2011) 26
2.5 Cabeçalho IPv6 Fonte: (SHELBY; BORMANN, 2011) 27
2.6 Formato geral do quadro 802.15.4 Fonte: (COMMITTEE et al., 2011) Adaptado . 28
2.7 Formação do endereço IPv6 no padrão 802.15.4 Fonte: (SHELBY; BORMANN, 2011) 29
2.8 Relação entre os cabeçalhos do padrão 802.15.4 e os cabeçalhos das camadas superiores Fonte: Produzido pelos autores. 30
2.9 Formato do quadro do padrão 802.15.4 e sua relação com a segurança Fonte: (RAZA et al., 2014) 32
2.10 Descrição funcional da aplicação de segurança no padrão 802.15.4 Fonte: (COMMITTEE et al., 2011) adaptado. 32
2.11 Formato do cabeçalho do primeiro fragmento Fonte: Produzido pelos autores. . . . 33
2.12 Formato do cabeçalho dos fragmentos subsequentes Fonte: Produzido pelos autores. 33
2.13 Alocação dos cabeçalhos das camadas superiores quando acontece fragmentação Fonte: (HUMMEN et al., 2013) 34

4.1 Comparação entre a transmissão de dados tradicional e a transmissão utilizando TSS Fonte: Produzido pelos autores. 52
4.2 Relação entre o nível de segurança, a fragmentação e a quantidade de dados disponível por quadro, representando os "Limites de Fragmentação"Fonte: Produzido pelos autores. 54
4.3 Relação entre o comprimento da mensagem, o nível de segurança e a quantidade de fragmentos Fonte: Produzido pelos autores. 56
4.4 Fluxograma para o funcionamento do Serviço de Segurança Adaptável em redes 6loWPAN baseadas em 802.15.4 Fonte: Produzido pelos autores. 57

5.1 Abrangência do simulador COOJA em relação a outros simuladores. Fonte: (OSTERLIND et al., 2006) 60
5.2 Cenário de transmissão dos dados entre 6LN e 6LBR Adaptado de KEOH; KUMAR; TSCHOFENIG (2014) 62
5.3 Teste de hipóteses 64
5.4 Rede com dois dispositivos (5.4a) e rede com 11 dispositivos (5.4b) 64
5.5 Rede com 15 dispositivos (5.5a) e rede com 21 dispositivos (5.5b) 65

5.6 Diminuição no atraso relacionada a redução na quantidade de fragmentos na rede com 2 dispositivos 66
5.7 Diminuição no atraso relacionada a redução na quantidade de fragmentos na rede com 11 dispositivos 67
5.8 Diminuição no atraso relacionada a redução na quantidade de fragmentos na rede com 16 dispositivos 67
5.9 Diminuição no atraso relacionada a redução na quantidade de fragmentos na rede com 21 dispositivos 68
5.10 Distribuição das dimensões e critérios de segurança pela Árvore Marcada e Ponderada e atribuição de importância 71

LISTA DE TABELAS

2.1 Características Físicas do padrão 802.15.4 Fonte: (SHELBY; BORMANN, 2011) Adaptada 28
2.2 Níveis de Segurança no Modo Seguro do Padrão 802.15.4 Fonte: Produzido pelos autores. 31
2.3 Classificação de serviços de segurança baseada em uma abordagem binária. A presença de cada dimensão de segurança é indicada por um Y (yes, sim). Fonte: (AGARWAL; WANG, 2007) 36
2.4 Classificação de serviços de segurança baseada em uma abordagem com atribuição de pesos. Fonte: (AGARWAL; WANG, 2007) 37

3.1 Trabalhos relacionados a fragmentação do 6loWPAN na comunicação 41
3.2 Trabalhos relacionados com o impacto da fragmentação do 6loWPAN em outros protocolos 43
3.3 Modelos analíticos baseados em QoP 47
3.4 Avaliações de desempenho relacionadas a QoP 48

4.1 Valores para as variáveis dos Algoritmos de acordo com a especificação do padrão 802.15.4 54

5.1 Parâmetros das simulações 63
5.2 Diminuição no atraso relacionada a redução na quantidade de fragmentos na rede com 2 dispositivos 65
5.3 Diminuição percentual no atraso relacionada a redução da quantidade de fragmentos na rede com 11 dispositivos 66
5.4 Diminuição percentual no atraso relacionada à redução da quantidade de fragmentos na rede com 16 dispositivos 67
5.5 Diminuição percentual no atraso relacionada à redução da quantidade de fragmentos na rede com 21 dispositivos 68
5.6 Queda percentual no tempo de rádio ligado relacionada à redução da quantidade de fragmentos na rede com 2 dispositivos 69
5.7 Rótulos das dimensões e dos critérios de segurança 72
5.8 Pesos atribuídos a cada critério de segurança 72
5.9 Abordagem binária para atribuição de identificação da conformidade de uma cifra de segurança com os critérios estabelecidos 73
5.10 Valores da Recompensa para as cifras de segurança do padrão 802.15.4 73

LISTA DE ACRÔNIMOS

6LBR 6loWPAN Border Router 18

6LN 6loWPAN Node 18

6loWPAN IPv6 over LowPower Personal Area Networks 18

AODV Ad-hoc On-demand Distance Vector 42

BS Base Station 70

CoAP Constrained Application Protocol 23

CORE Contrained Restful Environments 24

CRC Cyclic Redundancy Check 53

CSMA Carrier Sense Multiple Access 28

DTLS Datagram Transport Layer Security 42

HTTP Hyper Text Tranfer Protocol 23

HVM Historical Vulnerabilities Measurement 36

ICMP Internet Control Message Protocol 29

IEEE Institute of Electrical and Electronics Engineers 23

IETF Internet Engineering Task Force 24

IoT Internet of Things 18

IPv6 Internet Protocol Version 6 18

ISM Industrial, Scientific and Medical Radio Bands 28

MAC Media Access Control 23

MIC Message Integrity Code 30

MS Mobile System 70

MTU Maximum Transmission Unity 18

NIST National Institute of Standards and Technology 45

OSI Open Systems Interconnection 23

PACP Port Access Control Protocol 70

PAN Personal Area Network 23

PID Controlador Proporcional-Integral-Derivativo 42

QoE Quality of Experience 35

QoP Quality of Protection 19

QoS Quality of Service 19

REST Representational State Transfer 24

RFC Request for Comments 27

RFID Radio-frequency identification 22

RPL Routing Protocol for Low power and Lossy Networks 23

RSSF Redes de Sensores sem Fio 18

SNMP Simple Network Management Protocol 42

TCP Transmission Control Protocol 25

TSS Tunable Security Service 19

UDP User Datagram Protocol 23

URI Uniform Resource Identifier 24

WPAN Wireless Personal Area Network 28

LISTA DE ALGORITMOS

1 Estimativa da quantidade de fragmentos 52
2 Redução do Nível de Segurança 56

SUMÁRIO

1 INTRODUÇÃO 17
1.1 Contextualização 18
1.2 Caracterização do Problema e Solução Apresentada 19
1.3 Delimitações do Escopo 19
1.4 Organização da Dissertação 19
2 CONCEITOS BÁSICOS 21
2.1 Introdução 22
2.2 Internet das Coisas 22
2.2.1 Camadas Padronizadas para a Internet das Coisas 23
2.2.2 Camadas de Aplicação e Transporte - CoAP e UDP 23
2.2.3 Camadas de Rede e Roteamento 25
2.2.4 Camada de Adaptação, Camada de Acesso ao Meio e Camada Física - 6loWPAN e 802.15.4 27
2.2.5 Segurança no padrão 802.15.4 30
2.2.6 Fragmentação em 6loWPAN 33
2.3 Qualidade de Proteção 34
2.3.1 Modelos 35
2.3.1.1 Função de Utilidade 36
2.3.1.2 Recompensa 37
2.3.2 Outros Modelos 38
2.3.3 Aplicações da Qualidade de Proteção 38
2.4 Conclusão 38
3 TRABALHOS CORRELATOS 40
3.1 Introdução 41
3.2 Fragmentação 41
3.3 QoP e TSS 43
3.4 Conclusão 49
4 SERVIÇO DE SEGURANÇA ADAPTÁVEL 50
4.1 Introdução 51
4.2 Serviço de Segurança Adaptável 51
4.3 Módulo para Detecção dos Limites de Fragmentação 52
4.4 Aplicação da Detecção dos Limites de Fragmentação 54
4.5 Módulo de Ativação do Serviço de Segurança Adaptável 56
4.6 Conclusão 58
5 AVALIAÇÃO, RESULTADOS E DISCUSSÃO 59
5.1 Introdução 60
5.2 O simulador COOJA 60

5.3 Cenários e Parâmetros das Simulações 62
5.4 Avaliação dos Resultados: Redução no Atraso 65
5.5 Avaliação dos Resultados: Impacto no Consumo Energético 69
5.6 Modelo de Qualidade de Proteção para o Padrão 802.15.4 69
5.7 Conclusão 73
6 CONCLUSÕES 75
6.1 Considerações Finais 76
6.2 Contribuições 76
6.3 Trabalhos futuros 77
Referências 79

1

INTRODUÇÃO

Este capítulo apresenta a contextualização e a caracterização do problema desta dissertação, bem como sua delimitação de escopo e a descrição de sua estrutura.

1.1 Contextualização

A Internet das Coisas - *Internet of Things (IoT)* - se apresenta como uma arquitetura que serve de base para a evolução da Internet do Futuro. (GUBBI et al., 2013) Trata-se da conexão de objetos à Internet através de sensores, atuadores e tecnologias sem fio. A adoção do Protocolo de Internet, versão 6 - *Internet Protocol Version 6 (IPv6)* - permite que cada objeto seja endereçado individualmente, tornando possível que eles se comuniquem e troquem dados, mesmo sem a intervenção humana.

A conexão de objetos à Internet passa pela consolidação das Redes de Sensores sem Fio (RSSF) e das tecnologias de conexão dessas redes com a Internet. Geralmente, a conexão das RSSF com a Internet é realizada através de *gateways*, dispositivos responsáveis por coletar e armazenar dados os sensores de uma RSSF e transmití-los quando necessário. (RACHEDI; HASNAOUI, 2015) (YICK; MUKHERJEE; GHOSAL, 2008).

Nos últimos anos surgiram iniciativas que pretendem mudar o paradigma de conectividade das RSSF para que os dispositivos conectem-se à Internet sem dispositivos intermediários. A utilização de uma subcamada - *IPv6 over LowPower Personal Area Networks (6loWPAN)* - provê conectividade com a Internet para dispositivos que tenham camada de acesso ao meio e camada física diferenciadas. Seu surgimento é reflexo da tentativa de padronização das tecnologias que compõem a arquitetura da IoT. Ainda existem muitas tecnologias divergentes atuando nesse contexto, mas espera-se que a padronização seja o caminho para a consolidação da arquitetura da IoT.

A adaptação realizada pelo 6loWPAN consiste em tradução de endereços, compressão de cabeçalhos e tratamento de fragmentação (MONTENEGRO et al., 2007). A função do *gateway* foi substituída pela presença do Roteador de Borda da Rede 6loWPAN - *6loWPAN Border Router (6LBR),* que já não armazena dados dos sensores, mas age como um roteador, apenas direcionando as requisições e o envio de dados diretamente para os dispositivos através da Internet. Dispositivos das RSSF passam a ser chamados de *6loWPAN Node (6LN)* (SHELBY; BORMANN, 2011).

Ao se conectar diretamente à Internet, as redes 6loWPAN entram em contato com redes que possuem características diferenciadas, abrindo novos campos para o estudo de seu funcionamento. Uma das diferenças está relacionada à quantidade e ao comprimento dos dados trafegados. A unidade máxima de transmissão - *Maximum Transmission Unity (MTU)* - do IPv6 é de 1280 *bytes* (DEERING; HINDEN, 1998). Quando pacotes com esse comprimento precisam trafegar por redes 6loWPAN, passam por um processo de fragmentação.

Redes 6loWPAN geralmente apresentam tráfego de dados, como sinalização e controle, que não excedem o espaço disponível em seus quadros (KUSHALNAGAR; MONTENEGRO; SCHUMACHER, 2007). Mas existem tipos de redes que precisam enviar registros de várias medições que não cabem em um único quadro. Esses registros podem variar de centenas de *bytes* a *quilobytes* (LUDOVICI et al., 2014). Este é um caso em que os dados gerados pela rede

6loWPAN passam por fragmentação.

1.2 Caracterização do Problema e Solução Apresentada

A fragmentação causa impactos negativos no desempenho, no consumo energético, na taxa de entrega de pacotes numa rede e pode causar transbordamento de *buffer*, resultando em perda de pacotes. Reduzir seus efeitos permite economizar os recursos escassos das redes 6loWPAN (HUMMEN et al., 2013) (KURYLA; SCHÖNWÄLDER, 2011) (LUDOVICI et al., 2014) (POPE; SIMON, 2013) (SILVA; SILVA; BOAVIDA, 2009) (SUH; MIR; KO, 2008).

Este trabalho apresenta a proposta de um Serviço de Segurança Adaptável - *Tunable Security Service (TSS)* - baseado no padrão 802.15.4 e voltado para aplicações da Internet das Coisas. O serviço de baseia na manipulação do nível de segurança do padrão para que os dados possam ser transmitidos de forma mais eficiente. Neste trabalho, o TSS é aplicado com a finalidade de agir sobre a fragmentação e seus efeitos, buscando reduzí-los. São propostos módulos que identificam as situações em que existe relação entre o comprimento dos dados, o nível de segurança e a fragmentação.

1.3 Delimitações do Escopo

Este trabalho não se destina a fazer nenhuma modelagem da relação entre os ganhos, perdas, ou quantificação de força de protocolos quando relacionados à manipulação de segurança. Os resultados deste trabalho explicitam que existem benefícios quando a segurança é manipulada, que existem situações onde esses benefícios são aplicáveis e que existem situações onde os ganhos não se aplicam.

1.4 Organização da Dissertação

Este trabalho está organizado da seguinte forma:

No Capítulo 2 são apresentados os conceitos básicos que norteiam esse trabalho. São discutidos temas relacionados a Internet das Coisas e os principais protocolos envolvidos. A apresentação dos protocolos é finalizada com o foco na relação entre o protocolo IPv6 e o padrão 802.15.4, o funcionamento e as configurações de segurança. A relação é realizada pelo protocolo de adaptação 6loWPAN. São apresentadas as funções dessa adaptação, bem como o processo de fragmentação. Também é iniciada a apresentação da Qualidade de Proteção - *Quality of Protection (QoP)* - e dos Serviços de Segurança Adaptáveis. Esses temas se relacionam com a caracterização da segurança como um fator que afeta a Qualidade de Serviço - *Quality of Service (QoS)* - das aplicações.

Em seguida, no Capítulo 3, são apresentados os principais trabalhos relacionados aos temas da fragmentação e TSS. O capítulo busca listar os problemas relacionados à fragmentação, bem como as características e os benefícios que TSS pode proporcionar quando são aplicados.

No Capítulo 4 é apresentado o Serviço de Segurança Adaptável que é o núcleo deste trabalho. O TSS é utilizado para identificar a relação entre o comprimento dos dados e a fragmentação. Dessa forma, surge a proposta deste trabalho e a discussão de sua aplicabilidade. A análise é realizada através da demonstração da atenuação da fragmentação por TSS.

No Capítulo 5 é apresentada a avaliação do TSS. São realizados experimentos para averiguar a validade da proposta e avaliar seu desempenho. É possível encontrar a descrição de benefícios e os cenários onde eles são perceptíveis. Também são apresentados cenários onde seus benefícios podem não ser aplicáveis.

Por fim, no Capítulo 6, são apresentadas as conclusões e contribuições deste trabalho, bem como propostas para a realização de trabalhos futuros.

2

CONCEITOS BÁSICOS

Este capítulo apresenta uma revisão de literatura relacionada às tecnologias de comunicação padronizadas para a Internet das Coisas, que converge para o 6loWPAN e para o padrão 802.15.4. O conceito de Serviço de Segurança Adaptável é introduzido, além da demonstração de sua relação com o conceito de Qualidade de Proteção.

2.1 Introdução

A revisão bibliográfica realizada neste capítulo tem como objetivo fundamentar a decisão da aplicação de um Serviço de Segurança Adaptável (TSS). Para isso são apresentados os cenários e as tecnologias relacionadas ao trabalho atual, bem como os motivos que levaram outros TSS a serem implantados e seus respectivos cenários. O conceito de TSS está estreitamente relacionado ao conceito de Qualidade de Proteção, que é uma forma de calcular os benefícios de segurança dentro de um cenário.

2.2 Internet das Coisas

A Internet passou por várias transformações desde sua criação. As evoluções mais notáveis aconteceram quando ocorreu a inserção de tráfegos multimídia, na adoção de redes sem fio e na utilização de dispositivos heterogêneos. Tem sido intensivamente discutido na academia e na indústria que outra mudança está em curso (XU; HE; LI, 2014). Trata-se do advento da Internet das Coisas. Uma das definições mais completas pode ser encontrada em KRANENBURG (2008):

> *uma infra-estrutura de rede dinâmica e global com capacidade de autoconfiguração baseada em protocolos de comunicação padronizados e interoperáveis, onde 'coisas' físicas e virtuais têm identidade, atributos físicos, personalidades virtuais e usam interfaces inteligentes, e estão perfeitamente integrados na rede de informação* (tradução livre)

Outros autores como ATZORI; IERA; MORABITO (2010) e MAINETTI; PATRONO; VILEI (2011) corroboram essa definição em seus trabalhos, reforçando o interesse acadêmico e industrial neste tema. Esse interesse se justifica, na maioria das vezes, pelas aplicações econômicas que a IoT possibilita. Uma lista não exclusiva de aplicações contém: automação e manufatura industrial, logística, gestão de processos de negócios, transporte inteligente de pessoas e bens, monitoramento de saúde, casas e cidades inteligentes e socialidade.

Como foi visto, o conceito de IoT se relaciona com: conexão e endereçamento de uma quantidade muito grande de dispositivos; e a integração através de tecnologias padronizadas. A quantidade de "coisas" conectadas à Internet superou a quantidade de pessoas em 2011 e existem previsões que apontam que em 2020, esses dispositivos serão mais de 24 bilhões (GUBBI et al., 2013). De acordo com a definição, esses dispositivos precisam ter identificação, atributos e interfaces. Isso lhes é dado através de tecnologias como Identificação por Radiofrequência - *Radio-frequency identification (RFID)* - e RSSF (GRANJAL; MONTEIRO; SILVA, 2015).

Para que a IoT se consolide, esses dispositivos precisam trocar dados entre si e precisam ser acessados por aplicações que transformem esses dados em informações úteis. Isso só se torna possível com mecanismos escaláveis de endereçamento e descoberta de serviços, que podem ser fornecidos pelo Protocolo de Internet versão 6 (IPv6) (THOMSON, 1998).

Entretanto, a maior parte dos dispositivos relacionados a RFID e RSSF apresentam limitações de poder computacional, memória e disponibilidade energética. Isso pode ser uma limitação quando se pretende criar uma arquitetura complexa como pode ser a Internet das Coisas (MAINETTI; PATRONO; VILEI, 2011). Nesse contexto se apresentam duas soluções: a criação de novos protocolos e a adaptação de protocolos existentes. As duas soluções podem ser tratadas como complementares, pois o processo de criação de novos protocolos não deixa de se basear nos protocolos existentes. Da mesma forma se observa que a adaptação dos protocolos exististes leva a otimizações que podem ser propagadas para os protocolos legados (GRANJAL; MONTEIRO; SILVA, 2015).

Assim, se chega à segunda parte da definição. É bastante defendido que, para se alcançar a arquitetura necessária para estabelecer a Internet das Coisas, é preciso utilizar tecnologias e protocolos padronizados (XU; HE; LI, 2014) (BANDYOPADHYAY; SEN, 2011) (GRANJAL; MONTEIRO; SILVA, 2015). Por muito tempo, empresas propuseram, e ainda propõem, soluções proprietárias para o que chamavam de IoT. As particularidades de cada solução dificultam ao desenvolvimento da arquitetura e a falta de padronização impede o desenvolvimento de uma arquitetura que atenda as necessidades de troca de informações entre as aplicações.

2.2.1 Camadas Padronizadas para a Internet das Coisas

A consolidação da Internet das Coisas depende da maturação e da padronização das diversas tecnologias que irão interagir entre si. Essas tecnologias estão distribuídas em todos os níveis da pilha de protocolos do modelo OSI - *Open Systems Interconnection (OSI)*. Uma das principais pilhas de protocolos nesta arquitetura está relaciona com o padrão 802.15.4 (COMMITTEE, 2003).

O padrão 802.15.4 (COMMITTEE et al., 2011) vem sendo mantido e desenvolvido pelo Instituto de Engenheiros Eletricistas e Eletrônicos - *Institute of Electrical and Electronics Engineers (IEEE)* - desde 2003. O padrão define camadas de acesso ao meio - *Media Access Control (MAC)* - e física para Redes de Área Pessoal - *Personal Area Network (PAN)*. Desde sua criação, ele evoluiu para se tornar uma das tecnologias mais utilizadas nas Redes de Sensores sem Fio (ATZORI; IERA; MORABITO, 2010). A pilha de protocolos padronizados para a IoT, e que tem como base o padrão 802.15.4, é formada, em uma abordagem *top-down*, por *Constrained Application Protocol (CoAP)*, *User Datagram Protocol (UDP)*, *Routing Protocol for Low power and Lossy Networks (RPL)*, IPv6 e 6loWPAN. A relação entre os protocolos pode ser vista na Figura 2.1 (GRANJAL; MONTEIRO; SILVA, 2015) (KEOH; KUMAR; TSCHOFENIG, 2014).

2.2.2 Camadas de Aplicação e Transporte - CoAP e UDP

A *Web* é um dos serviços mais comuns na Internet. O principal protocolo utilizado para esse tipo de serviço é o Protocolo de Transferência de Hipertexto - *Hyper Text Tranfer Protocol (HTTP)* (MOGUL et al., 1997). Desde a sua criação, o protocolo passou por melhorias

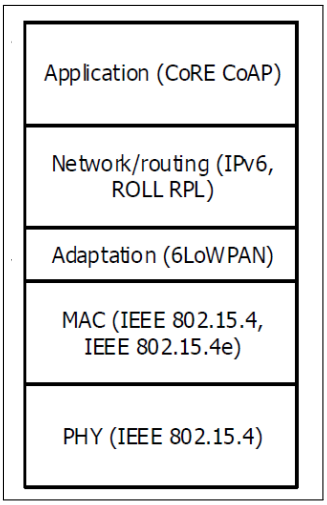


Figura 2.1: Camadas padronizadas para Redes de Sensores sem Fio na Internet das Coisas
Fonte: (GRANJAL; MONTEIRO; SILVA, 2015) (KEOH; KUMAR; TSCHOFENIG, 2014)

para se adaptar às novas aplicações que vem surgindo para Web. Dentre as otimizações destacam-se compressão de cabeçalhos, utilização de conexões simultâneas e utilização de mensagens *push* do servidor para o cliente (BELSHE; THOMSON; PEON, 2015).

Nesse contexto, é esperado que serviços da Internet das Coisas também se utilizem da *Web* para conectar os dispositivos entre si e aos usuários, porém as otimizações do HTTP não se apresentaram adequadas, pois elas dependem do aumento no poder de processamento. Para viabilizar essa comunicação, principalmente devido às limitações dos dispositivos, foi criado o protocolo CoAP (SHELBY; HARTKE; BORMANN, 2014). CoAP é um protocolo de Transferência de Estado Representacional - *Representational State Transfer (REST)* - para transferência de dados em dispositivos limitados da Internet das Coisas. Ele vem sendo desenvolvido pelo grupo de trabalho *Contrained Restful Environments (CORE)* da Força Tarefa de Engenharia da Internet - *Internet Engineering Task Force (IETF)*. CoAP é baseado no HTTP e foi criado com menor sobrecarga de cabeçalhos. Também foram feitas otimizações em seu código para a redução da complexidade e para uma menor utilização de banda (KEOH; KUMAR; TSCHOFENIG, 2014). Como no protocolo HTTP, a comunicação acontece, prioritariamente, através de requisições de um cliente e respostas de um servidor. As mensagens são identificadas por códigos, que representam ações realizadas com o recurso do servidor. Um recurso é identificado por um Identificador Uniforme de Recurso - *Uniform Resource Identifier (URI)*.

CoAP define quatro tipos de mensagens: confirmável, não-confirmável, *acknowledgement* (*ack*) e *reset*. Essas mensagens carregam códigos e dados que indicam se elas são requisições ou respostas. Mensagens dos tipos confirmável e *ack* estão estreitamente relacionadas, uma vez que uma mensagem confirmável requer um *ack*. Em casos especiais, o próprio *ack* pode carregar a resposta a uma requisição, evitando que novas mensagens sejam geradas, reduzindo o tráfego de dados na rede. Esse mecanismo é conhecido como *piggyback*. Esse mecanismo permite que o servidor responda a uma requisição utilizando o próprio *ack*. A especificação recomenda que servidores implementem o mecanismo de *piggyback* sempre que possível

para que os dispositivos possam economizar seus recursos sempre que necessário (SHELBY; HARTKE; BORMANN, 2014).

Mensagens do tipo não confirmável não requerem *ack*. Elas são usadas por aplicações que não tem confiabilidade como requisito. Mensagens de *reset* podem servir de resposta para mensagens confirmáveis ou não confirmáveis. Elas indicam que a mensagem foi recebida, mas faltam dados necessários para que ela possa ser processada corretamente. Isso pode acontecer quando um dos dispositivos da rede perdeu informações de contexto da rede por algum motivo, como uma reinicialização (SHELBY; HARTKE; BORMANN, 2014).

O protocolo CoAP foi criado para manter interoperabilidade com o protocolo HTTP. Para isso, é necessário utilizar um *proxy* reverso HC (HTTP-CoAP). Esse tipo de *proxy* se comporta como um servidor com que o cliente se comunica de forma transparente. Isso significa que, para que um cliente CoAP consiga trocar dados com um servidor HTTP, o proxy reverso receberá as requisições CoAP e passará para o servidor (DIJK et al., 2015).

Dispositivos que usam o protocolo CoAP podem fazer o papel de cliente ou servidor. Essa possibilidade viabiliza a comunicação M2M (*Machine to Machine*). Nesse modo de operação, os dispositivos realizam as funções de cliente e servidor ao mesmo tempo. Também existe a possibilidade de que o dispositivo apenas envie mensagens não confirmadas, não se encaixando em nenhuma das funções anteriores (KEOH; KUMAR; TSCHOFENIG, 2014).

Diferentemente do protocolo HTTP, que usa prioritariamente o Protocolo de Controle de Transmissão - *Transmission Control Protocol (TCP)* - como protocolo de transporte, CoAP utiliza UDP, que não oferece garantia de entrega e nem controle de fluxo. A utilização de UDP faz com que a aplicação seja responsável pelo controle sobre o fluxo de dados, tornando-se mais adaptável a diferentes dispositivos e situações. Assim, funções como a verificação de entrega e o controle de fluxo são realizadas diretamente pelo protocolo de aplicação.

Por utilizar UDP, o protocolo CoAP permite o suporte a aplicações *unicast* e *multicast*. Esses modos de transmissão, principalmente *multicast*, são utilizados para descoberta de recursos. Dispositivos que implementem CoAP devem estar preparados para receber requisições *multicast*, mesmo que seja para ignorá-las.

2.2.3 Camadas de Rede e Roteamento

Na IoT, espera-se que bilhões de dispositivos se conectem à Internet. Algumas aplicações precisam que eles troquem dados sem intervenção humana, sendo necessário publicar e descobrir recursos automaticamente (XU; HE; LI, 2014). Essas aplicações necessitam do suporte de mecanismos robustos de endereçamento, descoberta de serviços e roteamento para que possam trocar mensagens de forma satisfatória. Os protocolos IPv6 e RPL são os responsáveis por prover estas funcionalidades.

A principal vantagem do IPv6 em relação ao IPv4, e a principal característica do protocolo em relação ao IoT, é o comprimento do endereço (SHELBY et al., 2012). São 128 *bits*

disponibilizados para endereçamento comparados aos 32 *bits* disponíveis no IPv4. A quantidade de *bits* do IPv4 permite endereçar 4.294.967.296 de interfaces de rede, sem repetições ou uso de NAT *(Network Address Translation)*. Com o IPv6 será possível prover 7,9e1028 vezes mais endereços.

Os bits iniciais de um endereço IPv6 indicam seu tipo. Entre esses tipos destacam-se o endereço *unicast* de enlace local, o endereço *unicast* global e o endereço *multicast*. O primeiro tipo é relacionado a tarefas de escopo de enlace, como a inicialização e o encerramento de conexões. É possível observar, na Figura 2.2, que ele é formado por um preâmbulo, que indica o tipo de endereço, e o Identificador de Interface. O restante do endereçamento é completado por zeros, totalizando 8 *bytes*.

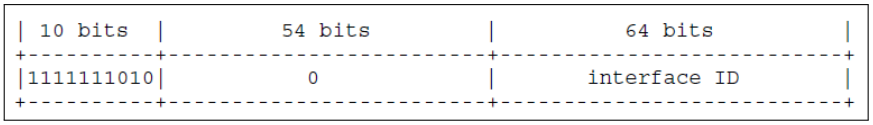


Figura 2.2: Endereço Unicast de Enlace
Fonte: (SHELBY; BORMANN, 2011)

A estrutura de um endereço global e de um endereço de *multicast* são mostrados na Figura 2.3 e na Figura 2.4, respectivamente. O endereço global é utilizado para identificar interfaces de rede de forma única e inequívoca. Ele é formado pelo Identificador de Interface, além de um Preâmbulo, que identifica o tipo de endereço, um Identificador de Sub-rede e um Prefixo Global de Roteamento.

Endereços de *multicast* servem para identificar grupos de interfaces, geralmente representados por grupos de dispositivos. Uma interface pode participar de vários grupos de *multicast*. Endereços *multicast* tem sinalizadores (*flgs*) e um escopo (*scop*). Os sinalizadores servem para indicar estados do endereço como o tempo de alocação e informações de alocação de endereços *multicast* entre domínios. O escopo identifica o alcance do endereço *multicast*. O alcance pode ser reservado, local, enlace, administrativo e global. Existem outras opções, mas elas são relacionadas àquelas mencionadas ou são de uso reservado.

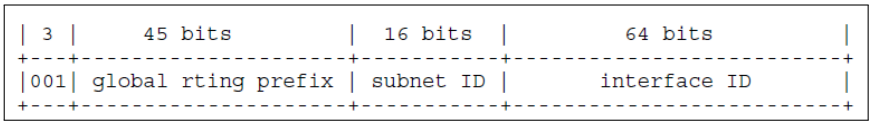


Figura 2.3: Endereço Unicast Global
Fonte: (SHELBY; BORMANN, 2011)

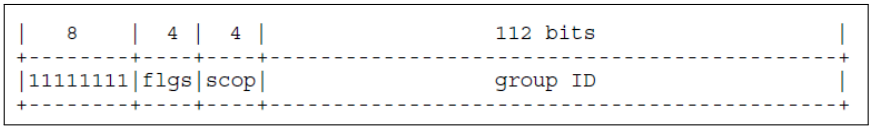


Figura 2.4: Endereço Multicast
Fonte: (SHELBY; BORMANN, 2011)

Um mecanismo de endereçamento tão robusto tende a gerar um cabeçalho extenso, como pode ser observado na Figura 2.5. Este cabeçalho está representado na notação de 64 *bits*, totalizando 40 *bytes*.

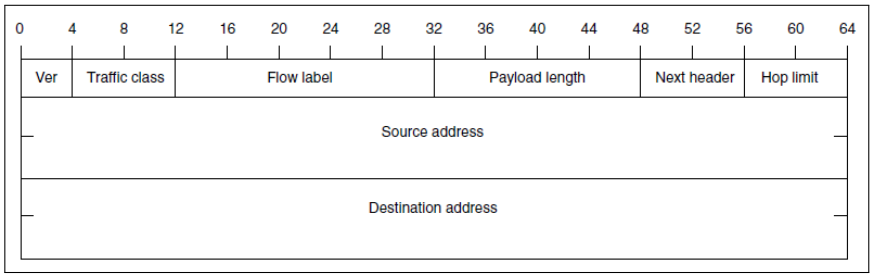


Figura 2.5: Cabeçalho IPv6
Fonte: (SHELBY; BORMANN, 2011)

Mas o IPv6 tem outros mecanismos, além do endereçamento, que dão viabilidade à Internet das Coisas. Destacam-se os mecanismos de Descoberta de Vizinhança (NARTEN et al., 2007) e Autoconfiguração de Endereços (THOMSON, 1998). O protocolo de Descoberta de Vizinhança é usado pelos dispositivos em tarefas da camada de enlace. Entre essas tarefas destacam-se a obtenção dos endereços de enlace dos seus vizinhos; a detecção de mudanças nas características ou nos endereços da rede; e a descoberta de roteadores que possam encaminhar seus pacotes de acordo com suas necessidades.

Usando a Descoberta de Vizinhança, os dispositivos devem ser capazes de obter seus endereços globais de forma automática por Autoconfiguração de Endereços. Isso é feito através da definição do Identificador de Interface, realizado pelo próprio dispositivo, e da obtenção de informações dos dispositivos vizinhos e dos roteadores alcançáveis. Os roteadores são responsáveis por fornecer o prefixo de sub-rede que identifica aquele enlace na relação com outras redes ou com a Internet.

2.2.4 Camada de Adaptação, Camada de Acesso ao Meio e Camada Física - 6loWPAN e 802.15.4

Para que fosse possível utilizar toda a robustez proveniente do IPv6 em dispositivos com limitações computacionais, foi necessário criar uma camada de adaptação. Essa camada ficou conhecida como 6loWPAN, acrônimo que significa *IPv6 over Low Power Wireless Personal Area Networks*. A adaptação consiste em tradução de endereços, compressão ou transformação de cabeçalhos e tratamento de fragmentação (SHELBY; BORMANN, 2011).

É preciso ressaltar que 6loWPAN foi originalmente projetado para transportar pacotes IPv6 em redes 802.15.4, portanto as duas tecnologias estão estreitamente relacionadas (MONTENEGRO et al., 2007). Apesar dessa relação, já existem rascunhos e *Request for Comments (RFC)* no IETF sobre utilização de 6loWPAN em outras tecnologias como *Bluetooth Low Energy* (BLE) (NIEMINEN et al., 2015), *Digital Enhanced Cordless Telecommunications Ultra Low Energy* (DECT-ULE) (MARIAGER; PETERSEN, 2013) e ITU-T G (BRANDT; BURON, 2015).

O padrão 802.15.4 define as camadas MAC e física para Redes de Área Pessoal sem Fio - *Wireless Personal Area Network (WPAN)*. O padrão é destinado a utilizar as bandas destinadas a uso Industrial, Científico e Médico - *Industrial, Scientific and Medical Radio Bands (ISM)* - ao redor do mundo. Essas redes tendem a transmitir poucos dados, utilizar baixas taxas de transmissão e com baixo consumo energético. O comprimento padrão do quadro é de 127 *bytes*. Esse quadro, curto em relação à Unidade Máxima de Transmissão - *Maximum Transmission Unity* (MTU) - do IPv6, pode ter o espaço destinado a carga útil ainda mais reduzido quando é necessário utilizar cabeçalhos das camadas superiores ou utilizar segurança. Rádios que utilizam o padrão podem transmitir dados a até 250 kbps, dependendo da região onde se encontram. A relação entre a região, a faixa de frequência e a taxa de transmissão de dados é ilustrada na Tabela 2.1 (COMMITTEE et al., 2011) (SHELBY; BORMANN, 2011).

Tabela 2.1: Características Físicas do padrão 802.15.4
Fonte: (SHELBY; BORMANN, 2011) Adaptada

Faixa de Frequência (MHz)	Região	Canal	Taxa de Bits (kbps)
868	Europa	0	20
902–928	EUA	1 - 10	40
2400–2483.5	Resto do Mundo	11 - 26	250

As redes baseadas em 802.15.4 possuem dois modos de funcionamento: *beaconless* e *beacon-enabled*. No primeiro modo, a rede funciona em modo de Acesso Múltiplo com Sensoriamento da Portadora - *Carrier Sense Multiple Access (CSMA)* - puro, como a maior parte das redes 802.11. No modo *beacon-enabled* existe a possibilidade de reserva de canal para a transmissão de dados críticos. A reserva é feita através de *beacons* e quadros de comando. O padrão determina 4 tipos de quadros: dados, *ack*, comando e *beacon*. Quadros de dados transportam os dados propriamente ditos. Quadro do tipo *ack* são enviados como reposta a um quadro recebido. O emissor precisa definir explicitamente que deseja receber um *ack* quando envia um quadro. Quadros de comando são usados no modo *beacon-enabled* e são destinados a controlar serviços da rede como associação, desassociação e sincronização. Os quadros do tipo *beacon* são utilizados para determinar o início e o fim de um período de reserva do meio de transmissão. O formato geral de um quadro 802.15.4 é demonstrada na Figura 2.6.

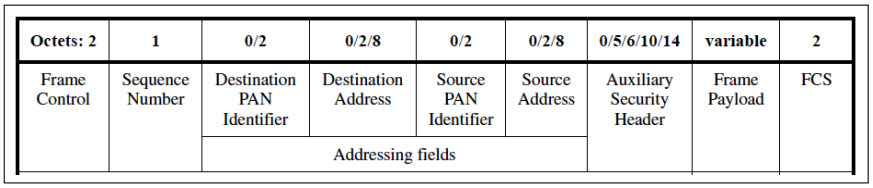


Figura 2.6: Formato geral do quadro 802.15.4
Fonte: (COMMITTEE et al., 2011) Adaptado

Para que pacotes IPv6 possam trafegar por redes 802.15.4, eles precisam ser endereçados corretamente. A tradução de endereços IPv6 utilizando 6loWPAN é necessária pois o padrão

802.15.4 apresenta formas de endereçamento específicas: o endereçamento estendido, com 64 *bits* e o endereçamento curto, com 16 *bits*. É esperado que os dispositivos, mesmo em redes isoladas, obtenham um dos dois tipos de endereços do coordenador da Rede Pessoal - *Personal Area Network (PAN)*. A conversão acontece, prioritariamente, a partir de endereços de 64 bits, que são diretamente atribuídos ao Identificador de Interface do IPv6.

Quando um dispositivo possui um endereço de 16 *bits*, o primeiro passo é o mapeamento desse endereço para 64 *bits* através da adição de um pseudo endereço de 48 bits. Esse pseudo endereço é formado a partir do identificador (ID) da PAN, do endereço MAC, do próprio endereço curto. O endereço de 64 *bits* pode ser preenchido por zeros caso algum dos dados requeridos não esteja disponível. O endereço IPv6 de uma interface de rede 802.15.4 é formado pela união do Identificador de Interface de 64 bits com um prefixo, conforme a Figura 2.7.

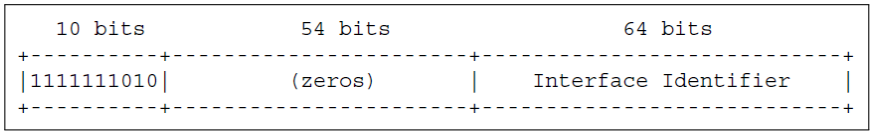


Figura 2.7: Formação do endereço IPv6 no padrão 802.15.4
Fonte: (SHELBY; BORMANN, 2011)

É esperado que as redes 802.15.4 compartilhem dados de estado e configuração em seus cabeçalhos. Várias seções do cabeçalho tendem a ser comuns entre os dispositivos ou podem ser inferidas a partir de dados de outras camadas. Isso pode fazer com que os cabeçalhos da camadas superiores possam ser reduzidos, gerando economia de espaço e permitindo o transporte de mais carga útil.

Dados que se repetem, como a versão do IPv6 e o endereço de origem ou destino do enlace local da rede, podem ser removidos ou utilizados para inferir o endereço de rede. Outros campos, como Classe de Tráfego (tradução livre) e Etiqueta de Fluxo (tradução livre) possuem valor zero. O campo Próximo Cabeçalho (tradução livre) tende a ser apenas UDP, TCP, ou mesmo *Internet Control Message Protocol (ICMP)*. Outros cabeçalhos, porém, podem não suportar supressão ou compressão, limitando a economia que pode ser alcançada. Esse é o caso do campo de contagem de salto, que precisa ser sempre carregado e atualizado, além de outros cabeçalhos adicionais (MONTENEGRO et al., 2007). A relação do padrão 802.15.4 com os cabeçalhos das camadas superiores é ilustrada na Figura 2.8.

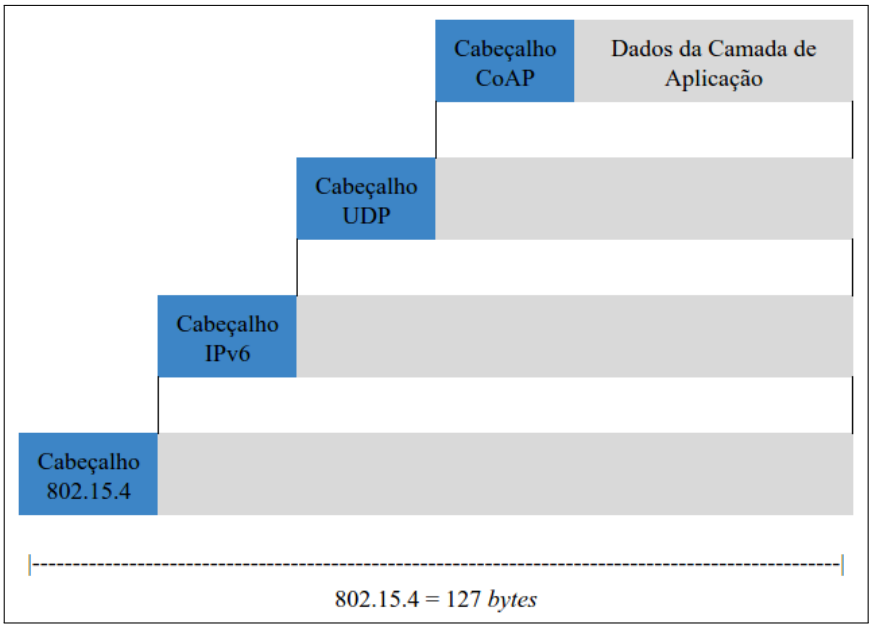


Figura 2.8: Relação entre os cabeçalhos do padrão 802.15.4 e os cabeçalhos das camadas superiores
Fonte: Produzido pelos autores.

2.2.5 Segurança no padrão 802.15.4

O protocolo 6loWPAN ainda depende, prioritariamente, dos mecanismos de segurança provenientes do padrão 802.15.4 (RAZA et al., 2014). Mesmo assim existem mecanismos de segurança próprios ou herdados do IPv6, que podem ser utilizados. O protocolo IPSec (GLENN; KENT, 1998) é um mecanismo de segurança consolidado em relação ao protocolo IP. É possível encontrar menções à utilização de IPSec em 6loWPAN no trabaho de KUSHALNAGAR; MONTENEGRO; SCHUMACHER (2007) e tentativas de utilização nos trabalhos de Raza (RAZA et al., 2013) (RAZA et al., 2014).

O padrão 802.15.4 prevê três modos de segurança: Modo Inseguro, Modo de ACL e o Modo Seguro. O Modo Inseguro não proporciona nenhuma proteção para os quadros transmitidos. No Modo de ACL (*Access Control List*), um dispositivo pode se comunicar apenas com dispositivos que estejam em uma lista pré-configurada. Quadros recebidos de outros dispositivos são descartados. Esse modo não fornece nenhuma garantia de confidencialidade, integridade ou proteção contra reenvio (XIAO et al., 2006).

O Modo Seguro prevê a utilização de 7 níveis de segurança para a camada de enlace e física. Os níveis podem ser vistos na Tabela 2.2. Esses níveis podem prover proteção de integridade, confidencialidade, ou proteção de integridade e confidencialidade combinadas. Existe também proteção contra reenvio de mensagens (XIAO et al., 2006) (SASTRY; WAGNER, 2004).

O nível zero não prevê nenhuma proteção para as mensagens. A proteção de integridade é fornecida pela cifra AES-CBC-MAC-X. O “X” corresponde à extensão do Código de Integridade de Mensagem - *Message Integrity Code (MIC)*. Essas mensagens não são criptografadas. Essa

Tabela 2.2: Níveis de Segurança no Modo Seguro do Padrão 802.15.4
Fonte: Produzido pelos autores.

Nível de Segurança	Descrição	Dados Criptografados	Proteção de Integridade e Autenticidade	Informações de Segurança (Bytes)
0	Inseguro			0
1	AES-CBC-MAC-32		X	4
2	AES-CBC-MAC-64		X	8
3	AES-CBC-MAC-128		X	16
4	AES-CTR	X		5
5	AES-CCM-32	X	X	9
6	AES-CCM-64	X	X	13
7	AES-CCM-128	X	X	21

cifra protege a mensagem e seu cabeçalho com um código de integridade, que é calculado por blocos. O MIC é adicionado ao final da carga útil (XIAO et al., 2006) (SASTRY; WAGNER, 2004).

A confidencialidade é provida pelas cifras AES-CTR e AES-CCM-X. A cifra AES-CTR protege os dados utilizando AES sobre blocos de dados. Para isso um dado é dividido em blocos de 16 Bytes. Cada bloco usa um contador diferente durante o processo de criptografia. O contador faz parte do Vetor de Inicialização (*Initialization Vector,* IV), também conhecido como *nonce*. Este vetor é formado pela conjunção de alguns campos como um marcador estático e o endereço do emissor. Também é formado por três contadores: o contador de quadros (4 *Bytes*), contador de chave (1 *Byte*) e o contador para os blocos (2 *Bytes*). O emissor inclui o contator de quadros e o contador de chave na carga útil do quadro (XIAO et al., 2006) (SASTRY; WAGNER, 2004). Existem recomendações para a não utilização da cifra AES-CTR de forma isolada. A cifra não oferece proteção de integridade e já foi demonstrado que o mecanismo de proteção de reenvio é falho (SASTRY; WAGNER, 2004) (RAZA et al., 2014).

A cifra AES-CCM provê confidencialidade e proteção de integridade. Trata-se da aplicação dos dois mecanismos descritos anteriormente. Inicialmente é aplicada a proteção de integridade, que adiciona o MIC ao fim da carga útil. Em seguida, o processo de criptografia é aplicado sobre a carga útil e o MIC. O processo de criptografia adiciona os contadores à carga útil. Na Figura 2.9 é ilustrado o formato dos cabeçalhos e rodapés adicionais requeridos com a aplicação de segurança na camada física do padrão 802.15.4.

De acordo com sua especificação, o padrão 802.15.4 deve fornecer mecanismos para que camadas superiores controlem o nível de segurança com que os quadros serão transmitidos. O mecanismo é chamado de “Procedimento de Segurança do Quadro de Saída” (tradução livre). O procedimento depende de cinco entradas e gera uma ou duas saídas. As entradas são o quadro a ser protegido, o Nível de Segurança (*SecurityLevel*), o modo para identificar a chave utilizada para criptografia e autenticação (*KeyIdMode*), o originador da chave (*keySource*) e o índice da chave (*keyIndex*). As saídas do processo são o estado da operação e o quadro com segurança

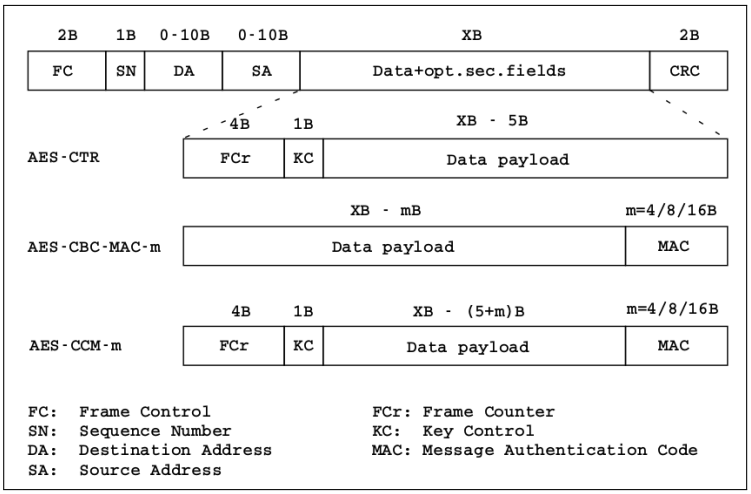


Figura 2.9: Formato do quadro do padrão 802.15.4 e sua relação com a segurança
Fonte: (RAZA et al., 2014)

aplicada, caso a operação seja realizada com sucesso. As entradas e saídas do "Procedimento de Segurança do Quadro de Saída" estão ilustradas na Figura 2.10.

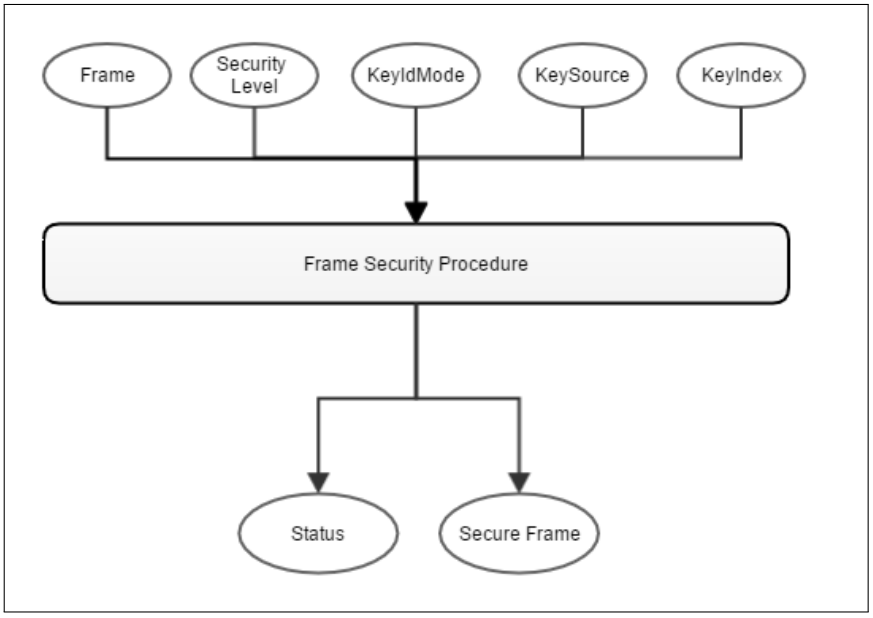


Figura 2.10: Descrição funcional da aplicação de segurança no padrão 802.15.4
Fonte: (COMMITTEE et al., 2011) adaptado.

O procedimento ocorre principalmente através da definição do nível de segurança. O nível de segurança e o comprimento dos dados são passados como parâmetros. O procedimento pode ser abortado caso algum desses valores seja passado de forma incorreta. Esse seria o caso de um nível de segurança inválido ou um valor para o comprimento dos dados que exceda o valor disponível por quadro. No melhor do nosso conhecimento, não existe referência para o funcionamento deste procedimento na presença de fragmentação (COMMITTEE et al., 2011).

2.2.6 Fragmentação em 6loWPAN

Quando um dado oriundo da subcamada 6loWPAN não couber em apenas um quadro 802.15.4, ele deve ser fragmentado. Para isso é adicionado um cabeçalho auxiliar de fragmentação. Qualquer mecanismo de segurança, quando houver, é aplicado após o processo de fragmentação (RAZA et al., 2014) (MONTENEGRO et al., 2007).

O cabeçalho auxiliar de fragmentação varia de acordo com a quantidade de fragmentos. O primeiro fragmento recebe um cabeçalho auxiliar composto por 4 octetos. Esses octetos são divididos entre um preâmbulo de 5 bits, o campo *datagram_size* e o campo *datagram_tag*. O cabeçalho auxiliar do primeiro fragmento é ilustrado na Figura 2.11. A partir do segundo fragmento, o cabeçalho auxiliar ganha o campo *datagram_offset*. O formato do cabeçalho auxiliar dos fragmentos subsequentes é representado na Figura 2.12.

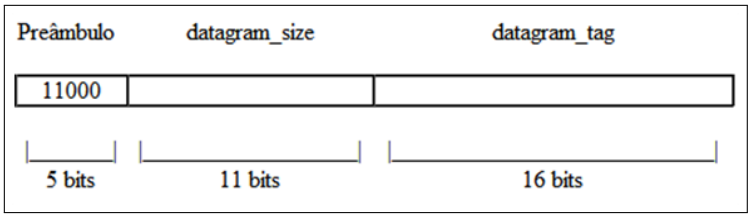


Figura 2.11: Formato do cabeçalho do primeiro fragmento
Fonte: Produzido pelos autores.

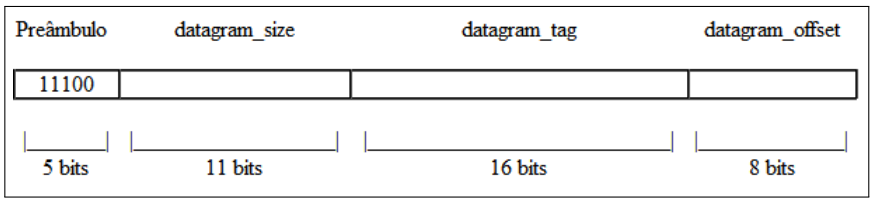


Figura 2.12: Formato do cabeçalho dos fragmentos subsequentes
Fonte: Produzido pelos autores.

O preâmbulo identifica se aquele é o primeiro fragmento, chamado de FRAG1, ou algum fragmento subsequente, chamado de FRAGN. O campo *datagram_size* contém o comprimento do pacote completo, antes da fragmentação. Seu valor é comum a todos os fragmentos, pois pode auxiliar na alocação de *buffer* caso os fragmentos cheguem fora de ordem. O campo *datagram_tag* contém um valor que identifica se um fragmento pertence a um determinado pacote. Esse valor é incrementado a cada novo pacote que necessita de fragmentação. O valor do campo *datagram_offset* indica o deslocamento de cada fragmento subsequente em relação ao primeiro fragmento. Ele permite que o pacote seja remontado de forma correta.

Quando o dado é fragmentado, os cabeçalhos do 6loWPAN e, consequentemente, das camadas superiores, são adicionados apenas ao primeiro fragmento. Isso reduz ainda mais o espaço disponível para carga útil, mas alivia os fragmentos subsequentes. Essa relação pode ser vista na Figura 2.13.

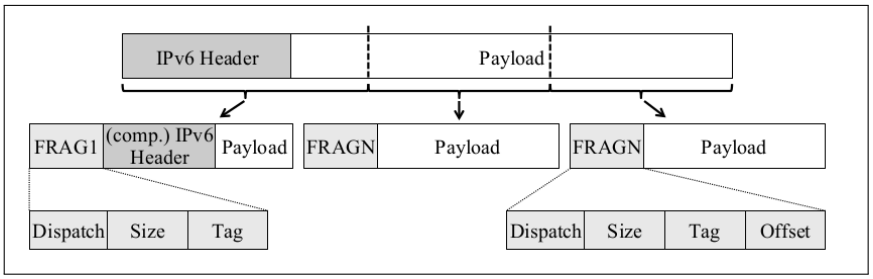


Figura 2.13: Alocação dos cabeçalhos das camadas superiores quando acontece fragmentação
Fonte: (HUMMEN et al., 2013)

Redes 6LoWPAN são propensas a perdas e esses defeitos são agravados pela presença da fragmentação. Os principais impactos para a transmissão de dados é que a fragmentação muda a modalidade de envio de mensagens. Geralmente, a taxa de geração de mensagens em uma rede é modelada por uma distribuição Poisson. Na presença de fragmentação, a rede se torna congestionada, uma vez que se considera que os fragmentos são transmitidos em rajadas (LUDOVICI et al., 2014) (POPE; SIMON, 2013). Além disso, as RSSF tendem a apresentar redes com muitos saltos entre o emissor e o receptor do dado. Quando um pacote passa por fragmentação, ele pode ter que ser remontado em cada salto, para depois ser encaminhado. Esse processo de montagem e desmontagem de pacotes reduz a quantidade de *buffers* nos dispositivos, gerando perda de pacotes (POPE; SIMON, 2013) (LUDOVICI et al., 2014).

2.3 Qualidade de Proteção

A popularização da Internet criou novas formas de comunicação, trabalho e sociabilidade. Muitas esferas da vida de uma pessoa começaram a migrar para os sistemas de informática e a quantidade de dados que trafegam por eles cresce a cada ano. O aumento da quantidade de dados na Internet leva a novas preocupações em como tratar esses dados, tanto em questões de processamento e armazenamento, quanto de utilização da rede.

A quantidade de pessoas conectadas à Internet tem aumentado. Mas a quantidade de dispositivos autônomos, que não precisam de um usuário para se conectar ou trafegar dados na Internet, superou a quantidade de usuários e esse número tende a crescer (GUBBI et al., 2013). O crescimento na quantidade de usuários e de dispositivos autônomos leva ao crescimento da preocupação com o armazenamento, processamento e tráfego desses dados além de uma preocupação com sua segurança.

Questões como autenticação e confidencialidade se tornaram críticos pela migração de vários serviços para as redes, pela quantidade de *hosts* e pelo tipo de informação que passou a trafegar por ela. Soma-se a isso a presença massiva de dispositivos com baixo poder de processamento e disponibilidade energética que estão conectados à Internet (GUBBI et al., 2013).

Uma das primeiras e mais conhecidas formas de quantificação é a Qualidade de Serviço - *Quality of Service* (QoS). A QoS é um conjunto de métricas, como largura de banda, atraso de

pacotes e flutuação de atraso, relacionadas com as necessidades de aplicações e com os recursos oferecidos pela rede (TANENBAUM, 2003). Outra metodologia de medição conhecida é a Qualidade da Experiência - *Quality of Experience (QoE)* -, que vem sendo largamente utilizada por relacionar os parâmetros da rede com as necessidades dos usuários (AGBOMA; LIOTTA, 2008) (KUIPERS et al., 2010) (SILLER; WOODS, 2003).

No quesito de quantificação de segurança existe a Qualidade de Proteção - *Quality of Protection* (QoP). QoP trata de como medir segurança e como aplicar essa medição de forma a levar agum benefício aos dados que trafegam por uma rede. Na maior parte dos trabalhos QoP é tratado como uma extensão de QoS, sendo tomada como uma medida da influência que a segurança tem sobre a qualidade na entrega de um serviço. QoP é relacionado a contextos sendo possível encontrar trabalhos em que a segurança é quantificada em cenários específicos. A principal aplicação de QoP é para a criação de serviços de segurança adaptáveis - *Tunable Security Service* (TSS). Esses serviços podem se adaptar as condições da rede, dos dispositivos ou da aplicação que pretendem atender, de acordo com alguma manipulação da rede ou do usuário.

Vários autores utilizaram a variação de segurança para manutenção dos parâmetros de QoP (AGARWAL; WANG, 2007) (LINDSKOG et al., 2006) (RACHEDI; HASNAOUI, 2015) (ONG; NAHRSTEDT; YUAN, 2003). Alguns deles procuram construir modelos para a relação entre a variação de segurança em QoS (AGARWAL; WANG, 2007) (LINDSKOG; FAIGL; BRUNSTROM, 2008) (LIM et al., 2009) (SUN; KUMAR, 2008). Uma parte deles, avalia o impacto da segurança em aplicações multimídia (AGARWAL; WANG, 2007) (ONG; NAHRSTEDT; YUAN, 2003) (LINDSKOG et al., 2006). Estes modelos, análises e avaliações fazem parte da Qualidade de Proteção. QoP pode ser definido como "uma medida dos benefícios de segurança fornecidos por abordagens de segurança" (ZHU et al., 2015).

Os primeiros a utilizar TSS foram ONG; NAHRSTEDT; YUAN (2003). A segurança é descrita como um fator que afeta a QoS em dispositivos com heterogeneidades em relação a recursos computacionais e de rede. Um dos resultados do trabalho é um equilíbrio entre segurança e performance para que os requisitos de serviços de multimídia sejam atendidos dispositivos com capacidades diferentes.

2.3.1 Modelos

A Qualidade de Proteção pode ser quantificada de duas formas: *Função de Utilidade* e *Recompensa*. A Função de Utilidade serve para quantificar as dimensões de segurança de um determinado protocolo ou um conjunto de protocolos AGARWAL; WANG (2007) (LIM et al., 2009) (LIM et al., 2009). Os principais modelos propõem a atribuição de valores relacionados à presença de um determinado serviço de segurança ou a força desse serviço. A função de Recompensa é o valor final obtido após as atribuições da função de utilidade (ONG; NAHRSTEDT; YUAN, 2003) (AGARWAL; WANG, 2007) (LIM et al., 2009) (LIM et al., 2009). Esse valor

pode ser usado para classificar os protocolos de acordo com algum critério preestabelecido como força ou desempenho.

2.3.1.1 Função de Utilidade

Para montar a função de utilidade, na maior parte dos casos, são utilizadas dimensões de segurança baseadas naquelas previstas nos serviços de segurança da ISO 7498-2 (STANDARDIZATION , GÈNEVE): autenticação (*authentication*), controle de acesso (*access control*), confidencialidade (*data confidentiality*), integridade (data integrity) e não-repúdio (*non-repudiation*). Existem variações em relação à utilização das dimensões de segurança, como discutido a seguir.

A primeira classificação, vista em ONG; NAHRSTEDT; YUAN (2003), é baseada em autenticação e criptografia, sendo esta última dimensão baseada em confidencialidade e integridade. Os serviços de segurança eram classificados principalmente de acordo com o comprimento da chave do algoritmo de criptografia. A possibilidade de adição de serviços de autenticação e de outros parâmetros no cálculo de QoP foi deixada em aberto.

Depois disso, AGARWAL; WANG (2007) inciou a utilização de mais parâmetros para montar a função de utilidade de um serviço de segurança. Foram utilizados autenticação, autenticação mútua, confidencialidade, integridade e não-repúdio. Inicialmente foi testada uma avaliação binária através da tentativa de identificar a presença ou ausência de cada uma das dimensões de segurança em uma *cipher suite*. Essa tentativa deixou espaço para muitos valores ambíguos, sendo necessária a atribuição de pesos para as dimensões. As duas abordagens podem ser vistas na Tabela 2.3 e na Tabela 2.4. A abordagem por atribuição de pesos tornou-se comum em outros trabalhos com QoP, principalmente porque ela remove a ambiguidade da classificação.

Tabela 2.3: Classificação de serviços de segurança baseada em uma abordagem binária. A presença de cada dimensão de segurança é indicada por um Y (yes, sim).
Fonte: (AGARWAL; WANG, 2007)

Policy	Security policies	Authentication	Confidentiality	Data integrity	Non repudiation	Mutual auth
P_1	No security (NS)					
P_2	WEP-128 bit key	Y	Y			
P_3	IPsec-3DES-SHA	Y	Y	Y	Y	Y
P_4	IPsec-3DES-SHA-WEP-128	Y	Y	Y	Y	Y
P_5	8021x-EAP-MD5	Y				
P_6	8021x-EAP-TLS	Y			Y	Y
P_7	8021X-EAP-MD5-WEP-128	Y	Y			
P_8	8021X-EAP-TLS-WEP-128	Y	Y		Y	Y
P_9	8021X-EAP-MD5-WEP-128-IPsec-3DES-MD5	Y	Y	Y	Y	Y
P_{10}	8021X-EAP-TLS-WEP-128- IPsec-3DES-MD5	Y	Y	Y	Y	Y
P_{11}	8021X-EAP-MD5-WEP-128-IPsec-3DES-SHA	Y	Y	Y	Y	Y
P_{12}	8021X-EAP-TLS-WEP-128-IPsec-3DES-SHA	Y	Y	Y	Y	Y

As mesmas dimensões de segurança utilizadas por AGARWAL; WANG (2007), foram utilizadas por LIM et al. (2009), com a adição de uma dimensão que leva em consideração as vulnerabilidades conhecidas de um protocolo de segurança. Essa dimensão é conhecida como Medida do Histórico de Vulnerabilidades (tradução livre) -*Historical Vulnerabilities Measurement (HVM)*. HVM é utilizada para indicar que um protocolo de segurança é mais

Tabela 2.4: Classificação de serviços de segurança baseada em uma abordagem com atribuição de pesos.
Fonte: (AGARWAL; WANG, 2007)

Security feature	Authentication (w_A)	Mutual authentication (w_M)	Confidentiality (w_C)	Data integrity (w_T)	Non-repudiation (w_R)
WEP-128 (shared)	1	–	1	–	–
802.1x-EAP-MD5	2	–	–	–	–
IPsec	3	1	2 (3DES)	2 (SHA)	1 (ESP)
IPsec/802.1x-EAP	–	–	–	1 (MD5)	–
802.1x-EAP-TLS	4	2	–	–	2

fraco de acordo com as vulnerabilidades que ele tenha ou caso ele tenha uma vulnerabilidade facilmente atacada ou conhecida. Foi atribuído um peso para cada uma das dimensões e para cada um dos protocolos de segurança em relação a uma dimensão de forma semelhante ao trabalho de AGARWAL; WANG (2007).

Em outro trabalho de LIM et al. (2009), a HVM foi retirada desse modelo, que foi formalizado com a utilização de 5 dimensões: autenticação e controle de acesso; gerenciamento de chaves; proteção de repetiçaõ do tráfego; autenticidade; e confidencialidade. Cada uma dessas dimensões possui caraterísticas, que tem pesos. A presença das dimensões e de duas características ditava o valor relativo de QoP de um protocolo ou de uma *Cipher Suite*.

2.3.1.2 Recompensa

A recompensa é um valor obtido a partir da função de utilidade que indica a força relativa de um protocolo de segurança. ONG; NAHRSTEDT; YUAN (2003) a define como "o benefício de segurança que a aplicação do usuário recebe em função dos parâmetros de qualidade de proteção fornecidos" (tradução livre). AGARWAL; WANG (2007) reforça o conceito afirmando que um "modelo de recompensa aditivo oferece uma visão macro dos benefícios associados com um protocolo de segurança" e pode ajudar a "decidir se uma determinada política é adequada para suas necessidades ou não". LUO et al. (2009) relaciona o termo à força de um protocolo de segurança. No contexto de redes heterogêneas, LIM et al. (2009) relaciona a função de recompensa com heterogeneidade e QoS. Ele afirma que esse valor obtido pode servir para "discriminar a avaliação das políticas de segurança híbridas e projetar componentes de segurança equilibrados".

O valor da recompensa não é absoluto, pois depende do cenário onde a medição de QoP está sendo aplicada. Serve, portanto, para classificar as configurações de segurança disponíveis. Como apresentado na seção anterior, a recompensa geralmente é obtida a partir da atribuição de valores para as dimensões de segurança. Essa atribuição pode ser binária ou por pesos.

Em ONG; NAHRSTEDT; YUAN (2003) as configurações de segurança acabam sendo elencadas apenas de acordo com o comprimento da chave de segurança. São atribuídos valores de 1 a 6 para os algoritmos e são atribuídos níveis de segurança. Chaves de 64 *bits* e 128 *bits* são consideradas de baixo nível, chaves de 196 *bits* são consideradas de nível médio e chaves de 256

bits são consideradas de alto nível de segurança. AGARWAL; WANG (2007) e LIM et al. (2009) adotaram modelos de pesos e tabelas para fazer a classificação dos protocolos de segurança.

2.3.2 Outros Modelos

Existem abordagens diferenciadas para quantificar segurança. Uma delas é encontrada em SUN; KUMAR (2008), que adotou um modelo de árvore de pesos. Nesse modelo, as características são organizadas como folhas e galhos de uma árvore. A soma de pesos das características entre a raiz e as folhas resulta o QoP de um sistema. Uma abordagem mais simples, é vista em no trabalho de LINDSKOG et al. (2006). Ao afirmar que segurança pode ser tratada como um parâmetro para QoS, e que existem ganhos em sua manipulação, eles basearam sua classificação na tabela de *cipher suites* do NIST (*National Institute of Standards and Technology*). Para justificar sua escolha, ele critica outros modelos de QoP afirmando que, apesar de o comprimento de uma chave de segurança poder ser usado para impor alguma ordem, como em ONG; NAHRSTEDT; YUAN (2003), nem sempre é possível elencar diferentes tipos de algoritmos criptográficos.

2.3.3 Aplicações da Qualidade de Proteção

A criação de Serviços de Segurança Adaptáveis é a principal aplicação de QoP. Para criar serviços adaptáveis é necessário quantificar a força de cada protocolo e seu impacto no desempenho da aplicação. Com essas informações são construídas aplicações ou serviços que buscam encontrar a melhor relação entre segurança e desempenho.

É possível ver um modelo teórico de TSS no trabalho de LINDSKOG; FAIGL; BRUNSTROM (2008). O modelo baseia-se em Configurações de Segurança, Preferências de Sintonização e Descritores de Ambiente e Aplicação. Este modelo é usado na maior parte dos trabalhos de QoP e TSS. As configurações de segurança são todas as *cipher suites* disponíveis em um serviço. Elas devem ser corretamente separadas segundo algum fator. Os autores do trabalho sugerem que esse fator seja o desempenho, que é facilmente mensurável, ou "diferenças de importância entre configurações", ou seja, QoP.

As preferências de sintonização são aquelas requeridas por usuários, administradores de rede ou mesmo as aplicações. Essas preferências podem ser definidas em termos de segurança ou performance. Por último são elencados os fatores ambientais que podem influenciar em desempenho e segurança. Esses fatores podem ser carga da rede ou sensibilidade dos dados.

2.4 Conclusão

O estabelecimento da Internet das Coisas depende da conexão de bilhões de dispositivos à Internet. Como a maior parte deles possui limitações de poder computacional, é preciso adotar algumas estratégias para que essa estrutura se consolide. Duas possíves estratégias podem ser

destacadas. A primeira, a utilização de tecnologias padronizadas, permitirá que aplicações independentes possam interagir de forma eficiente. Dessa forma, elas produzirão informações relevantes para os serviços que a Internet das Coisas fornece. A segunda, a adaptação de protocolos, é representada pelo 6loWPAN e pelos Serviços de Segurança Adaptáveis (TSS). Essa adaptação permite que os dispositivos limitados tenham ganhos de desempenho, possam atuar em ambientes heterogêneos e possam ser acessados diretamente através da Internet.

3

TRABALHOS CORRELATOS

O objetivo deste capítulo é apresentar os principais trabalhos relacionados com a avaliação da fragmentação, com a Qualidade de Proteção e com os Serviços de Segurança Adaptáveis.

3.1 Introdução

Este capítulo apresenta os principais trabalhos relacionados aos problemas da fragmentação nas aplicações da Internet das Coisas. É demonstrado que existem impactos na transmissão de dados, mas também existem trabalhos que demonstram sua influência em protocolos de negociação, gerenciamento de rede e mesmo de segurança. Também são apresentados trabalhos relacionados a Qualidade de Proteção e Serviços de Segurança Adaptáveis, buscando demonstrar os cenários em que foram aplicados e como foram aplicados.

3.2 Fragmentação

A preocupação com a fragmentação está presente desde o desenvolvimento das RSSF. Esse problema voltou à discussão quando tornou-se necessário conectar esses dispositivos diretamente à Internet. Essa nova conectividade faz dispositivos das redes 6loWPAN, cuja unidade máxima de transmissão é 127 *bytes*, terem que lidar com o troca de dados diretamente com a Internet usando IPv6, cujo MTU - *Maximum Transmission Unity* - é de 1280 *bytes*. (DEERING; HINDEN, 1998) Procurou-se então propor novos protocolos de transmissão, assim como melhorias nos protocolos existentes para lidar com o problema. (MONTENEGRO et al., 2007) (SHELBY; BORMANN, 2011).

Desde HARVAN; SCHÖNWÄLDER (2008) e CODY-KENNY et al. (2009) até LUDOVICI et al. (2014) a preocupação com a fragmentação é constante. O trabalho de HARVAN; SCHÖNWÄLDER (2008) apresenta uma das primeiras análises do impacto da fragmentação em dispositivos limitados. Seus resultados apontam um crescimento no *round-trip* time usando ICMP - *Internet Control Message Protocol* - com mensagens echo que vão de 100 *bytes* a 1280 *bytes*. Apesar disso, seu cenário é simplificado com a presença de apenas um sensor. (CODY-KENNY et al., 2009) avaliaram o impacto no atraso e na perda de pacotes usando ICMP num *testbed* contendo 3 dispositivos e 1 estação base. Seus resultados mostraram aumento no atraso relacionado ao aumento no tamanho das mensagens. POPE; SIMON (2013) fizeram uma avaliação usando cenário com 16, 36 e 64 dispositivos, mas avaliaram apenas o processo de fragmentação até 2 fragmentos. Um resumo desses trabalhos pode ser visto na Tabela 3.1. Existem buscas de métodos para eliminar ou atenuar os efeitos da fragmentação, como pode ser visto em KEOH; KUMAR; TSCHOFENIG (2014).

Tabela 3.1: Trabalhos relacionados a fragmentação do 6loWPAN na comunicação

	HARVAN; SCHÖNWÄLDER, 2008	CODY-KENNY et. al. 2009	POPE; SIMON, 2013
Descrição	RTT em,ICMP de 100 bytes a 1280 bytes	Atraso e perdas em ICMP	16, 36 e 64 dispositivos
Pontos Negativos	1 sensor	4 sensores	2 fragmentos

O estudo e correta avaliação do impacto na fragmentação não é necessário apenas em cenários de transmissão de dados. Alguns protocolos que auxiliem no gerenciamento, formação e manutenção de uma rede também podem precisar levá-la em consideração. KURYLA; SCHÖNWÄLDER (2011) são levados a analisar o impacto da fragmentação no desenvolvimento de uma versão do Protocolo Simples de Gerência de Rede - *Simple Network Management Protocol (SNMP)* - para redes de dispositivos limitados. Algumas das mensagens trocadas pelo protocolo tinham tamanho próximo ou eram maiores que os 127 *bytes* permitidos no quadro do padrão 802.15.4. Essas mensagens sofriam fragmentação, e isso foi analisado como um problema para a implantação do protocolo.

No trabalho de RAZA et al. (2013) existe a preocupação com fragmentação no desenvolvimento de uma implementação de uma versão leve e segura do CoAP - *Constrained Application Protocol*. Métodos de compressão de mensagens de negociação do Protocolo de Segurança da Camada de Transporte de Datagramas - *Datagram Transport Layer Security (DTLS)* - foram propostos. Mesmo assim, nem sempre era possível evitar fragmentação, pois algumas mensagens permaneciam com comprimento maior do que o máximo permitido.

O desenvolvimento de novos protocolos e a evolução dos antigos requer novas avaliações dos mecanismos de fragmentação existentes. O protocolo CoAP oferece a possibilidade de transferência de dados através de *blockwise tranfer*. Trata-se de uma forma de dividir uma requisição ou uma resposta, de forma que cada parte seja transmitida como uma requisição independente nas camadas mais baixas da pilha de protocolos. Dessa forma, cada parte é transmitida e confirmada individualmente e pode ser retransmitida em caso de perda. Caso a requisição completa fosse enviada para as camadas inferiores e sofresse fragmentação, a perda de um dos fragmentos poderia gerar a retransmissão de toda a requisição. A retransmissão causa atrasos e aumento no consumo energético. (BORMANN; SHELBY, 2013)

Pensando nisso, LUDOVICI et al. (2014) realizaram uma comparação entre fragmentação e *blockwise tranfer*. Seus resultados apontam que a transmissão da requisição completa para que seja fragmentada na camada de rede pode ser mais eficiente que a utilização do mecanismo de *blockwise transfer*. Isso ocorre pois o CoAP demanda a troca de mais mensagens, gerando mais ocupação no canal que as confirmações da camada de rede.

No trabalho de RACHEDI; HASNAOUI (2015) é observada a avaliação do impacto da segurança para a construção de rotas pelo protocolo RPL em redes 6loWPAN. Para isso eles se preocuparam com o impacto computacional de criptografar e descriptografar os dados. Esse impacto alimentava um Controlador Proporcional-Integral-Derivativo (PID) para a construção de rotas do tipo Vetor de Distância - *Ad-hoc On-demand Distance Vector (AODV)*. Ainda assim não foram investigados os impactos que a fragmentação podia proporcionar, visto que a transmissão de dados pode acarretar a elevação do atraso e do consumo energético. Um resumos dos trabalhos que relacionam a fragmentação do 6loWPAN com outros protocolos pode ser visto na Tabela 3.2.

Apesar destes trabalhos proporem melhorias, a maior parte dos cenários avaliados se constitui de cenários simplificados no contexto da Internet das Coisas. A simplicidade ocorre,

Tabela 3.2: Trabalhos relacionados com o impacto da fragmentação do 6loWPAN em outros protocolos

	KURYLA; SCHÖNWÄLDER, 2011	RAZA et. al., 2013	LUDOVICI et. al., 2014	RACHEDI; HASNAOUI, 2015
Descrição	SNMP para redes de sensores	Atraso e perdas em ICMP	16, 36 e 64 dispositivos	Segurança para determinação de rotas
Pontos Negativos	Sem proposta de redução	Sem proposta de redução	Sem proposta de redução	Sem avaliação da fragmentação

principalmente, em relação a quantidade reduzida de dispositivos, onde o modelo mais comum trata da avaliação utilizando apenas dois dispositivos. Essa simplificação pode não condizer com a realidade de um cenário de Internet das Coisas. LUDOVICI et al. (2014) realizou a avaliação em ambientes com mais dispositivos, mas não propôs mecanismos de eliminação ou atenuação dos efeitos da fragmentação.

3.3 QoP e TSS

Os primeiros a se preocupar com os efeitos que o nível de segurança pode causar em aplicações que utilizem redes de computadores foram ONG; NAHRSTEDT; YUAN (2003). Sua principal preocupação foi com aplicações multimídia para as quais tentou avaliar a melhor relação entre desempenho e nível de segurança. Dessa forma, seu modelo de Qualidade de Proteção - *Quality of Protection* (QoP) - ficou definido como uma extensão de um modelo de Qualidade de Serviço - *Quality of Service* (QoS). Seguindo esse raciocínio, LINDSKOG; FAIGL; BRUNSTROM (2008) afirmou que a mesma configuração de segurança pode causar efeitos diversos dependendo do cenário onde é aplicada. Alguns desses efeitos podem ser a maior utilização da banda disponível ou o aumento no tempo para o início de uma conexão.

A questão dos níveis de segurança pode ser vista parcialmente no trabalho de LIM et al. (2009) com a afirmação de que mecanismos de segurança pode ser adicionados a camadas superiores para sobrepor as falhas de camadas mais baixas. ONG; NAHRSTEDT; YUAN (2003) e LINDSKOG et al. (2006) relacionaram QoP e os níveis de segurança lembrando da existência de dispositivos com limitações de processamento e com as questões de desempenho que podiam ser percebidas pelos usuários, principalmente em redes sem fio. Autores como AGARWAL; WANG (2007) e LIM et al. (2009) fizeram análises de QoP em redes sem fio. Esse tipo de análise se fortaleceu desde ONG; NAHRSTEDT; YUAN (2003). A maior parte dos estudos se deteve a esse tipo de rede devido as suas características de limitações de desempenho.

Em AGARWAL; WANG (2007) e LIM et al. (2009) são demonstradas relações de QoP com redes heterogêneas e ambientes de mobilidade. Uma preocupação semelhante é vista em SUN; KUMAR (2008). Em seu trabalho existe a análise do fluxo de dados entre dispositivos com diferentes níveis de segurança. Para isso, segurança deveria ser efetiva e sistematicamente

medida e classificada em todos os níveis de todos os dispositivos. Essa preocupação surgiu pois alguns dados precisavam trafegar por redes cujo nível de segurança era considerado mais baixo que o requerido no momento da transmissão.

Em alguns trabalhos, QoP é definido como a medida de força de um protocolo de segurança. (LIM et al., 2009) Entretanto, esta não parece ser uma definição adequada, visto que QoP é aplicada em cenários muito específicos e não existem trabalhos que procuram fornecer valores absolutos para a quantificação.

À partir das motivações dos principais trabalhos relacionados verifica-se que QoP pode ser definida como uma métrica que quantifica relativamente protocolos de segurança em um dado cenário, determinando níveis de segurança. (AGARWAL; WANG, 2007) Esses níveis podem ser estudados sob algumas perspetivas: nível de segurança e sua influência no desempenho da aplicação; nível de segurança nas camadas de uma pilha de protocolos; e níveis de segurança em redes heterogêneas .

Na primeira dela os níveis são compreendidos como os diferentes serviços de segurança que um protocolo pode fornecer e a influência de cada serviço no desempenho da aplicação. Nem sempre o protocolo de segurança mais forte causa uma maior degradação do desempenho. QoP trata, então, da busca pela melhor relação entre desempenho e segurança.

Outra forma de estudar os níveis de QoP é na relação entre a segurança aplicada nas diversas camadas de uma pilha de protocolos. O conjunto de protocolos de segurança aplicado as camadas é chamado *Cipher Suite* (Conjunto de Cifras de Segurança, em tradução livre). Cada camada possui um conjunto de protocolos de segurança. Níveis de segurança diferentes podem ser combinados de diversas maneiras enquanto o dado é encapsulado nas camadas. (LINDSKOG et al., 2006) (AGARWAL; WANG, 2007) (LINDSKOG; FAIGL; BRUNSTROM, 2008). Dependendo da aplicação, pode ser aplicada um nível mais alto de segurança nas camadas mais baixas (ambientes de redes sem fio) e um nível mais baixo de segurança nas camadas mais altas (dados não sigilosos). Aplicar níveis altos de segurança em todas as camadas pode causar aproveitamento ineficiente da banda disponível da camada física, como é o caso protocolo 802.15.4 para redes de sensores, que disponibiliza quadros de apenas 127 *bytes* e banda de 250 kbps. (LINDSKOG et al., 2006) (AGARWAL; WANG, 2007) (LINDSKOG; FAIGL; BRUNSTROM, 2008)

Uma terceira abordagem sobre os níveis de QoP é relacionada ao tratamento de heterogeneidade de protocolos e dispositivos. A Internet atualmente é formada por diversos tipos de rede. Dados podem trafegar por diversas redes com configurações de segurança e desempenho diferentes. O nível de segurança deve ser mantido durante o trajeto dos dados apesar das diferenças de protocolos. (LIM et al., 2009)

Cada trabalho, com suas motivações, deu origem a um modelo de QoP. Os modelos presentes nos trabalhos de AGARWAL; WANG (2007) e LIM et al. (2009) são baseados em Função de Utilidade e Recompensa. SUN; KUMAR (2008) criaram modelos de QoP baseados em pesos e rótulos.

A principal aplicação de modelos de QoP são os Serviços de Segurança Sintonizáveis - *Tunable Security Service* (TSS). A maior parte deles é baseado na recompensa fornecida pela QoP.Podem ser encontradas utilizações práticas em ONG; NAHRSTEDT; YUAN (2003), LINDSKOG et al. (2006) e LINDSKOG; FAIGL; BRUNSTROM (2008).

Para usar TSS, ONG; NAHRSTEDT; YUAN (2003) classificaram os protocolos de segurança com base no comprimento da chave de segurança, no método de autenticação, no algoritmo de criptografia e no comprimento do dos blocos criptográficos. O TSS foi configurado para manipular o comprimento da chave e o método de autenticação. Baseado nisso, as métricas avaliadas foram a sobrecarga de segurança e a vazão. O TSS foi operacionalizado através de um *media-player* baseado em QoP.

O TSS em LINDSKOG et al. (2006) manipulava as suítes de segurança, classificadas de acordo com as regras do Instituto Nacional de Padrões e Tecnologia dos Estados Unidos - *National Institute of Standards and Technology (NIST)* - para obter ganhos em relação a latência computacional e a latência da rede. Também foram avaliadas redes com dispositivos heterogêneos.

O trabalho de (RACHEDI; HASNAOUI, 2015), é baseado na numa classificação de segurança em nível alto, médio e baixo, cada um deles fornecendo combinações de integridade, confidencialidade, proteção de repetição e não repúdio. O nível mais baixo possui apenas integridade, o nível médio provê apenas integridade e confidencialidade, e o nível alto provê uma tudo isso além de proteção de repetição e não repúdio. São avaliados o consumo energético, o atraso, a vazão e a segurança da rede.

A modelagem de TSS no trabalho de LINDSKOG; FAIGL; BRUNSTROM (2008) é baseado em três blocos: as Configurações de Segurança - *Security Configurations (S)* - , as Preferências de Sintonização - *Tuner Preferences (T)*, e os Descritores de Ambiente e Aplicação - *Environment and Application Descriptors (E)* . A relação entre os blocos é demonstrada na equação (3.1).

$$\boxed{TSS{:}\, T \times E \rightarrow S} \tag{3.1}$$

De acordo com a equação, as Configurações de Segurança, as Preferências de Sintonização e as Descritores de Ambiente, são as entradas do TSS. O criador do modelo, define que os três blocos devem ser definidos pelo projetista do TSS. (LINDSKOG; FAIGL; BRUNSTROM, 2008) alega que as Configurações de Segurança devem ser classificadas segundo algum critério, mas não determina qual deve ser usado. As Preferências de Sintonização são fatores que influenciam a decisão de manipular a segurança. As decisões de usuários ou os fatores de desempenho, relacionados, principalmente, a QoS, compõem o escopo do bloco. Por fim, os Descritores de Ambiente são fatores que são independentes das decisões dos usuários, mas que influenciam a tomada de decisão sobre o TSS. Entre eles estão:o tipo de dispositivos, o tipo de rede, o comprimento dos dados e o nível de confidencialidade requerida pelos dados.

Ainda no tocante a TSS, ONG; NAHRSTEDT; YUAN (2003) criaram um *middleware* que possuía vários módulos responsáveis por procurar o equilíbrio entre fornecer QoP e QoS para sua aplicação de multimídia. O nível de segurança é apresentado para escolha do usuário e o nível de QoS é apresentado pela aplicação. Um *middleware* ficava responsável por encontrar os níveis de segurança disponíveis na rede e o nível de QoS necessário para a aplicação. Para isso foram medidos os tempo de autenticação e encriptação de diversos protocolos de segurança.As medições no trabalho de LINDSKOG et al. (2006) foram usadas para construir uma aplicação onde era possível definir manualmente o equilíbrio entre segurança e desempenho em um ambiente 802.11i. O trabalho de RACHEDI; HASNAOUI (2015) também está relacionado a QoP, apesar de não estar explicitado no trabalho, devido a sua preocupação com o impacto da segurança na definição de rotas.

Os principais trabalhos relacionados a QoP, e apresentados nesta seção, foram divididos em trabalhos que fornecem modelos e avaliações de desempenho, ou TSS. Um resumo desses trabalhos é apresentado nas tabelas 3.3 e 3.4. Na Tabela 3.3 são apresentados os trabalhos cuja proposta é um modelo analítico sobre QoP. Os modelos foram utilizados para quantificar QoP de diferentes formas.

A Tabela 3.4 contém um resumo avaliações de desempenho, apresentadas nesta seção, relacionadas a QoP e TSS.

Tabela 3.3: Modelos analíticos baseados em QoP

	AGARWAL; WANG (2007)	LINDSKOG; FAIGL; BRUNSTOM (2008)	SUN; KUMAR (2008)	LIM et. al. (2009)
Justificativa	Existe muita heterogeneidade nas redes sem fio	Uma determinada configuração de segurança pode causar impactos diferentes em redes diferentes. Essa decisão é tomada pelo projetista do sistema	Falta de sistematização na avaliação de segurança	Preocupação com o balanço entre o nível de segurança e os parâmetros de QoS
Classificação	Função de utilidade e Recompensa	Configurações de Segurança	Pesos e rótulos	Função de utilidade e Recompensa
Parâmetros	Nível de segurança	Análise	Dependem da aplicação	Análise
Métricas	Tempo de autenticação, Sobrecarga de autenticação, Vazão	Análise	Mensuráveis e previsíveis	Análise
Solução	Análise	Análise	Análise	Análise
Cenário	Cenários de *Roaming* e Não-*roaming* em redes IP sem fio	Redes 802.11	Sistema Cibernético (Qualquer sistema)	Redes sem fio

Tabela 3.4: Avaliações de desempenho relacionadas a QoP

	ONG; NAHRSTEDT; YUAN, 2003	LINDSKOG et al., 2006	RACHEDI; HASNAOUI, 2015
Justificativa	Dispositivos com caracteristicas diferentes na mesma rede	Segurança deve ser usada como um parâmetro de QoS devido as restrições de alguns dispositivos	Existem aplicações na Internet das coisas que necessitam de garantias de QoS
Classificação	Tamanho da chave, método de autenticação, algoritmos de criptografia, Comprimento de um bloco	NIST	Nivel alto, médio e baixo
Parâmetros	Comprimento da chave, Método de autenticação	Suites de segurança, Tráfego da rede, Tipos de Dispositivos	Densidade da rede, tráfego, tempo
Métricas	Sobrecarga de Segurança e Atraso	Latência computacional, Latência na rede	Consumo energético, atraso, vazão e segurança
Solução	*QoP-aware media player*	Gui contendo uma régua para escolha da relação entre segurança e performance	QwS AODV - Framework baseado em controlador PID para a integração entre QoS e Segurança na determinação de rotas
Cenário	Rede local	Rede local	Redes 802.15.4

3.4 Conclusão

Neste capítulo verificou-se que existe uma preocupação com a transmissão de dados pelos dispositivos limitados das Redes de Sensores sem Fio na Internet das Coisas. Dentre os fatores que impactam a transmissão, a fragmentação ainda é um problema, uma vez que existe uma tendência ao aumento no comprimento dos dados transferidos nessas redes. Os impactos da fragmentação tem sido analisados de forma extensiva, mas ainda existe uma demanda pela busca de soluções que podem atenuar seus efeitos.

A Qualidade de Proteção procura encontrar a melhor relação entre desempenho da rede e nível de segurança, principalmente a partir de TSS. QoP foi aplicada em cenários de redes sem fio e com heterogeneidade. Esse tipo de cenário é semelhante ao que se encontra na Internet das Coisas.

4

SERVIÇO DE SEGURANÇA ADAPTÁVEL

Neste capítulo é apresentada uma proposta de aplicação de Serviços de Segurança Adaptáveis - TSS - para redes 6loWPAN baseadas em 802.15.4.

4.1 Introdução

Este capítulo apresenta a descrição do Serviço de Segurança Adaptável - TSS - destinado a aplicações da Internet das Coisas baseadas em 6loWPAN e no padrão 802.15.4. O Serviço foi traduzido para "Adaptável"e não "Sintonizável", por ser um Serviço ativo e não depender de configuração manual, como outros trabalhos citados. O TSS utiliza a adaptação do nível de segurança para prover melhoras de desempenho para o sistema em que está inserido (LINDSKOG; FAIGL; BRUNSTROM, 2008). No cenário apresentado, o resultado da adaptação do nível de segurança, feito pelo TSS, é o controle da fragmentação. O TSS adapta o nível de segurança para encontrar uma quantidade ótima de fragmentos a ser transmitida. Dessa forma é possível obter redução no atraso da entrega de mensagens e no consumo energético. A ativação do TSS acontece com base na premissa de que a carga útil de cada fragmento do padrão 802.15.4 pode variar dependendo do nível de segurança e dos cabeçalhos que são inseridos.

4.2 Serviço de Segurança Adaptável

A utilização de TSS em aplicações da Internet das Coisas que utilizam o padrão 802.15.4 é capaz de manter a fragmentação controlada, principalmente quando se procura transmitir apenas um fragmento, ou quadro (MONTENEGRO et al., 2007), reduzir a fragmentação, mesmo quando não for possível transmitir apenas um fragmento; e reduzir os efeitos da fragmentação em termos de atraso e consumo energético.

Para isso, dois módulos são propostos. O primeiro módulo detecta os Limites de Fragmentação e o segundo módulo utiliza o resultado da detecção para ativar o serviço, provendo o nível de segurança adequado para a transmissão de dados pelo padrão 802.15.4. Juntos, os dois módulos formam o TSS que é a proposta deste trabalho. O termo Limite de Fragmentação representa um intervalo de valores em que a quantidade de dados provenientes da camada de rede apresenta variação na quantidade de fragmentos de acordo com o nível de segurança da transmissão. A utilização do TSS se justifica nas situações em que a fragmentação é originada pela aplicação de segurança.

Algumas implementações do protocolo IPv6, como é o caso do Uip (lê-se micro IP) (DUNKELS, 2003), oferecem mecanismos para estimar a quantidade de fragmentos que serão gerados na camada MAC, de acordo com a quantidade de dados. Essas estimativas são utilizadas para determinar se existem *buffers* de transmissão suficientes para receber os dados que chegam à subcamada 6loWPAN. Para o cálculo é levada em consideração apenas a adição do cabeçalho de endereçamento do padrão do 802.15.4. O TSS apresentado é capaz de fazer uma estimativa precisa da quantidade de fragmentos a partir da relação entre a quantidade de dados por fragmento e o nível de segurança. A comparação entre a transmissão de dados tradicional e a transmissão utilizando TSS é demonstrada na Figura 4.1.

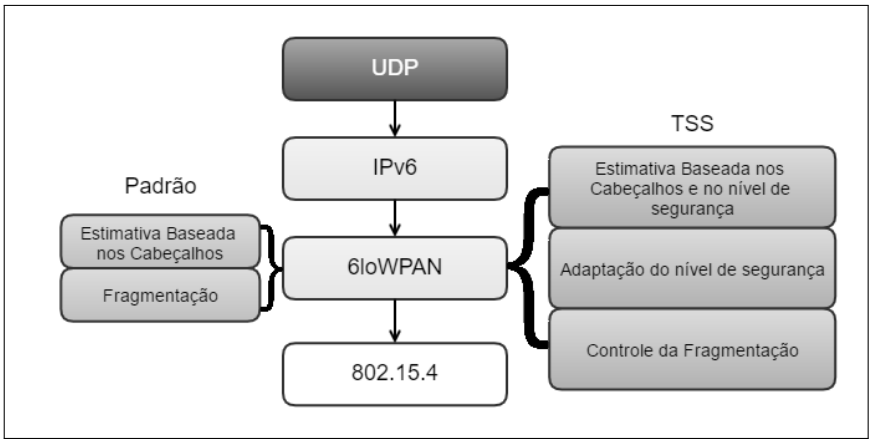


Figura 4.1: Comparação entre a transmissão de dados tradicional e a transmissão utilizando TSS
Fonte: Produzido pelos autores.

4.3 Módulo para Detecção dos Limites de Fragmentação

O primeiro módulo da proposta deste trabalho consiste em determinar uma forma precisa de estimar a quantidade de fragmentos. Essa estimativa deve ser utilizada pelo 6loWPAN. Neste módulo, busca-se levar em consideração os dados de segurança e o cabeçalho de fragmentação adicionados em cada fragmento e não apenas o comprimento do cabeçalho de endereçamento, como implementado no padrão do protocolo.

A estimativa da quantidade de fragmentos é implementada pelo módulo "Limites de Fragmentação", representado pelo Algoritmo 1. O algoritmo possui três variáveis: *SicsLowOneFragLen*, *SicsLowFrag1Len* e *SicsLowFragNLen*. Essas variáveis representam a quantidade de carga útil que um quadro pode transportar após a adição do MIC de acordo com o nível de segurança. A estimativa deve ser feita para todos os níveis de segurança disponíveis do dispositivo 802.15.4 utilizado para a transmissão de dados. Os valores são deixados como variáveis, pois a implementação do padrão 802.15.4 e do 6loWPAN pode variar entre os dispositivos.

Algoritmo 1: Estimativa da quantidade de fragmentos

Algoritmo *Fragmentation Threshold*
Entrada
    len: Data Length
Saída $estimated\_fragments$
1 **se** $len <= SicsLowOneFragLen$ **então**
2 $estimated\_fragments = 1$
3 **senão**
4 $estimated\_fragments = roundUp((len - SicsLowFrag1Len)/SicsLowFragNLen) + 1$
5 **devolva** $estimated\_fragments$

Na estimativa encontrada na implementação do Uip, não existe separação entre o comprimento da carga útil no primeiro fragmento e os fragmentos subsequentes. Essa separação deve ser feita, uma vez que a quantidade de dados disponível por quadro é pequena. Por este motivo, a variável *SicsLowOneFragLen* é deixada isolada para detectar a criação de apenas um fragmento. Isso é demonstrado nas linhas 1 e 2 do algoritmo 1.

A presença de duas variáveis, *SicsLowFrag1Len* e *SicsLowFragNLen*, na linha 4 do Algoritmo 1 é relacionada à adição do cabeçalho de fragmentação, que possui valores diferentes para o primeiro fragmento e para os fragmentos seguintes. Para esse cálculo, a quantidade de dados do fragmento inicial é subtraída da quantidade total de dados. A quantidade de dados restante é, então, dividida pelos fragmentos seguintes.

Os valores das variáveis podem ser obtidos em função dos cabeçalhos e dados adicionais de segurança e fragmentação encontrados em cada quadro, como demonstrado nas Equações 4.1 e 4.2. A variável *SicsLowOneFragLen*, exposta na Equação 4.1, representa a carga útil de apenas um dado não fragmentado após a adição do cabeçalho de endereçamento, dos cabeçalho adicional de segurança, do MIC e do Código de Verificação de Redundância Cíclica -*Cyclic Redundancy Check (CRC)*. O MIC e o cabeçalho adicional de segurança são representados pela variável $SecurityLevelData$. A variável *SicsLowOneFragLen* representa uma quantidade maior de carga útil por quadro, pois nenhum cabeçalho de fragmentação foi adicionado.

$$SicsLowOneFragLen = frameSize - HeaderLenght - SecurityLevelData - CRC \tag{4.1}$$

As variáveis *SicsLowFrag1Len* e *SicsLowFragNLen*, representadas pela Equação 4.2, correspondem a carga útil dos quadros de um dado fragmentado. Seus valores representam a quantidade de *bytes* disponíveis para dados após a adição dos mesmos cabeçalhos e dados adicionais da *SicsLowOneFragLen*, além do cabeçalho de fragmentação. A variável *SicsLowFrag1Len* apresenta um valor menor que *SicsLowOneFragLen*, devido à subtração do valor do comprimento do cabeçalho de fragmentação, mas é maior que *SicsLowFragNLen*. Isso acontece porque o cabeçalho de fragmentação nos fragmentos subsequentes é maior, reduzindo o espaço para carga útil.

$$SicsLowFrag1Len = SicsLowOneFragLen - fragmentationHeader \tag{4.2}$$

Como demonstrado pelas Equações 4.1 e 4.2, os valores que alimentam o Algoritmo 1 são diferentes para cada nível de segurança quando esses valores estiverem dentro dos Limites de Fragmentação. Os valores obtidos de acordo com os dados presentes na especificação do padrão 802.15.4 são apresentados na Tabela 4.1.

Tabela 4.1: Valores para as variáveis dos Algoritmos de acordo com a especificação do padrão 802.15.4

	SicsLowFragOneFragLen (bytes)	SicsLowFrag1Len (bytes)	SicsLowFragNLen (bytes)
Nivel 5	93	89	88
Level 6	89	85	84
Nivel 7	81	77	76

4.4 Aplicação da Detecção dos Limites de Fragmentação

A construção de uma relação entre aplicação de segurança e fragmentação é a principal função do Módulo de Detecção dos Limites de Fragmentação. Conforme apresentado na Tabela 2.2, cada nível de segurança adiciona uma quantidade de dados em cada quadro. Independente disso, um cabeçalho extra é adicionado caso seja necessário fragmentar os dados. Assim, a redução do espaço disponível para dados úteis, causada pela adição de segurança, pode ser agravada pelo processo de fragmentação, pois cada novo fragmento tem dados de segurança independentes.

A relação entre o nível de segurança e a quantidade de dados disponível por quadro pode ser vista na Figura 4.2. É possível observar a redução percentual entre um dado transmitido sem fragmentação e sem adição de segurança, na parte superior, e um dado fragmentado e com o nível máximo de segurança. Relações semelhantes são encontradas nos outros níveis de segurança.

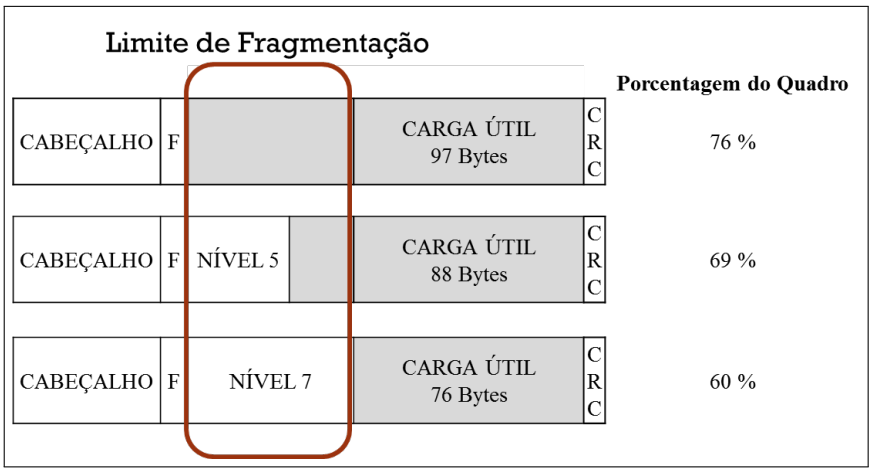


Figura 4.2: Relação entre o nível de segurança, a fragmentação e a quantidade de dados disponível por quadro, representando os "Limites de Fragmentação"
Fonte: Produzido pelos autores.

À partir da Figura 4.2, é possível compreender o termo "Limite de Fragmentação". O quadro com segurança em nível 7 pode transmitir até 75 *bytes* em apenas um fragmento. Se for necessário transmitir 76 *bytes*, dois fragmentos serão gerados. Se a aplicação precisar entregar 76 *bytes*, mas depender da entrega de apenas um fragmento, seja por questões de atraso, consumo energético ou ocupação da rede, não será possível utilizar o nível 7 de segurança e ela deverá utilizar um nível inferior. NEste caso, e de acordo com a Figura 4.2, pode ser utilizado o nível 5.

O mesmo pressuposto se aplica para dados de até 88 *bytes*, que não poderão ser transmitidos em apenas um fragmento caso o nível 5 de segurança seja utilizado. A essa diferença, entre a quantidade de dados disponíveis por fragmento de acordo com o nível de segurança, é dado o nome de Limite de Fragmentação. O Limite de Fragmentação entre os níveis 5 e 7 é o intervalo $[76, 83]$ pois, para acada um desses valores, o nível de segurança impactará na quantidade de fragmentos transmitidos.

A Equação 4.3, baseada no algoritmo 1, serve para derivar os Limites de Fragmentação. De acordo com a equação, a diferença encontrada em cada quadro se intensifica conforme a quantidade de dados aumenta. Utilizado os valores da Tabela 4.1 na equação é possível obter a relação entre a quantidade de dados, o nível de segurança e a quantidade de fragmentos. Essa relação é ilustrada no gráfico da Figura 4.3. Nele, verifica-se o impacto do tamanho da mensagem na fragmentação quando a quantidade de dados que chega a subcamada 6loWPAN está dentro dos Limites de Fragmentação. É possível observar que existe uma tendência a um aumento cada vez maior na quantidade de fragmentos se uma determinada quantidade de dados for transmitida com níveis de segurança diferentes.

$$\begin{cases} ft(dataLen) = 1, \ \ if \ dataLen < SicslowOneFragLen \\ ft(dataLen) = \ roundUp\left[\dfrac{dataLen - SicsLowFrag1Len}{SicsLowFragNLen}\right] + 1, otherwise \end{cases} \tag{4.3}$$

O gráfico na Figura 4.3, demonstra que uma transmissão de 80 bytes pode gerar 1 ou 2 fragmentos dependendo no nível de segurança. Algumas aplicações podem ser impactadas caso isso ocorra. Desde 80 até 540 *bytes*, quando a mesma quantidade de dados é transmitida com nível 7 ocorre o aumento de 1 fragmento em relação à transmissão com nível 5, ou mesmo com nível 0. Depois disso começam a aparecer discrepâncias maiores. É possível observar, já na transmissão de 640 *bytes*, que existe um aumento de fragmentos na transmissão de dados com nível 7 e com nível 0, sendo mantido o aumento de 1 fragmento em relação ao nível 5. À partir da transmissão de 940 *bytes*, começa a existir uma diferença de 2 fragmentos mesmo entre dados seguros do nível 5 e do nível 7. Nesse contexto, justifica-se a utilização de um mecanismo que se utilize do nível de segurança para reduzir ou mesmo evitar fragmentação, nesse caso, o TSS (RACHEDI; HASNAOUI, 2015) (MONTENEGRO et al., 2007).

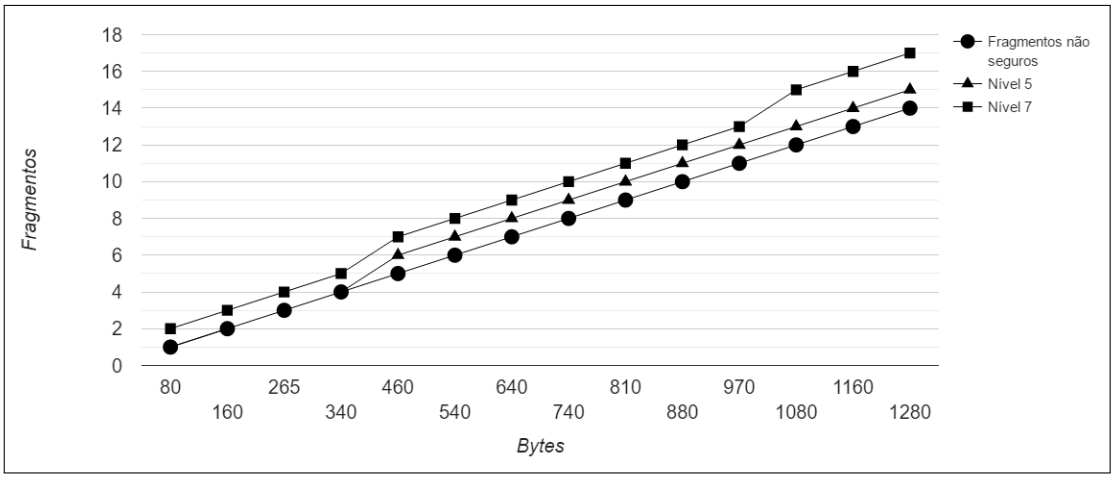


Figura 4.3: Relação entre o comprimento da mensagem, o nível de segurança e a quantidade de fragmentos
Fonte: Produzido pelos autores.

4.5 Módulo de Ativação do Serviço de Segurança Adaptável

As estimativas otimizadas para a quantidade de fragmentos, obtidas através do Algoritmo 1, são utilizadas como entrada para o módulo de ativação do TSS, representado pelo Algoritmo 2, apresentado a seguir. O Algoritmo 2 verifica se, para uma determinada quantidade de dados, a redução no nível de segurança resultará na redução da quantidade de fragmentos. Para isto, ele precisa de todas as estimativa da quantidade de fragmentos que foram geradas.

Algoritmo 2: Redução do Nível de Segurança

```
Algoritmo Thresholds
Entrada
        data_size
        default_security
Saída  security_level
 1  fragments_security = Array(FT1..FT7)
 2  security_level
 3  para security_level de 1 para 7 faça
 4      data_size = FT.estimated_fragments(data_size, security_level)
 5      fragments_security[security_level][0] = security_level
 6      fragments_security[security_level][1] = size
 7  para security_level de 5 para default_security faça
 8      se fragments_security[security_level][1] <
        fragments_security[default_security][1] então
 9          devolva security_level
10  fimpara
11  devolva default_security
```

O acrônimo *FT* representa o *Fragmentation Threshold*, e faz referência ao Módulo para

Detecção dos Limites de Fragmentação, quando este for alimentado com os valores da Tabela 4.1, de acordo com o nível de segurança aplicado. No Algoritmo 2, a quantidade de fragmentos resultante da aplicação de cada nível de segurança é comparada. Quando a quantidade de fragmentos for menor, para um nível menor de segurança, esse nível é utilizado como entrada para o "Procedimento de Segurança do Quadro de Saída" do padrão 802.15.4.

O funcionamento do TSS é demonstrado através do fluxograma da Figura 4.4. O TSS é formado pela união entre o Módulo para Detecção dos Limites de Fragmentação e Módulo de Ativação do Serviço de Segurança Adaptável. Eles são representados, respectivamente, por "Módulo 1" e "Módulo 2". O bloco 802.15.4 representa o "Procedimento de Segurança do Quadro de Saída."

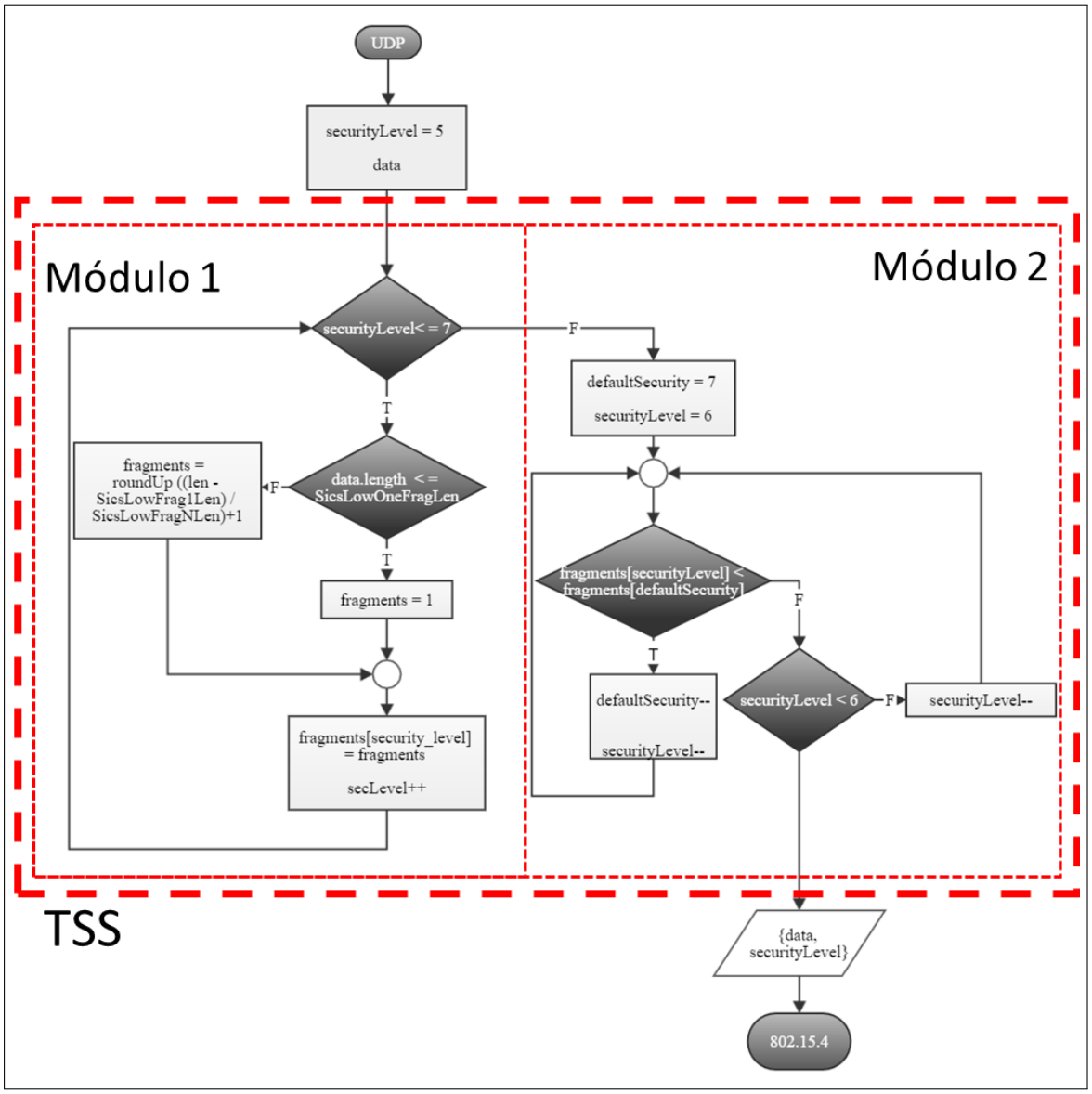


Figura 4.4: Fluxograma para o funcionamento do Serviço de Segurança Adaptável em redes 6loWPAN baseadas em 802.15.4
Fonte: Produzido pelos autores.

4.6 Conclusão

Este capítulo abordou a proposta de um Serviço de Segurança Adaptável para redes 6loWPAN baseadas no padrão 802.15.4. O serviço consiste na variação do nível de segurança na camada MAC do padrão, tendo como objetivo inicial a manutenção de uma quantidade baixa de fragmentos, ou a redução dessa quantidade. A redução é feita em duas etapas. Inicialmente é realizado um mapeamento entre a quantidade de dados e a quantidade de fragmentos que indica para quais quantidades de dados é possível reduzir a quantidade de fragmentos através da redução do nível de segurança. Quando essa região é identificada, o Serviço reduz o nível de segurança e transmite os dados.

5

AVALIAÇÃO, RESULTADOS E DISCUSSÃO

Este capítulo apresenta a avaliação de desempenho do Serviço de Segurança Adaptável para o padrão 802.15.4 descrito no Capítulo 4. A avaliação é realizada através do simulador COOJA. Também é apresentado um modelo para o cálculo da Recompensa de QoP para o padrão 802.15.4

5.1 Introdução

A avaliação do Serviço de Segurança Adaptável foi realizada no simulador COOJA (OSTERLIND et al., 2006), que foi desenvolvido inicialmente para o sistema operacional Contiki (DUNKELS et al., 2011). A análise dos resultados consiste na comparação das métricas resultantes da transmissão de dados antes e depois da utilização do serviço. Para isso, são utilizados mecanismos estatísticos de comparação de alternativas (JAIN, 1990).

5.2 O simulador COOJA

O simulador COOJA (OSTERLIND et al., 2006) foi criado para aumentar o nível de abstração na programação de dispositivos para Redes de Sensores sem Fio (RSSF). Pelas suas características, é possível simular dispositivos em três níveis: instruções em nível de máquina, nível de rede e nível de sistema operacional, sendo possível coletar informações de cada um desses níveis. Essa característica faz com que o COOJA seja um simulador completo, contendo características de vários outros tipos de simuladores existentes, e que servem para simulações em apenas um desses níveis.

A relação do simulador COOJA com outros simuladores é ilustrada na Figura 5.1. COOJA é comparado com os simulaores NS2 (NSAM, 1989), em nível de rede; TOSSIM ((LEVIS; LEE, 2003)), em nível de sistema operacional; e AVRORA (TITZER; LEE; PALSBERG, 2005), em nível de instruções de máquina.

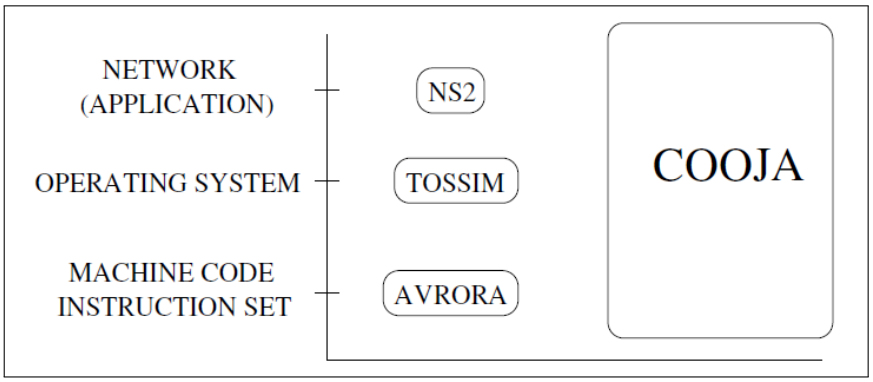


Figura 5.1: Abrangência do simulador COOJA em relação a outros simuladores.
Fonte: (OSTERLIND et al., 2006)

Um dos benefícios de sua abrangência é que o COOJA pode realizar simulações e emulações: as simulações são realizadas utilizando o processador do computador hospedeiro e as emulações utilizam dispositivos virtuais utilizando um emulador de hardware chamado de MSPSIM (ERIKSSON et al., 2007), que se vale de uma emulação do microcontrolador MSP430 (DAVIES, 2008). Nas simulações são utilizados dispositivos emulados na linguagem java. Esses dispositivos são simplificados e programados para exercer funções específicas na rede, seja ela em nível de rede, de sistema operacional ou de máquina.

O segundo modo, a emulação, provê mais realidade às simulações. O emulador deve estar instalado no computador hospedeiro. Ele fornece abstrações de tipo de dispositivos, de memórias, e de interfaces. Os tipos de dispositivos são emulações de dispositivos reais que se utilizam da arquitetura MSP430. O dispositivos mais completo, e o único com suporte a simulação em modo texto, é o Tmote Sky (MOTEIV, 2006), por isso ele foi usado. No emulador é possível alocar até 600 *bytes* para o *buffer* de transmissão de dados. Mesmo assim é possível encontrar outros dispositivos presentes no mercado como Micaz (INC, 2006) e Z1 (ZOLERTIA, 2010).

Além da abstração de memória, o emulador oferece as interfaces. As interfaces são abstração de *hardware* utilizadas pelos dispositivos emulados, e podem ser LEDs, botões ou antenas. As interfaces interagem através de eventos controlados pelo simulador COOJA. A sucessão de eventos gerados pelos três níveis de simulação (rede, sistema operacional e máquina) e pelas abstrações de memória e interfaces, geram as simulações.

É possível utilizar o emulador MPSIM para instalar e testar *firmwares* que seriam instalados em dispositivos reais. O *firmware* é instalado em um dispositivo e este pode ser replicado para formar uma rede. Apesar de vários dispositivos compartilharem o mesmo *firmware*, o simulador mantém isolamento de memória e de interfaces entre eles.

As simulações e emulações podem ser feitas utilizando interfaces gráficas ou utilizando modo texto. Simulações em modo gráfico dão mais acesso a detalhes, enquanto as simulações em modo texto permitem realizar repetições de experimentos de forma mais eficiente. As simulações devem ser criadas em modo gráfico e compiladas para que possam ser executadas em modo texto. Nos dois modos, a interação do usuário com a simulação é feita através de *plugins*. Através deles e possível ter acesso ou fornecer informações sobre a memória, as interfaces ou o sistema operacional. Os *plugins* utilizados para obter dados desta avaliação foram os *plugins*:

- *Simulation Control*: é possível controlar a simulação com interface gráfica. Ela fornece botões para iniciar, pausar e parar a simulação, além de uma indicação do tempo.

- *Network*: Este *plugin* também é de interface gráfica, e através dele é possível visualizar a topologia da rede e manipular os dados dos dispositivos.

- *Mote Output*: é acessível tanto na interface gráfica quanto no modo texto. Sua função é imprimir na tela as mensagens disparadas pelos dispositivos. As mensagens são configuradas no código do dispositivo ou no *firmware*. Esse *plugin* oferece uma das principais formas de obter dados da execução das simulações.

- *Radio Messages*: é possível visualizar dados da simulação em nível de rede. O *plugin* fornece analizadores baseados em *wireshark* para uma melhor visualização dos pacotes.

- *Simulation Script Editor*: é utilizado para criar *scripts* que controlam a simulação. Os *scripts* são criados em modo gráfico e controlam tanto a simulação em modo gráfico quanto em modo texto. Sua principal função é controlar a simulação em modo texto, uma vez que os *plugins Network*, *Simulation Control* e *Radio Messages* não são acessíveis.

5.3 Cenários e Parâmetros das Simulações

Foram realizados experimentos para avaliar a influência da redução na quantidade de fragmentos, causada pelo Serviço de Segurança Adaptável, no atraso e no consumo energético. No simulador, foi programada uma aplicação de entrega de mensagens utilizando UDP sobre 6loWPAN. Os dados são enviados para um receptor, no centro físico da rede em estrela, que emite uma mensagem na camada de aplicação quando recebe algum dado. Os experimentos foram feitos em redes de 1, 11, 16 e 21 dispositivos (LUDOVICI et al., 2014). Em cada rede, um dos dispositivos faz o papel de 6LBR e fica no centro da rede, representando a conexão da rede 6loWPAN com a Internet. O sentido de transmissão é sempre unidirecional e todos os dispositivos atuam como roteadores uns para os outros e levam os dados até o 6LBR. O funcionamento das redes é ilustrado na Figura 5.2.

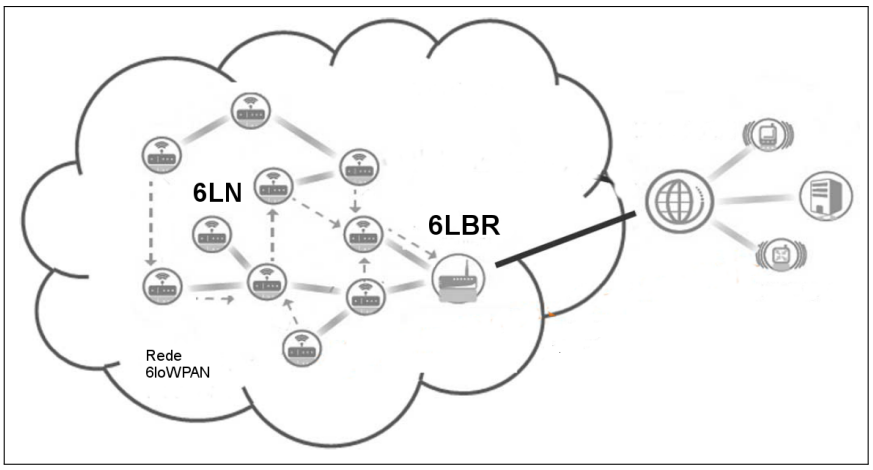


Figura 5.2: Cenário de transmissão dos dados entre 6LN e 6LBR
Adaptado de KEOH; KUMAR; TSCHOFENIG (2014)

Foram investigadas três taxas de envio de mensagens: 1, 5 e 10 mpm (mensagens por minuto) (LUDOVICI et al., 2014). O comprimento da mensagem foi controlado para simular o comportamento da aplicação de segurança sobre os dados. O experimento analisou a fragmentação de 1 até 6 fragmentos devido as limitações de *buffer* dos dispositivos emulados. Foi adotada a premissa de que o tempo gasto pelas operações criptográficas é desprezível quando realizado com o auxílio de aceleradores criptográficos em hardware, uma vez que não foi possível utilizar esse tipo de criptografia devido às características do simulador (LEE; KAPITANOVA; SON, 2010).

As características relacionadas à quantidade de dispositivos na rede, taxa de envio de mensagens e comprimento das mensagens foram baseadas nos principais trabalhos relacionados. A presença de mais de um fator de interesse leva à realização de experimentos fatoriais (JAIN, 1990) (MONTGOMERY; RUNGER; CALADO, 2012). Nesse tipo de experimento, os fatores são variados em conjunto em busca daquele que mais influencia as métricas de interesse. A cada variação de um fator dá-se o nome de nível.

A influência da quantidade de dispositivos na rede, do comprimento da mensagem e da taxa de envio de mensagens sobre as métricas de atraso e consumo energético nas RSSF já é conhecida da literatura. O objetivo deste experimento fatorial é avaliar a influência específica da redução da quantidade de dados gerada pelo TSS. Essa redução se refere aos valores de comprimentos de dados que estão dentro dos Limites de Fragmentação.

Foram realizados experimentos em modelo fatorial completo para cada rede (4), cada quantidade de fragmentos (6) e cada taxa de envio de mensagens (3), totalizando 72 tipos de experimentos. Cada uma dessas simulações foi repetida por 10 vezes (JAIN, 1990). Cada experimento foi executado durante 1 hora em tempo de simulação, de forma que são geradas entre 60, no caso da rede com 2 dispositivos e 13000 mensagens, no caso da rede com 20 dispositivos. A quantidade de mensagens é suficiente para se utilizar o Teorema do Limite central que determina a normalidade de uma amostra. O simulador gera sementes aleatórias da ordem de 19 dígitos para cada replicação e essa característica é indispensável neste tipo de experimento (MONTENEGRO et al., 2007) (JAIN, 1990). Os parâmetros das simulações podem ser vistos na Tabela 5.1. A diferença entre a quantidade de dados Tabela 5.1 e da Figura 4.2 acontece devido a algumas diferenças da implementação do 6loWPAN no sistema operacional Contiki, emulado no simulador.

Tabela 5.1: Parâmetros das simulações

Quantidade de Dispositivos	Taxa de Transmissão (mpm)	Carga útil (Bytes)		Fragmentos
		Nv5	Nv7	
1	1	88		1
11	5	168	88	2
16	10	288	168	3
21		345	288	4
		407	345	5
			407	6

A partir de cada uma das 10 repetições é gerada uma média. As amostras de 10 médias provenientes de simulações de quantidades de fragmentos adjacentes são comparadas (JAIN, 1990). Em JAIN (1990) existe a recomendação para a criação de intervalos de confiança em detrimento dos testes de hipóteses. Entretanto em todo o seu trabalho não existe referência à estatística não paramétrica, que parece mais adequada a este cenário com apenas 10 amostras. A estatística não paramétrica deve ser utilizada quando as características da amostra não atendem aos critérios de normalidade, como é o caso do mínimo de 30 amostras requerida pelo Teorema

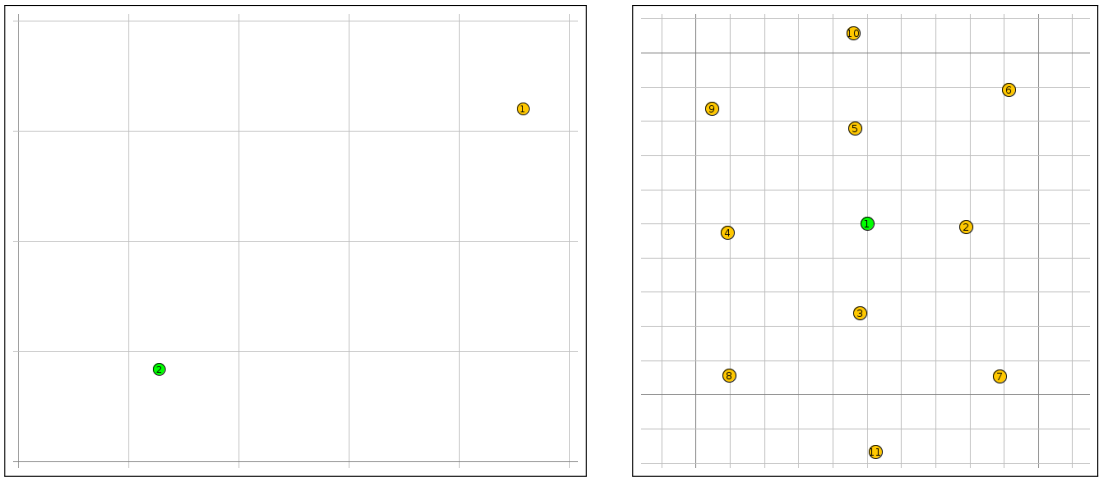
do Limite Central.

Optou-se, então, por utilizar o teste de hipóteses para a comparação das amostras de 10 médias, uma vez que eles são equivalentes aos limites de confiança e também podem auxiliar na tomada de decisão (JAIN, 1990) (MONTGOMERY; RUNGER; CALADO, 2012). Para a comparação, são usados testes estatísticos não paramétricos para a diferença de duas amostras com intervalo de confiança de 90%. A hipótese alternativa do teste é que as média do atraso e o do consumo energético medidos na rede que transmite menos fragmentos, representada pela $\mu 1$, são menores que as médias de atraso e consumo energético, medidos nas transmissões com mais fragmentos. As médias destas redes são representadas pela $\mu 2$ e a comparação está demonstrada na Figura 5.3.

$$H_0 : \mu_1 \geq \mu_2$$
$$H_1 : \mu_1 < \mu_2$$

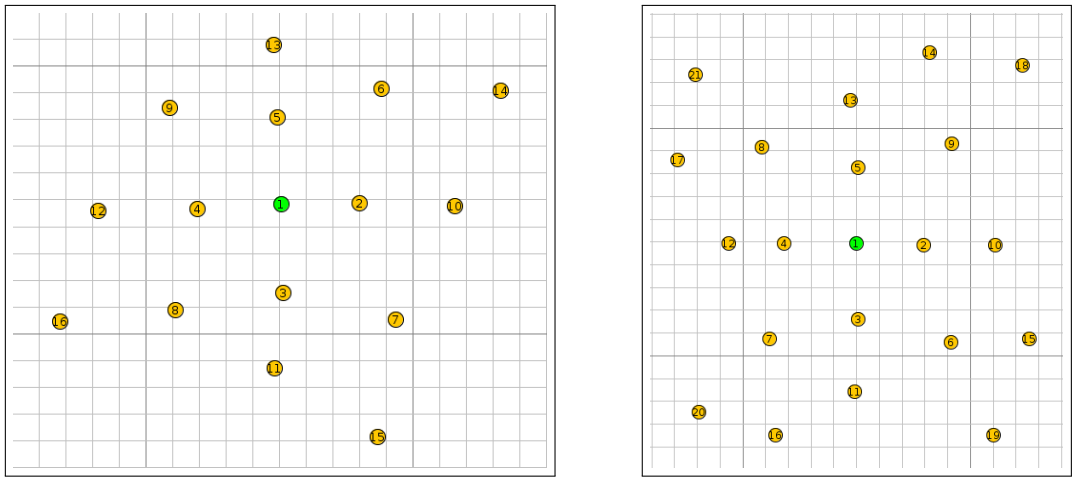
Figura 5.3: Teste de hipóteses

A Figura 5.4a ilustra o cenário de simulação com 2 dispositivos, na Figura 5.4b é visto o cenário da simulação para 11 dispositivos; na Figura 5.5a, a simulação com 16 dispositivos; e na Figura 5.5b, a simulação com 21 dispositivos. Os dispositivos tem rádio de alcance de 50 metros e a grade sob eles indica uma distância de 10 metros entre os vértices.



(a) Rede com 2 dispositivos **(b)** Rede com 11 dispositivos

Figura 5.4: Rede com dois dispositivos (5.4a) e rede com 11 dispositivos (5.4b)



(a) Rede com 15 dispositivos **(b)** Rede com 21 dispositivos

Figura 5.5: Rede com 15 dispositivos (5.5a) e rede com 21 dispositivos (5.5b)

5.4 Avaliação dos Resultados: Redução no Atraso

Pode-se observar, nos gráficos das Figuras 5.6, 5.7, 5.8 e 5.9 que a redução da fragmentação apresenta redução no atraso. Esses valores representam a redução no atraso médio quando o dado é enviado de um 6LN para o 6LBR. Porém, é possível observar que o aumento da quantidade de dispositivos e o aumento da quantidade de mensagens podem tornar os ganhos menos relevantes, uma vez que a rede está congestionada o tempo todo, reduzindo os *buffers* disponíveis para roteamento.

Os dados da Tabela 5.2, ilustrados na Figura 5.6, validam e servem para avaliar o desempenho do Serviço de Segurança Adaptável no ambiente mais simples. Os dados da Tabela 5.2 demonstram a diminuição percentual no atraso ocasionada pela redução da quantidade de fragmentos. O cenário com 2 dispositivos, descrito na Figura 5.4a, não apresenta interferências de outros dispositivos ou de outros protocolos, como o de roteamento, permitindo que os *buffers* do emissor sejam usados apenas para seus próprios dados. Por isso, na rede com 2 dispositivos existem reduções no atraso em todas as reduções na quantidade de fragmentos e em todas as taxas de envio de mensagens.

Tabela 5.2: Diminuição no atraso relacionada a redução na quantidade de fragmentos na rede com 2 dispositivos

Redução de Fragmentos	1 mpm	5 mpm	10 mpm
2 para 1	7%	7%	6%
3 para 2	7%	10%	7%
4 para 3	5%	13%	15%
5 para 4	11%	6%	11%
6 para 5	13%	11%	9%

Na Tabela 5.3 são expostas as reduções percentuais no atraso relacionadas à redução na quantidade de fragmentos nas redes com 11 dispositivos. Na Figura 5.7, é possível observar os

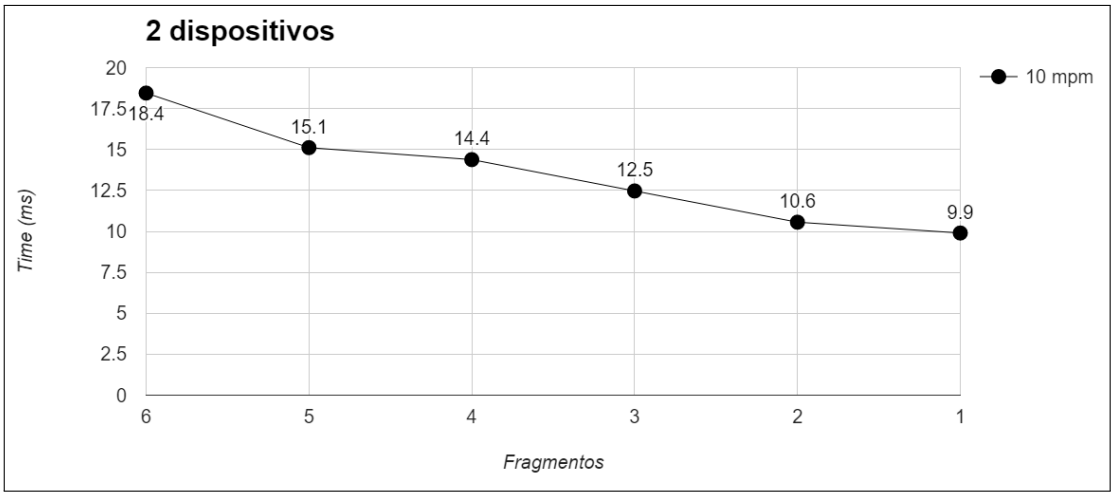


Figura 5.6: Diminuição no atraso relacionada a redução na quantidade de fragmentos na rede com 2 dispositivos

valores da redução no atraso médio da rede. Nas taxas de 1 mpm e 5 mpm todas as reduções apresentam ganhos significativos. Nas Figuras 5.7, 5.8 e 5.7, no envio de 10 mpm, não existem ganhos estatisticamente significativos, apesar de existirem ganhos percentuais. Esse comportamento ocorre devido à escassez de *buffers*, pois os dispositivos mantêm a rede transmitindo dados o tempo todo (HUMMEN et al., 2013) (LUDOVICI et al., 2014) (KIM, 2008) (POPE; SIMON, 2013).

Tabela 5.3: Diminuição percentual no atraso relacionada a redução da quantidade de fragmentos na rede com 11 dispositivos

Redução de Fragmentos	1 mpm	5 mpm	10 mpm
2 para 1	15%	14%	15%
3 para 2	8%	14%	15%
4 para 3	24%	6%	-7%
5 para 4	6%	10%	12%
6 para 5	9%	9%	9%

Os reduções percentuais das redes com 16 dispositivos são apresentados na Tabela 5.4, e as reduções das redes com 21 dispositivos, na Tabela 5.5. Os valores da redução e são ilustrados na Figura 5.8, para a rede com 16 dispositivos, e na Figura 5.9, para as redes com 21 dispositivos. Em redes com 16 e 21 dispositivos, os ganhos são expressivos quando o tráfego da rede é baixo. Nas redes com 16 dispositivos, os ganhos existem quando as mensagens são enviadas a, no máximo, 5 mpm. Até esse limite, são encontrados ganhos próximos a 20%. Nas redes de 21 dispositivos, os ganhos se concentram quando as mensagens são enviadas a 1 mpm. Quando a quantidade de mensagens aumenta, os ganhos passam a ser menos perceptíveis. O motivo da ausência de reduções nas taxas mais altas pode ser atribuído ao aumento do tráfego na rede e a ausência de *buffers* disponíveis para a transmissão de dados (HUMMEN et al., 2013) (LUDOVICI et al., 2014) (KIM, 2008) (POPE; SIMON, 2013).

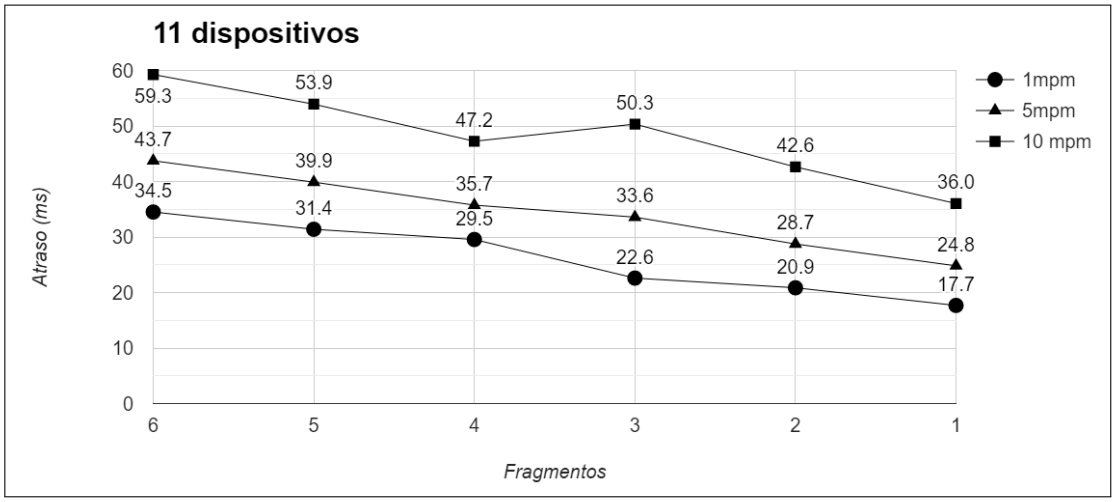


Figura 5.7: Diminuição no atraso relacionada a redução na quantidade de fragmentos na rede com 11 dispositivos

Tabela 5.4: Diminuição percentual no atraso relacionada à redução da quantidade de fragmentos na rede com 16 dispositivos

Redução de Fragmentos	1 mpm	5 mpm	10 mpm
2 para 1	9%	13%	13%
3 para 2	5%	8%	8%
4 para 3	19%	1%	1%
5 para 4	10%	12%	12%
6 para 5	8%	2%	2%

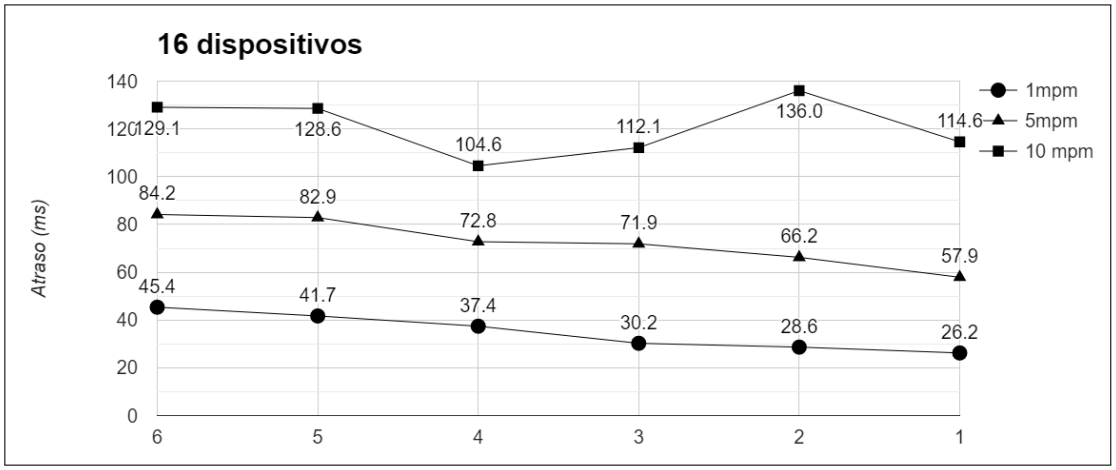


Figura 5.8: Diminuição no atraso relacionada a redução na quantidade de fragmentos na rede com 16 dispositivos

Tabela 5.5: Diminuição percentual no atraso relacionada à redução da quantidade de fragmentos na rede com 21 dispositivos

Redução de Fragmentos	1 mpm	5 mpm	10 mpm
2 para 1	14%	24%	10%
3 para 2	2%	14%	-15%
4 para 3	19%	-34%	-9%
5 para 4	11%	9%	-16%
6 para 5	4%	6%	5%

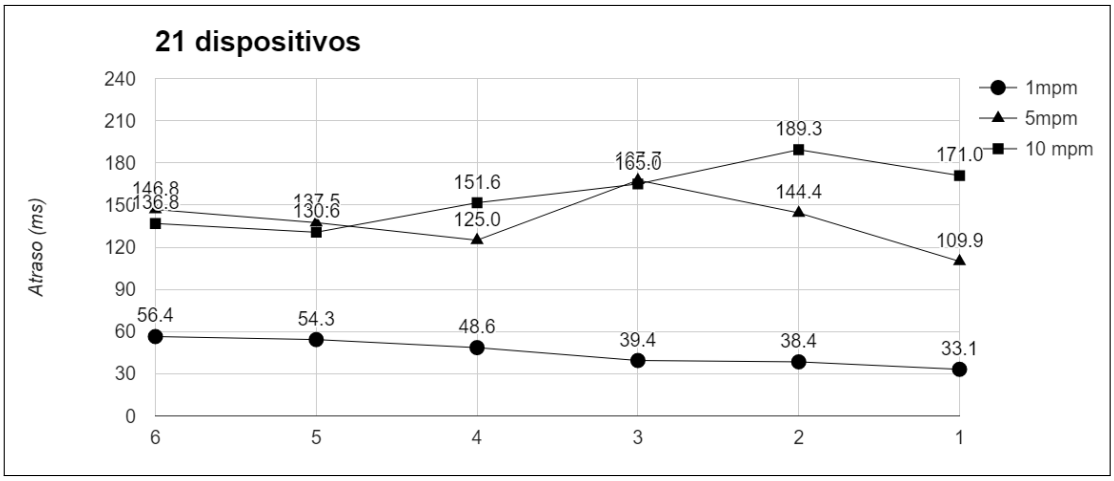


Figura 5.9: Diminuição no atraso relacionada a redução na quantidade de fragmentos na rede com 21 dispositivos

5.5 Avaliação dos Resultados: Impacto no Consumo Energético

A mesma metodologia de avaliação aplicada ao atraso, foi aplicada ao consumo energético. Na rede com 2 dispositivos existem ganhos em todas as reduções na quantidade de fragmentos e em todas as taxas de envio de mensagens. Alguns dos ganhos, sublinhados na tabela, não apresentam ganhos estatisticamente significativos, mas, ainda assim, apresentam ganhos percentuais. Nas redes com mais dispositivos não foram encontrados ganhos, uma vez que todos eles ficam transmitindo dados durante toda a simulação. Isso ocorre pois todos eles são roteadores para os outros dispositivos e mantém os *buffers* preenchidos até mesmo quando não estão transmitindo dados.

Tabela 5.6: Queda percentual no tempo de rádio ligado relacionada à redução da quantidade de fragmentos na rede com 2 dispositivos

Redução de Fragmentos	1 mpm	5 mpm	10 mpm
2 para 1	0	2%	1%
3 para 2	0	3%	5%
4 para 3	2%	2%	1%
5 para 4	3%	5%	4%
6 para 5	3%	3%	5%

5.6 Modelo de Qualidade de Proteção para o Padrão 802.15.4

Na descrição da proposta e nas avaliações de desempenho existe menção à utilização dos níveis de segurança 5 a 7. Isso acontece pois apenas os níveis de segurança 5, 6 e 7 do padrão 802.15.4 permitem o envio de dados criptografados e com proteção de integridade através da implementação da cifra AES-CCM. A utilização de outros níveis necessita de condições específicas. A utilização dos níveis 1, 2 e 3, que utilizam apenas a cifra AES-CBC-MAC, demanda a utilização de criptografia nas camadas superiores. A utilização do nível 4, que utiliza apenas a cifra AES-CTR, requer a utilização de mecanismos de integridade. A utilização do nível 4 de forma pura é desaconselhado, conforme foi apresentado na seção 2.2.5 (RAZA et al., 2014) (SASTRY; WAGNER, 2004) (XIAO et al., 2006).

Baseado nessas premissas, é possível construir um modelo de Qualidade de Proteção - QoP - para justificar essa decisão. O modelo é baseado naquele proposto por SUN; KUMAR (2008), mas utilizando as dimensões de segurança da ISO 7489-2.

Assim como os modelos existentes, este modelo é baseado em "Função de Utilidade"e "Recompensa". A Função de Utilidade consiste em um conjunto de dimensões de segurança e seus pesos. Os requisitos de segurança (Q) são usados para avaliar as dimensões de segurança. Cada dimensão tem um conjunto de requisitos que, uma vez atendidos, fornecem uma pontuação. As dimensões e os respectivos requisitos foram escolhidos com base no trabalho de (LIM et al., 2009), e estão listados a seguir:

1. Autenticação de Usuário e Controle de Acesso - *A*

    (a) Deve ser possível fornecer um método de autenticação para autenticar o usuário (a1);

    (b) Deve ser possível haver autenticação mútua entre o usuário e rede sem fio (a2);

    (c) Deve existir um certificado para autenticar o usuário com a rede sem fio (a3);

    (d) Deve haver uma chave simétrica para autentica o usuário com a rede sem fio (a4);

    (e) Deve ser possível fornecer um mecanismo como o Protocolo de Controle de Acesso a Porta - Port Access Control Protocol (PACP) - para ser utilizado após uma autenticação bem sucedida (a5).

2. Gerenciamento de Chaves (*Key Management*) - *K*

    (a) Deve ser impossível adivinhar chaves devido ao uso de um comprimento adequado (k1);

    (b) Deve ser possível ter uma hierarquia de chave (k2);

    (c) Deve ser possível que a chave de sessão entre o sistema móvel - *Mobile System (MS)* - e da estação base - *Base Station (BS)* - seja mutuamente derivado para encapsular o tráfego da rede sem fio (k3);

    (d) Deve ser possível para fornecer algoritmo de proteção de chave para proteger a chave, caso ela tenha que ser transmitida através da rede sem fio (k4);

    (e) Deve ser possível atualizar a chave de sessão com frequência e regularidade (k5);

    (f) Não deve ser possível reutilizar chaves de outras sessões de comunicação (k6) (KEOH; KUMAR; TSCHOFENIG, 2014) .

3. Proteção de Repetição de Tráfego (*Replay Protection*) - *R*

    (a) Deve ser impossível reutilizar qualquer tráfego da rede sem fio através da aplicação de *timestamp*, numeração de pacotes, contadores ou números de sequência (k1);

    (b) o mecanismo de controle de repetição deve estar de acordo com os métodos criptográficos de outras camadas (k2) (GRANJAL; MONTEIRO; SILVA, 2015);

(c) Deve ser difícil de adivinhar o número do pacote devido ao comprimento adequado do campo (k3);

(d) Deve ser possível controlar o contador de pacotes de outras camadas (k4) (GRANJAL; MONTEIRO; SILVA, 2015) ;

(e) Deve ser possível que o receptor verifique o contador de pacotes (k5).

4. Autenticidade da mensagem (*Message Authenticity*) - *M*

(a) deve ser possível proteger os dados contra modificação não autorizada (m1);

(b) deve ser possível para verificar a autenticidade da mensagem por meio de um Código de Autenticação de Mensagem (neste caso de usa o MIC) (m2);

(c) Deve ser possível confiar na força do algoritmo criptográfico (m3).

5. Confidencialidade - *C*

(a) Deve ser possível proteger a confidencialidade dos dados para evitar que usuários não autorizados utilizem mensagens interceptadas (c1);

(b) Deve ser possível confiar na força do algoritmo criptográfico (c2).

As dimensões e seus critérios foram dispostos em uma Árvore Marcada e Ponderada (SUN; KUMAR, 2008) de modo que eles podem ter pesos atribuídos. O rótulo e o peso do nó são baseados em sua importância. Todos os critérios de segurança recebem valor 1 para a importância. Um dos critérios de cada uma das dimensões é eleito como o mais importante dentre seus irmãos, e recebe um 2 como valor de importância. A disposição das dimensões e critérios pela árvore, bem como a atribuição dos valores de importância é ilustrada na Figura 5.10.

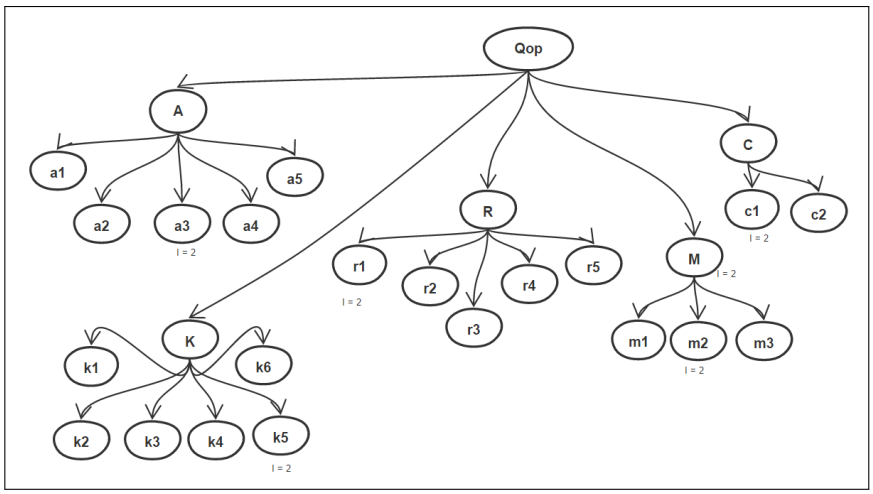


Figura 5.10: Distribuição das dimensões e critérios de segurança pela Árvore Marcada e Ponderada e atribuição de importância

O rótulo é o resultado da divisão da importância dos nós pela soma das importâncias dos nós do mesmo nível, chamados de "nós irmãos". O resultado do cálculo dos rótulos é apresentado na Tabela 5.7. O peso é atribuído apenas para nós nas extremidades da árvore. A soma dos pesos encontrados nas extremidades determina o valor da Recompensa da configuração de segurança. Os pesos atribuído a cada critério de segurança nas extremidades é apresentado na Tabela 5.8.

Tabela 5.7: Rótulos das dimensões e dos critérios de segurança

Dimensão/ Critério	Rótulo	Dimensão/ Critério	Rótulo	Dimensão/ Critério	Rótulo
QoP	1	a4	0.166	r2	0.166
A	0.166	a5	0.166	r3	0.166
K	0.166	k1	0.142	r4	0.166
R	0.166	k2	0.142	r5	0.166
M	0.333	k3	0.142	m1	0.25
C	0.166	k4	0.142	m2	0.5
a1	0.166	k5	0.285	m3	0.25
a2	0.166	k6	0.142	c1	0.666
a3	0.333	r1	0.333	c2	0.3

Tabela 5.8: Pesos atribuídos a cada critério de segurança

Dimensão/ Critério	Peso	Dimensão/ Critério	Peso	Dimensão/ Critério	Peso
a1	0.027	k3	0.023	r4	0.027
a2	0.027	k4	0.023	r5	0.027
a3	0.055	k5	0.047	m1	0.083
a4	0.027	k6	0.023	m2	0.166
a5	0.027	r1	0.055	m3	0.083
k1	0.023	r2	0.027	c1	0.110
k2	0.023	r3	0.027	c2	0.049

Uma vez definidos os pesos para cada critério, é preciso avaliar quais critérios podem ser atribuídos a cada cifra de segurança. A definição dos critérios existentes em cada cifra de segurança foi baseada, principalmente, no trabalho de SASTRY; WAGNER (2004), com contribuições retiradas de KEOH; KUMAR; TSCHOFENIG (2014) e GRANJAL; MONTEIRO; SILVA (2015). A abordagem binária, que atribui apenas a ausência e presença dos critérios, foi utilizada, uma vez que os pesos e rótulos já estão definidos na árvore. A abordagem é apresentada na Tabela 5.9.

O valor da Recompensa é calculado através da multiplicação entre os valores correspondentes entre a Tabela 5.8 e a Tabela 5.9. A abordagem binária, indicando a ausência ou presença de um critério, é utilizada.

Por fim, o resultado da Recompensa é apresenta no Tabela 5.10. O valor mais alto

Tabela 5.9: Abordagem binária para atribuição de identificação da conformidade de uma cifra de segurança com os critérios estabelecidos

Dimensão	Critério	Não Seguro	AES-CBC-MAC-*	AES-CTR	AES-CCM-*
Autenticação de Usuário e Controle de Acesso (A)	a1	0	0	0	0
	a2	0	0	0	0
	a3	0	0	0	0
	a4	0	0	0	0
	a5	0	0	0	0
Gerenciamento de Chaves (K)	k1	0	1	1	1
	k2	0	0	0	0
	k3	0	0	0	0
	k4	0	0	0	0
	k5	0	0	0	0
	k6	0	0	0	0
Proteção de Repetição de Tráfego (R)	r1	0	0	1	1
	r2	0	0	1	1
	r3	0	0	1	1
	r4	0	0	1	1
	r5	0	0	1	1
Autenticidade da Mensagem (M)	m1	0	1	0	1
	m2	0	1	0	1
	m3	0	1	0	1
Confidencialidade (C)	c1	0	0	1	1
	c2	0	0	1	1

atribuído a cifra AES-CCM valida as recomendações encontradas na literatura, tornando-a a cifra mais indicada para utilização nesse cenário.

Tabela 5.10: Valores da Recompensa para as cifras de segurança do padrão 802.15.4

	QoP
No Sec	0
CBC-MAC-*	0.357
AES-CTR	0.349
AES-CCM-*	0.682

5.7 Conclusão

Neste capítulo foi possível validar e avaliar a utilização de um Serviço de Segurança Adaptável para o padrão 802.15.4 quando ele funciona em conjunto com o 6loWPAN. Foram definidos os cenários e parâmetros para os quais o serviço apresenta ou não apresenta melhorias no desempenho. Os resultados das simulações da rede com 2 dispositivos demonstram que o TSS pode ser utilizado com bastante eficiência em cenários onde o 6LN não precise agir

como roteador. Os resultados observados nas redes com mais dispositivos demonstram que a quantidade de *buffers* disponíveis para transmissão influencia nos ganhos que podem ser obtidos. Quanto maior a taxa de geração de mensagens e quanto maior a quantidade de dispositivos na rede, os ganhos se tornam menos expressivos. Redes 6loWPAN cuja frequência de geração de dados está entre 1 e 5 mpm apresentam decréscimo significativo no atraso quando ocorre redução da fragmentação. Redes com até 10 dispositivos apresentam ganhos em todas as taxas.

É importante notar que, conforme a quantidade de dispositivos e a taxa de transmissão de mensagens aumenta, as economias de tempo e de energia se tornam menos expressivas. Isso se dá porque os dispositivos servem de roteadores uns para os outros, o que deixa suas interfaces de rádios ligadas a maior parte do tempo e seus *buffers* sempre ocupados.

Também foi apresentado um modelo para o cálculo da Qualidade de Proteção nesse cenário. O modelo aponta que a cifra AES-CCM é a mais indicada para ser utilizada no cenário apresentado e valida o que é encontrado na literatura. É importante frisar que os valores da Recompensa não são absolutos. Assim como qualquer outro modelo de QoP, eles são pertinentes apenas nos cenários em que estão inseridos. Caso outras cifras de segurança sejam incluídas no padrão 802.15.4 ou outras tecnologias possam ser inseridas no mesmo cenário, elas podem ser avaliadas nesse modelo. A avaliação pode ajudar a guiar a decisão da utilização ou não daquela cifra ou tecnologia.

6

CONCLUSÕES

Este capítulo apresenta as considerações e conclusões deste trabalho, além das principais contribuições e trabalhos futuros.

6.1 Considerações Finais

Na Internet das Coisas, dispositivos com pouco poder de processamento coexistem com dispositivos mais robustos. Nessa arquitetura, é necessário buscar alternativas para reduzir a diferença entre esses dispositivos. As alternativas passam pela criação de protocolos e a alteração, ou otimização, dos protocolos existentes. As duas alternativas são benéficas, pois permitem uma integração transparente entre os dois tipos de dispositivos.

A heterogeneidade de dispositivos na arquitetura da IoT é semelhante àquela que aconteceu no início da utilização de multimídia na Internet. Uma das adaptações propostas naquela época foi a utilização de serviços de segurança que fossem ajustáveis ou adaptáveis, dependendo das condições do dispositivo ou da rede. Abordagens como essa foram tomadas em outras épocas, principalmente quando a multimídia começou a trafegar com mais intensidade por redes e a chegar a dispositivos que não estavam totalmente preparadas para isso. Fatores como heterogeneidades de rede e limitações computacionais nos dispositivos, também foram utilizados para justificar esses estudos (ONG; NAHRSTEDT; YUAN, 2003).

Baseando-se nos pressupostos e no histórico apresentados, este trabalho apresentou a proposta de um Serviço de Segurança Adaptável - TSS - destinado a ser aplicado em redes 6loWPAN baseadas no padrão 802.15.4. O TSS se encaixa na categoria de otimização de protocolos, nesse caso, o 6loWPAN. Foram avaliadas as situações em que a redução do nível de segurança do padrão 802.15.4 auxilia na redução dos efeitos da fragmentação no atraso e no consumo energético de redes 6loWPAN. A redução da fragmentação é baseada nos "Limites de Fragmentação", que são os intervalos de valores em que a quantidade de dados proveniente da camada de rede apresenta variação na quantidade de fragmentos de acordo com o nível de segurança da transmissão quantidades de dados. Foram apresentados módulos para identificar os "Limites de Fragmentação" e acionar a redução no nível de segurança.

Foi possível avaliar que existem cenários em que ocorrem reduções de até 20% no atraso, e que existem reduções de até 5% no consumo energético. As reduções no atraso ocorrem com mais significância em redes com poucos dispositivos e com baixa taxa de entrega de mensagens. Em redes de 15 e 20 dispositivos os ganhos são significativos quando a taxa de transmissão de mensagens não ultrapassa 5 mpm. A redução no consumo energético foi observada apenas nas redes com dois dispositivos. Conclui-se que a manipulação do nível de segurança, através de um TSS é método viável para reduzir fragmentação e reduzir o atraso em redes 6loWPAN.

6.2 Contribuições

Os temas, modelos, avaliações e resultados apresentados neste trabalho têm funções implícitas e explícitas. Como função implícita se destacam a continuação da discussão sobre os impactos da Internet das Coisas nas Redes de Computadores, principalmente no que diz respeito a adoção de tecnologias e protocolos padronizados e a retomada da discussão da utilização de

Serviços de Segurança Adaptáveis. Com esses serviços é possível obter ganhos de desempenho da redes que servirão de base para a Internet das Coisas. Alguns ganhos são descritos neste trabalho, enquanto são deixadas possibilidades para realização de novos trabalhos relacionados ao tema.

Além disso existem contribuições explícitas referentes a revisões de literatura, códigos, modelos e avaliações de desempenho. O trabalho apresentou uma revisão de literatura sobre modelos de Qualidade de Proteção e sobre Serviços de Segurança Sintonizáveis aplicados em redes sem fio. Existem também a apresentação de códigos e equações que podem ser usados por outros pesquisadores na implementação do TSS em outras tecnologias. Eles foram apresentados dessa forma pois a implementação do protocolo 6loWPAN, apesar de ter sido pensada inicialmente para 802.15.4, pode variar dependendo da tecnologia de camada MAC. A própria implementação do padrão 802.15.4 pode variar em relação às funções disponíveis, entradas ou saídas de seus processos.

Foi proposto um modelo de Qualidade de Proteção para o padrão 802.15.4. Modelos como este são usados para determinar uma Recompensa de acordo com as suítes de segurança existentes e auxiliar na tomada de decisão sobre a utilização ou não de uma suíte de segurança. As avaliações de desempenho apresentaram ganhos que podem acontecer em relação ao atraso e ao consumo energético

Uma parte dessas contribuições, relacionadas à revisão de literatura, códigos e avaliação, estão publicadas nos anais da XXXIV Conferência da Sociedade Brasileira de Redes de Computadores e Sistemas Distribuídos (SBRC), em 2016:

1. MENDONÇA JÚNIOR, F. F. de; NÓBREGA, O. O.; CUNHA, P. R. F. Avaliação do Impacto da Segurança sobre a Fragmentação em Redes de Sensores Sem Fio na Internet das Coisas. In: COMPUTER NETWORKS AND DISTRIBUTED SYSTEMS (SBRC), 2016 XXXIV BRAZILIAN SYMPOSIUM ON. Proceedings, 2016. p.228–236.

6.3 Trabalhos futuros

Trabalhos futuros podem propor outras técnicas que utilizem a flexibilidade existente na subcamada de segurança do padrão 802.15.4, como demonstrado na seção 2.2, para economizar energia e diminuir o atraso no envio das mensagens. Podem ser investigadas mais situações onde ganhos são expressivos. Além disso, podem ser estudados os casos em que a criptografia é realizada por software, uma vez que parte dos rádios ainda não fornece suporte completo à criptografia realizada por hardware.

Também é possível realizar avaliações do TSS em outras tecnologias que possam ser usadas com 6loWPAN, ou mesmo outras tecnologias que possuam flexibilidade para aplicação de segurança. Podem ser feitos estudos sobre a aplicação de TSS na integração entre várias camadas do sistema de camadas padronizado da Internet das Coisas. Deve ser possível fazer a

integração dos protocolos de segurança entre todas as camadas, como o DTLS para CoAP, e o IPsec para 6loWPAN, aumentando ou reduzindo o nível de segurança em camadas diferentes para se obter ganhos em diversas métricas.

O modelo de Qualidade de Proteção apresentado pode ter duas aplicações futuras. Ele pode ser atualizado quando surgirem novas funções de segurança no padrão, ou pode ser usado em outras tecnologias da Internet das Coisas, e auxiliar na tomada de decisão sobre a utilização de algum protocolo de segurança.

Referências

AGARWAL, A. K.; WANG, W. On the Impact of Quality of Protection in Wireless Local Area Networks with IP Mobility. **Mobile Networks and Applications**, Secaucus, NJ, USA, v.12, n.1, p.93–110, Jan. 2007.

AGBOMA, F.; LIOTTA, A. QoE-aware QoS Management. In: INTERNATIONAL CONFERENCE ON ADVANCES IN MOBILE COMPUTING AND MULTIMEDIA, 6., New York, NY, USA. **Proceedings...** ACM, 2008. p.111–116. (MoMM '08).

ATZORI, L.; IERA, A.; MORABITO, G. The Internet of Things: a survey. **Computer Networks**, [S.l.], v.54, n.15, p.2787 – 2805, 2010.

BANDYOPADHYAY, D.; SEN, J. Internet of Things: applications and challenges in technology and standardization. **Wireless Personal Communications**, [S.l.], v.58, n.1, p.49–69, 2011.

BELSHE, M.; THOMSON, M.; PEON, R. Hypertext Transfer Protocol Version 2 (HTTP/2). **Disponível em: https://tools.ietf.org/html/rfc7540 (Acessado em 20 de junho 2016)**, [S.l.], 2015.

BORMANN, C.; SHELBY, Z. Blockwise Transfers in CoAP draft-ietf-core-block-14. **Disponível em: http://tools.ietf.org/html/draft-ietf-core-block-14 (Acessado em 3 junho 2014)**, [S.l.], 2013.

BRANDT, A.; BURON, J. Transmission of IPv6 packets over ITU-T G. 9959 Networks. **Disponível em: https://tools.ietf.org/html/rfc7428.html (Acessado em 19 de setembro de 2016)**, [S.l.], 2015.

CODY-KENNY, B. et al. Performance Evaluation of the 6LoWPAN Protocol on MICAz and TelosB Motes. In: ACM WORKSHOP ON PERFORMANCE MONITORING AND MEASUREMENT OF HETEROGENEOUS WIRELESS AND WIRED NETWORKS, 4., New York, NY, USA. **Proceedings...** ACM, 2009. p.25–30. (PM2HW2N '09).

COMMITTEE, L. S. Part 15.4: wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (lr-wpans). **IEEE Computer Society**, [S.l.], 2003.

COMMITTEE, L. S. et al. IEEE Standard for Local and metropolitan area networks-Part 15.4: low-rate wireless personal area networks (lr-wpans). **IEEE Computer Society**, [S.l.], 2011.

DAVIES, J. H. **MSP430 Microcontroller Basics**. Newton, MA, USA: Newnes, 2008.

DEERING, S.; HINDEN, R. Internet Protocol, Version 6 (IPv6) Specification. **Disponível em: https://tools.ietf.org/html/rfc2460 (Acessado em 20 de Junho 2016)**, United States, 1998.

DIJK, E. et al. Guidelines for HTTP-CoAP Mapping Implementations. **Disponível em: https://tools.ietf.org/html/draft-ietf-core-http-mapping-14 (Acessado em 20 de junho 2016)**, [S.l.], 2015.

DUNKELS, A. Full TCP/IP for 8-bit Architectures. In: INTERNATIONAL CONFERENCE ON MOBILE SYSTEMS, APPLICATIONS AND SERVICES, 1., New York, NY, USA. **Proceedings...** ACM, 2003. p.85–98. (MobiSys '03).

DUNKELS, A. et al. The Contiki OS: the operating system for the internet of things. **Disponível em http://www.contikios.org (Acessado em 18 de Março de 2016**, [S.l.], 2011.

ERIKSSON, J. et al. Mspsim–an extensible simulator for msp430-equipped sensor boards. In: EUROPEAN CONFERENCE ON WIRELESS SENSOR NETWORKS (EWSN), POSTER/DEMO SESSION. **Proceedings...** [S.l.: s.n.], 2007. p.27.

GLENN, R.; KENT, S. The NULL Encryption Algorithm and Its Use With IPsec. **Disponível em: https://tools.ietf.org/html/rfc2410.html (Acessado em 20 de junho 2016)**, United States, 1998.

GRANJAL, J.; MONTEIRO, E.; SILVA, J. S. Security for the Internet of Things: a survey of existing protocols and open research issues. **IEEE Communications Surveys Tutorials**, [S.l.], v.17, n.3, p.1294–1312, thirdquarter 2015.

GUBBI, J. et al. Internet of Things (IoT): a vision, architectural elements, and future directions. **Future Generation Computer Systems**, [S.l.], v.29, n.7, p.1645 – 1660, 2013. Including Special sections: Cyber-enabled Distributed Computing for Ubiquitous Cloud and Network Services amp; Cloud Computing and Scientific Applications — Big Data, Scalable Analytics, and Beyond.

HARVAN, M.; SCHÖNWÄLDER, J. TinyOS Motes on the Internet: ipv6 over 802.15. 4 (6lowpan). **PIK-Praxis der Informationsverarbeitung und Kommunikation**, [S.l.], v.31, n.4, p.244–251, 2008.

HUMMEN, R. et al. 6LoWPAN Fragmentation Attacks and Mitigation Mechanisms. In: SIXTH ACM CONFERENCE ON SECURITY AND PRIVACY IN WIRELESS AND MOBILE NETWORKS, New York, NY, USA. **Proceedings...** ACM, 2013. p.55–66. (WiSec '13).

INC, C. technology. Micaz: wireless measurement system. **Disponível em http://edge.rit.edu/edge/P08208/public/Controls**$_{F}iles/MICaZ - DataSheet.pdf(Acessadoem20dejunho2016),[S.l.],2006.$

JAIN, R. **The art of computer systems performance analysis**: techniques for experimental design, measurement, simulation, and modeling. [S.l.]: John Wiley & Sons, 1990.

KEOH, S. L.; KUMAR, S. S.; TSCHOFENIG, H. Securing the Internet of Things: a standardization perspective. **IEEE Internet of Things Journal**, [S.l.], v.1, n.3, p.265–275, June 2014.

KIM, H. Protection Against Packet Fragmentation Attacks at 6LoWPAN Adaptation Layer. In: CONVERGENCE AND HYBRID INFORMATION TECHNOLOGY, 2008. ICHIT '08. INTERNATIONAL CONFERENCE ON. **Anais...** [S.l.: s.n.], 2008. p.796–801.

KRANENBURG, R. v. The Internet of Things: a critique of ambient technology and the all-seeing network of rfid. **Institute of Network Cultures. Disponível em: http://www.networkcultures.org/_uploads/notebook2_theinternetofthings.pdf (Acessado em 20 de junho 2016)**, [S.l.], 2008.

KUIPERS, F. et al. Techniques for Measuring Quality of Experience. In: WIRED/WIRELESS INTERNET COMMUNICATIONS: 8TH INTERNATIONAL CONFERENCE, WWIC 2010, LULEÅ, SWEDEN, JUNE 1-3, 2010. PROCEEDINGS, Berlin, Heidelberg. **Anais...** Springer Berlin Heidelberg, 2010. p.216–227.

KURYLA, S.; SCHÖNWÄLDER, J. Evaluation of the Resource Requirements of SNMP Agents on Constrained Devices. In: MANAGING THE DYNAMICS OF NETWORKS AND SERVICES: 5TH INTERNATIONAL CONFERENCE ON AUTONOMOUS INFRASTRUCTURE, MANAGEMENT, AND SECURITY, AIMS, Berlin, Heidelberg. **Anais...** Springer Berlin Heidelberg, 2011. p.100–111.

KUSHALNAGAR, N.; MONTENEGRO, G.; SCHUMACHER, C. **IPv6 over low-power wireless personal area networks (6LoWPANs)**: overview, assumptions, problem statement, and goals. [S.l.: s.n.], 2007.

LEE, J.; KAPITANOVA, K.; SON, S. H. The price of security in wireless sensor networks. **Computer Networks**, [S.l.], v.54, n.17, p.2967 – 2978, 2010.

LEVIS, P.; LEE, N. Tossim: a simulator for tinyos networks. **Disponível em http://cs.uccs.edu/c̃s526/mote/doc/nido.pdf (Acessado em 20 de junho 2016)**, [S.l.], 2003.

LIM, S. H. et al. Formalizing the design, evaluation, and analysis of quality of protection in wireless networks. **Journal of Communications and Networks**, [S.l.], v.11, n.6, p.634–644, Dec 2009.

LIM, S. H. et al. Evaluation of Quality of Protection Adding HVM in Wireless Network. In: INTERNATIONAL CONFERENCE ON WIRELESS COMMUNICATIONS, NETWORKING AND MOBILE COMPUTING, 2009. **Anais...** [S.l.: s.n.], 2009. p.1–4.

LINDSKOG, S. et al. Providing Tunable Security Services: an ieee 802.11i example. In: SECURECOMM AND WORKSHOPS, 2006. **Anais...** [S.l.: s.n.], 2006. p.1–10.

LINDSKOG, S.; FAIGL, Z.; BRUNSTROM, A. A conceptual model for analysis and design of tunable security services. **Journal of Networks**, [S.l.], v.3, n.5, p.1–12, 2008.

LUDOVICI, A. et al. Analytical model of large data transactions in CoAP networks. **Sensors**, [S.l.], v.14, n.8, p.15610–15638, 2014.

LUO, A. et al. Quality of protection analysis and performance modeling in {IP} multimedia subsystem. **Computer Communications**, [S.l.], v.32, n.11, p.1336 – 1345, 2009. Special Issue of Computer Communications on Heterogeneous Networking for Quality, Reliability, Security, and Robustness - Part I.

MAINETTI, L.; PATRONO, L.; VILEI, A. Evolution of wireless sensor networks towards the internet of things: a survey. In: SOFTWARE, TELECOMMUNICATIONS AND COMPUTER NETWORKS (SOFTCOM), 2011 19TH INTERNATIONAL CONFERENCE ON. **Anais...** [S.l.: s.n.], 2011. p.1–6.

MARIAGER, P.; PETERSEN, J. Transmission of IPv6 Packets over DECT ultra low energy. **Disponível em https://tools.ietf.org/html/draft-ietf-6lo-dect-ule-05 (Acessado em 20 de junho 2016)**, [S.l.], 2013.

MOGUL, J. C. et al. Hypertext Transfer Protocol–HTTP/1.1. **Disponível em https://www.rfc-editor.org/html/rfc2616 (Acessado em 20 de junho 2016)**, [S.l.], 1997.

MONTENEGRO, G. et al. Transmission of IPv6 packets over IEEE 802.15. 4 networks. **Disponível em https://tools.ietf.org/html/rfc4944 (Acessado em 20 de junho 2016)**, [S.l.], 2007.

MONTGOMERY, D. C.; RUNGER, G. C.; CALADO, V. **Estatística Aplicada e Probabilidade para Engenheiros**. [S.l.]: Grupo Gen-LTC, 2012.

MOTEIV. Tmote Sky: ultra low power ieee 802.15.4 compliant wireless sensor module. **Disponível em http://www.eecs.harvard.edu/ konrad/projects/shimmer/references/tmote-sky-datasheet.pdf (Acessado em 20 de junho 2016)**, [S.l.], 2006.

NARTEN, T. et al. Neighbor discovery for IP version 6 (IPv6). **Disponível em https://tools.ietf.org/html/rfc4861 (Acessado em 20 de junho 2016)**, [S.l.], 2007.

NIEMINEN, J. et al. Ipv6 over bluetooth (r) low energy. **Disponível em https://www.rfc-editor.org/rfc/rfc7668.txt (Acessado em 20 de junho 2016)**, [S.l.], 2015.

NSAM. ns-2. **Disponível em http://nsnam.sourceforge.net/wiki/index.php/Main**$page(Acessadoem20de\,junho2016), [S.l.], 1989.

ONG, C. S.; NAHRSTEDT, K.; YUAN, W. Quality of protection for mobile multimedia applications. In: MULTIMEDIA AND EXPO, 2003. ICME'03. PROCEEDINGS. 2003 INTERNATIONAL CONFERENCE ON. **Anais...** [S.l.: s.n.], 2003. v.2, p.II–137.

OSTERLIND, F. et al. Cross-level sensor network simulation with cooja. In: LOCAL COMPUTER NETWORKS, PROCEEDINGS 2006 31ST IEEE CONFERENCE ON. **Anais...** [S.l.: s.n.], 2006. p.641–648.

POPE, J.; SIMON, R. The Impact of Packet Fragmentation and Reassembly in Resource Constrained Wireless Networks. **CIT. Journal of Computing and Information Technology**, [S.l.], v.21, n.2, p.97–107, 2013.

RACHEDI, A.; HASNAOUI, A. Advanced quality of services with security integration in wireless sensor networks. **Wireless Communications and Mobile Computing**, [S.l.], v.15, n.6, p.1106–1116, 2015.

RAZA, S. et al. Lithe: lightweight secure coap for the internet of things. **Sensors Journal, IEEE**, [S.l.], v.13, n.10, p.3711–3720, 2013.

RAZA, S. et al. Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN. **Security and Communication Networks**, [S.l.], v.7, n.12, p.2654–2668, 2014.

SASTRY, N.; WAGNER, D. Security considerations for IEEE 802.15. 4 networks. In: ACM WORKSHOP ON WIRELESS SECURITY, 3. **Proceedings...** [S.l.: s.n.], 2004. p.32–42.

SHELBY, Z.; BORMANN, C. **6LoWPAN**: the wireless embedded internet. [S.l.]: John Wiley & Sons, 2011. v.43.

SHELBY, Z. et al. Neighbor discovery optimization for IPv6 over low-power wireless personal area networks (6LoWPANs). **Disponível em https://tools.ietf.org/html/rfc6775 (Acessado em 20 de junho 2016)**, [S.l.], 2012.

SHELBY, Z.; HARTKE, K.; BORMANN, C. The constrained application protocol - CoAP. **Disponível em https://tools.ietf.org/html/rfc7252 (Acessado em 20 de junho 2016)**, [S.l.], 2014.

SILLER, M.; WOODS, J. Improving quality of experience for multimedia services by QoS arbitration on a QoE framework. In: PROC. OF THE 13TH PACKED VIDEO WORKSHOP 2003. **Anais...** [S.l.: s.n.], 2003.

SILVA, R.; SILVA, J. S.; BOAVIDA, F. Evaluating 6lowPAN implementations in WSNs. In: CONFERNCIA SOBRE REDES DE COMPUTADORES OEIRAS, PORTUGAL, 9. **Proceedings...** [S.l.: s.n.], 2009. v.21.

STANDARDIZATION (GÈNEVE), I. O. for. **Information Processing Systems**: open systems interconnection: lotos: a formal description technique based on the temporal ordening of observational behaviour. [S.l.]: International Organization for Standardization, 1989.

SUH, C.; MIR, Z. H.; KO, Y.-B. Design and implementation of enhanced IEEE 802.15. 4 for supporting multimedia service in Wireless Sensor Networks. **Computer Networks**, [S.l.], v.52, n.13, p.2568–2581, 2008.

SUN, Y.; KUMAR, A. Quality-of-Protection (QoP): a quantitative methodology to grade security services. In: THE 28TH INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS WORKSHOPS, 2008. **Anais...** [S.l.: s.n.], 2008. p.394–399.

TANENBAUM, A. **Redes de Computadores, 4ª. edição traduzida, Editora Campus**. [S.l.]: Elsevier, 2003.

THOMSON, S. IPv6 stateless address autoconfiguration. **Disponível em https://tools.ietf.org/html/rfc2462 (Acessado em 20 de junho 2016)**, [S.l.], 1998.

TITZER, B. L.; LEE, D. K.; PALSBERG, J. Avrora: scalable sensor network simulation with precise timing. In: INTERNATIONAL SYMPOSIUM ON INFORMATION PROCESSING IN SENSOR NETWORKS, 4., Piscataway, NJ, USA. **Proceedings...** IEEE Press, 2005. (IPSN '05).

XIAO, Y. et al. MAC security and security overhead analysis in the IEEE 802.15. 4 wireless sensor networks. **EURASIP Journal on Wireless Communications and Networking**, [S.l.], v.2006, n.2, p.81–81, 2006.

XU, L. D.; HE, W.; LI, S. Internet of Things in Industries: a survey. **IEEE Transactions on Industrial Informatics**, [S.l.], v.10, n.4, p.2233–2243, Nov 2014.

YICK, J.; MUKHERJEE, B.; GHOSAL, D. Wireless sensor network survey. **Computer networks**, [S.l.], v.52, n.12, p.2292–2330, 2008.

ZHU, H. et al. Quality of experience and quality of protection provisions in emerging mobile networks Guest Editorial. **Wireless Communications, IEEE**, [S.l.], v.22, n.4, p.8–9, 2015.

ZOLERTIA, W. platform, Z1 Datasheet. **Disponível em http://zolertia.sourceforge.net/wiki/images/e/e8/Z1_RevC_Datasheet.pdf (Acessado em 20 de junho 2016)**, [S.l.], 2010.