Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Estudo de segurança nos principais protocolos da Internet das Coisas

Gabriel G. M. S. de Magalhaes

Monografia apresentada como requisito parcial
para conclusão do Curso de Engenharia da Computação

Orientador
Prof. M. Sc. João José Costa Gondim

Brasília
2016

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Estudo de segurança nos principais protocolos da Internet das Coisas

Gabriel G. M. S. de Magalhaes

Monografia apresentada como requisito parcial
para conclusão do Curso de Engenharia da Computação

Prof. M. Sc. João José Costa Gondim (Orientador)
CIC/UnB

Prof. Dr. André Costa Drummond
CIC/UnB

Prof. Dr. Robson de Oliveira Albuquerque
ENE/UnB

Prof. Dr. Ricardo Pezzuol Jacobi
Coordenador do Curso de Engenharia da Computação

Brasília, 4 de julho de 2016

Dedicatória

Dedico este trabalho a Deus, em quem eu deposito toda minha esperança, à minha família, amigos e a toda comunidade interessada em um desenvolvimento saudável da Internet das Coisas.

Agradecimentos

Agradeço ao meu orientador, João Gondim, por ter me apoiado durante o estudo e ter me inserido na área de segurança;

Ao meu pai, Gilson Souto, por ser um excelente conselheiro em todas as áreas e por ter, para este trabalho, disponibilizado o material do IDC sobre futuras tendências no mercado de T.I, além do apoio e conversas que acrescentaram ao estudo;

À minha mãe, Marília Gonzaga, por ser um refúgio e uma excelente companhia. Também, pela ajuda dada na revisão ortográfica e de forma do trabalho;

À minha irmã mais velha, Ana Luíza Magalhães, por todo apoio dado e companheirismo, desde sempre;

À CAPES e UnB, pela disponibilização do portal de periódicos, de onde tive acesso a praticamente todos os trabalhos aqui citados;

A todos os demais grandes amigos, pelo estímulo, paciência e companheirismo durante esse período.

Resumo

A partir de uma observação introdutória das questões atuais de segurança e privacidade na Internet das Coisas (IdC), os principais protocolos que compõem este paradigma são estudados, tendo-se em vista seus mecanismos de segurança e vulnerabilidades. O estudo traz, portanto, uma revisão de tais protocolos, propiciando uma análise do estado atual da segurança dos mesmos, que é, ao final, resumido em tabelas explicativas. Espera-se futuramente que o estudo siga atualizado com novos relatos de vulnerabilidades e com mais protocolos que possuam relevância, de modo a mantê-lo como referência por indivíduos envolvidos com o desenvolvimento da IdC.

Palavras-chave: IdC, segurança, protocolos

Abstract

From an introductory observation of the central security and privacy issues in the Internet of Things, the main protocols in this paradigm are studied, taking in consideration their security mechanisms and vulnerabilities. The study continues with a revision of such protocols, providing a brief analysis of each protocol's state in terms of security and, at the end, a summary of what was presented in explanatory tables. In the future, the study shall be updated with new reported vulnerabilities and other protocols that might acquire relevance in the IoT scenario, in such a way that the produced material remains updated as a reference for those involved with IoT.

Keywords: IoT, security, protocols

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

6LoWPAN IPv6 over Low-power Wireless Personal Area Networks.

AAA Authentication, Autorization and Accounting.

ACL Access Control List.

AH IP Authentication Header.

APP Australian Privacy Principles.

ASN Absolute Slot Number.

DODAG Destination Oriented Directed Acyclic Graph.

DoS Denial of Service.

EAP Extensible Authentication Protocol.

ESP Encapsulating Security Payload.

FR Frequência de Rádio.

HIPAA Health Insurance Portability and Accountability Act.

ICS Industrial Control System.

IdC Internet das Coisas.

IEEE Institute of Electrical and Electronics Engineers.

IETF Internet Engineering Task Force.

IP Internet Protocol.

LLC Logical Link Control.

LLN Low-Power and Lossy Network.

M2M Machine to Machine.

MAC Media Access Control.

NFC Near Field Communication.

OTA Online Trust Alliance.

OWASP Open Web Application Security Project.

SCADA Supervisory Control And Data Acquisition.

SITP Secure Internet of Things Project.

TSCH Timeslotted Channel Hopping.

VI Vetor de Inicialização.

WPA WiFi Protected Access.

WSN Wireless Sensors Network.

Capítulo 1

Introdução

> "As tecnologias mais importantes são aquelas que desaparecem. Elas se integram à vida no dia a dia até serem indistinguíveis dele."
>
> Mark Weiser

Uma das maiores revoluções trazidas pela humanidade, a Internet, se tornou parte do cotidiano de governos, empresas e indivíduos, ao ponto de ser difícil imaginar a vida sem a mesma. A criação de dispositivos com a capacidade de se integrar a essa grande rede tem se tornado cada vez mais acessível, com o desenvolvimento tecnológico e o consequente barateamento de custos de produção, além da redução de tamanho, peso e consumo energético.

A Internet das Coisas (IdC), que remete a este paradigma em que "tudo" está conectado, levanta sérios questionamentos no âmbito filosófico, técnico e arquitetônico, onde a presença de dispositivos em todas as áreas trará mudanças de comportamento e de processos, tanto positivamente quanto negativamente[28].

As previsões para o crescimento da IdC são enormes, o que demonstra ainda mais a relevância desse tema para novas pesquisas. Segundo o instituto Gartner, até 2020, 13.5 bilhões de dispositivos estarão conectados[34]. Segundo a IDC (International Data Corporation), o número de novos Apps e Serviços de IdC e Inteligência Artificial terá um crescimento de dez vezes nos próximos três a quatro anos[45]. Todos concordam que o aumento do número de dispositivos na IdC deve ser acompanhado por uma infraestrutura capaz de suportar a enorme quantidade de tráfego, armazenamento e processamento dos dados gerados, de maneira eficiente e segura.

É preocupante, entretanto, o fato do crescimento estar sendo impulsionado por organizações com objetivos primordialmente econômicos e que, em contáveis situações, não

se atentam aos riscos trazidos para a sociedade pela implementação das soluções criadas. As aplicações, que variam desde sensores para o controle de usinas nucleares quanto para lâmpadas e geladeiras, trazem sérios riscos se não forem desenvolvidas levando-se em consideração questões de segurança da informação colhida, tratada e transmitida.

1.1 Internet das Coisas - Conceituação

O termo Internet das Coisas (IdC) foi citado, em 1999, por Kevin Ashton, cofundador do Auto-ID Center no Massachusetts Institute of Technology (MIT), que sustenta ter sido o primeiro a ter utilizado este termo[7]. Ele descreveu a Internet das Coisas para a Procter & Gamble (P&G), como a união de dispositivos rastreados por RFID com a crescente Internet, para o controle logístico.

Atzori et. al. [8] retratam a dificuldade em se estabelecer uma definição única a respeito do que é a IdC. Primeiramente, a "Internet" se refere a um conceito já conhecido de rede e o segundo, "Coisas", abrange um leque maior de objetos genéricos que irão fazer parte de um framework pré-estabelecido. As diferenças conceituais em relação à IdC, segundo o autor, ocorrem devido aos interesses dos Stakeholders envolvidos, que podem ter uma visão mais orientada para a Internet ou mais orientada para as "Coisas". Porém, ao se juntar as duas, há um sentido mais elevado, que semanticamente significa "uma rede global de objetos conectados, unicamente endereçáveis, baseados em protocolos padrão de comunicação"[8, p.2].

Adiciona-se a isso também uma visão semântica da IdC, que trata da visualização, interpretação, busca, endereçamento e armazenamento de todos os dados. Ao se unir essas três visões, o autor extrai uma visão macro que compõe a Internet das Coisas, conforme mostra a Figura 1.1[8]

O leque de aplicações para as "Coisas" é tão abrangente quanto o nome sugere. Diversas soluções são desenvolvidas para a automação na indústria, pela união de máquinas que se comunicam entre si (M2M) com servidores na nuvem; automação residencial, em que objetos espalhados pela casa ajudam nas tarefas do lar, monitorando o ambiente e auxiliando nas tarefas; veículos que se comunicam e estão conectados; aparelhos na área médica, para verificar sinais vitais e atuar no corpo para a melhora da saúde; cidades conectadas, com informação fluindo para auxiliar na infraestrutura pública; distribuição energética(Smart Grids); além de tecnologias ainda desconhecidas, que, no futuro, poderão se integrar a essa grande rede.

Borgia[19, p. 1] resume a IdC como "computação ubíqua[1], computação pervasiva,

[1]Segundo o dicionário Michaelis: u.bí.quo adj (lat ubiquu) 1. Que está ou pode estar em toda parte ao mesmo tempo; onipresente. 2. Filos Que realmente está presente em todos os lugares ao mesmo tempo; onipresente.

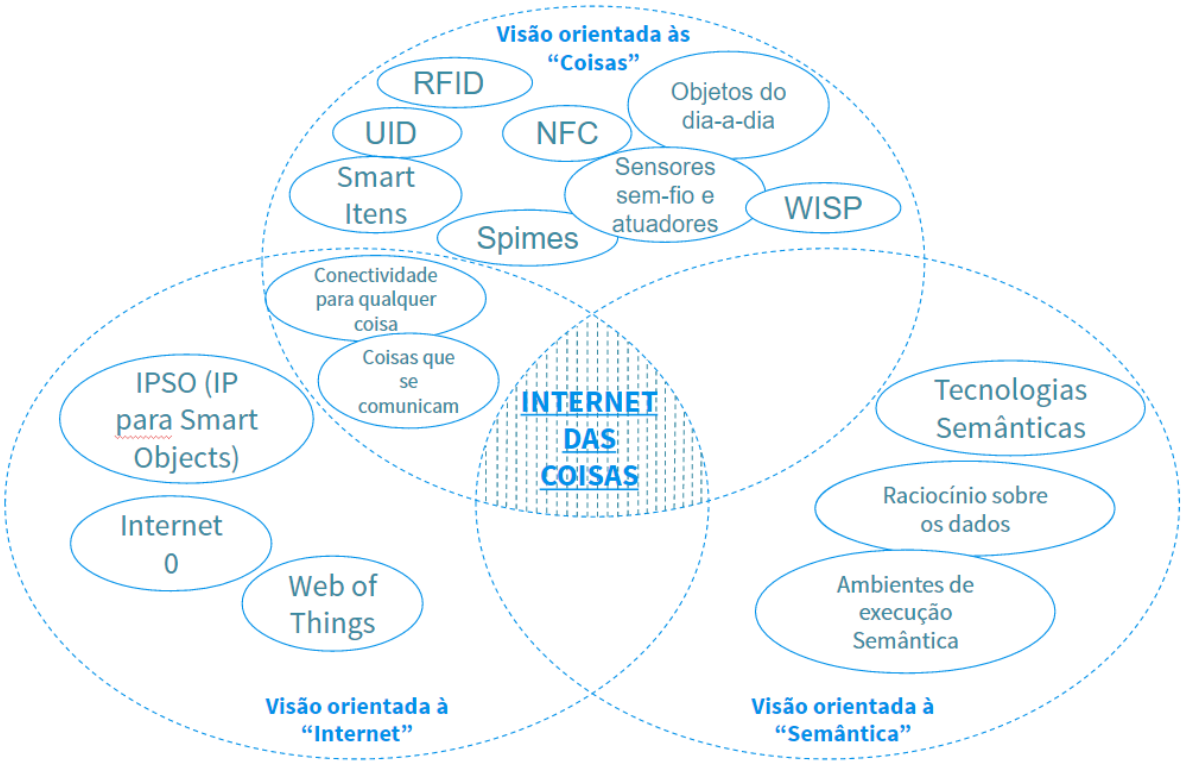

Figura 1.1: A visão da IdC como a intersecção entre uma visão orientada à Internet e às Coisas sob o viés da Semântica [8].

Internet Protocol (IP), tecnologias de sensores, tecnologias de comunicação e dispositivos embarcados, unidos para formar um sistema em que o mundo real e digital se encontram em uma interação contínua e simbiótica."

Apesar das divergências na definição exata do que a IdC representa, alguns pontos são comuns na maioria das definições: trata-se da inclusão de dispositivos, com capacidade de interagir com um meio físico e múltiplos usuários, para obtenção de dados. Além disso, possui, em algum estágio, comunicação com a Internet e alguma "inteligência" para a análise e utilização dos dados. Dentro desta concepção, podem ser interpretados como parte da definição de IdC o paradigma Machine to Machine (M2M) e redes sem-fio de sensores (WSNs).

1.1.1 M2M

Machine to Machine, que traduzido significa Máquina para Máquina, se refere à comunicação entre dispositivos heterogêneos por canais cabeados ou sem-fio. Nesse paradigma, as máquinas - ou dispositivos - são capazes de se comunicar uns com os outros independentemente e podem ser controlados remotamente. Originado pelo modelo SCADA de

automação e controle em ambiente industrial, o paradigma traz soluções para a infraestrutura que garantem a conectividade entre os participantes da rede[57].

O conceito de M2M e de IdC se esbarram e, em muitos casos, são considerados como equivalentes. Há de se notar, porém, que quando se trata de IdC, utiliza-se uma visão mais ampla, que emerge do M2M, mas abrange novas funcionalidades, principalmente por sua forte relação com soluções na nuvem.

1.1.2 WSN

Entende-se por Redes Sensoriais Sem-Fio, do inglês Wireless Sensors Network (WSN), como o conjunto de dispositivos autônomos, espalhados em um ambiente físico, com capacidade sensorial, que coletam informações do ambiente e se comunicam entre si[51]. "Sensores são categorizados por seu pequeno tamanho, sua habilidade de sentir fenômenos do ambiente por meio de uma série de transdutores e um transceptor de rádio com fonte de energia autônoma"[9, p. 1657]. Sensores espalhados sem-fio trazem relativa economia na infraestrutura, pois diminui-se o esforço e custo da instalação e manutenção da rede. Aliado a isso, o barateamento do custo de produção de sensores e dispositivos eletrônicos, como antenas, processadores e unidades de armazenamento, amplifica o ritmo de crescimento de tais redes.

Diversos fatores influenciam a definição das características de WSNs, como mencionado por Romer e Mattern [91] ao estudar o espaço no qual se constroem tais redes:

- A forma como são instalados os sensores, seja aleatoriamente, em casos como um avião que lança sensores em determinada área, ou deliberadamente, em que os sensores são instalados em lugares pré estabelecidos;
- A mobilidade desses sensores é de grande influência, quer estes sejam fixos ou possam se movimentar no espaço;
- Questões relativas a custo, tamanho, recursos e energia disponível, definem como os sensores se comportam baseando-se na necessidade da aplicação dos mesmos;
- A heterogeneidade dos sensores, que influencia no nível de complexidade do software executado e na administração do sistema como um todo;
- As diferentes modalidades, como som, luz e rádio;
- Qual a topologia utilizada, que influencia no diâmetro, ou seja, o maior número de nós entre dois que se comunicam em uma rede. A escolha da topologia influencia na latência, robustez e capacidade da rede, assim como na complexidade no roteamento e processamento;

- A cobertura dada pela rede, que pode ser: esparsa, cobrindo apenas uma região; densa, cobrindo completamente ou quase completamente toda a área; e redundante, onde mais de um sensor cobre a mesma área;
- A conectividade da rede, que pode ser conectada, intermitente ou esporádica;
- O tamanho da rede;
- O tempo de vida: existem casos em que os sensores estão ligados a uma fonte de energia, casos em que funcionam por baterias com trocas espaçadas no tempo e, também, para casos onde não há possibilidade de troca de bateria;
- Aspectos de qualidade de serviço (QoS)

Todos os fatores mencionados acima impõem restrições e dão o direcionamento para a definição das funcionalidades implementadas em uma WSN. Ao se considerar WSN de baixo custo energético e de processamento, a exposição dos sensores e ondas de rádio, a implementação de segurança é mais complexa, dada a maior dificuldade em se aplicar os mecanismos tradicionais.

1.2 Justificativa

O crescimento exponencial da IdC e sua utilização nas mais diversas áreas traz consigo ameaças em relação à segurança. Os dispositivos que irão formar as redes de comunicação apresentam, em sua maioria, restrições que dificultam a implementação de mecanismos de segurança. Além disso, muitas soluções são lançadas no mercado levando-se em conta apenas sua aplicação, sem a garantia de segurança necessária, o que expõe indivíduos e organizações a constantes ameaças e os mais diversos riscos.

De uma forma especial, no ambiente da IdC, percebe-se um agravamento das consequências geradas por falhas de segurança. Ao se pensar na segurança em IdC, não se pode restringir tais ameaças apenas a hackers ou outras instituições interessadas em furtar dados, desviar dinheiro ou apenas inviabilizar um serviço. Problemas de segurança em IdC vão muito além de questões éticas ou criminais, pois envolvem ameaças até mesmo à vida humana, uma vez que muito dela se tem utilizado no âmbito da saúde e da segurança mundial. Desta feita, os cuidados com tais ameaças deve ser permanente e receber a devida atenção. Por exemplo, Charlie Miller and Chris Valasek[36] conseguiram demonstrar ser possível *hackear* um veículo, que possui uma central multimídia, remotamente, realizando ações como ligar o para-brisa, acionar o ar-condicionado, controlar os freios e até mesmo desligar os motores. Em um outro exemplo, *hackers* foram capazes de acessar um dispositivo que controla batimentos cardíacos para "matar" um ser humano simulado por

iStan[108]. Aplicações de IdC podem estar presentes também em usinas nucleares e hidrelétricas, em que vulnerabilidades exploradas podem causar danos a cidades e populações inteiras.

A presença dos dispositivos em casa e de *wearables*, que colhem informações pessoais a todo instante, apresentam também ameaça à privacidade do ser humano, uma vez que os dados colhidos, em diverssas ocasiões, são transmitidos sem criptografia na rede e podem ser utilizados para fins duvidosos, como prever comportamentos e identificar indivíduos sem a autorização dos mesmos.

A segurança nos dispositivos da Internet das Coisas não deve ser tida de forma binária, como sendo apenas seguro ou não seguro, mas sim como um espectro, que varia desde dispositivos que não apresentam segurança alguma até dispositivos com várias camadas de mecanismos para prover segurança[92].

Tendo em vista o cenário preocupante em termos de segurança, neste trabalho, procurou-se desenvolver uma revisão resumida no tocante aos mecanismos de segurança dos protocolos que compõem a Internet das Coisas, de modo a auxiliar àqueles que estão de alguma forma envolvidos com a implementação deste paradigma. Muito do que é apresentado como vulnerabilidade não vem por falta de mecanismos de proteção, mas sim por configurações inadequadas ou pela não utilização dos mesmos. Espera-se, portanto, que uma abordagem resumida das principais características de segurança destes protocolos servirá de base para o crescimento mais saudável da Internet das Coisas, em que os participantes estão à par do conhecimento necessário para a construção de um ambiente mais seguro.

1.3 Objetivos

O trabalho tem como objetivo principal analisar o cenário de segurança atual da Internet das Coisas, a partir de questões de segurança e privacidade, dando ênfase aos protocolos que a compõem.

1.3.1 Objetivos Específicos

O trabalho busca, especificamente, então:

- Revisar as principais iniciativas relativas à segurança em IdC;
- Abordar a discussão acerca da privacidade em IdC e
- Estudar as questões de segurança relativas aos principais protocolos utilizados na IdC, identificando possíveis vulnerabilidades.

1.4 Organização do Trabalho

O trabalho se organiza como segue. O Capítulo 2 apresenta a descrição dos principais projetos existentes envolvidos na análise de segurança em IdC e quais são os pontos relevantes nessa temática que darão base para o presente estudo.

A IdC, como enfatizado anteriormente, traz sérios questionamentos em relação à privacidade do usuário, visto que os diversos dispositivos, colhendo informações das mais variadas formas, o fazem de maneira pervasiva. Nesse sentido, o Capítulo 3 traz uma abordagem voltada para a preservação da privacidade no ambiente da IdC, selecionando alguns conceitos e demonstrando algumas ações que indivíduos, empresas, fabricantes e governos devem observar ao definir suas políticas em termos de privacidade em IdC.

O Capítulo 4 elicita quais são os principais protocolos que formam a Internet das Coisas, fazendo uma breve apresentação de suas características determinantes e mencionando os mecanismos mais utilizados para a segurança com baixo consumo computacional, além de mencionar possíveis vetores de ataque.

Com os dados relativos a cada protocolo, é possível se obter tabelas que sumarizam o que fora apresentado anteriormente, como resultado do estudo. Tais tabelas estão expostas no Capítulo 5 e por fim, no Capítulo 6 concluí-se o trabalho com uma reflexão do que foi abordado e recomendações para futuros estudos.

Capítulo 2

Principais Projetos e Organizações Voltadas para Segurança em IdC

> "Um princípio fundamental é que tudo o que fazemos se baseia em risco vs. recompensa, porém, no momento, nosso entendimento de risco não está baseado em informações completas"
>
> Joshua Corman, Co-fundador do I am The Cavalry

Instituições e grupos de empresas e pesquisadores se unem em projetos para discutir os riscos e elaborar soluções para os problemas de segurança, em alguns casos, especificamente em relação à segurança da Internet das Coisas. Tais projetos são de extrema importância, pois trazem a união do conhecimento na busca das melhores soluções, que podem ser compartilhadas, trazendo benefícios a toda sociedade.

A seguir são descritos alguns desses projetos e instituições, bem como seus principais focos de atuação e como vêm abordando as questões relativas a segurança, principalmente no âmbito de Internet das Coisas.

2.1 OWASP

O projeto Open Web Application Security Project (OWASP), iniciado em dezembro de 2001, é totalmente *open source* e tem como missão "tornar a segurança de software visível para que indivíduos e organizações ao redor do mundo possam tomar decisões embasadas a respeito dos verdadeiros riscos de segurança em software" [83]. Tem sido um excelente

auxílio para o desenvolvimento de aplicações mais seguras, pois conta com o apoio da comunidade, fornecendo diversos recursos para projetos, testes e validação.

Os projetos desenvolvidos no OWASP são divididos em quatro categorias[84]:

- Documentação: trazem informações das mais variadas fontes a respeito de determinado assunto;
- Ferramentas: construção de ferramentas para testar sistemas, detectar erros, proteger e ensinar conceitos de segurança;
- Códigos de Bibliotecas: prover bibliotecas que serão utilizadas por programadores para aumentar a segurança em código e
- Projetos Operacionais: envolvem a manutenção de operações relacionadas ao OWASP.

A partir dessas categorias, são desenvolvidos os recursos para a comunidade aprimorar suas soluções de segurança.

Dentro do OWASP, existe um projeto voltado exclusivamente para o estudo de segurança em Internet das Coisas. Esse projeto é composto por oito artefatos. O primeiro, que será detalhado abaixo, traz uma análise dos riscos que são definidos como os dez principais problemas de segurança em IdC. São também disponibilizados: uma lista com as principais vulnerabilidades que podem ser exploradas, categorizadas por sua superfície de ataque; um guia, em nível básico, de condições que devem ser asseguradas para a realização dos testes de segurança, separados de acordo com cada um dos dez problemas levantados como principais; um guia que define padrões de segurança no desenvolvimento de programas em dispositivos e na cloud, desenvolvimento de hardware e questões relativas a privacidade; uma lista com os dez principais problemas relativos a vulnerabilidades em ICS/SCADA; princípios de desenvolvimento; guia para o desenvolvedor e informações da comunidade que suporta o projeto.

2.1.1 Top 10 Problemas de Segurança em IdC 2014

OWASP é bastante conhecido na indústria por prover uma lista com os 10 principais problemas de segurança em aplicações web. Tal lista é atualizada à medida em que as questões de segurança vão se movendo para diferentes pontos, seja pelo aumento dos mecanismos de defesa, lançamento de novas tecnologias, ou pelo surgimento ou crescimento dos riscos de outras ameaças. [85]

Como mostra a Figura 2.1[85], a partir de vulnerabilidades, podem ser encontrados vetores de ataque que permitem a um atacante trazer impactos negativos, os quais, dependendo da gravidade, necessitam de especial atenção. Para cada um dos dez pontos da

lista são levantados os agentes de ameaça, quais são os riscos, baseado na Metodologia OWASP de Avaliação de Riscos, e quais são os impactos técnicos e de negócio que cada ameaça traz, como mostra a Figura 2.2[85]

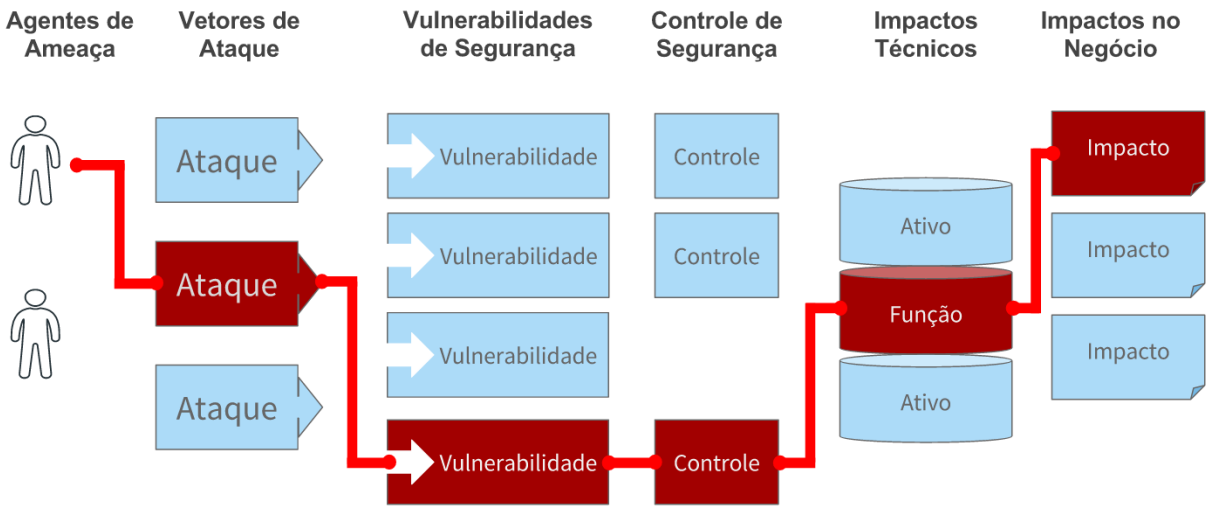

Figura 2.1: Caminho de um atacante para causar danos [85].

Agentes de Ameaça	Vetores de Ataque	Prevalência da Vulnerabilidade	Detecção Vulnerabilidade	Impactos Técnicos	Impactos no Negócio
Específico da Aplicação	Fácil	Generalizada	Fácil	Severo	Específico do Negócio/ Aplicação
	Média	Comum	Média	Moderado	
	Difícil	Rara	Difícil	Pequeno	

Figura 2.2: Possibilidades de classificação de cada risco [85].

Seguindo o sucesso de tal ferramenta, o projeto de IdC do OWASP segue o mesmo padrão, levantando quais são os dez principais problemas no âmbito de segurança para Internet das Coisas. O tratamento dado a cada problema tende a ser bastante prático. Muito do que é abordado nessa lista da OWASP será tratado, posteriormente, de forma mais detalhada, ao longo deste estudo.

A lista desenvolvida foi baseada em um estudo, liderado pela HP, em que dez dos principais dispositivos de IdC foram analisados e, em média, 25 vulnerabilidades foram

encontradas para cada dispositivo[42]. Foi a partir desta análise que os dez principais riscos, apresentados a seguir, foram levantados, são eles:

I1 - Interfaces Web Inseguras

O primeiro risco apontado se refere à falta de segurança que algumas interfaces web apresentam, tanto para ameaças externas como internas. Os atacantes podem usar credenciais fracas ou que não são cifradas e enumeração de contas do sistema. Por exemplo, quando um usuário requisita uma nova senha, o sistema deve bloquear o número de tentativas caso o usuário passado não exista e deve limitar o número de tentativas de login, caso contrário, um atacante pode tentar indefinidamente até encontrar o nome de usuário válido, ou a senha para um usuário. Segundo o Relatório de Investigações sobre Vazamento de Dados da Verizon 2013[114], 76% de intrusões na rede ocorrem por credenciais fracas ou roubadas.

Algumas sugestões dadas para se evitar isso envolvem modificar os valores padrões de usuário e senha; garantir que a interface não esteja suscetível a ataques como injeção SQL, *Cross-Site Scripting* (XSS) ou *Cross-Site Request Forgery* (CRSF); não expor credenciais no tráfego interno ou externo; garantir que as senhas não sejam fracas e que as contas sejam bloqueadas quando o número de tentativas atingir um certo limite.

I2 - Autenticação e Autorização Insuficientes

A fragilidade no processo de autenticação e autorização pode vir tanto de interfaces web, móvel e da nuvem, presentes em muitas aplicações de Internet das Coisas. Senhas fracas, mecanismos de recuperação de senha frágeis, credenciais pouco protegidas ou falta de um acesso granular no controle de acesso compõem os principais vetores de ataque para esse risco.

As sugestões dadas para mitigação dos riscos incluem tratar a qualidade nas senhas, permitir acesso granular, garantir que credenciais possam ser revogadas, requisitar sempre autenticação em apps, dispositivos e servidores e, por fim, administrar seguramente as identificações de usuários.

I3 - Serviços de Rede Inseguros

Os diversos serviços, que formam a rede na qual os dispositivos de IdC estão inseridos, podem trazer vulnerabilidades que facilitam o ataque a outros dispositivos conectados na mesma rede, além de ataques de negação de serviço e perda ou corrupção dos dados transmitidos. É necessária uma verificação das portas, utilizando um scanner de portas, para verificar a presença de vulnerabilidades de negação de serviço, relacionadas a UDP, buffer

overflow e ataques fuzzing, que serão tratadas no Capítulo 4. Também, recomenda-se verificar se as portas são realmente necessárias e se existe alguma delas exposta utilizando UPnP.

I4 - Falta de Criptografia no Transporte

Garantir que o transporte de dados terá confidencialidade, integridade, autenticação dos envolvidos e garantia de irretratabilidade são os principais objetivos da criptografia, objetivos estes fundamentais para um transporte de dados seguro. Todavia, muitas vezes, por uma série de motivos, opta-se por abrir mão dos mecanismos de criptografia no tráfego interno, o que é um erro, visto que não há como se ver livre de ameaças internas. Uma má configuração de uma rede sem fio, por exemplo, pode tornar o tráfego visível a qualquer um. Deve-se, portanto, criar um mecanismo que assegure que nenhuma informação está sendo transmitida na forma de texto claro e que apenas técnicas de criptografia com alto padrão de confiabilidade são utilizadas. Além disso, assgurar que protocolos SSL e TLS sejam utilizados sempre. É fácil descobrir se dados estão sendo transmitidos abertamente com ferramentas que verificam se os dados transmitidos são legíveis.

I5 - Privacidade

Os dados gerados pelos diversos dispositivos que compõem a Internet das Coisas passam por uma rede e muitas vezes passam por aplicativos móveis e são armazenados na nuvem. Há então uma preocupação relacionada à privacidade, já que os dados passam por diferentes ambientes que fogem do controle do usuário. Os vetores de ataque vêm da falta de autenticação, ausência de criptografia no transporte, serviços de rede inseguros e dados que são colhidos sem necessidade. Para prevenção de problemas com privacidade o sistema deve verificar quais dados são colhidos, se a coleta desses é realmente necessária e está autorizada. Deve-se, também, procurar evitar, ao máximo, o uso de dados sensíveis, garantindo que os dados colhidos permaneçam no anonimato e protegidos com criptografia, assegurando que somente as pessoas autorizadas terão acesso aos dados. Por fim, dar liberdade e transparência ao usuário quanto a coleta dos dados. Uma análise de privacidade para IdC é feita no Capítulo 3.

I6 - Interfaces de Nuvem Inseguras

Muitos dados e informações de controle dos diversos dispositivos de IdC são armazenados externamente na nuvem. É necessário garantir que o acesso a essas informações seja feito de forma segura, a partir de controles de autenticação, criptografia e de mecanismos que trazem prevenção de injeção SQL, cross-site scripting e falsificação de requisições a

usuários na interface da nuvem. Para isso, faz-se necessário a verificação de que os nomes de usuário e senhas-padrão sejam trocadas periodicamente, que ocorra o bloqueio de acesso após um certo número de tentativas, que haja proteção das credenciais do usuário e, por fim, que a detecção e bloqueio de requisições não usuais possa ocorrer.

I7 - Interfaces Móveis Inseguras

Assim como muitos dispositivos utilizam a nuvem, muitos também utilizam recursos mobile e é fundamental que a interface móvel seja utilizada de maneira segura. Para isso, mais uma vez, recomenda-se verificar senhas e credenciais, modificando valores padrões, aplicar técnicas de ofuscação de aplicativos móveis para evitar ataques por engenharia reversa. Deve-se também utilizar mecanismos contra adulteração de aplicativos móveis e restringir o uso dos aplicativos apenas a sistemas operacionais móveis confiáveis.

I8 - Configurabilidade de Segurança Insuficiente

A insuficiência de configurabilidade de segurança ocorre quando os usuários não possuem recursos para modificar ou adequar os controles de segurança disponíveis. Os vetores de ataque podem vir tanto intencionalmente como acidentalmente por dispositivos e usuários. Tais vetores incluem a ausência de granularidade nas permissões de acesso, falta de criptografia e de opções para senhas. É necessário, então, verificar na interface administrativa a possibilidade de separar usuários regulares de usuários administrativos, criptografar dados armazenados e em trânsito, definir políticas de senhas fortes, disponibilizar logs de eventos e notificar usuários sobre eventos.

I9 - Softwares e Firmwares Inseguros

Considerado como um risco de difícil explorabilidade, os vetores de ataque para softwares e firmwares incluem a captura de arquivos de atualização sendo transmitidos sem criptografia ou o atacante conseguindo fornecer uma atualização própria pelo sequestro de um servidor DNS. A impossibilidade de atualização de um software ou firmware é um grande problema, em termos de segurança, pois, justamente, a partir de atualizações é que falhas de segurança são corrigidas. Outra falha vem da disponibilização em código de informações sensíveis, como credenciais por exemplo. Esta falha pode ser verificada com editores hexadecimais, que verificam os dados binários do arquivo. Para reduzir os riscos trazidos por software e firwmwares inseguros, sugere-se verificar que os dispositivos podem ser atualizados quando necessário, que o arquivo de atualização seja transmitido de forma cifrada e possa ter sua autenticidade checada, com funções hash, por exemplo. Também, garantir que o servidor esteja seguro e, se possível, implementar boot seguro.

I10 - Segurança Física Fraca

Por meio do acesso físico aos componentes dos dispositivos, um atacante pode ter acesso à memória e consequentemente ao sistema operacional, ganhando uma gama de exploração e de ataques incontrolável. Para previnir que componentes sejam utilizados maliciosamente, podem ser aplicadas técnicas para dificultar o acesso a estes, como por exemplo componentes auto-destrutivos que liberam uma substância que apaga a memória quando o componente é burlado. Os dados armazenados devem estar sempre cifrados e portas externas não podem ser usadas para funções diferentes das que foram planejadas.

2.2 I am the Cavalry

I am the Cavalry, que traduzido literalmente significa "Eu sou a cavalaria", surgiu em 2013 no evento DEFCON e Bsides Las Vegas. A cavalaria remete à idade média em que existia uma cavalaria responsável por se locomover e proteger contra ameaças. Segundo Joshua Corman[40], ao analisar a situação em que as ameaças trazidas pela tecnologia apresentam, não é viável aguardar por uma "cavalaria" que irá chegar para defender e sanar os problemas, as pessoas devem se envolver mais com as questões de segurança e não simplesmente aguardar que as coisas se resolvam. Nesse sentido, foi feito um chamado aos presentes na conferência e membros externos para uma união com o foco na "interseção entre a segurança de computação com aspectos de segurança pública e ameaça à vida humana". [44]

A tecnologia vem crescendo em um ritmo mais acelerado do que mecanismos que permitem se proteger do mal uso da mesma. Em sua descrição, é levantado o questionamento se uma solução de IdC deve realmente ser construída e não simplesmente se é possível construí-la. O grande objetivo é trazer visibilidade a esse questionamento, provendo recursos para que tomadores de decisão possam tomar decisões conscientes dos riscos envolvidos quando fazem uso dessas novas tecnologias. O projeto busca amplificar e revelar, também, os benefícios trazidos por pesquisas relativas às consequências em relação a segurança e trazer um pensamento que envolva a análise de interdependência e externalidades e não apenas essas partes separadas.

A cavalaria(The Cavalry), como "Eu sou a Cavalaria"(I am the Cavalry) é mencionada, tem seu foco em quatro áreas:

- Médica: diversas aplicações médicas tem se desenvolvido tecnologicamente para trazer mais conexão, análises computadorizadas e aceleração no lançamento de novos dispositivos. Os tópicos abordados nessa área incluem telemetria, implantáveis, imagens, diagnósticos, radiologia, medicina nuclear e assistência médica domiciliar.

- Automotiva: seja para entreterimento ou para aprimorar as funcionalidades, cada vez mais os carros vem sendo conectados e embarcados com tecnologias como estacionamento automático, desligamento remoto de veículos roubados, piloto automático, entre outros. É necessário analisar então até que ponto tais mecanismos são seguros, mostrando também a seriedade das ameaças em tais aplicações.

- Residencial: no que se refere ao ambiente residencial, diversas soluções novas trazem automação de tarefas rotineiras, de forma prática e eficiente, incluindo: controle de iluminação e temperatura dos ambientes, travas eletrônicas, eletrodomésticos inteligentes, entre outros, conectando toda a casa. Os sistemas devem ser de fácil uso e manutenção e prover a segurança ao ambiente e à privacidade do usuário.

- Infraestrutura Pública: na busca por uma sociedade mais ágil, responsiva e eficiente, diversas aplicações buscam conectar cidades com aplicações tecnológicas. Os riscos envolvidos devem ser analisados de uma maneira formal e sistemática para garantir a segurança dos cidadãos. Os tópicos abordados envolvem sistemas de aviação, coleta de lixo, transporte público e serviços.

A Cavalaria ainda está em seus passos iniciais, tendo alcançado sucesso em reunir diversos pesquisadores e promover palestras e discussões. O caminho a se trilhar envolve desenvolver mais pesquisas, ter uma representação legal, mais patrocinadores e prover cada vez mais recursos para guiar o desenvolvimento seguro de aplicações nos diversos tipos de sistemas.

2.3 BuildItSecure.ly

BuildItSecure.ly, que traduzido remete-se a “construa seguramente”, é um projeto que visa fomentar o desenvolvimento de aplicações de IdC de forma segura, principalmente para pequenos negócios, crowd-funded e demais vendedores interessados. Dessa forma, estes podem estar conectados com pesquisadores e especialistas de segurança para desenvolver dispositivos e ambientes seguros.

Muitos dispositivos de IdC que chegam ao mercado são financiados por um método conhecido por crowd-fouding, ou financiamento coletivo. Nesse modelo, um empreendedor que deseja lançar um produto não precisa mais de empresas investindo, bancos, investidores anjo ou afins, basta divulgar o seu projeto em uma das diversas plataformas de financiamento coletivo que qualquer pessoa interessada pode financiá-lo. Esse processo facilita a entrada de produtos no mercado, porém, como é dito por March e Zach (fundadores do builditsecure.ly)[107], a maioria desses empreendedores não possuem ex-

periência com segurança da informação, muito menos recursos para investir em segurança, principalmente nos estágios iniciais.

Buscando facilitar o acesso de empreendedores como esses a informações para um desenvolvimento seguro desde o projeto, criou-se o builditsecure.ly. O projeto visa também estimular o desenvolvimento de pesquisas e a regularização do trabalho de pesquisadores de segurança, batalhando para que haja uma mudança de visão a respeito destes, que muitas vezes são vistos como inimigos pelas empresas por estarem explorando vulnerabilidades.

Além do que é produzido pelos próprios envolvidos no projeto, grande parte do que é utilizado vem das parcerias que são construídas. Vale destacar a parceria com a plataforma Bugcrowd [1], que guia testes de segurança por uma comunidade envolvida em segurança, que recebe retorno financeiro quando encontram falhas, estipulando quais acordos devem ser cumpridos no processo.

Build It Secure.ly também está em seus estágios iniciais. O projeto já conseguiu atrair suas primeiras parcerias, em uma delas com Pinoccio[2], o projeto já recebeu hardware para ser testado.

2.4 SITP

Diversas universidades e instituições de ensino possuem departamentos dedicados ao estudo de segurança de IdC. A Stanford University, UC Berkeley e a University of Michigan englobam um projeto intitulado Secure Internet of Things Project (SITP), que concentra os esforços dos diversos pesquisadores da área e organiza eventos, workshops e discussões a respeito das questões de segurança em IdC.

O projeto se divide em três áreas fundamentais: (1) Analytics, que aborda questões relativas à integração dos diversos dados levantados pelos dispositivos com aplicações reais, trazendo análises proveitosas; (2) Segurança, que questiona como os sistemas pervasivos conseguirão prover segurança a usuários e sistemas e, por fim, (3) Harware e Software, que explora o que poderá ser feito quando o desenvolvimento de IdC for tão simples quanto aplicações web modernas.

Um dos focos do projeto é prover recursos de segurança que durarão por pelo menos vinte anos. Isso se dá pois os dispositivos criados agora serão os mesmos dispositivos que deverão funcionar também até lá, sem poder passar por manutenção e, consequentemente, terão de suportar as novas tecnologias que surgirão, como a computação quântica, por

[1] Bugcrowd - `https://www.bugcrowd.com` - Acesso em 14/04/2016

[2] `https://pinocc.io/`

exemplo, que pode em alguns anos se tornar uma realidade em computadores, permitindo a violação dos esquemas de criptografia atuais.

O projeto busca para os próximos cinco anos estudar e definir os padrões criptográficos que serão utilizados por décadas e fornecer frameworks para um desenvolvimento de hardware e software que sejam seguros e open-source para a correta utilização destes mecanismos[105].

2.5 OTA

A Online Trust Alliance (OTA) surgiu como um grupo informal na indústria e, atualmente, é uma organização beneficente com mais de 100 empresas apoiadoras. Sua preocupação está na confiança e reputação de negócios que possuem atividades online, fornecendo recursos para que os mesmos possam se desenvolver utilizando as melhores práticas para garantir a segurança e privacidade dos usuários[80]. Surgiu em 2004, quando emails apresentavam grandes vulnerabilidades e atualmente atua em diversas áreas na internet.

Dentro da OTA, existe uma iniciativa voltada exclusivamente para questões de segurança em IdC. Formado em 2015, esse grupo foca em privacidade, segurança e sustentabilidade de dispositivos e serviços[81]. Mais precisamente, buscam valorizar a segurança e privacidade desde o projeto, perpassando todas as demais etapas de execução, devendo ser uma prioridade no desenvolvimento de uma forma holística.

É disponibilizado um framework com 30 princípios e critérios que são sugeridos para o aumento da segurança, privacidade e controle de acesso das partes que compõem um ambiente de IdC. Essa iniciativa provê também guias de auxílio, um check-list para consumidores e outras pesquisas no tema.

2.6 Comentários Finais

As diversas instituições e projetos envolvidos com segurança na IdC revelam que é necessário que hajam esforços para que a base de toda infraestrutura da IdC esteja implementada de maneira segura. Estão envolvidos, nesse processo: o entendimento dos riscos trazidos pela implementação de soluções de IdC; a regulamentação a partir de um entendimento dos princípios de privacidade e segurança; a definição de protocolos eficientes e seguros; utilização de boas práticas no desenvolvimento de software e, principalmente, a elaboração do projeto pensando-se na segurança desde o início.

Capítulo 3

Privacidade na IdC

> "Aqueles que abrem mão da liberdade essencial, para obter uma pequena segurança temporária, não merecem nem segurança, nem liberdade"
>
> Benjamim Franklin

Em todos os projetos analisados no capítulo anterior, é crescente a preocupação com questões relativas à privacidade. Com o crescimento do número de dispositivos conectados, cada vez mais dados são colhidos, a partir de fontes antes não exploradas, sendo utilizados para os mais variados fins. Tendo em vista que os dados carregam em si informações valiosas a respeito de indivíduos, torna-se crescente a ameaça à privacidade dos mesmos.

A privacidade, quando se trata de Tecnologia da Informação (TI), em especial, no universo da IdC, nem sempre é algo essencial ou imprescindível, como será abordado no seguinte tópico, que contrasta o bem estar coletivo com a necessidade de privacidade de indivíduos. Apesar de ser um tema complexo, deve ser abordado de forma prática no desenvolvimento da IdC, para que o que as definições, tendo em vista a regulamentação local e questões morais, sejam corretamente aplicadas e respeitadas.

3.1 Privacidade x Segurança

Existe uma diferença nos conceitos de privacidade e segurança, apesar de em alguns pontos os dois estarem interligados. A privacidade, segundo Gibbs[22], se refere às "limitações de acesso de outros a um indivíduo". A engenharia de segurança segundo Ross Anderson,[6], se refere à "construção de sistemas confiáveis ante a malícia, erros e o acaso". Entende-se, também, por segurança como os mecanismos utilizados para se preservar o bem estar social. Há, porém, um conflito quando soluções motivadas pelo bem estar social vão

contra a privacidade dos indivíduos. Isso acontece no universo de TI como um todo, não apenas em se tratando de IdC.

Um exemplo recente do embate entre segurança e privacidade envolveu a Apple e o FBI. Em 2015, um ataque terrorista a um centro regional americano, em San Bernardino, causou a morte de 14 pessoas e deixou 21 seriamente feridos[77], sendo o segundo ataque terrorista mais mortal nos Estados Unidos desde os ataques do 11 de setembro. No processo de investigação, agentes do FBI buscavam acessar o iPhone do atirador, que estava bloqueado por senha. Foi então que a agência decidiu entrar com uma ação na justiça americana demandando a liberação, por parte da Apple, de um mecanismo que permitisse ao FBI quebrar a autenticação por senha, o que daria acesso aberto aos dados do dispositivo. Isso, que seria um grande *backdoor* nos produtos da Apple, gerou uma reação na indústria, que decidiu apoiar a Apple contra tal decisão, visto que uma vez aberto o precedente outras companhias também poderiam ser afetadas no futuro. O FBI não deu prosseguimento ao pedido pois alegou ter sido capaz de desbloquear o iPhone com o auxílio de um "terceirizado"[76].

No Brasil, também houve um caso parecido: a 1ª Vara Criminal de São Bernardo do Campo determinou que o serviço do Whatsapp fosse retirado do ar pois a empresa não havia concordado em liberar os dados de conversa entre investigados[112]. O vice-presidente da América Latina do Facebook, empresa que controla o Whatsapp, chegou inclusive a ser preso preventivamente, mas foi logo liberado[33].

Existe, pois, uma dualidade nessas duas situações apresentadas: por um lado, há os que defendem a "invasão de privacidade" em nome da Lei e, por outro, existem aqueles que defendem a garantia de privacidade dos usuários, independentemente da situação. Vale salientar que a própria Lei, ou seja, a legislação vigente não necessariamente acompanha todos os avanços no universo de TI.

Segundo Glenn Greenwald, em sua palestra para o TED[37], "abrir mão da privacidade é um caminho sem volta". Segundo ele, uma vez que indivíduos optem por abrir mão de sua privacidade em troca de mais segurança, por exemplo, não há como reverter o processo. Isso significa que, se o governo ou as instituições controladoras, as quais detêm tal confiança, mudarem em um futuro próximo, não há como reverter e recuperar a privacidade. Hoje, as motivações podem ser legítimas; hoje, talvez os indivíduos "não estejam fazendo nada de errado" e uma eventual perda de privacidade não trará maiores problemas; mas, amanhã, talvez não seja assim, acrescenta ele. O controle pode estar nas mãos de governos autoritários, que perseguem de acordo com etnias, ou regras morais diferentes ou até mesmo escolhas religiosas, possuindo, consequentemente, o poder sobre a individualidade de cada um, o que é um enorme risco para a liberdade. Não é possível prever quem estará no controle das informações individuais, conclui.

Um ponto que foi levantado na questão Apple vs. FBI é que, ao se abrir um *back-door* para uma agência como o FBI, abrem-se possibilidades para que indivíduos mal intencionados também possam explorá-lo[124].

Outro ponto preocupante quando se trata de privacidade é o monitoramento realizado sem que indivíduos tenham previamente concordado. Informações secretas reveladas pelo WikiLeaks[122] e por Edward Snowden trouxeram à discussão informações relativas ao uso controverso do poder de vigilância de agências que eram antes vistas como confiáveis e transparentes, todavia, por razões escusas, apresentam outra postura.

Gibbs ressalta que a privacidade individual deve ser balanceada com as necessidades de outros indivíduos e ações que garantam o bem estar social[22]. Às vezes, é necessário abrir mão da privacidade na busca pela garantia da segurança, como ocorrem nos aeroportos, por exemplo, em que indivíduos são vistoriados antes de entrar na sala de embarque para se evitar atentados em voos.

3.2 Dados gerados na IdC

Um dos bens mais valiosos das empresas que trabalham com IdC são os dados coletados. Os dados, provenientes das mais diversas fontes, formam um rico celeiro de informações a serem reaproveitadas e exploradas de inúmeras formas. Não obstante, o uso de tais dados traz consigo ameaças à privacidade que devem ser levadas em consideração. Ziegeldorf et. al.[128] citam em sua pesquisa sete categorias de ameaça à privacidade e como se aplicam no universo de IdC, que serão apresentadas a seguir.

3.2.1 Identificação

Identificação é a "capacidade de se associar [...] um indivíduo a dados relativos a ele".[128, p. 7] Para garantir a privacidade de um indivíduo, os dados relativos a ele tendem a ser armazenados de forma anônima para evitar sua identificação. Muitas ameaças em termos de identificação são facilitadas, em se tratando de IdC, pois, os dados auxiliares podem ser utilizados para identificar um indivíduo. Por exemplo, as câmeras de vigilância tem sido utilizadas em aplicações que vão além de segurança e podem ser integradas a aplicações de detecção facial para identificação. Outro exemplo é o reconhecimento por voz e fingerprinting. No caso da identidade, a criptografia é muito utilizada para preservá-la, mas, seu uso é mais complexo no ambiente de IdC, como detalhado no Capítulo 4.

3.2.2 Rastreamento e Localização

O Rastreamento e Localização tratam de todo processo de "determinar e gravar a localização de um indivíduo no tempo e espaço"[128]. Relacionam-se à identificação do local, em tempo real, onde a pessoa se encontra e conta com tecnologias como GPS, análise de tráfego de internet ou localização por torres de celular. Problemas de privacidade ocorrem quando os dados são colhidos sem o conhecimento dos usuários e seu tratamento é realizado sem transparência e/ou autorização. A IdC agrava ainda mais o problema por permitir localização mais precisa e em ambientes internos. À medida em que os dados são colhidos de maneira mais "passiva, pervasiva e menos intrusiva, os usuários estão menos conscientes de quando estão sendo rastreados e dos riscos envolvidos"[128]. Da mesma forma, a utilização de dispositivos deixam rastros, por exemplo, ao pegar um ônibus que possui um sistema de pagamento via RFID que guarda o histórico de passagens do usuário.

3.2.3 Caracterização

A caracterização de um indivíduo ocorre quando as informações a respeito do mesmo são correlacionadas com a de outros para inferir conhecimentos de interesse. Exemplos de violações de privacidade nesse sentido são "discriminação de preço, propagandas não-solicitadas, engenharia social ou erros de decisões automáticas"[128], por exemplo, quando o Facebook busca detectar automaticamente estupradores e acaba cometendo enganos no processo de decisão. O crescimento da IdC para aplicações antes não exploradas permite um maior conhecimento a respeito de indivíduos, o que faz aumentar as possibilidades de caracterização e consequentemente das ameaças à privacidade do mesmo. Para preservá-la, técnicas como "personalização no lado do cliente, perturbação de dados, ofuscação, anonimizar os dados, distribuição e trabalhos em cima de dados criptografados"[128] podem ser utilizadas.

3.2.4 Interação e Apresentação

Quando se fala em Interação e Apresentação, é analisado o relacionamento do usuário com tecnologias no processo de disponibilização de informações. Esse processo pode vir a ser feito de maneira pública, expondo a uma audiência o que não era desejado que o fosse. Por exemplo, ao se fazer compras em uma farmácia, um sistema que sugere itens de compra para um usuário, não deveria fazê-lo de forma a expor as informações para outras pessoas ao redor, em uma tela grande ou na prateleira, expondo aos outros quais são as doenças ou outros problemas que este guarda para si. Para amenizar o problema, buscam-se técnicas de detecção automática de conteúdo que é privado e sensível, para decidir como a informação pode ser passada ao usuário, se pode ser de maneira pública, como em uma

grande tela, ou privada, na tela do celular por exemplo. Também são estudadas técnicas que visam limitar a visualização para uma audiência específica, como telas com películas que somente quem está de frente para a mesma consegue ver o conteúdo.

3.2.5 Transições de Ciclo de Vida

A transição de ciclo de vida dos dispositivos causa uma grande ameaça à privacidade. Por exemplo, ao se transferir um dispositivo entre um usuário e outro, as informações privadas do primeiro devem ser resguardadas do segundo. A IdC agrava esse problema ao compartilhar cada vez mais informações pela interação de vários usuários com os mesmos dispositivos. Os dispositivos tendem a ser compartilháveis, logo garantir que os dados não serão divulgados torna-se uma atividade complexa. Também, muitos logs são guardados para validar a garantia de um produto. Por mais que seja um problema conhecido, a maioria das aplicações são projetadas segundo o modelo "compre uma vez e seja o dono para sempre". Pouco é feito para uma completa limpeza da memória, o que garantiria a desvinculação completa do dispositivo com o usuário anterior. Técnicas para esse problema envolvem a detecção automática de transições de ciclo de vida, por exemplo, uma lata de lixo que apague informações médicas de um dispositivo que contenha prescrições médicas e o bloqueio temporário de informações privadas, como feito no caso do iPhone, mencionado na primeira seção deste capítulo.

3.2.6 Ataques a Inventários

Os ataques a inventários envolvem a "coleta não autorizada de informações a respeito da existência e características de assuntos pessoais"[128]. Da mesma forma que o usuário legítimo pode realizar buscas na internet de dados provenientes de seus dispositivos de IdC, indivíduos não-autorizados também o podem, com técnicas como fingerprinting e espionagem. À medida em que aumentam as possibilidades de comunicação, crescem também ameaças de ataques. Esses ataques permitem, por exemplo, que ladrões saibam o melhor momento para invadir uma casa, também que agências reguladoras e investigativas possam realizar buscas não autorizadas, informações pessoais possam ser divulgadas e permitem a espionagem industrial. A prevenção, nesse caso, envolveria autenticar os usuários que podem realizar buscas aos dados e deveria também ser robusto contra *fingerprinting*.

3.2.7 Acoplamento

O acoplamento de diferentes sistemas que estavam antes separados é um grande problema para a manutenção da privacidade, pois as informações podem ser combinadas para revelar informações indevidas. Nesse processo, mecanismos de proteção de privacidade podem

ser transpassados com o acesso não autorizado e vazamento de informações privadas no processo de junção dos sistemas. Há também o risco de *re-identificação* de dados anônimos, ao se juntar dados de fontes distintas. O problema é agravado com IdC à medida em que a "integração horizontal de sistemas de diferentes companhias e fabricantes irá ligá-los para formar um sistema-de-sistemas heterogêneo, distribuído e que fornecerá serviços que nenhum sistema isolado conseguiria prover"[128]. Também, à medida em que os sistemas se tornam cada vez mais interligados, é mais difícil manter a transparência da coleta de dados.

3.3 Regulamentação de Privacidade

Segundo Weber[120], é improvável que a curto prazo sejam definidas regulamentações globais para a IdC. A tendência é que esse processo seja definido nacionalmente, de acordo com os princípios de privacidade que cada país definiu para si, mas eventualmente se ampliará para uma definição mais global. De qualquer modo, sugere-se, pelo autor, que agentes responsáveis pelo processo de definição de diretrizes regulatórias levem em consideração quatro aspectos chaves:

- **Tecnologia** "deve ser global no sentido de que processos técnicos sejam aplicados em todo o mundo para garantir interoperabilidade e segurança"[120]. Regulamentações que não levam em conta a globalidade de padrões das tecnologias implementadas dificultam o avanço da IdC.

- **Ubiquidade** se refere à onipresença da IdC que deve ser levada em consideração na estipulação das regras. Tanto na vida de seres humanos, plantas, animais, todos de certa maneira devem ser levados em consideração na análise do ambiente tecnológico para a implementação das regras, com implicações na proteção de dados, leis de privacidade e padrões tecnológicos.

- **Verticalidade** diz respeito ao "potencial de durabilidade do ambiente técnico"[120]. É importante que se leve em consideração as medidas técnicas em todas as fases, desde a criação até a administração do processo de despojo dos dispositivos.

- **Tecnicidade** envolve a análise da complexidade das técnicas e dos dispositivos envolvidos na estipulação de regras, de modo a escolher técnicas viáveis para aplicação.

A figura Figura 3.1[55] destaca quais fatores influenciam na definição de privacidade a partir de uma análise voltada ao consumidor. No âmbito legal e regulatório, instituições que colhem e armazenam dados de usuários devem garantir que os mesmos tenham o devido acesso aos dados sendo colhidos e tenham o poder de escolher quais dados podem

ser utilizados. A instituição deve manter um processo transparente e ser capaz de prestar contas do que foi definido. Além de seguir o que é imposto como regulamentação legal, o mercado, em si, possui um processo de auto-regulamentação, onde o interesse em alcançar os consumidores e manter um relacionamento de confiança gera, por si só, regras que acabam por ser comuns no mercado. Consequentemente, a aplicação da privacidade requer um avanço técnico de medidas de segurança robustas, capazes de avalizar o que foi estipulado em termos de proteção da privacidade dos consumidores. Estão incluídas neste processo técnicas como criptografia, que deve ser dimensionada de acordo com o grau de sigilo dos dados, protocolos *challenge-response* e outras técnicas de anonimização dos dados. Também, tecnologias para eliminar a informação contida nos dispositivos, como etiquetas RFID.

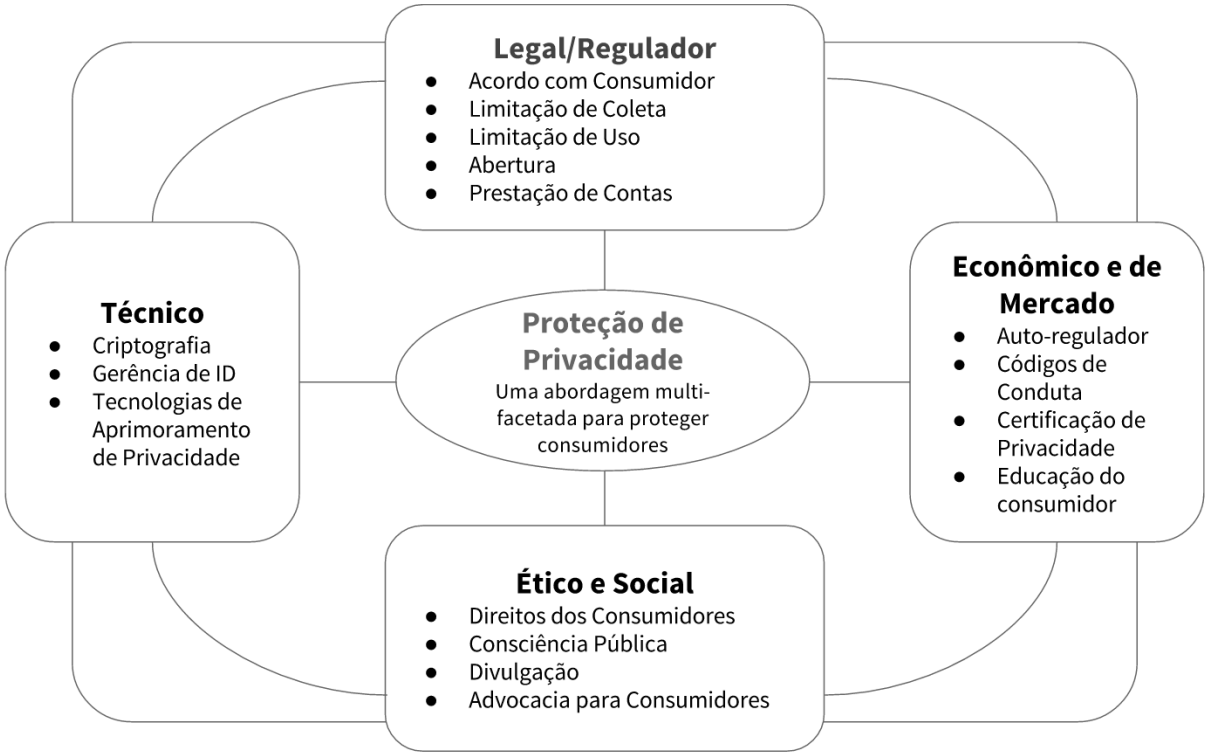

Figura 3.1: Fatores que influenciarão a proteção de privacidade na IdC [55].

Um estudo[22] buscou analisar os 13 princípios de privacidade conhecidos como Australian Privacy Principles (APP), definidos pelo Gabinete do Comissário de Informação Australiano, do inglês Office of the Australian Information Comissioner, no contexto de IdC. A definição dos princípios serve de base para a política de leis a serem definidas em relação à privacidade na Austrália. Tais princípios são divididos em cinco partes: "(1) consideração de privacidade de informação pessoal; (2) coleta de informação pessoal;

(3) tratamento de informação pessoal; (4) integridade da informação pessoal e (5) acesso e acurácia de informação pessoal". A partir desses princípios, organizações que cuidam da coleta, armazenamento e tráfego de dados se tornam legalmente responsáveis pela privacidade dos usuários.

No caso da Europa, os esforços em estudo pela UE são os mais avançados para estudar as necessidades regulatórias da IdC, de modo a "garantir direitos fundamentais como privacidade, proteção dos dados pessoais e proteção ao consumidor"[119]. Seus esforços, iniciados em 2006, que geraram um estudo, em 2008, entitulado "Staff Working Document", porém, focavam em tecnologias como RFID, o que foi criticado pela Amcham EU como sendo precipitado e pedindo que o estabelecimento das regras fosse feito a partir de uma "abordagem com um framework neutro em relação à tecnologia"[119]. A EPC Global acrescenta que os "direitos fundamentais de indivíduos à privacidade e à proteção dos dados já são bem definidos pela legislação Europeia"[119]. O estudo visa reunir as principais implicações da IdC na privacidade e o estabelecimento de regulamentação para esse novo paradigma.

Nos Estados Unidos, setores específicos também trazem regulamentações para a coleta e privacidade dos dados, como por exemplo Health Insurance Portability and Accountability Act (HIPAA)[120].

Uma das características das soluções de IdC é que são, em sua maioria, dispositivos simples e de fabricação relativamente barata. Nesse aspecto, muitas soluções chegam a partir de startups ou pequenos vendedores, que muitas vezes não estão preparados para lidar com as diferenças regulatórias e podem acabar sucumbindo em processos legais por quebrar diretrizes impostas ou por perda de credibilidade com seus clientes ao desrespeitar políticas de privacidade.

De igual modo, empresas com iminência de falência formam uma grande ameaça à privacidade pela fragilidade em que se encontram, estando mais vulneráveis a ataques pela escassez de recursos e a tentação de descumprir políticas de privacidade vendendo dados que não deveriam. Empresas nessa condição(falência eminente) devem receber especial atenção e leis específicas para que a privacidade dos usuários não seja prejudicada[109].

Movido pela globalização, a expansão de produtos ao redor do mundo é cada vez mais facilitada, porém ainda mantém a complexidade relativa a diferenças culturais. Com isso em mente, os fabricantes de dispositivos conectados devem estar sempre atentos às leis vigentes nos países em que serão comercializados e devem estar preparados para lidar com as diferenças em termos de regulamentação. As empresas devem conhecer e respeitar as leis tanto para o local onde os dispositivos se encontram, quanto para o de servidores que armazenam os dados. Além disso, devem ser absolutamente transparentes no tratamento com os usuários, evidenciando quais são as políticas de privacidade e até que ponto as

soluções de IdC conseguem realmente assegurar a privacidade dos indivíduos.

3.4 Comentários Finais

Os diversos fatores relativos à privacidade mostram que é necessário que governos e sociedades, juntos, discutam pontos fundamentais para a regulamentação da privacidade. Algumas características relativas ao assunto são agravadas com o crescimento pervasivo da IdC. Para cumprir com o estabelecido para a privacidade, são necessários cuidados na fase de desenvolvimento, atentando-se para as melhores práticas de desenvolvimento de software, dando ao usuário informações quanto aos dados sendo colhidos e utilizando criptografia confiável, e no processo de implementação e descarte, com a garantia de inviolabilidade dos dispositivos com informações sensíveis.

Capítulo 4

Segurança nos Protocolos da IdC

> "A ciência, assim como a vida, se alimenta no próprio decaimento. Novos fatos rompem regras antigas; então concepções recém-descobertas unem o antigo ao novo em uma lei de reconciliação."
>
> William James, The Will to Believe and Other Essays in Popular Philosophy, 1910

Tendo em vista o que foi apresentado anteriormente como os principais problemas de segurança em IdC e de questões relativas à privacidade, entende-se que o amadurecimento da IdC deve ser orquestrado a partir da estipulação de padrões que permitam a implementação de soluções para estes problemas. Os protocolos nada mais são do que regras a serem seguidas para realizar a comunicação entre duas entidades interessadas. Nesse sentido, devem prover mecanismos de segurança, ao mesmo tempo que fornecem a agilidade e escalabilidade necessária para o fluxo de dados.

Quando se trata de IdC, diversos fatores influenciam a escolha pelos protocolos a serem utilizados. Tempo de vida da bateria, necessidades da troca de dados, alcance mínimo e máximo, mobilidade dos nós na rede, taxas de perda e de erro, comunicação com a nuvem, entre outros. Além de utilizar os protocolos já conhecidos da internet convencional como TCP/IP, HTTP/REST, WiFi e Ethernet, novos protocolos ganham importância, principalmente nas camadas físicas e de ligação, em que dispositivos com sensores que formam WSNs possuem restrições energéticas e de processamento.

Conhecer quais são os protocolos e suas principais características é extremamente importante no processo de projeto da arquitetura do ambiente de IdC, de modo a prover

segurança. Falhas de transmissão, negação de serviço, interceptação dos dados, ataques de autenticação, spoofing, entre outros, podem vir a acontecer caso a escolha do protocolo não esteja condizente com as especificações e limitações dos dispositivos e das diversas interfaces com as quais eles se comunicam. Uma comunicação segura envolve confidencialidade, integridade, autenticação e não-repudio, que podem ser endereçadas pelos protocolos ou por mecanismos externos[35].

A seguir, serão visitados alguns dos conceitos que são importantes para o entendimento dos protocolos abordados. Em seguida, os protocolos que possuem relevância no contexto de IdC serão apresentados, com ênfase nas suas principais características, garantias de segurança e possíveis vetores de ataque e vulnerabilidades que possam apresentar.

4.1 IEEE e IETF

O grupo Institute of Electrical and Electronics Engineers (IEEE) assim como o Internet Engineering Task Force (IETF) são grandes influenciadores para a definição de padrões que auxiliam a integração das diversas tecnologias e o crescimento da internet. A criação do IEEE data do ano de 1884, com o crescimento da eletricidade e do telégrafo, inicialmente se chamava AIEE (American Institute of Electrical Engineering). Foi se estabelecendo como uma associação de renome, com a presença de cientistas renomados e inovadores, como Thomas Edison e Alexander Graham Bell. Teve forte influência na disseminação de energia elétrica e na expansão da comunicação, tanto por telefone quanto por telégrafo, a partir de encontros científicos em conferências técnicas e com estudantes, inúmeras publicações e os diversos padrões que foram desenvolvidos.[1]

Para ser definido um padrão pelo IEEE, primeiro um corpo patrocinador, seja uma única instituição ou um conjunto, entram com um pedido formal. Assim que aprovado, o IEEE provê regras para o processo de recrutamento e criação de uma equipe de colaboração, denominado "Working Group", formado por indivíduos, instituições e outras entidades interessadas em se voluntariar para o desenvolvimento do padrão. Esse grupo e o corpo patrocinador elegem quem serão os diretores e definem as políticas de administração e desenvolvimento do projeto. Busca-se uma colaboração democrática entre os membros envolvidos, com diversas reuniões agendadas, apresentações e debates para resolver as questões que forem surgindo. A partir destas atividades, o padrão vai se construindo até se obter um projeto do mesmo, o "Standard Draft", que irá passar por diversas revisões. Após ser amplamente testado e verificado pelo Working Group, o projeto vai para o corpo patrocinador para a decisão por votação. Em seguida, o padrão que foi votado segue para um comitê de revisão (RevCom) que, após revisá-lo, envia para o comitê

[1]IEEE - History - `http://www.ieee.org/about/ieee_history.html` - Acesso em 13/06/2016

de padrões para a aprovação final. Uma vez aprovado, o padrão é publicado e divulgado em diversos meios. Vale ressaltar que, mesmo após publicado, o padrão ainda pode sofrer atualizações, revisões e ser arquivado[46].

O IEEE 802 contém os padrões que estão relacionados a redes sem-fio de área local (LANs) e de áreas metropolitanas (WANs). Dentro deste, existem Working Groups que se especializam em determinadas áreas para prover padrões específicos. Os serviços e protocolos produzidos encontram-se majoritariamente nos níveis de enlace e físico. Protocolos nesse grupo possuem especial relevância para o funcionamento da internet.

O Internet Engineering Task Force (IETF) foi criado inicialmente, em 1986, para coordenar os contratos da agência americana DARPA (U.S. Defense Advanced Projects Agency). Assim como o IEEE, o grupo IETF é organizado em Working Groups que se dividem para desenvolver padrões e possui também grupos de discussão informal. É mais flexível que o IEEE quanto à fidelização dos membros e à obrigatoriedade de que os mesmos estejam presentes nas reuniões, dado que a maior parte do trabalho é organizada por listas de email. [27]

O foco dos projetos administrados pelo IETF é na internet, em propor soluções que otimizem a utilização, identifiquem e resolvam problemas técnicos. Os Working Groups se dividem em oito áreas principais: (1) Aplicações, (2) IP, (3) Requisitos Operacionais, (4) Segurança, (5) Transporte, (6) Internet, (7) Gerência de Redes e (8) Roteamento. [27] O principal documento produzido pelos Working Groups são os RFCs (Request For Comment), que contém todo o resultado de determinado projeto. Uma vez aprovado como padrão para a Internet, a versão final do RFC é escolhida como sendo o padrão e nenhuma modificação mais é permitida. O padrão pode, porém, vir a se atualizar, logo, sua definição oficial passa para outro RFC que atualiza o anterior.

4.2 Categorização dos Protocolos Abordados em Camadas

A abstração de rede mais conhecida é a do modelo OSI, em que as funcionalidades de comunicação são categorizadas de acordo com sete camadas: (1) Física, (2) Enlace, (3) Rede, (4) Transporte, (5) Sessão, (6) Apresentação e (7) Aplicação. A partir desse modelo, o grupo IEEE 802 divide a camada de enlace em outras duas sub-camadas para melhor representar a rede: Controle de Acesso ao Meio, do inglês Media Access Control (MAC) e Controle Lógico de Enlace, do inglês Logical Link Control (LLC). No TCP/IP, as camadas de sessão, apresentação e aplicação são agregadas em uma única camada, a de aplicação.

Os protocolos podem ser categorizados como específicos de determinada camada ou presentes entre várias camadas. Um conjunto de protocolos relacionados, presentes em

diferentes camadas, formam pilhas de protocolos, para prover a integração de funcionalidades.

Para o presente estudo, os protocolos escolhidos foram categorizados de acordo com as camadas que os definem. A Figura 4.1 representa o posicionamento dos protocolos que serão abordados de acordo com suas camadas principais. No capítulo seguinte, as ameaças de cada camada serão colocadas juntas para uma análise comparativa entre os protocolos.

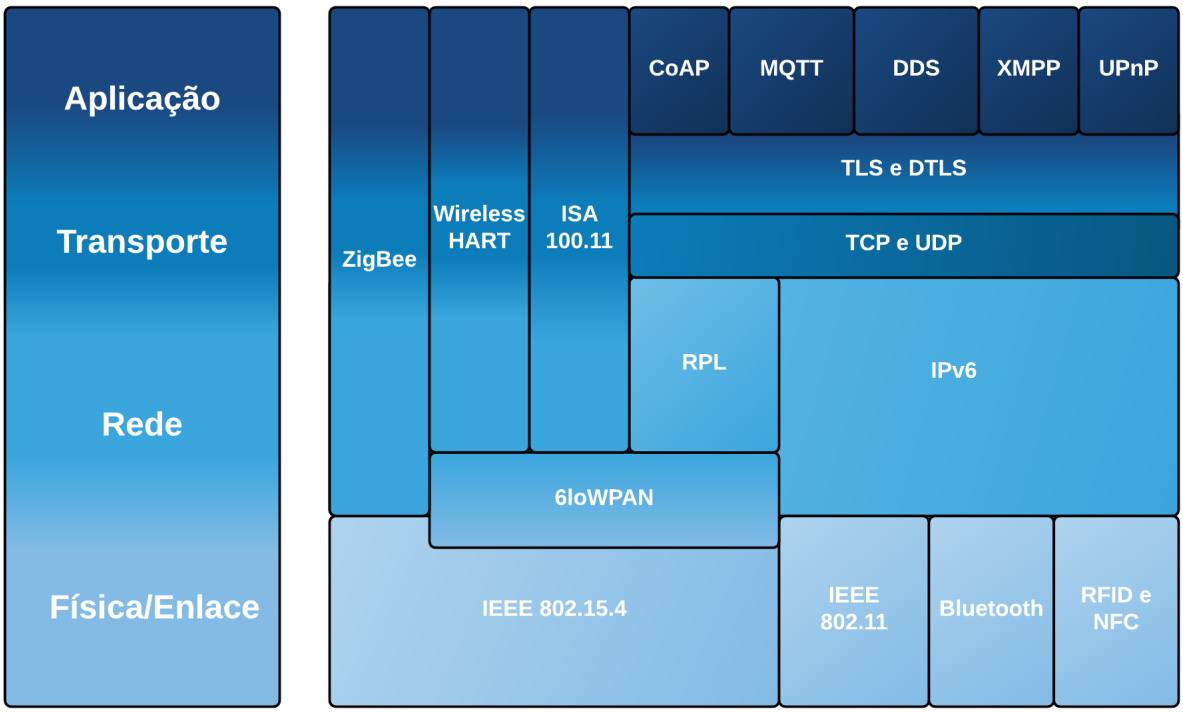

Figura 4.1: Divisão por camadas dos protocolos que serão abordados.

4.3 Camadas Física e de Enlace

A camada física, segundo o modelo OSI, engloba as funcionalidades de hardware relativas à transmissão em um meio físico. Essa camada trata os bits de forma crua, preocupando-se apenas em como estes irão ser transmitidos pelo meio. A camada de enlace de dados é responsável por administrar a transmissão entre dois nós e pode envolver controles de erros que ocorrem na camada física.

4.3.1 IEEE 802.11 e WiFi

Em 1985 foi liberada para uso a banda Industrial, Científica e Médica, do inglês Industrial, Scientific and Medical (ISM), de modo a garantir para aplicações não relacionadas à telecomunicação uma banda de Frequência de Rádio (FR) para a comunicação. Em cima dessa banda, em 1997, o IEEE 802.11-1997 foi lançado, em 1999, após revisão, o IEEE 802.11 se concretizou. Em seguida, novas alterações foram sendo adicionadas, sendo que as versões que mais se popularizaram foram a 802.11a, 802.11b e 802.11g e, na versão 802.11i, os mecanismos de segurança foram atualizados. A versão considerada padrão, atualmente, é a 802.11-2012. Bellalta et. al[11]. trazem um estudo atualizado, em 2015, com o status corrente, futuras direções e desafios abertos das novas atualizações[2] para o 802.11 em desenvolvimento.

A associação WiFi Alliance[3] busca prover a interoperabilidade e proteções de segurança entre os dispositivos com comunicação sem-fio. A certificação envolve as tecnologias de FR do IEEE 802.11 além dos mecanismos de segurança WPA e WPA2, que serão abordados a seguir.

O 802.11 define quais são os padrões no processo de codificação dos dados e mecanismos de segurança em uma transmissão para redes locais sem-fio (WLAN). Na transmissão de dados, o IEEE 802.11b utiliza do modo *Direct Sequence Spread Spectrum* (DSSS), que "utiliza apenas um canal que espalha os dados pelas frequências definidas para o canal"[69, p. 213], sua taxa de dados máxima é de 11 Mbps e opera no espectro de 2.4 GHz. O IEEE 802.11a utiliza *Orthogonal Frequency Division Multiplexing* (OFDM), que divide o espectro em menores pedaços, sua taxa de dados máxima é de 54 Mbps e utiliza do espectro de 5 GHz. O IEEE 802.11g utiliza o OFDM, mas mantém a compatibilidade para o DSSS, possuindo uma taxa de transmissão de 54MBps e operando no espectro de 2.4 GHz.

Existem dois modos de operação para o IEEE 802.11: (1) Infraestrutura e (2) Ad-Hoc. No primeiro, a comunicação é realizada entre um dispositivo e um *Access Point* (AP), que é conectado à rede. O AP é responsável por prover a autenticação, autorização e segurança a nível de enlace, como controle de acesso e a criptografia para o tráfego dos dados. No segundo, a comunicação é realizada diretamente entre os dispositivos, que devem cuidar de todo o processo e garantias de segurança. Para identificar a rede, o protocolo trabalha com um identificador conhecido por *Service Set Identification* (SSID)[125].

O primeiro modo de segurança disponibilizado no IEEE 802.11 foi o *Wired Equivalent Privacy* (WEP), que visa proteger a integridade e confidencialidade na transmissão. É utilizado criptografia a partir do RC4 com chaves de 64 ou 128 bits, sendo que na prática

[2] aa, ac, af, ah, ax

[3] WiFi Alliance - `http://www.wi-fi.org/` - Acessado em 31/05/2016

é menor, pois uma parte da chave é transmitida abertamente. A chave é formada pela concatenação de um Vetor de Inicialização (VI) com a parte estática da chave. Para se comunicar, os participantes do processo de comunicação devem compartilhar das mesmas chaves. O WEP teve um tempo de duração curto, dada sua fragilidade com chaves estáticas, uma implementação repleta de falhas do RC4 e um vetor de inicialização curto que, com o tempo, fornecia chaves repetidas[18].

Buscando um mecanismo de segurança mais robusto, o WiFi Alliance definiu um novo modo de segurança WiFi Protected Access (WPA) que foi ratificado pelo IEEE 802.11i em seguida. O WPA utiliza, por motivos de compatibilidade, do RC4, porém, diferentemente do WEP, as chaves são dinâmicas, como será mostrado a seguir. Os três principais componentes para o WPA são: (1) TKIP, (2) 802.1x e (3) MIC[125].

- **TKIP:** O Temporal Key Integrity Protocol (TKIP) modifica o WEP para prover uma administração de chaves mais robusta, calculando um código de integridade para mensagem criptográfica chaveada (MIC) e adicionando ao pacote enviado um código de sequência (TKIP Sequence Counter - TSC) para evitar ataques de replay. Também é utilizado uma função de mistura criptográfica para formar a semente WEP, que pode ser calculada utilizando uma chave temporária, o endereço de transmissão (Transmitter Address - TA) e o TSC. Essa semente é calculada também pelo receptor para recuperar a mensagem criptografada.

- **802.1x:** O padrão 802.1x define a autenticação por portas, em LANs e WLANs, por um servidor de autenticação. É baseado no Protocolo de Autenticação Extensiva, do inglês Extensible Authentication Protocol (EAP), definido pela IETF, para troca de mensagens. O EAP possui vários modos de operação no WPA, que provêm um mecanismo de autenticação seguro, além da negociação de pares de chaves mestra. O 802.1x cria uma porta virtual para cada cliente em um AP, que funciona como o autenticador, bloqueia todos os dados que não sejam baseados no 802.1x, passa os dados para o servidor de Autenticação, Autorização e Prestação de Contas, do inglês Authentication, Autorization and Accounting (AAA), através do AP e, se a autenticação for bem sucedida, o servidor AAA envia para o AP uma mensagem de sucesso, de modo a permitir o fluxo de tráfego para o cliente autenticado[25].

- **MIC:** O WPA utiliza do algoritmo Michael para calcular um código de integridade de mensagem, do inglês Message Integrity Code (MIC), de 8 bytes. Este código, que é enviado junto da mensagem, é gerado a partir de uma chave compartilhada e da mensagem, em uma função hash, para garantir que não houve adulteração da mensagem original enviada.

O WPA foi primeiramente designado pela indústria devido à demora do IEEE em publicar a versão final do IEEE 802.11i, utilizando do *draft* que já havia sido desenvolvido pelo grupo de trabalho deste padrão até aquele momento.[30, p. 208] Após a ratificação do padrão IEEE 802.11i, que endereçava as questões de segurança, foi definido o WPA2, que estava de acordo com as novas definições do IEEE 802.11i e é utilizado pela WiFi Alliance para certificação de dispositivos.

O WPA2 trouxe algumas modificações ao WPA, entre elas a principal é a definição de um mecanismo de criptografia mais robusto e amplamente aceito, o AES, no modo CCMP, que substitui o TKIP (mantido apenas para compatibilidade) e a utilização de CBC-MAC para integridade. Existem dois modos de execução do WPA2: (1) WPA2 Personal e (2) WPA2 Enterprise. No WPA2 Personal, a autenticação é realizada por chaves compartilhadas (Pre Shared Keys - PSK) entre um Access Point e um dispositivo, por exemplo. Já no WPA2 Enterprise, a autenticação é realizada pelo IEEE 802.1x/EAP e necessita de um servidor de autenticação, que normalmente é gerido através do protocolo RADIUS (Remote Authentication Dial-In User Service)

Tendo em vista que, a partir de 2006, todos os dispositivos verificados para WiFi devem fornecer o suporte para WPA2, assume-se para esse estudo apenas as vulnerabilidades e questões de segurança relacionadas ao WPA2, tendo em mente que a utilização de WEP apresenta vulnerabilidades desencadeadas por má configuração ou desatualização de dispositivos, que podem ser resolvidas migrando-se para o WPA2.

Dada a característica aberta do ambiente em que o protocolo se encontra e o fato de utilizar faixas de bandas não reguladas (ISM), o IEEE 802.11 apresenta diversas vulnerabilidades na manutenção do serviço. Seja intencional ou não, a informação transmitida está vulnerável a sofrer interferência. Quando esse processo é intencional, é chamado ataque de *jamming*, que pode ser facilmente implementado com dispositivos que emitam ruído[23]. Ronak e Rutvij[14] categorizam como *jammer constante* aquele que emite constantemente o ruído; um que só é ativado quando há comunicação entre dispositivos é chamado *reativo*; um que transmite pacotes comuns ao invés de um sinal randômico é *deceptivo* e os que enviam sinais aleatórios (pacotes normais ou ruído), quando ativos, mas entram aleatoriamente em um estado de espera, são conhecidos como jammers *randômicos*. Os autores apresentam um estudo dos métodos correntes e desenvolvem um novo método para se identificar quando um jammer constante está presente em um ambiente de rede sem-fio. Também sugerem para trabalhos futuros o estudo para jammer reativo, deceptivo e aleatório e também que o algoritmo criado seja utilizado para mitigar os ataques por jamming. Outras formas de se mitigar o ataque são sugeridas pelo autor.

O ataque conhecido como *probe request flooding* inviabiliza ou torna mais lento o serviço de autenticação na rede por um usuário legítimo, ao se enviar probes falsos, com

endereços MAC adulterados (MAC spoofing). O probe request é enviado para todos os APs, para se identificar redes próximas. O ataque explora o fato de que os APs devem responder a todo probe request, para poder autenticar usuários, e enviam mais pedidos do que o dispositivo de AP consegue suportar para manter a rede estável. É, portanto, um dos possíveis ataques de negação de serviço, do inglês Denial of Service (DoS)[23].

Ataques de de-autenticação envolvem o envio de pacotes por um atacante para o Access Point com o pedido de de-autenticação de um cliente da rede. Existem também ataques de desassociação, que encerram a associação do cliente a determinada rede. O IEEE 802.11w, grupo de tarefa responsável por definir *management frames* protegidos (Protected Management Frames), oferece a proteção dos pacotes por chave para evitar que esses tipos de ataque aconteçam. O WPA2 possui uma configuração que utiliza do modo com management frames protegidos[23].

Ataques de dicionário envolvem a observação, por parte do atacante, do processo de *four-way handshake* para se utilizar de um dicionário com várias possíveis PSKs. A partir dos pacotes capturados, tenta-se, por força bruta, desvendar qual é a PSK sendo utilizada. Caso a senha seja muito fácil, o processo será rápido, caso seja uma senha maior, com mais símbolos e outras funcionalidades, o processo tenderá a ser mais demorado[117].

Outros ataques em rede WiFi visam disponibilizar um Access Point trapaceiro, também conhecidos como ataques *Evil Twin*(Traduzido: Gêmeo Mau), ou *Caffe Latte Attack*(Traduzido: Ataque Cafe com Leite), por serem utilizados em pontos que disponibilizam WiFi gratuito, como cafeterias. Nesse caso, um atacante com um AP trapaceiro, que emite sinal na mesma área que um AP genuíno, engana os clientes, os quais pensam estar se conectando a um ponto confiável sendo que, todavia, estão sofrendo um ataque. Ao aproveitar-se desta brecha, diversos outros ataques podem ser efetivados, como Man-In-The-Middle e outras formas de phishing[96].

Bloessl et. al[15]. mostram um ataque na camada física que visa quebrar a privacidade que era creditada a técnicas de mudanças de endereços MAC, chamadas de pseudônimos. Conhecido como ataque de *scrambler*, este se aproveita da funcionalidade de embaralhamento utilizada para melhorar a performance da comunicação sem-fio. Como o ataque é realizado diretamente na camada física, as informações relativas aos dados não são relevantes para o ataque.

Amin e Abdel Hamid[5] trazem, em sua classificação e análise dos ataques na camada MAC, o ataque por jamming na camada de enlace. Assim como na camada física, seu objetivo é perturbar o meio para desabilitar o serviço, porém, ao invés de enviar sinais de rádio, envia pacotes. Pode ser classificado de duas maneiras: (1) Jamming aleatório ou (2) Jamming Inteligente. Em (1), o ataque apenas envia pacotes sem significado em intervalos de tempo randômicos. Em (2), os pacotes são enviados em tempos específicos

e com propósitos específicos, podendo ser aproveitados para introduzir novos ataques.

Os autores seguem com outros ataques identificados para a camada MAC, como o Flooding em um nó específico. Neste ataque, pacotes desnecessários são enviados para nós com endereço definido pelo atacante, de modo a congestionar determinado nó da rede. Outro ataque mencionado chama-se ataque de manipulação Backoff, que explora as regras do CSMA/CA de modo que o atacante use os períodos pequenos de back-off, deixando períodos maiores para os nós legítimos, aumentando o tempo de espera e desperdício de energia. Este ataque possui duas variantes: (1) Fingimento de extensão do tempo-de-vida da bateria, do inglês Battery Life Extension (BLE) Pretense, em que o nó se aproveita da propriedade do CSMA/CA que dá tempos menores para nós com pouca bateria, e (2) Expoente Constante de Back-off, do inglês Constant Back-off Exponent (BE), em que o atacante mantém o BE fixo, não permitindo que a janela de contenção aumente de tamanho.

Ainda no mesmo trabalho, é mencionado o ataque de adulteração do gerador de número randômico, que age como um DoS na camada de enlace por aumentar as chances de acesso de um nó atacante ao se modificar seu RNG, de maneira que seus períodos de back-off sejam menores. O ataque de omissão de contador do backoff é considerado pelo autor como equivalente à total omissão do CSMA/CA, o que permitiria ao atacante transmitir mais pacotes e causar mais colisões.

IEEE 802.11ah

O IEEE 802.11ah, ou “WiFi Halow”, está, atualmente, na fase de aprovação pelos patrocinadores do padrão e seu lançamento é aguardado para setembro de 2016. Nesta atualização do IEEE 802.11 busca-se uma solução compatível com o ambiente de IdC, ao competir com tecnologias como Bluetooth, fornecendo um alcance maior e um menor consumo de energia. Opera abaixo do espectro de 1GHz o que permite seu maior alcance. O Access Point pode negociar um "Tempo para Despertar"do inglês Target Wait Time (TWT) com os dispositivos participantes da rede, permitindo que os mesmos se mantenham em estado de repouso para reduzir os custos energéticos[60].

4.3.2 IEEE 802.15.1, Bluetooth e BLE

O Bluetooth Special Interest Group (SIG), formado em 1998 por 5 empresas, lançou a versão Bluetooth 1.0, em 1999, como uma alternativa para o uso de cabos e, em 2002, o IEEE definiu a especificação do 802.15.1 para estar de acordo com a tecnologia Bluetooth[17]. Atualmente, se encontra na versão 4.2 e, no período entre o fim de 2016 e começo de 2017, espera-se ser lançada a versão 5.0, em que sua velocidade será dobrada, o alcance

quadruplicado e a capacidade de broadcast aumente em até oito vezes[4]. Exitem duas implementações para a especificação do Bluetooth: Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR), para distâncias curtas e conexões contínuas, e Bluetooth with Low-Energy (BLE), para pequenos envios de conexões de rádio de longo alcance. Existe, também, o modo que utiliza ambas (Dual-mode). Apesar de certas diferenças entre as implementações, compartilham de conceitos base do Bluetooth.

A distância de operação varia de 10 a 100 metros e, utilizando uma antena direcional e amplificador, pode chegar até a uma milha. O Bluetooth funciona seguindo o modelo mestre-escravo, em que um dispositivo mestre pode ter até 7 escravos, conectados por *pairing*, formando as *piconets*. Duas ou mais *piconets* juntas formam uma *scatternet*, quando dispositivos atuam como mestres e escravos em diferentes *piconets* ao mesmo tempo, aumentando o alcance da rede[72].

Na Figura 4.2, Zou et. al [130] apresenta a arquitetura do Bluetooth. A controladora administra as transmissões dos canais de rádio na faixa 2.4GHz. Também na controladora, a gerente da camada de enlace define a estrutura e os canais para os pacotes, procedimentos de descoberta e conexão, além do envio e recebimento de dados. Uma interface de hospedeiro para controladora, do inglês Host to Controler Interface (HCI), pode ser utilizada entre um hospedeiro Bluetooth e o subsistema controlador. A camada para o Protocolo de Enlace Lógico de Controle e Adaptação, do inglês Logical Link Control and Adaptation Protocol (L2CAP) transmite pacotes diretamente para o HCI ou para o gerente da camada de enlace, no caso de um sistema sem hospedeiro. Esse protocolo fornece segmentação e reconstrução de pacotes, QoS, trabalha em cima de "canais", provendo a multiplexação de diferentes conexões lógicas, podendo ser orientado a conexão ou não. A comunicação de rádio-frequência (RFCOMM) define um protocolo da camada de transporte que emula uma porta serial do tipo RS-232. Acima, encontra-se o protocolo de atributos (ATT) que especifica a troca de dados segundo um modelo cliente/servidor e, exclusivamente para o Bluetooth LE, um perfil de atributo genérico (GATT) e um perfil de acesso genérico (GAP) são utilizados para agrupar serviços e funções dos dispositivos de maneira hierárquica[72].[16].

O gerente de segurança é responsável por definir os "protocolos e o comportamento para administrar a integridade no pareamento, na autenticação e a criptografia para a comunicação entre os dispositivos"[16]. São definidas quatro entidades para a segurança: (1) O endereço do dispositivo BD_ADDR, de 48 bits, único para cada dispositivo; (2) uma chave de autenticação de 128 bits; (3) uma chave de criptografia, que varia de 8 a

[4]Bluetooth 5 quadruples range, doubles speed, increases data broadcasting capacity by 800 - `https://www.bluetooth.com/news/pressreleases/2016/06/16/-bluetooth5-quadruples-rangedoubles-speedincreases-data-broadcasting-capacity-by-800` - Acesso em 20/06/2016

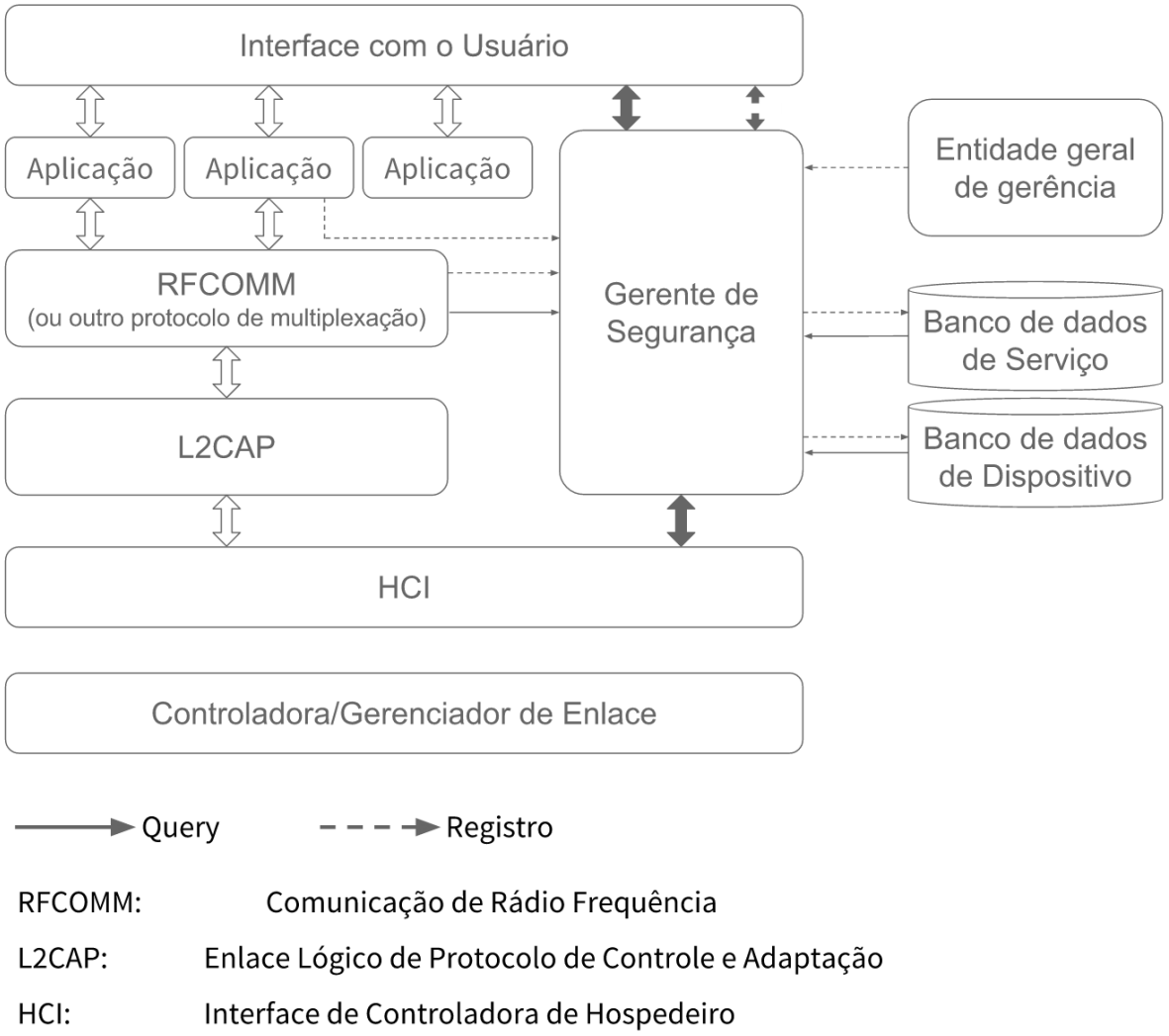

Figura 4.2: Arquitetura de Segurança no Bluetooth [130].

128 bits e (4) um número randômico RAND de 128 bits. Quatro modos de segurança são utilizados: (1) Não-Seguro: não implementa nenhum mecanismo de segurança; (2) Modo de Segurança Executado no Nível-de-Serviço: dois dispositivos podem se conectar sem segurança no Link Assíncrono para Conexões (ACL), e a segurança é feita apenas na camada de serviço pelo L2CAP; (3) Modo de Segurança Executado no Nível-de-Enlace: a segurança ocorre diretamente no ACL (nível de enlace) entre dispositivos e (4) Modo de Segurança Executado no Nível-de-serviço SSP: funciona como o (2), porém somente aceita dispositivos que utilizem Secure Simple Pairing (SSP). Os mecanismos de segurança do Bluetooth devem ser configurados pelo usuário e muitas falhas ocorrem por má configuração[72].

Existem três modos de descoberta para um dispositivo: (1) Silencioso: o dispositivo apenas observa o tráfego, mas não aceita nenhuma conexão, (2) Privado: o dispositivo

não pode ser encontrado e só se conecta se o endereço(BD_ADDR) for conhecido pelo mestre e (3) Público: pode ser descoberto e está aberto para conexão[72].

Três passos são fundamentais para o procedimento de segurança executado no Bluetooth: (1) Autenticação: trata da identificação entre uma *piconet* e outra e é feita pela verificação das chaves de link. O endereço é criptografado por uma chave de link com um número randômico para produzir um SRES (Signed Response Authentication Result), que é enviado e estabelece a conexão, caso as chaves sejam iguais; (2) Autorização: garante ou nega o acesso a um recurso e (3) Criptografia Opcional: Utiliza da chave criptográfica armazenada[72].

O protocolo apresenta algumas vulnerabilidades. Minar e Tarique[72] categorizam as ameaças de segurança no Bluetooth da seguinte maneira:

- Ameaça de Revelação Indevida: quando a informação passa por um ouvinte não autorizado a acessá-la.
- Ameaça à Integridade: A informação é alterada antes de chegar ao destino.
- Negação de Serviço: O usuário é impedido de acessar um serviço que almejava.

Os autores trazem ainda dezesseis ataques reportados para o Bluetooth:

– Ataque por MAC Spoofing: ocorre quando um atacante especializado consegue interceptar a comunicação no momento da geração de chave de link;

– Ataque de PIN Cracking: com um *sniffer* de frequência, um atacante colhendo as informações corretas, com os equipamentos certos e tempo suficiente, pode descobrir o PIN de maneira relativamente simples;

– Ataque de Man-In-The-Middle: elvolve modificar as informações sendo trocadas em uma *piconet*, pelo replicamento das mensagens, sem necessariamente conhecer as chaves, enganando as partes, que pensam estar se comunicando entre si quando, na verdade, se comunicam com o atacante;

– Ataque BlueJacking: envolve o envio de mensagens que não foram solicitadas;

– Ataque BlueSnarfing: quando um atacante *hackeia* um celular com Bluetooth para obter dados, como a agenda de contatos;

– Ataque BlueBugging: ocorre quando um atacante invade um dispositivo sem que o dono saiba, para furtar informações e, caso o dispositivo seja um telefone que forneça tradução de endereços do GSM (Global System for Mobile), consegue realizar ações como fazer ligações, enviar mensagens e alterar contatos;

- Ataque BluePrinting: quando o endereço BD_ADDR é conhecido, o atacante pode descobrir informações de fabricante, modelo e versão de firmware;
- Ataque por Blueover: é derivado do Bluetooth e utilizado em Java para testar vulnerabilidades, em que ataques nessa plataforma são explorados quando o dispositivo está vulnerável ao ataque BlueBugging;
- Ataque de Recuperação Off-line do PIN: ao se obter as variáveis randômicas utilizadas para se estabelecer o SRES, é possível calcular qual será o PIN provável;
- Ataque de Força Bruta: utiliza força bruta para descobrir os últimos 3 bits do endereço BD_ADDR, visto que os 3 primeiros são públicos;
- Ataque de Reflexão: para o Bluetooth, é como um ataque de Man-In-The-Middle para autenticação.
- Ataque de Backdoor: ocorre quando há a relação de confiança pelo pareamento, porém não aparece no dispositivo como pareado, dando acesso total ao dispositivo e também a outros serviços como modems, Internet, WAP e gateways GPRS;
- Ataques de Negação de Serviço: podem interferir na *piconet* inteira ou em um único canal de um dispositivo. Exemplos envolvem um dispositivo com bug que duplica o endereço BD_ADDR em cada requisição; estabelecer uma conexão de voz de mão dupla para sobrecarregar a rede; enviar NAK (Acknowledgments Negativos) para cada requisição; requisitar a maior taxa de dados possível ou menor latência em um dispositivo e também ataques que esgotam a bateria;
- Cabir Worm: utiliza do bluetooth para encontrar novos dispositivos e se espalhar;
- Skull Worm: funciona como o Cabir Worm e desativa os mecanismos antivírus e anti-worm;
- Lasco Worm: funciona como o Cabir e Skull, porém consegue se infiltrar em outros arquivos de sistema de telefones Symbian.

Para o caso do Bluetooth LE, em que beacons são enviados no modo broadcast, para sensorear a proximidade, Hassidim et. al. [39] sugerem que estes sejam enviados com um identificador efêmero criptografado, ao invés do identificador estático, para se prevenir ataques de reflexão, evitar que o ID obtido permita um rastreamento indesejado e que a informação sendo propagada seja forjada.

4.3.3 IEEE 802.15.4

O grupo de trabalho IEEE 802.15 TG4, busca "investigar uma solução de baixa taxa de dados, com tempo de vida de bateria de vários anos, ou meses, e de baixa complexidade."[47] O protocolo IEEE 802.15.4 define quais são as condições necessárias para a comunicação entre dispositivos com baixo consumo energético e de pouco alcance, as Low-power Wireless Personal Area Network (loWPAN). Esse protocolo trabalha tanto na camada física (PHY) quanto na camada de acesso aos meios (MAC).

A versão inicial IEEE 802.15.4-2003 utilizava do Direct Sequence Spread Spectrum (DSSS) para espalhamento dos dados nas frequências e uma taxa de transmissão entre 20 e 40kbits. Foi atualizado, no IEEE 802.15.14-2006, para suportar taxas de dados maiores e adicionar o espalhamento por Parallel Sequence Spread Spectrum (PSSS). E, na sua versão IEEE 802.15.4a-2007, adiciona Direct Sequence Ultra-wideband (UWB) e Chirp Spread Spectrum (CSS) à versão de 2006. O IEEE 802.15.4e inclui o Timeslotted Channel Hopping (TSCH), adicionado em 2012[49]. O TSCH é definido como o "[...] padrão emergente para automação industrial e controle de processo LLNs, com uma herança direta do WirelessHART e ISA100.11a"[49], que serão visitados mais a frente.

A camada física do protocolo administra o transceptor de Frequência de Rádio (FR) em cada dispositivo, assim como seleção de canais e administração de energia e sinal[35]. A camada de acesso ao meio administra operações como acesso ao canal físico, *beaconing* de redes[5], validação de frames, garantia de *time-slots*, associação de nós e segurança[35]. Para isso existem frames do tipo: beacon; comando; dados e *acknowledgement*. Dentro do protocolo, os dispositivos são divididos de acordo com suas capacidades e funcionalidades dentro da rede e podem ser dispositivos com funcionamento integral, do inglês Full-Function Device (FFD), que coordenam a rede, ou dispositivos com funcionamento reduzido, do inglês Reduced-Function Device (RFD), que apenas se comunicam entre si, podendo formar topologias de estrela, *peer-to-peer* e *cluster*. Utiliza-se a tecnologia CSMA/CA para evitar colisões na transmissão[35].

Uma das características importantes desse modelo é a utilização de um endereço conhecido por Endereço IEEE extendido de 64 bits, único globalmente (EUI-64)[48]. Em um frame, pode ser transmitido o endereço completo, global, ou o endereço curto, que remete a nós dentro da PAN, de modo a diminuir o overhead. Podem ser utilizados, também, superframes, que contém espaços de tempo garantidos para cada dispositivo, do inglês Guaranteed Time-Slots (GTS), dividindo o canal, o que permite que dispositivos possam ser desligados em certos momentos do superframe[95].

Além de prover uma lista de controle de acesso, do inglês Access Control List (ACL), o protocolo define vários modos de segurança, como visto na Tabela 4.1[35]. A segurança

[5]Beacons : informações utilizadas na administração do estado da rede

nesse protocolo é opcional e configurável, dadas as diversas circunstâncias em que esse pode ser empregado. O protocolo segue os padrões AES para definir a criptografia e autenticidade dos dados. O modo Counter (AES-CTR) provê confidencialidade com chaves de 128 bits; os modos AES-CBC-MAC provêm um código, que pode ser de 32, 64 ou 128 bits, para verificar a autenticidade e integridade dos dados, a partir do cabeçalho e do payload (não-criptografado)[35]. Para prover tanto confidencialidade como integridade e autenticidade dos dados, combinam-se o AES-CTR com o CBC (CCM).

Segundo Granjal et. al[35]., o protocolo previne ataques de replay e mantém a segurança semântica com identificadores no cabeçalho, criptografando unicamente cada bloco transmitido. O protocolo possui funcionalidades de controle de acesso, em que cada chip de rádio contém uma Access Control List (ACL) de no máximo 255 entradas. Também está presente sincronização de tempo na rede, em que os contadores de frame geram um Absolute Slot Number (ASN) contendo o número de *time-slots* passados desde o início da rede, que permite que novos dispositivos possam sincronizar.

O autor elicita, ainda, algumas limitações dos mecanismos de segurança empregados no protocolo IEEE 802.15.4. Primeiramente, não há um modelo de chaves, pois assume-se que esse é específico da ameaça na aplicação e das limitações dos dispositivos em prover operações de gerência de chaves. Também, a gerência de VI pelo ACL é conturbada, ao se utilizar a mesma chave em mais de uma entrada na tabela, permitindo que o remetente da mensagem reuse o *nonce*, o que possibilitaria que um atacante recupere a mensagem a partir do texto cifrado. A tabela ACL também não permite modelos de chaves por grupo (group keing) ou compartilhada na rede (network-shared keying), pois cada entrada na tabela deve estar associada a um único endereço. O modelo, como está definido, não permite a proteção de mensagens de *acknowledgment* em relação à integridade ou confidencialidade, o que permite que essas mensagens sejam forjadas para gerar ataques de negação de serviço.

Assim como no WiFi, o IEEE 802.15.4 também está vulnerável a ataques de jamming em seu meio físico e MAC. Os ataques mencionados por Amin et. al[5]. no caso do WiFi para vulnerabilidades do CSMA/CA também se aplicam ao IEEE 802.15.4. Ainda no mesmo trabalho, os autores elicitam alguns ataques que são característicos por irem contra os modos de segurança do IEEE 802.15.4, são eles: (1) Same-nonce attack; (2) Replay-protection attack e (3) Steganography attack. Em (1), como mencionado por Granjal no parágrafo anterior, ao se ter duas entradas em uma lista de controle de acesso, do inglês Access Control List (ACL), com a mesma chave e o mesmo nonce, um *eavesdropper* pode calcular as mensagens a partir dos textos cifrados, dado que, de acordo com o explicado em [103, p. 2], "se c1 = [dado1 XOR Echave(nonce)] e c2 = [dado2 XOR Ekey(nonce)], o atacante pode obter [dado1 XOR dado2] ao computar [c1 XOR c2]". Em (2), o atacante

Tabela 4.1: Modos de segurança do protocolo IEEE 802.15.4 na camada MAC (Fonte: [35]).

Modo de Segurança	**Segurança Provida**
Sem Segurança	Dados não são criptografados Autenticidade não é verificada
AES-CBC-MAC-32	Dados não são criptografados Autenticidade verificada utilizando 32-bit MIC
AES-CBC-MAC-64	Dados não são criptografados Autenticidade verificada utilizando 64-bit MIC
AES-CBC-MAC-128	Dados não são criptografados Autenticidade verificada utilizando 128-bit MIC
AES-CTR	Dados são criptografados Autenticidade não é verificada
AES-CCM-32	Dados são criptografados Autenticidade verificada utilizando 32-bit MIC
AES-CCM-64	Dados são criptografados Autenticidade verificada utilizando 64-bit MIC
AES-CCM-128	Dados são criptografados Autenticidade verificada utilizando 128-bit MIC

se aproveita do mecanismo de proteção de replay, que verifica um contador e descarta pacotes que cheguem com valores menores. O atacante então envia vários pacotes com valores altos de contador, de modo que os pacotes do nó legitimo com valores de contador menor serão rejeitados. Finalmente, em (3), é criado um canal oculto entre dois atacantes de modo que os mesmos possam se comunicar e prevenir de serem identificados como maliciosos.

Em casos de mensagens não criptografadas, um atacante pode verificar o número de sequência do frame, enviar um ACK para quem enviou a mensagem e impedir que o destinatário a receba, por jamming, por exemplo. Este é conhecido como ataque ACK, que pode ser estendido para um ataque de Man-in-the-middle quando o atacante modifica a mensagem para o destinatário, recebendo um ACK genuíno do mesmo[103]. Outros ataques mencionados[103][5] são o PANid conflict attack e Guaranteed Time Slot (GTS) attack. No primeiro, é inserido um conflito com o identificador do coordenador da PAN, o PANid. Com isso, o coordenador PAN deve tratar o conflito, o que gera atrasos caso os conflitos sejam constantes. O outro ataque utiliza da informação de GTS do superframe para fazer um DoS direcionado por colisão.

Alguns protocolos foram desenvolvidos em cima do IEEE 802.15.4 e possuem características próprias de implementação. São desenvolvidos para camadas acima das camadas física e de acesso ao meio: ZigBee, WirelessHART e ISA100.11, que serão descritos em seções à frente.

4.3.4 RFID e NFC

Considerado como base fundamental para a definição do que é a Internet das Coisas, o RFID se apresenta como uma solução para o endereçamento único de dispositivos. Funciona pela emissão de ondas eletromagnéticas por leitores que, por sua vez, ativam as etiquetas, que contém informações elétricas armazenadas e as transmitem por uma antena. Tais etiquetas podem ser passivas, ou seja, só são ativadas no momento em que recebem o estímulo da onda eletromagnética, ou ativas, em que se encontram ligadas a uma fonte de energia, possuindo, por conseguinte, um alcance maior.

Em sua análise dos principais aspectos de segurança dos protocolos de baixo custo utilizados para o RFID, Zavvari e Patel[126], definem os objetivos de segurança para RFID:

- **Confidencialidade**: Requer que as etiquetas transmitam os dados debaixo de autenticação e criptografia, de modo a autenticar o leitor que faz a requisição por dados antes de transmitir a informação, ou transmiti-la com criptografia para que apenas agentes autorizados tenham acesso.
- **Integridade**: Caso a memória da etiqueta RFID puder ser reescrita, é possível forjar a informação sendo transmitida.
- **Disponibilidade**: Se refere ao nível de escalabilidade do sistema assim como a performance, em que ataques de negação de serviço são a maior ameaça.
- **Autenticidade**: assume que a identificação única, gravada na etiqueta, nunca será alterada.
- **Privacidade**: não permitir que, por ataques, adulteração ou acesso físico, informações do passado sejam descobertas nem que informações do tipo de item que a etiqueta está anexada sejam reveladas.

O autor provê ainda uma lista dos principais e mais comuns ataques aos protocolos RFID:

  - Eavesdropping: ocorre quando um espião consegue ter acesso à informação transmitida entre uma etiqueta e um leitor.
  - Ataques de Replay: são proporcionados por atacantes que tem acesso a um dado transmitido e repassam o dado com *spoofing* da identificação da etiqueta e também para ataques Man-in-the-middle.

– Ataques de De-sincronização: um tipo de ataque de negação de serviço em que a informação relativa a uma etiqueta armazenada em um servidor é confundida com a informação que está armazenada na etiqueta, inviabilizando a comunicação.

– Ataques de Personificação: um atacante faz uso da identificação da etiqueta para se autenticar em um servidor.

– Ataques Man-In-The-Middle: um atacante entre um servidor e uma etiqueta recebe os dados da comunicação sendo realizada, de modo que os participantes acreditem estar comunicando entre si.

– Ataques de Negação de Serviço: é adicionado ruído de modo a interromper a operação normal do RFID.

Um estudo mais detalhado das vulnerabilidades do RFID, trazido por Mitrokotsa et. al[73]., classifica os ataques de acordo com as camadas em que atuam. Adicionam-se aos ataques mencionados acima ataques como jamming; exploração de comandos KILL; envolver a tag com uma gaiola de Faraday; clonagem e spoofing das tags e ataques na camada de aplicação, como injeção de código.

O Near Field Communication (NFC) é um conjunto de protocolos para a comunicação, através do campo eletromagnético de transmissão de rádio, de dispositivos fisicamente próximos, inclui o RFID, porém é definido apenas para objetos com aproximadamente 10 cm de distância e não possui restrições quanto à direcionalidade da comunicação, em que uma etiqueta pode se comportar como um leitor e o leitor como etiqueta, possibilitando uma comunicação Peer-to-Peer[111]. Sua principal utilização tem sido para pagamentos sem cartão. Definido pelo padrão ISO-14443, o protocolo NFC possui três fases principais: (1) Evitar Colisão de FR: o Leitor só ativa sua FR quando nenhuma outra FR tiver sido detectada; (2) Detecção de Dispositivo: o Leitor sonda alvos próximos e recebe uma resposta em determinado time-slot e (3) Protocolo de Transporte: após ter encontrado um alvo, o Leitor inicia a transmissão utilizando do protocolo de transporte, o qual especifica parâmetros como o *timeout* esperado[3].

Por ser definido para distâncias curtas ($\tilde{1}$0cm), muitas vezes assume-se que o NFC é intrinsecamente protegido, dada a dificuldade de acesso para se alterar ou espionar os dados em tão curta distância. Essa afirmação é questionada porém, em [3], levantando-se a questão de que um adversário pode fornecer um canal rápido e transparente que permita uma retransmissão dos dados para distâncias maiores. O estudo, à vista disso, segue com uma análise formal de segurança para o NFC em relação a ataques de replay. Técnicas de mitigação envolvem restringir a distância com limitações de tempo pela análise do tempo de *roundtrip*, entretanto, é argumentado que tais técnicas, por hardware,

podem ser custosas de se implementar na prática e, por software, sofrem por problemas de confiabilidade e eficiência. Em seu trabalho, Gurulian et. al[38]. analisaram diversos sensores que utilizam análise de variáveis em sensores de ambientes[6] para mitigar ataques de replay e avaliaram que, ainda assim, a maioria dos dispositivos NFC não estão seguros quanto a ataques de retransmissão.

Um estudo liderado pela Infosec[50], lista ainda outras vulnerabilidades presentes na tecnologia NFC:

- Eavesdropping: sugere o autor, pode ser realizada mesmo para distâncias próximas. Wenxing et. al. [121] trazem um modelo que reduz em até 20% a probabilidade de espionagem dos dados, ao misturá-los
- Modificação dos dados: ocorre quando um dado transmitido é interceptado e modificado antes de chegar ao seu destino. Apesar de ser difícil é possível realizar um ataque no modo ativo de transmissão.
- Jamming: funciona como um ataque de DoS, ao se transmitir sinais de rádio que impõem ruído ao sinal transmitido.
- Spoofing: ocorre quando um atacante finge ser um tag genuíno para motivar o usuário a realizar a interação com a tag.
- Fuzzing na pilha de protocolos NFC: a partir da análise das fragilidades do protocolo que utiliza o NFC, um atacante pode realizar operações indesejadas no dispositivo de uma vítima.

Em um curto vídeo no youtube do canal de tecnologia playtechNZ[7], o autor demonstra na prática uma falha de segurança do NFC, por má configuração. Ao colocar o celular sobre a mesa, em um estabelecimento de fastfood, ele percebeu que, embutido nesta, estavam instaladas etiquetas NFC. Tais etiquetas podem ser configuradas para, ao serem ativadas, emitir um sinal que irá disponibilizar determinado conteúdo em um celular, que fora provavelmente pensado para ações publicitárias da marca. Foi constatado, porém, que as etiquetas poderiam ser reconfiguradas. Desta forma, qualquer pessoa poderia configurá-la para mostrar um conteúdo inadequado no celular dos clientes, vulnerabilidade tal que pode acarretar enormes prejuízos para a imagem da empresa.

[6]Segundo o autor, sensores de ambiente são sensores que medem informações como som, luz, ondas de rádio, para definir atributos únicos de determinado ambiente. Essa informação é utilizada para verificar a distância entre objetos, visando verficar que estão próximos.

[7]McDonalds NFC Tag Security Fail! - `https://www.youtube.com/watch?v=We2P1nDjpZg` - Acesso em 21/06/2016

4.4 Camada de Redes

A camada de redes é responsável pelo roteamento entre pacotes na rede. São definidas informações de endereçamento, qualidade de serviço, do inglês Quality of Service (QoS) e quantidades relativas ao uso da rede (para futuras cobranças ou análises).

4.4.1 IP - IPv4, IPv6, IPSec, 6loWPAN e 6TiSCH

Um dos principais protocolos que trouxeram à internet o crescimento que esta alcançou é o Internet Protocol (IP). Sua principal função é direcionar datagramas pela rede, fornecendo endereços conhecidos como endereços IP. O protocolo, que está na camada de rede segundo o modelo OSI, encapsula, ao pacote sendo enviado, informações relativas à versão, endereço IP do remetente e destinatário e informações de controle. O protocolo IP possui um modelo de melhor esforço para a entrega, ou seja, não garante necessariamente que os pacotes serão entregues, nem se os mesmos chegarão na ordem, o que pode ser verificado posteriormente por protocolos em camadas superiores, como o TCP.

A versão que foi utilizada no início da internet e segue amplamente utilizada é a IPv4, cujos endereços são formados por 32 bits, o que permite um total de 2^{32} ou 4'294'967'296 possíveis endereços. Como previsto pela Address Lifetime Expectations (ALE) Working Group[54] , era esperado que esse número um dia se esgotaria e é o que vem acontecendo entre os vários Regional Internet Registries (RIR), que são responsáveis pela administração regional de endereços IP para os diversos usuários: os endereços já se esgotaram, ou estão próximos de se esgotar. [8] [9] [10] [11] [12]

Tendo em vista o problema com o número de endereços e buscando desenvolver uma versão mais leve do protocolo IP, em 1998, foi apresentado o IPv6. Nessa versão, a principal mudança está no tamanho do endereço, que deixa de ser 32 e passa para 128 bits, o que permite 2^{138}, ou 340'282'366'920'938'463'463'374'607'431'768'211'456, possíveis endereços. Com tantos disponíveis, cada dispositivo conectado à internet pode ter seu próprio endereço.

O cabeçalho do IPv6 é mais simples que o do IPv4, com apenas 40 bytes, sendo 32 apenas de endereços de origem e destino, informações adicionais podem ser concatenadas

[8] ARIN finally runs out of IPv4 adresses - http://www.networkworld.com/article/2985340/ipv6/arin-finally-runs-out-of-ipv4-addresses.html - Acessado em 07/05/2016

[9] LACNIC Enters IPv4 Exhaustion Phase - http://www.lacnic.net/en/web/anuncios/2014-no-hay-mas-direcciones-ipv4-en-lac - Acessado em 07/05/2016

[10] AFRINIC IPv4 Exhaustion - http://www.afrinic.net/community/ipv4-exhaustion - Acessado em 07/05/2016

[11] APNIC IPv4 exhaustion details - https://www.apnic.net/community/ipv4-exhaustion/ipv4-exhaustion-details - Acessado em 07/05/2016

[12] RIPE NCC IPv4 Exhaustion - https://www.ripe.net/publications/ipv6-info-centre/about-ipv6/ipv4-exhaustion - Acessado em 07/05/2016

no final, o que facilita o processo de roteamento na rede, pois o tamanho de cabeçalho é sempre fixo. Caso o IPv6 receba um pacote grande demais para ser processado, envia um erro de volta à origem, ao invés de dividir o pacote, como é feito no IPv4, logo, informações como Identificação, Flags e Offset do fragmento não são necessárias. O ckecksum também foi eliminado por ser possível realizar a verificação em outras camadas do modelo OSI. Uma grande vantagem do modelo IPv6 é a possibilidade de se auto-configurar na rede com a utilização de seu endereço MAC, sem a necessidade de utilização do DHCP. O IPv6 apresenta também mecanismos de segurança como autenticação da origem, e criptografia do payload.

Um atacante pode utilizar técnicas para ataques de negação de serviço, dado que o protocolo de tráfego baseado em IP não possui uma identificação precisa da origem, por esse endereço poder ser facilmente manipulado. Podem ser utilizados ataques como IP spoofing, em que o endereço IP é forjado para poder realizar ataques; IP Hijacking, onde os valores tas tabelas de roteamento são alerados, e ataques Smurf, que enviam vários pacotes ICMP com o valor forjado de um IP, para que várias mensagens, de diferentes fontes, retornem a resposta para o nó, sobrecarregando-o. Em [101], foram revisados mais de 275 artigos que tratam do tema de rastreabilidade da origem real de endereços IPs para a mitigação de ataques DDoS. Os esquemas de rastreabilidade podem ser definidos de acordo com a forma em que são estruturados: teste de enlace; mensagem; marcação; logging; overlay; análise de padrão e híbrido.

Para tornar o IP mais seguro, o IETF definiu alguns protocolos de segurança, que formam o IPsec. Nesses protocolos, é acordado que toda comunicação na camada de rede deve ser autenticada e criptografada. O IPsec utiliza dois protocolos para prover segurança no tráfego de rede: IP Authentication Header (AH), responsável pela "integridade e autenticação da origem dos dados, com mecanismos opcionais para evitar *replay*" e Encapsulating Security Payload (ESP), que fornece "os mesmos serviços mais confidencialidade"[59].

6loWPAN e 6TiSCH

Como não é possível se estabelecer uma integração direta entre o IPv6 e o IEEE 802.15.4 [54], o grupo IPv6 sobre redes sem-fio de baixa potência em PANs, do inglês IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN), busca mecanismos para o desenvolvimento de uma pilha de protocolos que forneça essa integração. Técnicas como compressão de cabeçalho, fragmentação e reestruturação de pacotes, descoberta de vizinhos e auto-configuração são utilizadas na adequação do protocolo IPv6 para as redes sem-fio de baixa potência em WPANs.

O payload máximo para os pacotes em camadas acima, que utilizam do IEEE 802.15.4, é de 102 bytes, caso não seja utilizado nenhum mecanismo de segurança na camada de enlace, o que não chega nem perto do MTU do IPv6, que é de 1280 bytes[35]. O 6loWPAN, então, define uma nova camada de adaptação entre a camada de rede e de enlace (6loWPAN Adaptation Layer), na qual é realizada: a fragmentação e reconstrução dos pacotes enviados, que não podem ser fragmentados pelo IPv6; a compressão do cabeçalho e o roteamento para a camada de enlace[53, p. 242].

Granjal[35] ressalta que não são implementados mecanismos de segurança específicos para o 6loWPAN, dado que este conta com a segurança a nível de enlace provida pelo IEEE 802.15.4. O fato de não estar autenticado, permite que atacantes explorem vulnerabilidades no processo de fragmentação, em que deve ser mantido um buffer para a remontagem dos pacotes. Também, como os dados não são criptografados, Pongle e Chavan[88] afirmam que o 6lowPAN está vulnerável a ataques de eavesdropping, man-in-the-middle e spoofing.

Um estudo trazido por Vohra e Srivastava[115] elicita trabalhos de pesquisa de vulnerabilidades no 6loWPAN e técnicas para a segurança no mesmo. Entre as medidas elicitadas tem-se: a proteção de confidencialidade, integridade e autenticação, pela utilização de compressão do protocolo IPSEC, o que geraria uma segurança fim-a-fim, em contradição à segurança hop-a-hop do IEEE 802.15.4; proteção de chaves compartilhadas; proteção contra ataques de retransmissão e ataques de reserva de buffer na fragmentação; proteção contra ataques de botnet; proteção contra ataques internos de negação de serviço e proteção da privacidade, ao se rotacionar os endereços de IPv6, em uma técnica conhecida por Moving Target IPv6 Defense (MT6D), que dificulta um atacante de realizar ataques DoS e Man-in-the-Middle, porém não se mostrou, até o momento, adequada para redes de baixo custo energético e de processamento.

Ainda para a integração, o grupo 6TiSCH busca a integrar o IPv6 com a versão IEEE 802.15.4e. Nele, é realizada a divisão de tempo TDMA, em que uma faixa de banda é definida para a comunicação entre nós vizinhos[49].

4.4.2 RPL

A IETF define para redes que apresentam baixa potência e perdas na transmissão o termo Low-Power and Lossy Network (LLN), em que tanto routers como outros nós na rede possuem limitações, apresentando “altas taxas de perda, baixa taxa de transferência de dados e instabilidade”[123]. Para integrar o IPv6 em LLNs, foi elaborado um protocolo de roteamento conhecido por RPL[123].

O roteamento RPL trabalha com vetor de distância que especifica como construir um Grafo Acíclico Dirigido Orientado ao Destino[13], do inglês Destination Oriented Directed Acyclic Graph (DODAG), utilizando uma Função Objetiva, do inglês Objective Function (OF), e uma série de métricas/restrições para encontrar o melhor caminho. Algumas regras são criadas para a definição desse caminho pela OF, como, por exemplo, uma função que escolha não passar por nós que sejam sustentados por bateria. O grafo gerado, como mostra a figura Figura 4.3[113], representa critérios específicos para uma topologia de rede, criada em cima de uma camada física, podendo o administrador da rede escolher ter mais de uma topologia (grafo), a depender da implementação[113].

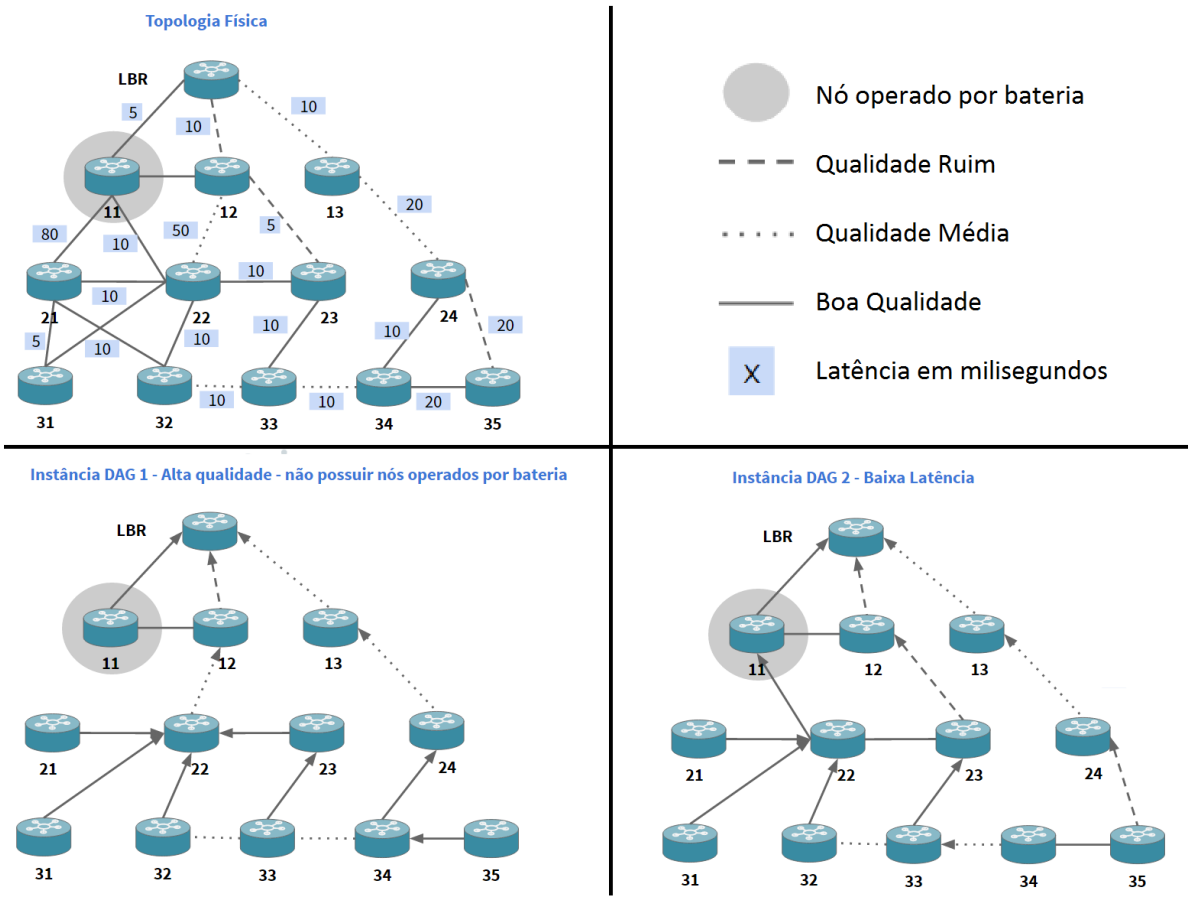

Figura 4.3: Conceito de Múltiplos DODAG's [113].

Quando um nó entra na rede, este aguarda por uma mensagem do tipo DODAG Information Object (DIO), com a qual ele se baseia para aplicar a OF e obter o nó parente

[13]Um grafo é um conjunto de vértices e arestas, com diversas características. Quando dito que é dirigido, entende-se que as arestas possuem uma direção definida. Acíclico significa que os caminhos não formam ciclos. Orientado ao Destino significa que, para cado nó no grafo, existe um caminho até o destino

mais adequado. O nó passa a enviar periodicamente mensagens DIO. Caso não receba nenhum DIO, o nó faz uma solicitação broadcast por uma mensagem do tipo DODAG Information Solicitation (DIS). Após ter sido gerado o grafo, a comunicação entre os nós pode ser ponto-a-multiponto, multiponto-a-ponto ou ponto-a-ponto. Cada rede possui um nó raíz, ou sink, e cada nó pode ou não armazenar informações de roteamento de outros nós. As informações são ditas como indo para cima, quando vão em direção ao nó raiz e para baixo quando vão em direção aos nós-folha. Ao ir para cima, o ranqueamento do próximo nó deve ser sempre menor do que o anterior e, quando vai para baixo, o ranqueamento do próximo nó deve ser maior[53].

A segurança é opcional no RPL. "A especificação atual define o uso de AES/CCM com chaves de 128 bits para a geração de MAC que suporta a integridade dos dados e RSA com SHA-256 para assinaturas digitais, que suportam integridade e autenticidade"[35, p. 1302]. O protocolo define três modos básicos de segurança: (1) Inseguro, em que as mensagens de controle não possuem segurança aplicada (2) Pré Instalada, utilizada por um dispositivo com uma chave simétrica para entrar em uma instância RPL[14] existente, e (3) Autenticada, onde o nó pode inicializar com uma chave e em seguida obter uma nova de uma *key authority* e passar a funcionar como um roteador, caso autorizado. Fora esses modos e a segurança nas mensagens de controle, nenhum outro mecanismo de segurança é implementado no RPL[35].

Muitas ameaças são comuns aos protocolos de roteamento. Pongle e Chavan [88] trazem uma pesquisa com onze ameaças presentes no RPL, que também são citadas no trabalho de Medjek et. al[70]. e são mencionadas abaixo:

- Selective Forwarding: podem ser realizados no RPL ao se transmitir apenas pacotes de controle e sumir com as mensagens de dados.

- Sinkhole: Um nó se coloca na rede como melhor opção para o roteamento, para, a partir daí, introduzir outros ataques, como o selective forwarding.

- Hello Flooding: um atacante envia mensagens de Hello, que para o RPL são os DIO, para vários outros nós, com valores altos de ranqueamento, de modo a ser escolhido como a opção para o roteamento. Desta forma, as mensagens serão perdidas quando enviadas para este nó.

- Wormhole: Dois atacantes conversam através de uma conexão por túnel, onde os pacotes da rede são retransmitidos. Pode ser explorado de diversas maneiras, tanto para ataques quanto para beneficiar a qualidade da rede. Uma aplicação de ataque

[14]Uma instância RPL pode ser entendida como um dos grafos gerados para representar a topologia da rede. Um nó só pode estar uma vez em um grafo, mas pode estar em vários grafos, por isso, entende-se um nó, em determinado grafo, como uma instância RPL.

possível é transmitir a informação entre um nó A e um nó B que estão distantes, através de um Wormhole com atacantes próximos a esses nós, de modo que o nó A acredite estar próximo do nó B, deixando-os vulneráveis. [43]

- Sybil e CloneID: Envolvem a cópia do identificador em um ou vários nós na rede para ganhar acesso ao tráfego para ou pela vítima. "O ataque pode ser minimizado ao se utilizar números de rastreamento para instâncias de cada identidade"[88, p. 2].

- Negação de Serviço: ataques que visam tornar os recursos indisponíveis ao usuário.

- Buraco-negro: Neste ataque, todos os pacotes que passam por determinado nó são descartados.

- Ranqueamento: envolve a mudança do ranqueamento e se apresenta de quatro formas: "formação de caminhos não otimizados; formação de loops não-detectados; mesmo ao existir em determinada topologia, não utilizar o caminho otimizado; decaimento da taxa da entrega de pacotes, com pequenas mudanças no atraso fim-a-fim quando o número de atacantes aumenta; [...] ao se atualizar informação de roteamento, os vizinhos terão de atualizar suas topologias, criando mais overheads de controle"[88, p. 3].

- Número de Versão: Ao se receber um número de versão mais alto de uma árvore DODAG, uma nova árvore será montada, o que pode ocasionar novas topologias não otimizadas e trazer inconsistências. Uma prevenção proposta envolve a utilização de assinatura digital e código MAC.

- Reparação Local: ocorre quando um atacante envia a nós vizinhos mensagens para a reparação local[15], desnecessariamente, sobrecarregando a rede.

- Vizinhos e DIS: Ocorre quando várias mensagens DIS são enviadas, aumentando o overhead na rede.

4.4.3 ZigBee

Controlado pela ZigBee Alliance[16], o ZigBee busca a interoperabilidade entre dispositivos, pela definição de protocolos de alto nível. Busca ser mais barato, simples e provê menor

[15] A reparação local é utilizada para reestruturar a rede quando nós saem. Dada as características de redes LLN's, isso pode ocorrer com frequência, logo, a reparação local não envolve reestruturar toda a topologia.

[16] ZigBee Alliance - `http://www.zigbee.org/` - Acesso em 18/05/2016

taxa de transmissão de dados do que tecnologias como WiFi e Bluetooth, como representado na Figura 4.4[58]. Adiciona ao IEEE 802.15.4 uma camada de rede que incorpora roteamento multi-hop, ad hoc, que se organiza automaticamente (AODV), uma camada de aplicação e mecanismos de segurança[58].

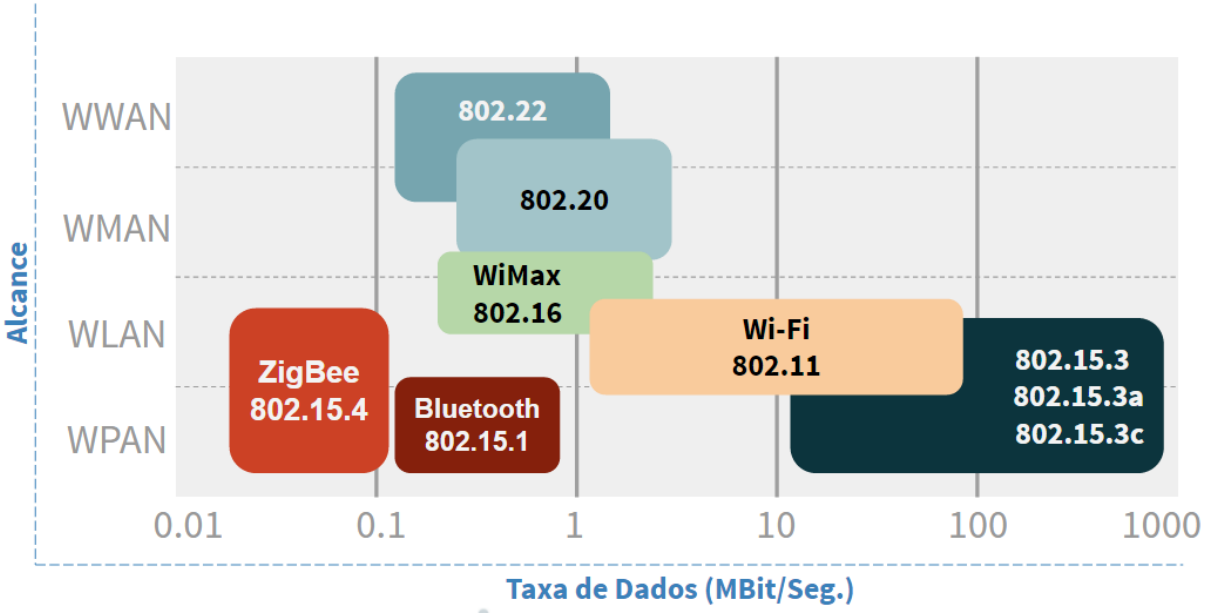

Figura 4.4: Comparação entre taxa de dados e alcance entre os protocolos [58].

O ZigBee opera segundo três tipos de dispositivos: (1) Coordenador ZigBee - inicia uma comunicação, guarda informações, administra a rede, com o envio de beacons, e faz a ponte entre várias redes e segurança, servindo como Trust Center (TC); (2) Roteador ZigBee - provê uma comunicação multi-hop entre os diversos dispositivos e (3) Dispositivos de Fim ZigBee - composto por sensores, atuadores e controladores, que coletam dados e se comunicam com outros componentes da rede[12]. O ZigBee pode ser configurado seguindo uma topologia de estrela, com um único coordenador ZigBee, peer-to-peer e mesh, as quais provêm múltiplos caminhos para que uma mensagem seja transmitida, pela utilização de roteadores ZigBee, com um coordenador responsável por formar e definir certos parâmetros fundamentais da rede. Uma rede ZigBee pode conter 255 nós, sendo um o mestre e os demais escravos. Ao se conectar diversos coordenadores, a rede pode chegar a até 65000 nós[66].

Como pode ser visto na Figura 4.5[82], o ZigBee possui diversos serviços nas camadas em que atua. O framework para a camada de aplicação é composto por uma subcamada de suporte à aplicação (APS), os objetos dos dispositivos ZigBee (ZDO) e os objetos de aplicação definidos pelos fabricantes. A camada de rede é formada por uma entidade de dados (NLDE-SAP), que provê serviços de comunicação dos dados e uma entidade de

gerência (NLME-SAP), que provê serviços de rede. São definidos também interfaces com a camada de acesso ao meio para dados (MLDE-SAP) e para gerência (MLME-SAP)[66].

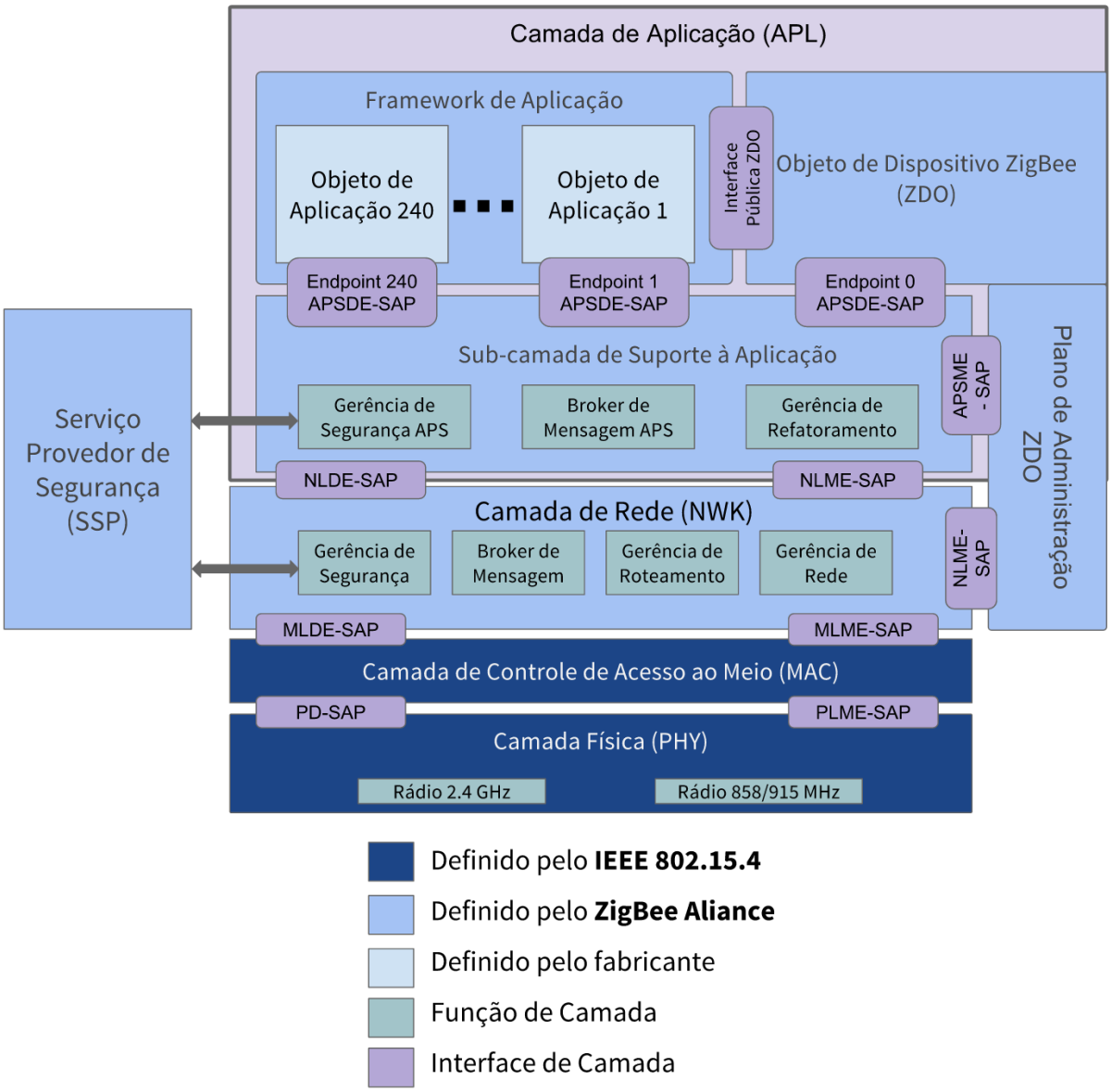

Figura 4.5: Pilha de Protocolo ZigBee [82].

A segurança no ZigBee, para as camadas de aplicação e de rede, inclui a utilização de listas de controle de acesso, temporizadores para a verificação de *freshness* de mensagens e criptografia baseada no AES com chave de 128 bits e, para camada MAC e PHY, utiliza os mecanismos de segurança já descritos no IEEE 802.15.4[58]. Quando um frame é transmitido utilizando determinado pacote de segurança, este utiliza do Security Service Provider (SSP) para processar este frame. O SSP verifica a origem/destino, obtém a chave associada e aplica o pacote associado àquele endereço. A segurança é processada

na camada de rede, porém é a camada de aplicação que a controla, definindo quais chaves e qual pacote para o CCM* deve ser utilizado em cada frame. Podem ser adicionados também um MIC para verificar integridade e contador de sequência para os frames de rede[61].

Thakur et. al[110]. trazem um mecanismo para proteger redes ZigBee de ataques do tipo Sybil. A solução proposta envolve o armazenamento no Trust Center (TC) de uma tabela com o IP de cada nó e a distância entre eles. Cada nó deve armazenar os valores de distância entre vizinhos. Desta forma, a identidade pode ser confirmada verificando-se o IP e a distância. Um ponto negativo é que exige um gasto maior de memória em cada nó. Coppolino et. al[26]. mostram como um ataque Sinkhole pode ser adaptado para o ZigBee. No ataque, um tablet Android é colocado na rede com um malware, que modifica os parâmetros de potência, se colocando como o nó que possui o melhor roteamento até a estação de base.

Muitos ataques ao ZigBee são relacionados à sua implementação, mais especificamente a como as chaves são trocadas no processo de comunicação. Zillner[129] afirma que os mecanismos de segurança do ZigBee são bons, porém, que "os fatores de compatibilidade contribuem para uma implementação frágil dos controles de segurança".[p. 3][129] O autor levanta que, em casos onde um dispositivo sem chaves pré configuradas entra na rede, as chaves para autenticar o dispositivo são transmitidas em aberto. Apesar do tempo de exploração ser curto, técnicas como jamming podem ser utilizadas para levar o usuário a iniciar um reset de fábrica ou outra forma de re-joining na rede, permitindo então que o atacante tenha acesso à chave transmitida, podendo causar danos na rede. Outro ponto abordado é o fato dos dispositivos que compõem uma rede ZigBee serem normalmente de baixo custo, os mesmos estão mais vulneráveis a uma invasão física, que revele as chaves por um acesso direto à memória. Os perfis de aplicação, do inglês application profiles, são um exemplo prático da vulnerabilidade das chaves a que o autor se refere. Tais perfis são utilizados na camada de suporte à aplicação do ZigBee, para facilitar a interoperabilidade entre as aplicações dos diversos fabricantes. O perfil público para automação residencial, do inglês Home Automation Public Application Profile (HAPAP), por exemplo, possui uma chave de TC padrão "ZigBeeAlliance09". Com isso, um atacante pode observar um dispositivo entrando na rede com esta chave e descobrir a chave de rede, comprometendo a confidencialidade da comunicação.

4.4.4 WirelessHART

Em 2007, a fundação High Addressable Remote Transducer (HART) Communication Foundation (HCF), lançou sua versão 7.0, com interface para dispositivos sem-fio, conhecida como WirellesHART, que, em 2010, foi padronizada no IEC 65291. Seu foco é em apli-

cações industriais e de automação que necessitam de garantias de tempo-real, utilizando uma arquitetura mesh sincronizada no tempo, com organização e cura automática[53].

O protocolo é composto por dispositivos de campo sem-fio e com fio, estações de base, adaptadores sem-fio, aparelhos portáteis sem-fio, gateways, administradores de rede e de segurança, que se comunicam para formar a rede, como mostra a Figura 4.6[24]. Faz o uso da camada física do IEEE 802.15.4 e implementa sua própria camada MAC sincronizada no tempo. A camada de aplicação é baseada nos comandos já estabelecidos em HART. Os dispositivos de campo podem ser organizados em uma topologia de estrela ou mesh[104].

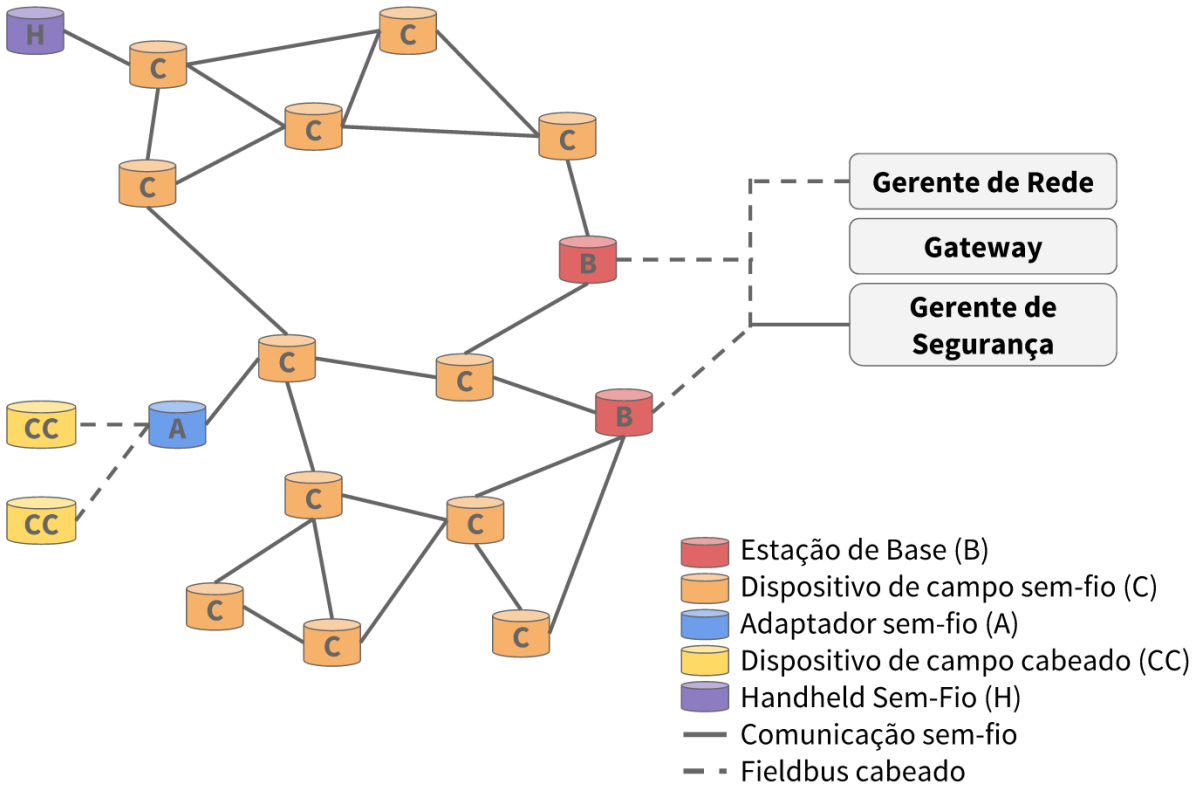

Figura 4.6: Elementos de Rede WirelessHART [24].

Os administradores de rede são os responsáveis por "manter caminhos atualizados e agendar a comunicação dentro da rede, garantindo sua performance"[p. 377][104]. O roteamento é feito por Grafo, em que o administrador da rede calcula o grafo e passa os caminhos para cada dispositivo na rede, que os mantém armazenados. Também pode-se utilizar do Roteamento de Origem, do ingês Source Routing, para diagnóstico da rede, onde o nó de origem passa uma lista de dispositivos que devem ser seguidos para o roteamento[104].

Os administradores de segurança no WirelessHART são responsáveis pela distribuição de chaves entre os dispositivos de campo. O protocolo utiliza de criptografia AES de 128

bits para confidencialidade, no modo CBC*, em que três chaves são utilizadas: (1) Chave de Sessão, que é utilizada para criptografia fim-a-fim na camada de rede, (2) Chave de Rede, para a criptografia de tráfego comum em cada hop e (3) Chave de Junção, utilizada para autenticar um novo nó que entra na rede. Todas as chaves devem ser administradas por um Gerente de Segurança. Cada rede WirelessHART possui um Gerente de Segurança associado, mas uma instância deste gerente pode ser associada a diferentes redes. O protocolo utiliza dos mecanismos definidos para o IEEE 802.15.4 na camada de enlace para a integridade dos dados. Através do *frequency hopping* e uma lista negra de canais, se protegem de interferências que ameaçam a disponibilidade de serviços[24].[68, p. 461] A especificação do WirelessHART define também que são guardadas listas ACL, no gateway, e que as chaves podem ser rotacionadas seguindo um modelo automático ou *on demand*[67].

Apesar dos mecanismos de segurança empregados, o protocolo está vulnerável a certos ataques. Um ataque de Sybil é descrito em [64, p. 225-239]. Neste ataque, ao se conhecer a chave de rede, o atacante envia requisição de desligamento para os nós vizinhos de um nó legítimo. Ao receber tais requisições, esses vizinhos retiram o nó de sua lista de roteamento e, também, enviam para o nó gerente informações para que este reconfigure suas rotas sem a presença do nó. Outros ataques, abordados em [68, p. 461] são: jamming; de-sincronização, em que um atacante prejudica a rede colocando informações de temporização falsas; Wormhole, em que o tráfego é redirecionado através de um túnel com um enlace mais forte e Redirecionamento Seletivo (do inglês Selective Forwarding), em que um nó comprometido escolhe quais pacotes deixa passar e quais serão perdidos, sendo difícil de se identificar, ou simplesmente perde todos os pacotes recebidos, formando um buraco negro, o qual é mais fácil de ser identificado. Raza et. al[90]. mostram que, pela limitação de tempo de 10ms. que o WirelessHART fornece, é inviável que os nós coloquem criptografia nos cabeçalhos para a camada de enlace e de rede, o que torna o processo de análise de tráfego mais fácil para um atacante.

Assim como no ZigBee, um dos grandes problemas do WirelessHART está em sua implementação[17]. Alcaraz e Lopez[2], mostram que o WirelessHART também apresenta ameaças de implementação em que um atacante, ao ter acesso físico a um dispositivo e, consequentemente, à chave pública, conseguiria enganar um nó e obter a chave de rede para observar o tráfego de forma clara. Os autores relatam, também, que, caso as políticas não especifiquem uma atualização frequente das chaves de rede e sessão, essas podem ser quebradas por criptanálise, possibilitando o ataque Sybil. Os autores dizem ainda que um atacante pode emitir informações falsas para o gerente da rede, sobre potencial energético

[17]The Register: WirelessHART industrial control kit is riddled with security holes - `http://www.theregister.co.uk/2016/02/01/wirelesshart_ics_vuln/` - Acesso em 15/06/2016

e outros fatores, que influenciam o processo de geração do grafo de roteamento, permitindo ataques de Sinkhole.

4.4.5 ISA 100.11

Assim como o WirelessHART, o grupo Internet Society of Automation (ISA) desenvolveu um padrão de comunicação voltado para aplicação industrial, conhecido por ISA100.11. Nele, todas camadas do modelo OSI são tratadas.

Os componentes que compõem o padrão são: gateways, administrador de sistema, administrador de segurança, roteador, roteador de backbone, dispositivo de entrada e saída e dispositivos móveis[4]. Diferentemente do WirelessHART, os dispositivos de entrada e saída são separados dos roteadores, podendo ser definida a distinção entre nós-fim e nós de roteamento. A rede pode ser organizada segundo uma topologia estrela, mesh, ou estrela-mesh. O ISA100.11 possui integração com o 6LoWPAN tanto na camada de rede quanto de transporte, com extensão do UDP para o IPv6, incluindo as compressões necessárias. Com isso, cada nó na rede pode conectar-se diretamente à internet. O roteamento, assim como no WirelessHART, pode ser tanto por grafo quanto por origem[65].[118]

Os mecanismos de segurança no ISA 100.11 utilizam de criptografia AES de 128 bits para a confidencialidade com encadeamento de modo CCM. Quando um dispositivo entra na rede, este recebe uma chave mestra, utilizada para a comunicação entre o dispositivo de campo e o gerente de segurança, uma chave DL, utilizada na comunicação com a camada de enlace de dados (DLL) para computar o MIC, e uma chave de sessão opcional para autenticação e/ou autorização[87]. O gerente de segurança define qual dos três modos de segurança serão utilizados: (1) Redes não seguras; (2) Redes seguras por chave simétrica e (3) Redes seguras por chaves assimétricas[2]. Utiliza também dos mecanismos de segurança do IEEE 802.15.4. Os dispositivos na rede sem fio ISA100.11 sincronizam entre si, na ordem de milissegundos para garantir *freshness* dos dados transmitidos, evitando ataques de repetição[62]. Assim como no WirelessHART, técnicas de saltos de frequência e blaklisting[18] de canais são utilizadas para prevenir contra ataques de interferência. A segurança fim-a-fim para ameaças internas é realizada na camada de transporte e é possível utilizar chaves assimétricas.

Alcaraz e Lopez[2] levantam o caso, assim como colocado para o ZigBee e WirelessHART, de que as chaves devem ser bem guardadas para se evitar ataques a partir da

[18]Para se evitar interferência, verificam-se quais canais de frequência estão sendo utilizados ou não. Essa análise pode ser feita verificando determinado *threshold* de energia, no qual, ao se verificar determinada quantidade de energia no canal, este é tido como ocupado, ou por sensoriamento de transportadora, que ao se identificar um padrão de modulação e espalhamento, como o IEEE 802.15.4, verifica que este está ocupado, ou por uma combinação dos dois. Ao se verificar um canal na lista negra, este não é colocado para ser utilizado nos saltos de frequência.

violação física dos dispositivos. Os autores relatam que o ISA 100.11a está protegido de ataques Sybil, por requisitar um processo de challenge-response para verificar que o gerente de segurança só se comunica com um nó específico e por atualizar as chaves periodicamente. Os autores seguem dizendo que o ISA 100.11a também está exposto a ataques de Wormhole e Sinkhole, por permitir que um grafo de roteamento possa ser construído maliciosamente por um atacante que injeta informações falsas e selective forward e blackhole, onde o atacante decide passar ou não a informação de roteamento. Uma possível solução proposta seria de colocar em cada nó, caminhos alternativos caso a mensagem não seja corretamente direcionada.

4.5 Camada de Transporte

A camada de transporte gerencia a transmissão de pacotes entre a origem e o destino, independente de detalhes da rede. Os protocolos mais comuns são o TCP e o UDP. O TCP garante que os pacotes chegarão ao destino final, reenviando em casos de falha e mantendo aberta a conexão. É mais utilizado quando a aplicação exige confiança de entrega, porém é mais custoso. Já o UDP envia os pacotes sem dar garantia de entrega, o que reduz a complexidade. Tendo em vista o ambiente de redes sem-fio com altas taxas de perda e necessidade de baixo consumo energético, a complexidade trazida pelo TCP pode ser custosa, o que torna o UDP uma solução mais adequada para o ambiente de IdC[63].

Apesar de suas vantagens, o UDP apresenta também algumas vulnerabilidades, como o ataque por UDP flooding, em que um atacante envia diversos pacotes UDP para uma vítima que é obrigada a responder, consumindo seus recursos[130].

4.5.1 DTLS

O TLS é o protocolo utilizado para garantir segurança na internet, desde aplicações bancárias até trocas de mensagem instantâneas, porém tem um alto custo computacional para ser implementado e não foi desenvolvido para aplicações de tempo crítico[32]. O DTLS se apresenta como um protocolo para trazer a segurança na comunicação de datagramas pela rede através do UDP, que é menos confiável para a entrega de pacotes, porém permite um maior fluxo de dados, para superar o problema de tempo crítico. O projeto inicial do DTLS buscava “imitar o mais próximo possível as operações realizadas no TLS”.[32, p. 3]

Fiser e Hancke [32] mostram que o DTLS é uma alternativa viável para o TLS, no que se refere à transferência de dados pela internet de WSNs conectados. Apesar de ter sido desenvolvido para superar questões relativas ao tempo-crítico na internet regular, como no caso de games, por exemplo, o protocolo DTLS ganha especial importância para a

IdC, em que os dispositivos apresentam restrições de energia e poder computacional, por ser leve e permitir um maior fluxo de dados.

O TLS funciona sobre 4 outros protocolos: (1) Record Protocol: protocolo padrão para as mensagens sendo trocadas, (2) Handshake Protocol: realiza o *handshake* inicial e configura a conexão, (3) Alert Protocol: avisa sobre qualquer mudança ou erro ocorrido e (4) Change Cipher Spec: usado para modificar o tipo de *cipher* no cliente ou servidor[32]. O DTLS é basicamente tudo o que o TLS é, adicionado de algumas características para lidar com os problemas de confiança do UDP[35].

Algumas vulnerabilidades conhecidas para o TLS e DTLS, são citadas no estudo exposto no RFC 7457: [98]

- SSL Stripping - retira o SSL ou TLS de dados não criptografados, de modo a impedir que o mecanismo de segurança opere. Esse ataque só funciona para casos em que o cliente acessa inicialmente o web server por HTTP e permite a execução de ataques MITM caso o usuário não perceba a falta do HTTPs.

- Injeção de Comandos STARTTLS - utiliza de uma falha ao se evoluir um texto puro para um texto protegido por TLS (STARTTLS) a nível de aplicação.

- Ataque BEAST (Browser Exploit Against SSL/TLS): permite que um Man-In-The-Middle seja capaz de descobrir o VI. Pode ser evitado utilizando a técnica de 1/n-1split[19]. Uma versão similar, porém mais estável, é o ataque Bar-Mitzvah, que analisa o tráfego na procura por uma chave RC4 fraca.

- Ataque Padding Oracle - utiliza dos valores colocados como padding no final do texto a ser criptografado para se quebrar a criptografia. O oracle é visto como uma caixa preta da criptografia sendo usada, com o qual o atacante pode interagir para calcular o valor intermediário do texto de cifra e quebrar a criptografia.

- Ataques no RC4 - O RC4 é conhecido por possuir diversas vulnerabilidades de criptografia, por isso, seu uso não é seguro e muitas instituições recomendam que seja descontinuado.

- Ataques de Compressão: CRIME, TIME, e Breach - O Compression Ratio Info-leak Made Easy (CRIME) é utilizado para se realizar um sequestro de sessão em uma sessão web autenticada, explorando-se os mecanismos de compressão pela análise da diferença de tamanho, ao se tentar obter informações criptografadas. Pode ser mitigado por não se utilizar a compressão, o que é feito atualmente pela maioria dos

[19]Quebra o CBC em dois: o primeiro com um único byte e o segundo com o restante, de modo a randomizar o VI e evitar o ataque

browsers. O TIME faz o ataque não pela análise do tamanho da compressão, mas na diferença do tempo de transmissão para encontrar as informações de sessão a partir da compressão do HTTP[10]. O Breach também utiliza da compressão HTTP e é mitigado ao se desativar a compressão.

– Ataques de certificado e RSA - Diversos ataques são utilizados no processo de obtenção de certificados RSA por implementações do TLS. Brubaker et. al [21] apresentam um modelo de testes para as diversas vulnerabilidades encontradas em bibliotecas que implementam certificados para o TLS.

– Roubo de chaves privadas do RSA - Quando utiliza-se o TLS com cifradores diferentes do Diffie-Hellman, ao se obter uma chave privada, é possível descriptografar todas as sessões, passadas e futuras com determinado servidor. Pode ser mitigado protegendo melhor as chaves privadas e oferecendo "forward-secrecy", propriedade que garante que mesmo que uma chave privada seja roubada, as informações de sessões passadas e futuras não serão reveladas.

– Parametros Diffie-Hellman - Para os modos de troca de chave, o TLS permite a implementação do modelo Diffie-Hellman e Diffie-Hellman com curvas elípticas, que podem ser explorados em um ataque.

– Renegociação - O TLS permite que as credenciais sejam renegociadas. Um ataque a essa função envolve um atacante enviando informações a um servidor, como se fosse o cliente, e, logo em seguida, o cliente negocia suas credenciais com o servidor pelo canal do atacante. Ou seja, os dados do atacante são interpretados pelo servidor como sendo dados legítimos do cliente.

– Ataque de Handshake Triplo - Um ataque no qual a utilização da mesma Master Secret no processo de handshake permite que um atacante injete dados na comunicação[13].

– Confusão do Hospedeiro Virtual - trata da exploração de vulnerabilidades no processo de roteamento entre hospedeiros virtuais, pois as decisões de roteamento são baseadas em informações não autenticadas, como endereços IP e portas, o que permite que um atacante desvie uma conexão HTTPS de um hospedeiro virtual para outro[29].

– Negação de Serviço - O processo de handshake consome tempo de processamento no lado do servidor e pode ser utilizado por um atacante para inviabilizar o serviço para usuários legítimos.

– Problema de Implementação - Ao se implementar o TLS em aplicações, sua má utilização pode trazer vulnerabilidades como o ataque Heartbleed, exposto em abril de 2014, que explorava entrada de dados sem verificar se estourava o tamanho máximo do buffers.

– Problema de Usabilidade - Muitas vezes é permitido que usuários aceitem certificados inválidos, o que pode ser utilizado por atacantes para ganhar acesso a informações não criptografadas.

Ao se utilizar o TLS as versões antigas devem ser evitadas, pois são consideradas inseguras. Deve se preferir a versão 1.2, tanto do TSL como DTLS, e não deixar que o protocolo permita cair a versão, pois esse processo pode ser ativado por meio de um ataque de Man-In-The-Middle, colocando o sistema em uma posição instável, dada a insegurança das versões antigas[97].

4.6 Camada de Aplicação

A camada de aplicação provê aos usuários uma interface para comunicação processo-a-processo entre nós fim. É a única em que há a interação direta com o usuário.

4.6.1 CoAP

Definido pela IETF, o CoAP[99] representa o protocolo para a camada de aplicação para redes e nós com restrições. É definido para aplicações M2M e, assemelha-se ao HTTP. Utiliza de comandos GET, PUT, POST e DELETE, do modelo REST, e faz uso de conceitos da web como URIs[20]. A implementação do CoAP, porém, se comporta tanto como servidor como cliente em uma comunicação M2M. “O modelo de mensagem do CoAP é baseado na troca de mensagem, sobre UDP, entre dois pontos” em que um cliente requisita uma ação (utilizando um código de método), de um recurso (identificado por uma URI), localizado em um servidor, que retorna uma resposta com um código de resposta[99]. “As mensagens são trocadas de maneira assíncrona” e, “[...] como é realizada sobre UDP, o protocolo fornece um mecanismo leve para a confiabilidade.”[35, p. 1303]

O CoAP é dividido em duas camadas, uma que lida com as requisições e respostas e outra para tratar as mensagens sendo transmitidas pelo UDP. Existem quatro possíveis tipos de mensagem no CoAP: (1) Acknowledgement, para sucesso; (2) Reset, para rejeitar uma mensagem confirmável o remover um observador; (3) Confirmável, indica uma entrega confiável da mensagem e (4) Não-Confirmável, não espera uma confirmação do envio. Como está sobre o UDP, em que a entrega não é garantida, a transmissão pode exigir confirmação de entrega, por isso mensagens do tipo confirmável sempre retornam um ACK

quando bem sucedidas[89]. Assim como no HTTP, o CoAP possui sua serie de códigos e mensagens de resposta[35].

Para a segurança, o CoAP utiliza do DTLS, logo, transfere para a camada de transporte a manipulação de mecanismos de segurança.[35, p. 1304] O protocolo provê quatro modos de segurança: (1) *NoSec*: nenhum mecanismo de segurança do DTLS é aplicado, (2) *PreSharedKey*: utilizado com dispositivos que já são pré-programados com as chaves simétricas necessárias, onde cada chave possui uma lista de nós que pode se comunicar, (3) *RawPublicKey*: o dispositivo possui um par de chaves assimétricas sem a utilização de certificado, que é validado por um mecanismo *out-of-band* e (4) *Certificate*: o protocolo faz o uso do DTLS com um certificado X.509, o dispositivo possui também uma lista de raízes confiáveis.[35, p. 1304][99, p. 68]

No RFC 7252, do CoAP[99], as possíveis ameaças ao protocolo são elicitadas:

- Parsing do Protocolo e Processamento de URIs: é possível explorar vulnerabilidades no processo de parsing, para, por exemplo, gerar um ataque de negação de serviço ao se inserir um texto que irá acarretar em parser muito extenso. O CoAP tenta evitar a vulnerabilidade ao se reduzir a complexidade dos parsers. Também, a maioria do processamento de URIs é realizado no lado do cliente, para se evitar explorações ao servidor.

- Proxying e Caching: o proxy é, por si só, um man-in-the-middle, segundo o autor, quebrando toda segurança do IPsec e DTLS. Ameaças são amplificadas quando os proxies permitem que haja uma cache dos dados.

- Risco de Amplificação: as respostas no CoAP são, geralmente, maiores do que as requisições, o que pode vir a facilitar ataques por amplificação. Dadas suas características repletas de restrições, tal ataque não é tão preocupante vindo de uma rede LLN, porém, se torna para ataques em direção a ela.

- Ataques de IP Spoofing: Como não há handshake para o UDP, o nó final que possui acesso à rede pode realizar spoofing para enviar mensagens de ACK no lugar de CON, prevenindo que haja retransmissão; spoofing em todo o payload; spoofing de pedidos multicast; etc.

- Ataques Cross-Protocol: envolvem utilizar o CoAP para enviar ataques a outros protocolos, para se passar pelo firewall, por exemplo.

- Nós com Restrições: sejam energéticas, de memória ou de processamento, dificultam que os dispositivos disponham de boa entropia[20]. Assume-se portanto que os pro-

[20]Randomização para aplicações criptográficas

cessos que necessitem de entropia, como o cálculo de chaves, o façam externamente. A falta de recursos também os torna suscetíveis a ataques de temporização.

4.6.2 MQTT

O MQTT (Message Queuing Telemetry Transport Protocol)[21], desenvolvido em 1999 originalmente pela IBM, se tornou um padrão aberto ISO (ISO/IEC 20922:2016 [52]). Trata-se de um protocolo para o enfileiramento e transporte de mensagens, que se utiliza do modelo *publish/subscribe*. É leve e foi desenvolvido com o intuito de ser simples de se implementar. Seus componentes principais são: *brokers*, sessões, assinaturas (*subscriptions*) e assunto (*topic*)[100].

O modelo publish/subscribe envolve a definição de um comunicante e de diversos ouvintes, conectados em um broker, que organiza a troca de mensagens entre assinantes e publicantes, como mostrado na Figura 4.7[41]. O assinante registra o interesse em determinado assunto e, assim que algum publicante disponibiliza conteúdo neste tópico, o broker direciona a mensagem para os assinantes registrados. A qualidade de serviço nesse processo é dividida em três categorias: (1) No máximo uma vez(*At most once/Fire and Forget*), que utiliza do melhor esforço para se enviar, caso não chegue em determinado envio pode chegar no próximo; (2) Ao menos uma vez(*At least once*), garante que a mensagem chega, mas pode ocorrer duplicatas e (3) Exatamente uma vez(*Exactly once*), que garante que a mensagem chegará e não irão ocorrer duplicatas[100]..

Buscando adaptar-se melhor ao ambiente de redes sem-fio, foi desenvolvido o MQTT-SN. Essa variação: não necessita do uso de TCP para o transporte; transmite apenas dois bytes do tópico (*topic id*); estabelece tópicos comuns, conhecidos pela aplicação e pelo servidor desde o início; apresenta um procedimento que facilita o processo de descobrimento do servidor/gateway por um cliente que não possua esse endereço pré-configurado; expande a semântica de clean session para mecanismos categorizados como Will (ex. Will topic e Will message) e provê um novo procedimento de *keep-alive* para tratar clientes no modo *sleep*, onde as mensagens destinadas a este cliente são colocadas em um buffer e enviadas assim que o cliente acorda[106].

É definido, pela IANA, para o MQTT, a porta TCP 8883. O protocolo em si não oferece mecanismos de segurança, que normalmente são endereçados pela utilização de mecanismos como o TLS. Cabe ao implementador configurar. No pacote de conexão, existem campos para o nome de usuário e senha, que podem ser utilizados no processo de autenticação. Entre outras coisas, o protocolo apresenta a função "Testamento para o Ultimo Desejo"(LWT - *Last Will Testament*), que define como o protocolo deve agir caso

[21]MQTT - http://mqtt.org/

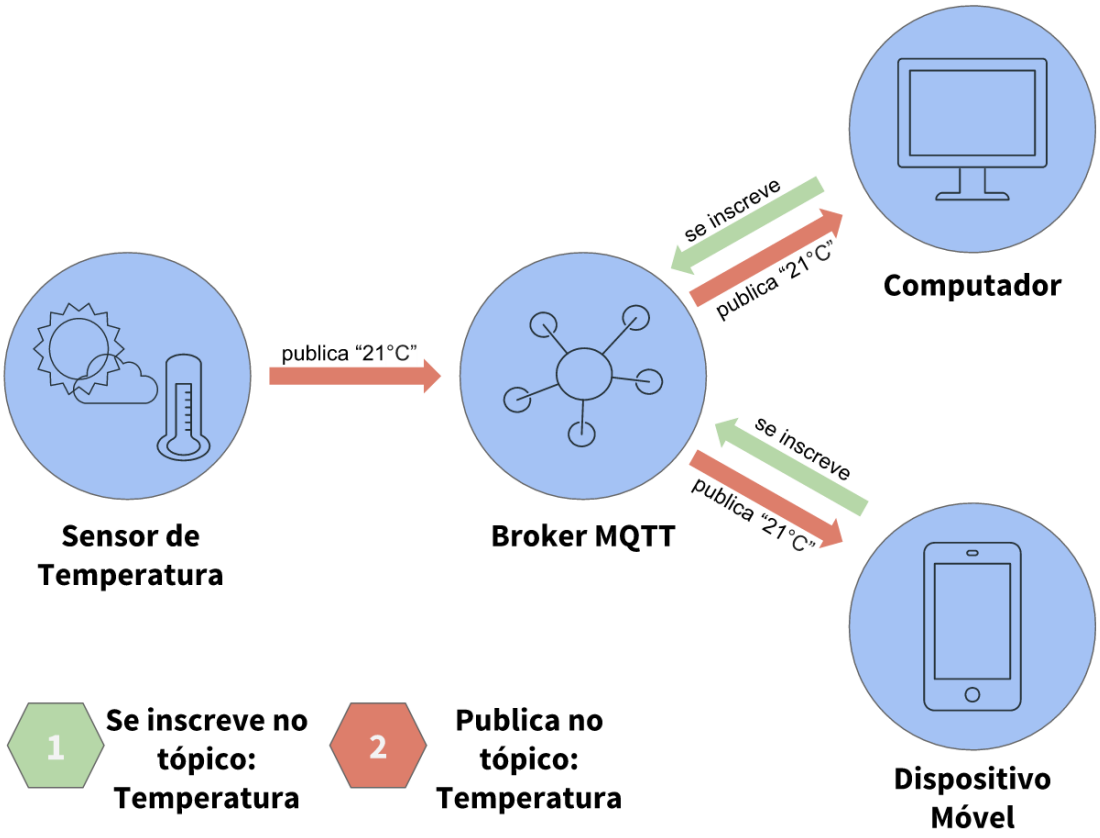

Figura 4.7: Modelo publish/subscribe utilizado no MQTT [41].

um nó vá offline. Essa técnica pode ser utilizada, por exemplo, para notificar o gerente de rede ou de negócios, caso um nó crucial tenha se desconectado.

Assim como no CoAP, a segurança é endereçada por fora, pelo TLS, que é muito pesado para os dispositivos de IdC. Singh et. al. [102] propõem um modelo de aplicação seguro para o MQTT, denominado SMQTT, por meio de criptografia baseada em atributo leve (Lightweight ABE), que provê criptografia por broadcast[22], sobre curvas elípticas. Esse modelo, segundo os autores, se mostrou resistente a ataques de *plaintext* conhecido, *ciphertext* conhecido e de *man-in-the-middle*.

4.6.3 XMPP

Extensible Messaging and Presence Protocol, foi desenvolvido pelo grupo open source Jabber[23], em 1999, mirando aplicações de chats e trocas de mensagens. Foi ratificado, pelo IETF, no RFC 3920 para a versão 1.0 (atualmente obsoleto), passou por alterações e sua versão mais recente é definida pelo RFC 6120[93] e por atualizações ao mesmo. É

[22]Com uma criptografia, a mensagem é enviada para diversos usuários.
[23]Jabber - www.jabber.org

estruturado em XML para a troca de dados estruturados, em um modelo que se aproxima de tempo-real. O protocolo faz a troca de pequenos pedaços de mensagem conhecidos por "XML Stanzas". Suporta o modelo cliente-servidor e publish/subscribe para a troca de mensagens.

No XMPP existem três principais funções para os integrantes da rede: (1) Cliente, (2) Servidor e (3) Gateway. O cliente se conecta, via TCP, se registra e loga, em um servidor e se utiliza do XMPP para usufruir do que o servidor oferece. O gateway é o responsável pela interoperabilidade entre outras plataformas. Os usuários em uma rede XMPP recebem um identificador JID (Jabber ID) como endereço único, que contém o identificador do domínio, do nó e do recurso.[56, p. 928-929]

A comunicação ocorre através de Streams XML, onde os Stanzas XML são enviados. Os Stanzas podem ser de três tipos: (1) Mensagem, são enviadas seguindo um mecanismo de *push*; (2) Presença, que avisa à rede informações de status e disponibilidade de entidades. Funciona como um modelo publish/subscribe em que membros autorizados e que tenham se inscrito, recebem notificações de mudança de status e quando se está online ou offline; (3) IQ (Info/Query) é um mecanismo de request/response parecido com o HTTP, onde uma entidade envia um pedido e recebe uma resposta.[56, p. 929]

O XMPP utiliza da segurança provida pelo TLS. No RFC 7590[94], são especificadas recomendações da utilização do TLS pelo protocolo de maneira segura. O documento provê também informações relativas ao que já está definido no padrão do protocolo (RFC 6120) em termos de segurança, como a obrigatoriedade de que clientes autentiquem servidores, servidores autentiquem clientes e que servidores não devem autenticar outros servidores. Todas as vulnerabilidades do TLS refletem nos protocolos que dependem do mesmo para a segurança, como uma vulnerabilidade reportada para a Cisco indicando que um de seus produtos poderia sofrer de ataque Man-in-the-Middle para fazer o STARTTLS downgrade em uma comunicação XMPP e transmitir os dados sem criptografia[116].

4.6.4 UpNP

O Universal Plug-and-Play (UPnP) foi desenvolvido para integrar de maneira simples a entrada e descoberta de dispositivos em redes residenciais, de pequenos negócios e em prédios comerciais, de maneira que possam prover e utilizar facilmente de serviços funcionais entre si. Foi lançado, em 1999, a partir da união de várias empresas de eletrônicos, impressoras, rede, utensílios para casa, automação, controle, entre outras, que formavam um grupo de mais de 1000 empresas reunidas no UPnP Forum. Desde 1 de janeiro de 2016 passou a ser controlado integralmente pela Open Connectivity Foundation (OCF).[24]

[24]OCP UPnP - `http://openconnectivity.org/upnp` - Acesso em 15/06/2016

Sua arquitetura é baseada em um modelo peer-to-peer em cima de tecnologias abertas como o TCP, IP, HTTP e XML. Os blocos principais do UpNP são: (1) Dispositivos, (2) Serviços e (3) Pontos de Controle. Os Dispositivos são "containers de serviços e dispositivos interligados".[71, p. 10] Para cada dispositivo, um documento XML descreve suas características principais e seus serviços disponibilizados, de modo a associá-los com outros dispositivos de categorias similares. O Serviço é a menor unidade de controle no UPnP e "expõe ações e modela seu estado com variáveis de estado"[71, p. 11]. Por exemplo, um relógio pode ter um serviço modelado com uma variável de estado tempo_corrente e ações como configurar_tempo e obter_tempo. O serviço possui uma tabela de estados, um servidor de controle e um servidor de eventos. Finalmente, os Pontos de Controle são controladores "capazes de descobrir e controlar outros dispositivos"[71, p. 11] e, após descobrir, pode obter quais são as características do dispositivo e quais serviços este fornece, invocar ações de controle e se inscrever para ouvir os eventos gerados.

Baseado na arquitetura de cada dispositivo, o UPnP Forum (agora OCF), define os protocolos gerais a serem utilizados, de acordo com cada categoria de dispositivos, e, em cima disso, cada vendedor pode estipular dados específicos de seus dispositivos. O UPnP se baseia na pilha de protocolos do modelo TCP/IP. Também utiliza-se do HTTP, HTTPU e HTTPMU (HTTP sobre UDP). O Simple Service Discovery Protocol (SSPD) é utilizado para descobrir serviços na rede, sobre o HTTPU e HTTPMU, de modo que cada ponto de controle mantem informações de estado da rede atualizadas, com uma necessidade menor de tráfego. O Generic Event Notification Architecture (GENA) é utilizado para prover informações de publish/subscribe. Também é utilizado o SOAP para a execução de chamadas de procedimento remotas[71].

Assim que entra na rede, o dispositivo obtém um endereço IP e envia seus serviços, de maneira multicast, via SSPD. Sempre que um Ponto de Controle entra na rede, este procura por dispositivos de interesse na rede e segue monitorando o estado e mudanças no mesmo. O UPnP não impõe nenhum mecanismo de autenticação ao usuário. Isso permite que qualquer programa em um computador, por exemplo, possa redirecionar portas de conexão, inclusive malwares. Por esse motivo, é amplamente recomendado que se desative o UPnP para o ambiente externo, de modo a evitar a exploração de portas.

O SSDP possui uma falha de larga escala que permite a realização de ataques distribuídos de DoS. Vários dispositivos que fornecem o serviço estão abertos, na porta 1900, e permitem a reflexão e amplificação de pacotes. A PLXsert[1] mostra que o ataque pode ser realizado primeiramente identificando quais dispositivos estão vulneráveis pelo envio da requisição SOAP (M-SEARCH). Com a lista de dispositivos, o atacante redireciona para a vítima os pacotes amplificados, segundo o autor, em até 33%.

Uma ameaça ao UPnP de 2012 ainda era vista até dezembro de 2015 e abrangia até

6.1 milhões de dispositivos, de acordo com a TrendLabs [127]. Essa ameaça envolvia a utilização de uma versão desatualizada de uma biblioteca conhecida por *libupnp*, que permitia um ataque por overflow no qual o atacante era capaz não só de desabilitar o uso, mas também de rodar um código arbitrário no dispositivo. O ataque é explorado a partir de uma falha no modo que a biblioteca lida com o SSDP.

Dados os níveis de exposição e os potenciais impactos de ataques bem sucedidos, recomenda-se que o UPnP não seja ativado em nenhum sistema voltado para fora ou dispositivos que realizam funções críticas[74].

4.6.5 DDS

O Object Management Group (OMG), define o padrão de middleware Data Distribution Service (DDS) para facilitar uma distribuição de dados eficiente em um sistema distribuído e com vários participantes. Ele provê um modelo centrado em dados para publish/subscribe. A especificação do DDS é definida segundo dois níveis de interface: (1) um nível mais baixo, Data-Centric Publish-Subscribe (DCPS), que visa "entregar a informação certa, na hora certa, para a pessoa certa"[79, p. 1], por meio da definição de um "Espaço Global de Informação", e (2) Data-Local Reconstruction Layer (DLRL), um nível mais alto, opcional, para uma integração simplificada com a camada de aplicação[86].

O modelo centrado em dados do DDS se baseia na definição de: sinais, que representam dados em constante mudança; streams, que são snapshots representando o valor de objeto de dados em determinado instante, e estado, que define a situação atual de objetos (ou sistemas). As principais entidades na arquitetura da camada DCPS do DDS são: (1) DomainParticipant, entidade participante de um domínio, (2) DataWriter, utilizado para comunicar mudanças em determinado tipo de dados, (3) DataReader, utilizado para acessar dados recebidos, (4) Publisher, publica informações, (5) Subscriber, recebe dados publicados e disponibiliza e (6) Topic, o assunto de interesse. Todos esses extendem *DCPSEntity* e, cada especialização desta, deve prover informações relativas a QoS e um ouvinte(listener) específico. Essas entidades se relacionam para prover a comunicação confiável, segundo o modelo publish/subscribe[86].

O DCPS divide-se ainda em cinco módulos: (1) Domínio, (2) Publicação, (3) Subscrição, (4) Tópico e (5) Infraestrutura. No módulo para infraestrutura, as classes abstratas e interfaces são definidas. O módulo de domínio contém a classe *DomainParticipant*, que é a porta de entrada para serviços e serve como fábrica para outras classes. O módulo de definição de tópico contém todo o necessário para a aplicação definir tópicos e definir QoS para os mesmos. Os módulos Publicação e Subscrição, abrigam todo o necessário do ponto de vista de publicação e subscrição, respectivamente.

Visando a estipulação de um "espaço de informação global", em que todos possuem acesso à informação que desejam, o processo de garantia de segurança no DDS se torna complexo. Originalmente, nenhum mecanismo de segurança é definido na especificação do DDS. Foi desenvolvido, então, um modelo de segurança, que está em sua versão 1.0, em estado beta[78]. Nele são estipulados 5 plugins de serviço para: autenticação, controle de acesso, criptografia, logging e tagging de dados.

Em uma análise de segurança para modelos publish/subscribe, Esposito e Ciampi[p.989-990][31] ressaltam que a característica aberta de publicação (OpenPublish) em modelos publish/subscribe, permite que atacantes executem ataques de mascaramento, flooding e trashing. O trashing é realizado pela mudança frequente e rápida do estado de anúncio(advertisement), no Serviço de Notificação. Tais ataques podem ser evitados ao se aplicar autenticação de usuário e controle de acesso ao serviço. No caso da abertura para a subscrição (OpenSubscribe), ataques como eavesdropping, trashing e replay podem ser explorados. O trashing nesse caso, também envolve o envio rápido e frequente de mudança de estado, porém nesse caso de subscrição, no Serviço de Notificação. A solução para os mesmos envolve criptografar os dados transmitidos e também definir autenticação e controle de acesso.

Para "mostrar as soluções as quais a comunidade está se direcionando" em termos da segurança do DDS, Esposito e Ciampi[31, p.989-990] analisaram duas implementações do DDS: RTI e OpenSplice, indicando como está implementada a segurança nestes modelos, como mostra a Figura 4.8[31][25]. Nessa imagem, é possível visualizar o funcionamento da transmissão de mensagens por publish/subscribe no DDS. Para a segurança, é utilizado o DTLS na camada de transporte para integridade e confidencialidade entre os nós finais. A especificação de segurança sendo desenvolvida pelo DDS, requer que as transmissões sejam feitas criptografadas e que seja disponibilizado código de integridade HMAC[78].

4.7 Ameaças Identificadas

4.7.1 Key Cracking

Toda informação transmitida por criptografia possui uma chave, que é utilizada para randomizar o texto. Uma vez conhecida essa chave, o dado pode ser descriptografado. Tendo a posse da chave, um atacante pode não só observar os dados sendo transmitidos, mas, em alguns casos, pode realizar uma serie de outros ataques como Man-in-the-middle e replay. O processo de quebra de chave é complexo, principalmente quando a criptografia utilizada é o AES. As principais técnicas para se quebrar uma chave são ataques por força

[25] O * na imagem indica que um controle de acesso adequado é implementado apenas no OpenSplice

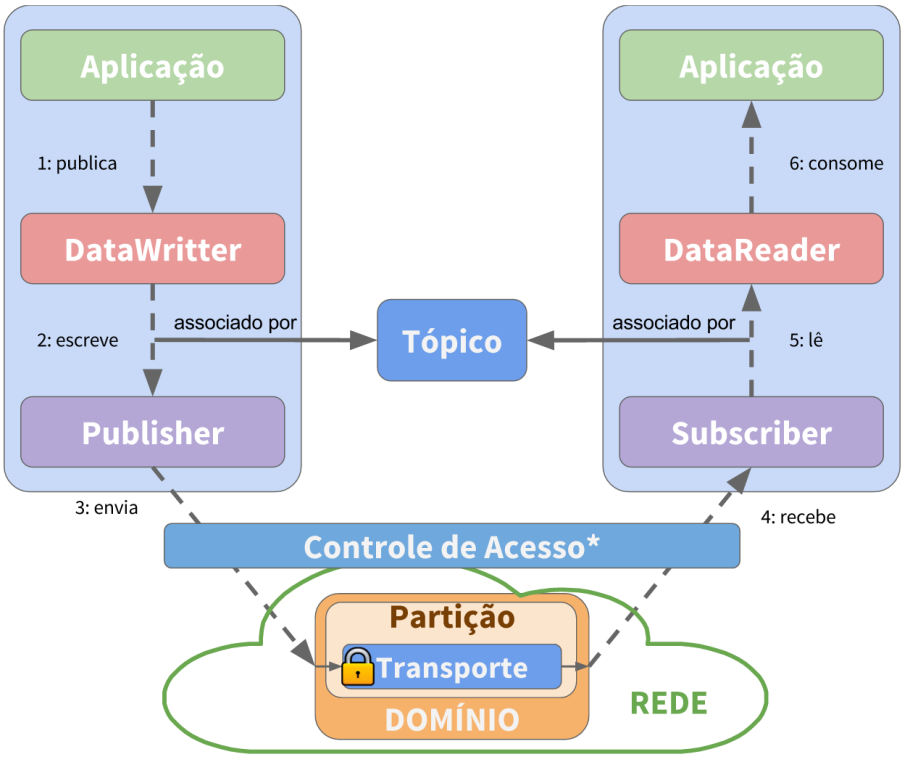

Figura 4.8: Notificação de Evento segura para middleware com DDS [31].

bruta, no qual todas as possibilidades são esgotadas até se encontrar a chave correta, ou ataque de dicionário, em que são escolhidas combinações com maior probabilidade de ocorrência. O ataque pode ser categorizado também como online ou offline. No primeiro, o atacante conta com respostas do serviço quanto ao sucesso ou falha da tentativa de quebra de chave, no segundo, o atacante conta apenas com alguns dados que conseguiu colher, mas não tem uma resposta do serviço para suas tentativas.

Para mitigar tal ataque, é necessário que sejam utilizadas técnicas de criptografia confiáveis. O VI deve sempre ser randomizado, o serviço não deve responder a um número de tentativas de acesso muito alto e as credenciais devem ser largas e com diferentes símbolos, fugindo ao máximo de valores comuns e de fácil associação.

4.7.2 Eavesdropping

Eavesdropping se refere ao processo de observar a informação sendo transmitida. Isso ocorre em casos onde os dados não possuem criptografia. Em um ambiente sem fio, como a comunicação ocorre por ondas de rádio, o acesso é mais facilitado, tanto por equipamentos próximos ao ambiente, quanto distantes, com antenas direcionais, capazes

de captar informação a vários metros de distância. Dada as limitações dos dispositivos de IdC, muitas vezes opta-se por não aplicar criptografia.

4.7.3 Replay

O ataque de *replay* envolve um atacante observando determinado tráfego de dados, criptografados ou não, os quais o atacante possui algum conhecimento a respeito, por exemplo, dados relativos ao processo de autenticação. Com essa informação em mãos, o atacante pode reenvia-los em um momento futuro, se passando pelo usuário. Para evitar esse tipo de ataque, anexa-se às mensagens um código *nonce*, que é incrementado a cada novo pacote enviado. Desta forma, uma vez recebido tal pacote, o mesmo não terá mais valor em um momento futuro.

4.7.4 Man-in-the-Middle

Ataques Man-in-the-Middle ocorrem quando duas entidades acreditam estar comunicando entre si diretamente, porém a informação sendo transmitida está, todavia, passando por um atacante, que modifica ou não a informação antes de repassá-la. A falta de autenticação das partes permite que tais ataques ocorram, logo, uma comunicação segura necessita de autenticação, que é endereçada pela maioria dos protocolos.

4.7.5 Jamming Físico

Dada a característica aberta do ambiente sem fio e, em alguns casos, a utilização de bandas não reguladas (ISM), seja intencional ou não, a informação transmitida está vulnerável a sofrer interferência. Quando esse processo é intencional, é chamado ataque de *jamming*, que pode ser facilmente implementado com dispositivos que emitam ruído[23]. Ronak e Rutvij[14] categorizam como *jammer constante* aquele que emite constantemente o ruído; um que só é ativado quando há comunicação entre dispositivos é chamado *reativo*; um que transmite pacotes comuns ao invés de um sinal randômico é *deceptivo* e os que enviam sinais aleatórios (pacotes normais ou ruído), quando ativos, mas entram aleatoriamente em um estado de espera, são conhecidos como jammers *randômicos*. Os autores apresentam um estudo dos métodos correntes e desenvolvem um novo método para se identificar quando um jammer constante está presente em um ambiente de rede sem-fio. Também sugerem para trabalhos futuros o estudo para jammer reativo, deceptivo e aleatório e também que o algoritmo criado seja utilizado para mitigar os ataques por jamming. Outras formas de se mitigar o ataque são sugeridas pelo autor. A melhor forma de se mitigar tal ataque, então, é por meio de detectores de intrusos na rede, que estão emitindo si-

nais, além de técnicas como *blacklisting*, que cria uma lista de frequências a não serem utilizadas, e *frequency hopping*, que espalha a informação em diferentes frequências.

4.7.6 Jamming Enlace

No jamming de enlace, ao contrário do jamming físico, o ruído na comunicação ocorre na camada de enlace, ou seja, são enviados pacotes com informações inúteis que são interpretadas nesta camada. Dessa forma, um atacante pode sobrecarregar um serviço com informações desnecessárias. A principal forma de se mitigar tal ataque, também envolve sistemas de identificação de intrusos e verificação da origem dos pacotes sendo recebidos.

4.7.7 MAC Spoofing

Cada dispositivo em uma rede possui um endereço MAC que o identifica. Ataques de MAC spoofing envolvem a falsificação, por parte de um atacante, de tal endereço, de modo a se passar por um usuário legítimo ou desviar o fluxo de dados para o usuário, inviabilizando o serviço para o mesmo. Para evitar tal ataque é necessário aplicar segurança nas portas, limitando o número de participantes autorizados.

4.7.8 IP Spoofing

Em uma comunicação na rede, o endereço IP define origem e destino dos pacotes sendo enviados. Um atacante pode então adulterar este endereço para realizar diversos ataques. A mitigação para tal é complexa e envolve a identificação da origem real dos endereços. Em [101], foram revisados mais de 275 artigos que tratam do tema de rastreabilidade da origem real de endereços IPs para a mitigação de ataques DDoS. Os esquemas de rastreabilidade podem ser definidos de acordo com a forma em que são estruturados: teste de enlace; mensagem; marcação; logging; overlay; análise de padrão e híbrido.

4.7.9 Fragmentação

Quando os pacotes enviados são muito grandes, aplica-se o processo de fragmentação, que divide os pacotes em unidades menores. O processo, então, exige que o receptor mantenha um *buffer* para receber os pacotes fragmentados e, após ter recebido todos, uní-los para ser capaz de interpretar a informação. Um atacante pode explorar tal característica, enviando diversos fragmentos, de modo a abrir vários *buffers* no receptor e consumir toda sua memória, ou enviar fragmentos adulterados de modo que o receptor não consiga

interpretar a informação sendo construída. Para se mitigar tal ataque, é necessário que o receptor mantenha um mecanismo de autenticação da origem[35, p. 1306].

4.7.10 Wormhole

Em um ataque de Wormhole, um atacante transmite pacotes de nós legítimos através de um túnel virtual, de modo a introduzir na rede informações falsas sobre a distância e características de qualidade de transmissão, adulterando todo o processo de roteamento, ainda que os nós estejam autenticados[43]. A mitigação para esse tipo de ataque segue como um tema aberto para pesquisas[70, p. 3].

4.7.11 Sinkhole

Em um ataque de Sinkhole, o atacante é um nó em uma rede, que propaga informações sobre a qualidade de transmissão, de modo que os outros participantes da rede o definam como vizinho principal no processo de roteamento. Tendo atraído vários nós para si, o atacante pode iniciar outros tipos de ataque, como Man-in-the-middle ou DoS. A mitigação para esse tipo de ataque envolve um processo de autenticação robusto, que não permita nós de fora participarem do processo de roteamento[67].

4.7.12 Selective Forward e Blackhole

Ao se inserir em uma rede como um nó de roteamento, um atacante pode iniciar um tipo de ataque de DoS em que nenhum pacote é retransmitido, formando assim uma espécie de buraco negro no processo de transmissão de dados, por isso, o ataque é denominado *Blackhole*. Quando o atacante escolhe alguns pacotes para transmitir e outros para abandonar, o ataque é denominado *Selective Forwarding*, que traduzido pode ser interpretado como Repasse Selecionado. O *Blackhole* é mais fácil de ser identificado pois todos os pacotes chegando em um nó são perdidos, então um caminho alternativo é definido. Para a mitigação, no caso do Selective Forwarding, podem ser utilizadas técnicas como criptografia, para evitar que o atacante saiba do teor das mensagens sendo transmitidas e caminhos dinâmicos entre os nós comunicantes[88].

4.7.13 Sybil

Nomeado em homenagem a uma paciente que sofria de distúrbio de múltiplas personalidades, o ataque Sybil envolve a obtenção de múltiplas identidades em uma rede. Para casos onde não há uma administração centralizada, esse ataque é mais fácil de ser implementado[90]. Em casos de redes peer-to-peer, um atacante consegue desequilibrar a

distribuição de arquivos entre os nós, o que pode ocasionar perda de informações. Para mitigar tal ataque, busca-se um controle de autenticação que garanta identidade única para os participantes da rede.

4.7.14 Reflexão e Amplificação

Um atacante pode emitir diretamente pacotes corrompidos para realizar um ataque, ou levar um serviço a direcionar pacotes para uma vítima. No segundo caso, o ataque é conhecido como Ataque de Reflexão. O atacante pode, ainda, explorar serviços que, além de refletir o ataque para a vítima, aumentam a quantidade de informação. Dessa forma, um atacante pode realizar um estrago maior, com menos recursos. Nesse caso, o ataque é conhecido como de Amplificação[127]. Para evitar que um serviço seja utilizado para esse tipo de ataque, é necessário um processo de autenticação robusto e que o tamanho da informação dada como resposta, para casos não-autenticados, não seja excessivamente maior do que a requisição.

4.7.15 Masquerading

Quando um atacante se apresenta como usuário legítimo de um serviço, considera-se que o mesmo está "utilizando uma máscara", do inglês Masquerading. A mitigação do ataque envolve a autenticação dos usuários e um controle de acesso a recursos de determinado serviço[31].

4.7.16 Trashing

Em um modelo publish-subscribe, um usuário pode se inscrever em determinado assunto e, sempre que houver alguma mudança de estado do assunto, este recebe a devida notificação. No ataque de Trashing, um atacante modifica várias vezes o estado de um assunto, ou se inscreve e sai várias vezes, gerando várias notificações, que podem inviabilizar o serviço da central de notificações. A mitigação deste tipo de ataque envolve a autenticação de usuários e um controle de acesso[31].

4.8 Comentários Finais

A maioria dos protocolos estudados são de desenvolvimento aberto, por instituições como IEEE, IETF, ISO, dentre outras. O fato da padronização estar disponível é, ao mesmo tempo, temerário, pois a implementação está aberta para análise por entidades mal intencionadas, assim como é oportuno, visto que o protocolo será amplamente testado e

lapidado para se chegar mais rapidamente a uma solução robusta, por atrair mais atenção. Ou seja, as vulnerabilidades tendem a ser descobertas e tratadas mais cedo, sendo, consequentemente, menores as chances de se ocorrerem vulnerabilidades zero-day.

A partir da análise de cada protocolo apresentado, é difícil prever quais terão sucesso neste novo paradigma. Tal escolha engloba diversos fatores, muitos de cunho econômico, tornando difícil a previsão. O que se conclui dos protocolos abordados, todavia, é que há um esforço em adequá-los às peculiaridades do ambiente de Internet das Coisas, dadas suas limitações de processamento, memória e energia. Protocolos que não se mostrarem eficientes na utilização dos recursos decerto sucumbirão. Ademais, o simples fato de se ter, no protocolo, segurança embutida, não indica necessariamente que o ambiente está seguro da melhor maneira. Cada caso de implementação tem suas exigências próprias, por isso, é necessário conhecê-las a fundo, assim como os protocolos, com seus modos de segurança e vulnerabilidades, para estar apto a definir corretamente suas configurações.

Capítulo 5

Síntese de Segurança dos Protocolos de IdC

O presente estudo teve seu foco principal na segurança dentro do universo de IdC, em especial, nos principais protocolos e projetos voltados para essa questão, procurando identificar as respectivas vulnerabilidades e ameaças. Nessa direção, como fruto dessa análise, criou-se um compêndio de todo esse material, apresentado aqui, em forma de tabela, para subsidiar consultas e futuras pesquisas sobre o tema. Vale ressaltar, contudo, que tal resultado ainda deve ser considerado parcial, uma vez que alguns dos protocolos estudados não deixam explícitas suas principais ameaças. Foi feito um agrupamento geral, reunindo as ameaças mais recorrentes, comuns aos principais protocolos. Tal produto foi classificado de acordo com as camadas nas quais os protocolos se encaixam. No decorrer da pesquisa, observou-se ausência de dados compilados dessa natureza, de fácil acesso e manipulação, voltados para segurança em IdC. Portanto, o resultado desse estudo tem como principal diferencial oferecer um material consistente para pesquisas futuras, de fácil acesso e possível de ser enriquecido e complementado ao longo do processo de consolidação da IdC, agregando novos protocolos com suas vulnerabilidades.

5.1 Modos de Segurança

A tabela a seguir apresenta um resumo dos modos de segurança implementados em cada protocolo, que foram descritos no Capítulo 4. AAA se refere a Autenticação, Autorização e Prestação de Contas, do inglês Authentication, Authorization and Accountability. Para confidencialidade, estão descritos os cifradores que o protocolo utiliza e, para disponibilidade, quais são os mecanismos aplicados no protocolo para proporcionar a disponibilidade dos serviços de rede ante a ataques, falhas e características do ambiente.

Protocolo	Modos de Segurança	AAA e Integridade	Confidencialidade	Disponibilidade
WiFi	-WEP -WPA -WPA2	PSK 802.1X/EAP	RC4 TKIP/RC4 CCMP-AES	CSMA/CA Topologia mesh
Bluetooth LE	- Não Seguro -Executado a Nível de Serviço -Executado a Nível de Enlace	Algoritmo E1 com Chaves de Link	Cifrador E0	
IEEE 802.15.4	- Sem segurança - Dados não criptografados e autenticados - Dados criptografados e não autenticado - Dados criptografados e autenticados	ACL AES-CBC-MAC	AES-CTR AES-CBC AES-CCM	CSMA/CA Superframe
ZigBee	Utiliza dos mecanismos de segurança do IEEE 802.15.4 e provê segurança para as camadas de rede e aplicação.	ACL CBC-MAC	AES-CCM-128 bits Chave Master, de Rede e de Link	Topologia mesh Automatic Repeat Request ACK na Camada de Enlace
WirelessHART	Segurança não é opcional. Utiliza-se da segurança do IEEE 802.15.4	ACL AES-CCM*-128 MIC	AES-CCM*-128 Chaves Pública, de Rede Join e de Sessão	Topologia mesh Blacklisting Frequency hopping Automatic Repeat Request ACK nas camadas de enlace e transporte
ISA 100.11	-Administrado por políticas definidas pelo administrador de segurança -Utiliza da Segurança do IEEE 802.15.4	Chaves simétricas e assimétricas utilizam AES-CCM*	AES-CCM*	Topologia mesh Blacklisting Frequency hopping Automatic Repeat Request ACK nas camadas de enlace e transporte
6loWPAN	Não implementa segurança			
RPL	- Inseguro - Pré-Instalada - Autenticada	Chaves pré-instaladas AES-CCM-MAC 128 bits RSA com SHA-256	AES-CCM*	
DTLS	- Record Protocol - Handshake Protocol - Alert Protocol - Change Cipher Spec	HMAC-SHA1, HMAC-SHA256/384 AEAD	Possui vários cifradores que podem ser selecionados	
CoAP	- No Sec - PreSharedKey - Raw Public Key - Certificate	Lista de Raízes Confiáveis Utiliza o DTLS	AES-CCM	
MQTT	Utiliza o DTLS	Campo para nome e senha Utiliza o DTLS	Utiliza o DTLS	
XMPP	Utiliza o DTLS	Utiliza o DTLS	Utiliza o DTLS	
UpNP	Específico para cada implementação			
DDS	Definição em estado beta			

Tabela 5.1: Resumo dos modos de segurança empregados para cada protocolo

5.2 Superfícies de Ataque Identificadas

Vários ataques e vulnerabilidades foram identificados em cada protocolo. As tabelas apresentadas a seguir buscam unir os ataques comuns em cada camada, onde, caso tenha sido identificado no trabalho, o ataque é marcado. Em alguns casos, são colocadas observações, dado que certos ataques só ocorrem quando mecanismos de segurança disponíveis não são aplicados.

5.2.1 Camadas Física e de Enlace

Dada a abertura em que a comunicação sem-fio se apresenta, diversos ataques podem ser explorados. Todos os protocolos estudados mostraram-se vulneráveis a ataques de jamming. Diversas soluções existem para tentar mitigar tal vulnerabilidade, porém, é intrínseco do ambiente que tais ataques possam ser aplicados. O jamming pode ocorrer também na camada de enlace. Ao se transmitir informação sem criptografia em redes sem-fio, qualquer indivíduo pode ter acesso a ela.
*Modos de segurança sem criptografia

Ameaça / Protocolo	Key Cracking	Eavesdropping	Replay	Man-in-the-Middle	Jamming Físico	Jamming Enlace	MAC Spoofing	Outros DOS
WiFi	X	X*	X	X	X	X	X	X
Bluetooth	X	X*	X	X	X		X	X
IEEE 802.15.4		X*		X*	X	X		X
RFID e NFC		X*	X	X	X			X

Tabela 5.2: Principais ataques que podem ser explorados em cada protocolo nas camadas Física e de Enlace

5.2.2 Camada de Rede

Foram identificados na camada de rede diversos ataques comuns dentro do processo de roteamento. Os ataques DOS ganham especial relevância no ambiente de IdC pois visam esgotar a bateria dos dispositivos. Aplicar o IPv6 nesse ambiente é também uma tarefa complexa, que envolve a compressão e fragmentação e pode, consequentemente, dar espaço a ataques.

Protocolo \ Ameaça	Spoofing	Fragmentação	Wormhole	SinkHole	BlackHole	Selective Forward	Replay Attack	Eavesdropping	Sybil	Man-in-the-Middle
ZigBee				X	X	X		X	X	
WirelessHART			X	X	X	X		X	X	
ISA 100.11			X	X	X	X		X		
6loWPAN	X	X					X	X		X
RPL				X	X	X				

Tabela 5.3: Principais ataques que podem ser explorados em cada protocolo na camada de Rede

5.2.3 Camada de Transporte

Nesse trabalho, o DTLS foi colocado na camada de transporte, apesar do mesmo ser uma adaptação para segurança entre as camadas de aplicação e de transporte. Consideram-se, então, como vulnerabilidades da camada de transporte as vulnerabilidades do DTLS, visto que a maioria dos protocolos da camada de aplicação aqui citados fazem uso do mesmo, visando a segurança fim-a-fim no processo de comunicação. Por utilizar o UDP, as vulnerabilidades relacionadas ao UDP mencionadas no trabalho também foram colocadas nesta tabela, que apenas lista tais vulnerabilidades.

DTLS				
SSL Stripping	Injeção de Comandos		BEAST	Padding Oracle
RC4	CRIME	TIME	Breach	Certificado e RSA
Roubo de Chaves do RSA	Parâmetros Diffie-Hellman			Renegociação
Handshake Triplo	Confusão de Hospedeiro Virtual		Problema de Implementação	
Problema de Usabilidade	UDP Flooding			DOS

Tabela 5.4: Principais ataques que podem ser explorados na camada de transporte

5.2.4 Camada de Aplicação

Dos protocolos da camada de aplicação, poucos possuem segurança embutida como padrão. A maioria se utiliza da segurança provida pelo DTLS. Cabe ao administrador da rede e desenvolvedores verificar a sensitividade dos dados e as restrições dos nós para

implementar corretamente a segurança. Também, manter fechadas as portas para o ambiente externo, principalmente portas que implementam o UPnP.

Vale ressaltar que as ameaças desta camada são mais relacionadas ao software da aplicação do que aos protocolos em si. Erros como: permitir que o usuário tente várias senhas, não verificar a entrada de dados e outros erros de implementação de interface - listados pela OWASP e descritos no Capítulo 2 - devem ser evitados a todo custo.

Segundo o que foi apresentado no Capítulo 3, os softwares da camada de aplicação devem fornecer ao usuário, de maneira clara, as configurações de privacidade, de modo que o mesmo saiba quais informações estão sendo transmitidas e possa escolher transmitilas ou não. Em seguida, os protocolos devem garantir, com a utilização de criptografia confiável e correta administração de chaves, que os dados serão resguardados.

* CoAP, MQTT, XMPP estão vulneráveis a certos ataques somente quando não utilizam DTLS.

Ameaça / Protocolo	Reflexão	Amplificação	Masquerading	Trashing
CoAP		X	X*	
MQTT			X*	X*
XMPP			X*	X*
UpNP	X	X		
DDS			X	X

Tabela 5.5: Principais ataques que podem ser explorados em cada protocolo na camada de Aplicação

Capítulo 6

Conclusão

O estudo apresentou os diversos componentes do paradigma de Internet das Coisas, tendo em vista as ameças trazidas para a garantia de segurança e privacidade. Nesse sentido, as diversas instituições e projetos envolvidos com segurança na IdC trazem recursos substanciais para que o crescimento da IdC ocorra de forma segura.

Em seguida, os diversos fatores relativos à privacidade mostram que é necessário que governos e sociedades, juntos, discutam pontos fundamentais para a regulamentação da privacidade, tendo em vista as novas características de um ambiente de IdC. Dada sua implementação em diversas áreas, tal processo envolve diversas análises, que vão desde a coleta, até o armazenamento e disponibilização da informação.

O presente estudo, ao abordar aspectos relevantes voltados para segurança em IdC, trouxe uma visão macro da importância que os protocolos existentes exercem para a eficácia e crescimento da IdC. Além disso, apontou as principais ameaças existentes e apresentou algumas sugestões para evitá-las. Foi possível, então, agrupar as ameças encontradas de cada protocolo em uma maneira, até onde pode se confirmar pelo autor, inovadora, visto que os dados dessa natureza encontram-se espalhados pela literatura.

6.1 Trabalhos Futuros

Percebe-se que as ameças identificadas são, em sua maioria, do tipo de negação de serviço e obtenção de dados, indevidamente, explorando-se as fragilidades do ambiente sem-fio e de dispositivos de baixo gasto computacional e energético. O fato dos dispositivos apresentarem essas características, os tornam vítimas mais vulneráveis, porém, acredita-se que, de igual modo, os tornam atacantes fracos para ataques distribuídos. Com isso, um possível estudo seria verificar o quão eficiente são os ataques DDOS por IdC se comparados aos métodos tradicionais.

O trabalho pode ser, no futuro, acrescido de novos protocolos, para uma análise comparativa mais ampla e também, com estudos que tratem as vulnerabilidades aqui citadas, com testes práticos e novas soluções. Espera-se, com isso, que o trabalho siga atualizado como referência para todos os envolvidos na implementação do ambiente de IdC de maneira segura.

Referências

[1] Akamai. SSDP Reflection DDOS Attacks. https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/ssdp-reflection-ddos-attacks-threat-advisory.pdf, 2014. Acesso em 29/06/2016. 66, 93

[2] Cristina Alcaraz e Javier Lopez. A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 40(4):419–428, 2010. 56, 57, 93

[3] Nikolaos Alexiou, Stylianos Basagiannis, e Sophia Petridou. Formal security analysis of near field communication using model checking. *Computers & Security*, 2016. 44

[4] Soroush Amidi. Wireless standards in action: A closer look at isa-100.11a. https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/2010/december/cover-story-wireless-standards-in-action/, 2010. Acesso em 19/05/2016. 57

[5] Yasmin M Amin, Amr T Abdel-hamid, e Senior Member. Classification and Analysis of IEEE 802.15.4 MAC Layer Attacks. In *11th International Conference on Innovations in Information Technology (IIT) Classification*, pages 74–79, Dubai, 2015. IEEE. 34, 41, 42, 92

[6] Ross Anderson. *Security Engineering*. Second edition, 2008. 18, 94, 95, 96, 97

[7] Kevin Ashton. That 'Internet of Things' thing. *The RFID Journal*, 2009. 2

[8] Luigi Atzori, Antonio Iera, e Giacomo Morabito. The Internet of Things: A survey. *Computer Networks*, 54(15):2787–2805, 2010. 2, 3

[9] Paolo Baronti, Prashant Pillai, Vince W C Chook, Stefano Chessa, Alberto Gotta, e Y. Fun Hu. Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. *Computer Communications*, 30(7):1655–1695, 2006. 4

[10] Tal Be'ery e Amichai Shulman. A Perfect CRIME? Only TIME Will Tell, 2013. 60

[11] B Bellalta, L Bononi, R Bruno, e A Kassler. Next generation IEEE 802.11 Wireless Local Area Networks: Current status, future directions and open challenges. *Computer Communications*, 75:1–25, 2015. 31

[12] Monika Bhalla, Nitin Pandey, e Brijesh Kumar. Security Protocols for Wireless Sensor Networks. *International Conference on Green Computing and Internet of Things (ICGCIoT)*, pages 1005–1009, 2015. 52

[13] Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Alfredo Pironti, e Pierre Yves Strub. Triple handshakes and cookie cutters: Breaking and fixing authentication over TLS. *Proceedings - IEEE Symposium on Security and Privacy*, pages 98–113, 2014. 60

[14] Ronak Bhojani e Rutvij Joshi. An Integrated Approach for Jammer Detection using Software Defined Radio. In *7th International Conference on Communication, Computing and Virtualization*, volume 79, pages 809–816, Gujarat, India Abstract, 2016. Elsevier. 33, 70, 92

[15] Bastian Bloessl, Christoph Sommer, Falko Dressier, e David Eckhoff. The scrambler attack: A robust physical layer attack on location privacy in vehicular networks. *2015 International Conference on Computing, Networking and Communications, ICNC 2015*, pages 395–400, 2015. 34, 92

[16] Bluetooth SIG. Bluetooth Core Specification. `https://www.bluetooth.com/specifications/bluetooth-core-specification`. Acesso em 20/06/2016. 36

[17] Bluetooth SIG. Our History. `https://www.bluetooth.com/media/our-history`. Acesso em 18/05/2016. 35

[18] Abhijit Bodhe, Mayur Masuti, e A. S. Umesh. Wireless LAN Security Attacks and CCM Protocol with some best practices in Deployment of Services. *International Research Journal of Engineering and Technology (IRJET)*, 3(1):429–436, 2016. 32

[19] Eleonora Borgia. The internet of things vision: Key features, applications and open issues. *Computer Communications*, 54:1–31, 2014. 2

[20] Bormann, Carsten. Coap Technology. `http://coap.technology/`, 2011. Acesso em 15/05/2016. 61

[21] Chad Brubaker, Suman Jana, Baishakhi Ray, Sarfraz Khurshid, e Vitaly Shmatikov. Using frankencerts for automated adversarial testing of certificate validation in SSL/TLS implementations. *Proceedings - IEEE Symposium on Security and Privacy*, pages 114–129, 2014. 60

[22] Xavier Caron, Rachelle Bosua, Sean B Maynard, e Atif Ahmad. The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. *Computer Law & Security Review*, 32(1):1–12, 2015. 18, 20, 24

[23] Sudeesh Chouhan e Sumit Sharma. A survey on de-authentication DOS Attack. *International Journal of Engineering, Management & Medical Research (IJEMMR)*, 2(3), 2016. 33, 34, 70, 92

[24] Delphine Christin, Parag S. Mogre, e Matthias Hollick. Survey on Wireless Sensor Network Technologies for Industrial Automation: The Security and Quality of Service Perspectives. *Future Internet*, 2(2):96–125, 2010. 55, 56

[25] Cisco. 802.11 Security Summary. In *Wireless and Network Security Integration Solution Design Guide*, chapter 3, pages 1–20. Cisco Systems, 2008. 32

[26] Luigi Coppolino, Valerio DAlessandro, Salvatore DAntonio, Leonid Levy, e Luigi Romano. My Smart Home is Under Attack. In *IEEE 18th International Conference on Computational Science and Engineering*, pages 145–151, Porto, 2015. IEEE. 54, 93

[27] Das, Kaushik. Internet Engineering Task Force (IETF) History. `http://ipv6.com/articles/organizations/IETF-History-IPv6.htm`. Acesso em 13/06/2016. 29

[28] Flávia Lacerda Oliveira de Macedo. *Arquitetura da Informação Pervasiva: projetos de ecossistemas de informação na Internet das Coisas*. Tese (Doutorado), Universidade de Brasília, 2015. 1

[29] Antoine Delignat-Lavaud e Karthikeyan Bhargavan. Virtual Host Confusion: Weaknesses and Exploits, 2014. 60

[30] Aaron E Earle. *Wireless Security Handbook*. 2006. 33

[31] Christian Esposito e Mario Ciampi. On Security in Publish / Subscribe Services : A Survey. *IEEE Communications Surveys & Tutorials*, 17(2):966–997, 2015. 68, 69, 73, 93

[32] Roy Fisher e Gerhard Hancke. DTLS for lightweight secure data streaming in the internet of things. *Journal of Digital Information Management*, 13(4):247–255, 2015. 58, 59

[33] G1. Polícia prende representante do Facebook na América do Sul em SP. `http://g1.globo.com/sao-paulo/noticia/2016/03/policia-prende-representante-do-facebook-na-america-do-sul-em-sp.html`. Acesso em 15/04/2016. 19

[34] Gartner. Gartner Says 6.4 Billion Connected "Things"Will Be in Use in 2016, Up 30 Percent From 2015. `http://www.gartner.com/newsroom/id/3165317`. Acesso em 07/05/2016. 1

[35] Jorge Granjal, Edmundo Monteiro, e Jorge Sa Silva. Security for the internet of things: A survey of existing protocols and open research issues. *IEEE Communications Surveys and Tutorials*, 17(3):1294–1312, 2015. 28, 40, 41, 42, 48, 50, 59, 61, 62, 72, 92, 93

[36] Andy Greenberd. Hackers Remotely Kill a Jeep on the Highway—With Me in It. *Wired.com*. Acesso em 01/05/2016. 5

[37] Glenn Greenwald. Why privacy matters. *TED Talks*, 2014. 19

[38] Iakovos Gurulian, Carlton Shepherd, Konstantinos Markantonakis, e Raja Naeem. When Theory and Reality Collide : Demystifying the Effectiveness of Ambient Sensing for NFC-based. 2016. 45

[39] Avinatan Hassidim, Yossi Matias, Moti Yung, e Alon Ziv. Ephemeral Identifiers : Mitigating Tracking & Spoofing Threats to BLE Beacons. pages 1–11, 2016. 39, 92

[40] Stacey Higginbotham e Joshua Corman. Podcast - Episode 2: Is it too late to secure the internet of things?, 2015. Acesso em 10/04/2016. 14

[41] HiveMQ Enterprise MQTT Broker. MQTT Essentials Part2: Publish & Subscribe. `http://www.hivemq.com/blog/mqtt-essentials-part2-publish-subscribe`. Acesso em 23/06/2016. 63, 64

[42] David Hopwood. Lack of security in Internet of Things devices. *Network Security*, 2014(8):2, 2014. 11

[43] Yih-Chun Hu Yih-Chun Hu, a. Perrig, e D.B. Johnson. Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):370–380, 2006. 51, 72

[44] I am the Cavalry. I am the Cavalry, 2014. Acesso em 07/04/2016. 14

[45] IDC. Competing and Leading in the New IT Market - 11 Numbers You Need to Know. 2016. 1

[46] IEEE. How are Standards made? `https://standards.ieee.org/develop/process.html`. Acesso em 18/06/2016. 29

[47] IEEE. IEEE TG4 Working Group. `http://www.ieee802.org/15/pub/TG4.html`. Acesso em 11/05/2016. 40

[48] IEEE Standards Association. Guidelines for 64-bit Global Identifier (EUI-64) General, 2010. 40

[49] IETF. IPv6 over the TSCH mode of IEEE 802.15.4e (6tisch). `https://datatracker.ietf.org/wg/6tisch/charter/`, 2011. Acesso em 18/05/2016. 40, 48

[50] InfoSec Institute. Near Field Communication (NFC) Technology, Vulnerabilities and Principal Attack Schema. http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/. Acesso em 21/06/2016. 45, 92

[51] National Instruments. What Is a Wireless Sensor Network? 2015(December):5–7, 2012. 4

[52] International Standard ISO/IEC 20922. Information technology — Message Queuing Telemetry Transport (MQTT) v3.1.1. `http://www.iso.org/iso/catalogue_detail.htm?csnumber=69466`, 2016. Acesso em 09/06/2016. 63

[53] Isam Ishaq, David Carels, Girum Teklemariam, Jeroen Hoebeke, Floris Abeele, Eli Poorter, Ingrid Moerman, e Piet Demeester. *IETF Standardization in the Field of the Internet of Things (IoT): A Survey*, volume 2. 2013. 48, 50, 55

[54] Nurul Halimatul Asmak Ismail, Rosilah Hassan, e Khadijah W M Ghazali. A study on protocol stack in 6lowpan model. *Journal of Theoretical and Applied Information Technology*, 41(2):220–229, 2012. 46, 47

[55] ITU. The Internet of Things. *Itu Internet Report 2005*, page 212, 2005. 23, 24

[56] Zhao Jiantao e Huang Yunyi. The Design and Implementation of Core Function of XMPP-Based Mobile Push System. In *2nd International Conference on Electrical, Computer Engineering and Electronics (ICECEE 2015)*, pages 928–932, Jinan, 2015. Atlantis Press. 65

[57] Bhagyashri Katole, Manikanta Sivapala, e V Suresh. Principle Elements and Framework of Internet of Things. *International Journal Of Engineering And Science*, 3(5):24–29, 2013. 4

[58] Russel Kay. ZigBee. In *ComputerWorld - Knowledge Center Mobile & Wireless*, page 1. Worcester, 2006. 52, 53

[59] S. Kent e K. Seo. Security Architecture for the Internet Protocol. *RFC 4301*, 2005. 47

[60] Evgeny Khorov, Andrey Lyakhov, Alexander Krotov, e Andrey Guschin. A survey on IEEE 802.11ah: An enabling networking technology for smart cities. *Computer Communications*, 58(May 2014):53–69, 2015. 35

[61] Patrick Kinney. ZigBee Technology : Wireless Control that Simply Works. In *Communications Design Conference*, number October, pages 1–20, 2003. 54

[62] Kinichi Kitano e Shuji Yamamoto. Strong Security Measures Implemented in ISA100.11a Wireless System. Technical Report 2, Yokogawa, 2014. 57

[63] Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Br??nig, e Georg Carle. DTLS based security and two-way authentication for the Internet of Things. *Ad Hoc Networks*, 11(8):2710–2723, 2013. 58

[64] C. Lambrinoudakis e A. Gabillon. *Risks and Security of Internet and Systems: 10th International Conference, CRiSIS 2015, Mytilene, Lesbos Island, Greece, July 20-22, 2015, Revised Selected Papers*. Lecture Notes in Computer Science. Springer International Publishing, 2016. 56, 93

[65] Clare M. Lewandowski, New Co-investigator, e Clare M. Lewandowski. *Industrial Wireless Networking with Resource Constraint Devices*. Ph. d., University of Twente, 2015. 57

[66] Pengfei Li, Jiakun Li, Luhua Nie, e Bo Wang. Research and application of ZigBee protocol stack. *2010 International Conference on Measuring Technology and Mechatronics Automation, ICMTMA 2010*, 2:1031–1034, 2010. 52, 53

[67] Emerson Process Management. Wireless Security Whitepaper. Acesso em 20/06/2016, 2016. 56, 72

[68] C.X. Mavromoustakis, G. Mastorakis, e J.M. Batalla. *Internet of Things (IoT) in 5G Mobile Technologies*. Modeling and Optimization in Science and Technologies. Springer International Publishing, 2016. 56, 93

[69] Steve McQuerry. Wireless LANs: Extending the Reach of a LAN. In *Interconnecting Cisco Network Devices, Part 1 (ICND1): CCNA Exam 640-802 and ICND1 Exam 640-822*, chapter 3, pages 207–235. Pearson Education, Cisco Press, Indianapolis,Indiana, 2 edition, 2008. 31

[70] Faiza Medjek, Djamel Tandjaoui, Mohammed Riyadh Abdmeziem, e Nabil Djedjig. Analytical evaluation of the impacts of Sybil attacks against RPL under mobility. *12th International Symposium on Programming and Systems, ISPS 2015*, pages 13–21, 2015. 50, 72, 93

[71] Microsoft Corporation. Understanding UPnP. `www.upnp.org/download/UPNP_understandingUPNP.doc`, 2000. Acesso em 15/06/2016. 66

[72] Nateq Be-nazir Ibn Minar e Mohammed Tarique. Bluetooth Security Threats and Solutions: A Survey. *International Journal of Distributed and Parallel Systems (IJDPS)*, 3(1):127, 2012. 36, 37, 38, 92

[73] Aikaterini Mitrokotsa, Melanie R. Rieback, e Andrew S. Tanenbaum. Classifying rfid attacks and defenses. *Information Systems Frontiers*, 12(5):491–505, 2010. 44

[74] HD Moore. Security Flaws in Universal Plug and Play. *Rapid Server*, (January):0–28, 2013. 67, 93

[75] National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. `http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf`, 2007. Acesso em 08/08/2016. 97

[76] CBS News. FBI able to hack San Bernardino phone; Apple case to be dropped. http://www.cbsnews.com/news/fbi-hacks-iphone-san-bernardino-gunman-syed-farook-drops-case-against-apple. Acesso em 15/04/2016. 19

[77] NYTimes. San Bernardino Shooting Kills at Least 14; Two Suspects Are Dead. `www.nytimes.com/2015/12/03/us/san-bernardino-shooting.html`. Acessado em 15/04/2016. 19

[78] OMG. DDS Security. Technical Report June, Object Management Group OMG, 2014. 68

[79] OMG. Data Distribution Service (DDS). Technical Report April, Object Management Group OMG, 2015. 67

[80] OTA. Página Web. `https://https://otalliance.org`, 2004. Acesso em 14/04/2016. 17

[81] OTA Alliance. IoT Trustworthy Working Group (ITWG). `https://https://otalliance.org/initiatives/internet-things`, 2015. Acesso em 14/04/2016. 17

[82] G. Ottoy, T. Hamelinckx, B. Preneel, L. De Strycker, e J.P. Goemaere. On the choice of the appropriate AES data encryption method for ZigBee nodes. *SECURITY AND COMMUNICATION NETWORKS*, 9(22):87–93, 2016. 52, 53

[83] OWASP. OWASP Web Page. `https://www.owasp.org`, 2001. Acesso em 02/04/2016. 8

[84] OWASP. 2014 OWASP Project Handbook. `https://www.owasp.org/images/d/d8/PROJECT_LEADER-HANDBOOK_2014.pdf`, 2014. Acesso em 02/04/2016. 9

[85] Marcio OWASP; Serrão, Carlos; Machry. OWASP Top 10 - 2013: Os dez riscos de segurança mais críticos em aplicações web. Acesso em 02/04/2016. 9, 10

[86] Gerardo Pardo-castellote e Real-Time Innovations. OMG Data-Distribution Service: Architectural Overview. In *23 rd International Conference on Distributed Computing Systems Workshops (ICDCSW'03)*, pages 200–206. IEEE, 2003. 67

[87] Stig Petersen e Simon Carlsen. WirelessHART versus ISA100.11a: The format war hits the factory floor. *IEEE Industrial Electronics Magazine*, 5(4):23–34, 2011. 57

[88] Pavan Pongle e Gurunath Chavan. A survey: Attacks on RPL and 6LoWPAN in IoT. In *2015 International Conference on Pervasive Computing: Advance Communication Technology and Application for Society, ICPC 2015*, pages 1–6, Pune, 2015. IEEE. 48, 50, 51, 72, 93

[89] Reem Abdul Rahman e Babar Shah. Security analysis of IoT protocols: A focus in CoAP. In *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, pages 1–7. IEEE, 2016. 62

[90] Shahid Raza, Adriaan Slabbert, Thiemo Voigt, e Krister Landernäs. Security considerations for the wirelessHART protocol. *ETFA 2009 - 2009 IEEE Conference on Emerging Technologies and Factory Automation*, 2009. 56, 72

[91] Kay Romer e Friedemann Mattern. The Design Space of Wireless Sensor Networks. *IEEE Wireless Communications*, 11(6):28–39, 2004. 4

[92] K. Rose, S. Eldridge, e C. Lyman. The internet of things: an overview. *Internet Society*, (October):53, 2015. 6

[93] P. Saint-Andre. Extensible Messaging and Presence Protocol (XMPP): Core. *RFC 6120*, 2005. 64

[94] P. Saint-Andre e T. Alkemade. Use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP) Abstract. *RFC 7590*, pages 1–9, 2015. 65

[95] Schonwalder, Jurgen. Internet of Things: 802.15.4, 6LoWPAN, RPL, COAP, 2010. 40

[96] Priyanka Sharma, Puneet Kumar Kaushal, e Parth Rai Sharma. Survey on Evil Twin Attack. *International Journal of Scientific Engineering and Research (IJSER)*, 4(4):54–58, 2015. 34, 92

[97] Y. Sheffer, R. Holz, e P. Saint-Andre. Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS), 2015. 61

[98] Y. Sheffer, R. Holz, e P. Saint-Andre. Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS), 2015. 59

[99] Z Shelby, ARM, K Hartke, e C Bormann. The Constrained Application Protocol (CoAP). *RFC 7252*, 2014. 61, 62, 93

[100] Shubhangi A. Shinde, Pooja A. Nimkar, Shubhangi P. Singh, Vrushali D. Salpe, e Yogesh R. Jadhav. MQTT - Message queuing telemetry transport. *International Journal of Research*, 3(3):240–244, 2016. 63

[101] Karanpreet Singh, Paramvir Singh, e Krishan Kumar. A systematic review of IP traceback schemes for denial of service attacks. *Computers and Security*, 56:111–139, 2016. 47, 71, 93

[102] Meena Singh, M. A. Rajan, V. L. Shivraj, e P. Balamuralidhar. Secure MQTT for Internet of Things (IoT). In *Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*, pages 746–751, Gwalior, 2015. IEEE. 64

[103] Radosveta Sokullu, Ilker Korkmaz, Orhan Dagdeviren, Anelia Mitseva, e Neeli R Prasad. An investigation on IEEE 802.15. 4 MAC layer attacks. In *Proc. of WPMC*, 2007. 41, 42, 92

[104] Jianping Song, Song Han, Aloysius K. Mok, Deji Chen, Mike Lucas, Mark Nixon, e Wally Pratt. WirelessHART: Applying wireless technology in real-time industrial process control. In *Proceedings of the IEEE Real-Time and Embedded Technology and Applications Symposium, RTAS*, pages 377–386, St. Louis, MO, 2008. IEEE. 55

[105] Stanford. Rethinking a Secure Internet of Things. *SITP*, pages 1–6, 2015. Acesso em 14/04/2016. 17

[106] Andy Stanford-Clark e Hong Linh Truong. MQTT For Sensor Networks (MQTT-SN) - Version 1.2 - Protocol Specification, 2013. 63

[107] Mark Stanislav e Zach Lanier. The Internet of Fails - Where IoT Has Gone Wrong. `http://sector.ca/Program/Sessions/Session-Details/the-internet-of-fails-where-iot-has-gone-wrong-and-how-were-making-it-right`, 2014. Acesso em 09/04/2016. 15

[108] Darlene Storm. Researchers hack a pacemaker, kill a man (nequin). *Computer World*. Acesso em 01/05/2016. 6

[109] Emily Tabatabai, Shea Gordon Leitch, Amy Pasacreta, e Matthew Fechik. Privacy policies and the sale of corporate assets: It pays to plan ahead to preserve the value of your data assets. http://blogs.orrick.com/trustanchor/2015/10/20/privacy-policies-and-the-sale-of-corporate-assets-it-pays-to-plan-ahead-to-preserve-the-value-of-your-data-assets/. Acesso em 23/04/2016. 25

[110] Pratiksha Thakur, Rajan Patel, e Nimisha Patel. A Proposed Framework for Protection of Identity Based Attack in Zigbee. In *2015 Fifth International Conference on Communication Systems and Network Technologies*, pages 628–632, Gwalior, 2015. IEEE. 54, 93

[111] James Thrasher. RFID vs. NFC: What's the Difference? `http://blog.atlasrfidstore.com/rfid-vs-nfc`. Acesso em 19/05/2016. 44

[112] UOL. Justiça determina bloqueio do WhatsApp em todo o Brasil por 48 horas. `http://www1.folha.uol.com.br/mercado/2015/12/1719934-justica-determina-bloqueio-do-whatsapp-em-todo-brasil-por-48-horas.shtml`. Acesso em 15/04/2016. 19

[113] J P Vasseur, Navneet Agarwal, Jonathan Hui, Zach Shelby, Paul Bertrand, e Cedric Chauvenet. RPL: The IP routing protocol designed for low power and lossy networks. *In Internet Protocol for Smart Objects (IPSO) Alliance*, (April):20, 2011. 49

[114] Verizon. 2013 Data breach investigations Report. pages 1–62, 2013. Acesso em 12/04/2016. 11

[115] Saniya Vohra e Rohit Srivastava. A survey on techniques for securing 6LoWPAN. *Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*, pages 643–647, 2015. 48, 93

[116] Common Vulnerabilities e Exposures. CVE-2015-6409, 2015. 65

[117] Md Waliullah, A B M Moniruzzaman, e Md. Sadekur Rahman. An Experimental Study Analysis of Security Attacks at IEEE 802 . 11 Wireless Local Area Network. *International Journal of Future Generation Communication and Networking*, 8(1):9–18, 2015. 34, 92

[118] Gengyun Wang. *Comparison and Evaluation of Industrial Wireless Sensor Network Standards ISA100.11a and WirelessHART*. Master, CHALMERS UNIVERSITY OF TECHNOLOGY, 2011. 57

[119] Rolf H. Weber. Internet of things – Need for a new legal environment? *Computer Law & Security Review*, 25(6):522–527, 2009. 25

[120] Rolf H. Weber. Internet of things: Privacy issues revisited. *Computer Law and Security Review*, 31(5):618–627, 2015. 23, 25

[121] Ou Wenxing, Wang Lei, Zhang Yu, e Yu Changhong. Research on Anti-eavesdropping Communication Mechanism for NFC. *2015 Seventh International Conference on Measuring Technology and Mechatronics Automation*, pages 839–841, 2015. 45

[122] Wikileaks. Página Web. `http://wikileaks.info`. Acesso em 17/05/2016. 20

[123] T Winter, P Thuber, B Brandt, et al. Ipv6 routing protocol for low-power and lossy networks. *RFC 6550*, 2008. 48

[124] Wired.com. The Apple-FBI Fight Isn't About Privacy vs. Security. Don't Be Misled. `http://www.wired.com/2016/02/apple-fbi-privacy-security/`. Acesso em 17/04/2016. 20

[125] Luis Carlos Wong. An Overview of 802.11 Wireless Network Security Standards & Mechanisms, 2005. 31, 32, 92

[126] Azam Zavvari e Ahmed Patel. Critical Evaluation of RFID Security Protocols. *International Journal of Information Security and Privacy*, 6(3):56–74, 2012. 43, 92

[127] Zhang, Veo. High-Profile Mobile Apps At Risk Due to Three-Year-Old Vulnerability. `http://blog.trendmicro.com/trendlabs-security-intelligence/high-profile-mobile-apps-at-risk-due-to-three-year-old-vulnerability/`, 2015. Acesso em 16/06/2016. 67, 73, 93

[128] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, e Klaus Wehrle. Privacy in the internet of things: Threats and challenges. *Security and Communication Networks*, 7(12):2728–2742, 2014. 20, 21, 22, 23

[129] Tobias Zillner. ZigBee Exploited - The Good, the Bad and the Ugly. *Cognosec*, 16(2):6, 2015. 54, 93

[130] Yulong Zou, Xianbin Wang, e Lajos Hanzo. A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends. *CoRR*, pages 1–31, 2016. 36, 37, 58, 92

Apêndice A

Referência para a marcação das Tabelas

Ameaça / Protocolo	Key Cracking	Eavesdropping	Replay	Man-in-the-Middle	Jamming Físico	Jamming Enlace	MAC Spoofing	Outros DOS
WiFi	[117]	[130][15]	[117]	[96]	[130][14][23]	[5]	[125] [117]	[96]
Bluetooth	[72]	[130][72]	[39]	[72]	[130]		[72]	[72]
IEEE 802.15.4		[35]		[5]	[130]	[5]		[5][103]
RFID e NFC		[50]	[126]	[126]	[50]			[126]

Tabela A.1: Referências utilizadas para a marcação dos principais ataques que podem ser explorados em cada protocolo nas camadas Física e de Enlace

Ameaça / Protocolo	Spoofing	Fragmentação	Wormhole	SinkHole	BlackHole	Selective Forward	Replay Attack	Eavesdropping	Sybil	Man-in-the-Middle
ZigBee				[26]	[2]	[2]		[129]	[110]	
WirelessHART			[68][2]	[68][2]	[68][2]	[68][2]		[2]	[64][2]	
ISA 100.11			[2]	[2]	[2]	[2]		[2]		
6loWPAN	[88][101] [115]	[35]					[35]	[88]		[88]
RPL				[88][70]	[88][70]	[88][70]				

Tabela A.2: Referências utilizadas para a marcação dos principais ataques que podem ser explorados em cada protocolo na camada de Rede

Ameaça / Protocolo	Reflexão	Amplificação	Masquerading	Trashing
CoAP		[99]	[99]	
MQTT			[31]	[31]
XMPP			[31]	[31]
UpNP	[1][127][74]	[1][127][74]		
DDS			[31]	[31]

Tabela A.3: Principais ataques que podem ser explorados em cada protocolo na camada de Aplicação

Apêndice B

AES

Um dos algoritmos de criptografia mais aceitos na atualidade é o *Advanced Encryption Standard* (AES), também conhecido por Rijndael, referenciando seus inventores Vincent Rijmen e Joan Daemen. Esse algoritmo foi escolhido dentre outros como o Serpent, Twofish, RC6 e MARS, na conferência AES que o definiu como o novo padrão a ser utilizado para criptografia. O AES foi ratificado pela National Institute of Standards and Technology (NIST) e é utilizado amplamente pelo governo americano e agências como a NSA.[6, p. 153-154]

O AES utiliza da técnica criptográfica de cifras de blocos, onde a mensagem a ser criptografada é separada em blocos de tamanho fixo. A mensagem passa por transformações designadas por uma chave simétrica, na qual, para cada chave deve-se existir uma única permutação, que é independente de todas as outras. Esse modelo traz tanto a *confusão*, ao se misturar a mensagem com uma chave que é desconhecida, como *difusão*, ao espalhar a mensagem pelo texto cifrado. Uma das formas de se estipular um bom cifrador de blocos é pela sucessiva aplicação de permutações e substituições. As primeiras aplicações dessa técnica eram feitas em redes, em que os circuitos que as formam eram combinados por substituições e permutações, logo, ficaram conhecidas como redes-SP.[6]

Ross Anderson[6] elicita características que influenciam a eficiência da criptografia por redes-SP: (1) Tamanho dos Blocos: quanto menor forem os blocos, mais fácil é para um atacante realizar *ataques de dicionário*, em que, para cada mensagem cifrada, relaciona-se a mensagem em texto simples para descobrir como é feito o relacionamento entre elas. Com blocos maiores, é probabilisticamente menos provável que se encontrem relações. (2) Número de rodadas: é importante que hajam suficientes permutações para que se dificulte o processo de relacionamento entre uma mudança na entrada com mudanças na saída. (3) Escolha das caixas de substituição: a escolha das operações que são realizadas entre os bits de entrada e saída das caixas de substituição são importantes, pois uma má escolha reduz a randomização da saída, por exemplo, mapear o bit 1 para a saída

1 e colocar duas caixas com essa operação sucessivamente, não gera randomização. (4) Criptoanálise Linear: de acordo com a teoria da probabilidade, se é possível encontrar relacionamentos algébricos lineares entre os bits de entrada e saída em todo o cifrador com uma probabilidade de p = 0.5 + 1/M, é possível recuperar bits da chave utilizada a partir de M^2 textos conhecidos. (5) Criptoanálise Diferencial: assim como a linear, busca estabelecer o relacionamento entre a entrada e a saída, porém pela verificação da probabilidade de mudanças na entrada gerarem mudanças específicas na saída, por exemplo, ao se mudar os bits 1, 3 e 5, alteram-se os bits 9 e 2, com uma probabilidade de 9/14.

Haja vista das características apresentadas, o AES é definido como um cifrador de bloco SP, que utiliza blocos de 128 bits e chaves de 128, 192 e 256bits. São utilizadas 10 rodadas para chaves de 128bits, 12 para 192bits e 14 para 256bits.

B.1 Encadeamento de Blocos

Mais importante do que o algoritmo de criptografia em si é como este é utilizado.[6] Um fator importante é a escolha do modo de operação, que define como cifras de bloco de tamanho fixo (16 bytes para o AES, por exemplo) podem ser utilizadas para mensagens maiores.[6, p. 160] Entre os principais modos de operação estão: (1) ECB, (2) CBC, (3) OFB, (4) CFB, (5) CTR, (6) MAC e (7) Modos Compostos.

B.1.1 ECB - Electronic Code Book

No modo ECB, cada bloco do texto a ser criptografado é colocado diretamente num bloco de cifra para se obter o texto cifrado. Logo, blocos do texto que são iguais, geram a mesma mensagem criptografada. Para operações simples, pode ser utilizado, porém, para dados redundantes, determinado padrão acaba sendo percebido, revelando informações da mensagem além de permitir adulterações de partes da mensagem criptografada com um intuito específico.[6]

B.1.2 CBC - Cipher Block Chaining

A maioria das aplicações comerciais utilizam do encadeamento de blocos para a criptografia. Essa técnica consiste em aplicar operações de XOR do texto criptografado no bloco anterior com o bloco de mensagem a ser criptografado em seguida. Desta forma, não há mais como haver um padrão pré estabelecido, visto que cada parte da mensagem depende da criptografia da parte anterior, gerando uma confusão na mensagem final. Como no

primeiro bloco de mensagem ainda não há um texto criptografado anteriormente, utiliza-se um Vetor de Inicialização para a operação de XOR. Esse número deve ser randômico, de modo a garantir que mensagens com um estereótipo padrão não sejam criptografadas em blocos de texto cifrado iguais.[6]

B.1.3 OFB - Output Feedback

No modo OFB, busca-se um funcionamento do cifrador de bloco de acordo com o modelo cifrador de stream. O Vetor de Inicialização (VI) passa pelo cifrador de bloco, gerando um bloco de texto criptografado. Este bloco gerado passa por uma operação de XOR com o bloco de mensagem, produzindo a mensagem criptografada. O mesmo bloco serve também de entrada para o próximo bloco cifrador e assim em diante. Dessa forma, após a execução, percebe-se que foi gerada uma grande chave (do tamanho da mensagem a ser criptografada) a qual adiciona-se a mensagem, para gerar o texto criptografado final, assim como ocorre em um cifrador de stream.[6]

B.1.4 CFB - Cipher Feedback

O modo CFB, busca também um funcionamento similar ao cifrador de stream, porém com uma sincronização. Esta permite recuperar parte da mensagem mesmo que alguns bits tenham se perdido durante a transmissão. Este modelo foi bastante utilizado por militares em rádios, que possuíam taxas de perda, logo, combinava-se criptografia com recuperação de erros. Com o barateamento de materiais eletrônicos, esse processo é realizado por protocolos a nível de enlace, não sendo mais necessário ser operado em conjunto com a criptografia.[6]

B.1.5 CTR - Counter

Outro que funciona como um cifrador de stream, porém, diferentemente dos modos que utilizam do valor anterior para produzir a próxima chave, o modo CTR apresenta um maior paralelismo, por ser independente dos valores passados. Esse modo funciona utilizando-se um número inicial de entrada, no primeiro bloco cifrador e, para cada bloco seguinte, adiciona-se um valor a esse número para ser a nova entrada. Desta forma, cada bloco cifrador produzirá um texto diferente, que será adicionado à mensagem para gerar a mensagem criptografada.

B.1.6 MAC - Message Authentication Code

"O modo MAC, não visa proteger a mensagem, porém proteger sua integridade e autenticidade" [6, p. 163] Nesse modelo, os cifradores de bloco são organizados segundo o modo CBC, porém descartam-se todos os blocos de mensagem criptografada com exceção do último, que é o MAC. Desta forma, é possível verificar a autenticidade de uma mensagem verificando se o último bloco do texto cifrado gerado corresponde ao MAC associado. Existem outras formas de se calcular o MAC em uma mensagem. Deve-se tomar cuidado com o termo MAC, que possui diversos significados no contexto de computação. Muitas vezes o código calculado é tratado como MIC (Message Integrity Code), para se evitar a ambiguidade.

B.1.7 Modos Compostos

Muitas vezes necessita-se não somente de confidencialidade, mas também de integridade da mensagem. Para isso, são utilizados diferentes modos em conjunto. Um modo composto é o CCM (Counter with CBC MAC), que combina o modo CTR com o CBC-MAC. Outro modo composto, o GCM (Galois Counter Mode), desenvolvido para ser utilizado paralelamente, utiliza do conceito de contador para a confidencialidade e de um mecanismo de autenticação chamado GHASH, que "traz a multiplicação por um parâmetro fixo, chamado de sub-chave hash, com um campo de Galois binário"[p. 9-10][75]