UNIVERSIDADE FEDERAL FLUMINENSE

Hytálo Prates Laipelt Benaventana

Internet das Coisas: Questões de Segurança e Ataques Relacionados à Radiofrequências

Niterói

2022

Hytálo Prates Laipelt Benaventana

Internet das Coisas: Questões de Segurança e Ataques Relacionados à Radiofrequências

Trabalho de Conclusão de Curso submetido ao Curso de Tecnologia em Sistemas de Computação da Universidade Federal Fluminense como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Computação.

Orientador:
Nilson Luís Damasceno

NITERÓI
2022

Ficha catalográfica automática - SDC/BEE
Gerada com informações fornecidas pelo autor

B456i Benaventana, Hytálo Prates Laipelt
Internet das Coisas: Questões de Segurança e Ataques Relacio-nados à Radiofrequências / Hytálo Prates Laipelt Benaventana ; Nilson Luís Damasceno, orientador. Niterói, 2022.
50 f. : il.

Trabalho de Conclusão de Curso (Graduação em Tecnologia de Sistemas de Computação)-Universidade Federal Fluminense, Instituto de Computação, Niterói, 2022.

1. Internet das coisas. 2. Segurança da informação. 3. Produção intelectual. I. Damasceno, Nilson Luís, orientador. II. Universidade Federal Fluminense. Instituto de Computação. III. Título.

CDD -

Bibliotecário responsável: Debora do Nascimento - CRB7/6368

Hytálo Prates Laipelt Benaventana

Internet das Coisas: Questões de Segurança e Ataques Relacionados à Radiofrequência

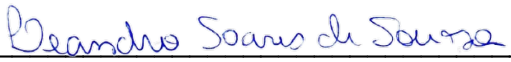
Trabalho de Conclusão de Curso submetido ao Curso de Tecnologia em Sistemas de Computação da Universidade Federal Fluminense como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Computação.

Niterói, 24 de junho de 2022.

Banca Examinadora:

Professor Nilson Luís Damasceno, MSc. - Orientador

UFF - Universidade Federal Fluminense



Professor Leandro Soares de Sousa, DSc. - Avaliador

UFF - Universidade Federal Fluminense

Dedico este trabalho a minha família e a todos que prestaram suporte durante a minha vida acadêmica.

AGRADECIMENTOS

A minha mãe por todo esforço prestado na conclusão da minha vida acadêmica.

Ao meu Orientador Nilson Luís Damasceno por todo esforço e ensinamentos diversos durante tão pouco tempo.

Aos Colegas de curso pelo incentivo e troca de experiências.

“Nós só podemos ver um pouco do futuro, mas o suficiente para ver que há muito a fazer”.

Alan Turing

RESUMO

A evolução da tecnologia vem permitindo a utilização de computadores miniaturizados nos mais diversos objetos ou “coisas”. Essa mesma evolução também possibilita que esses objetos computadorizados, chamados de dispositivos, sejam conectados à Internet, dando origem ao termo Internet das Coisas (*Internet of Things* - IoT). Contudo, essa conexão à Internet pode deixar esses dispositivos expostos a ações à distância de pessoas mal-intencionadas. Este trabalho apresenta questões de segurança presentes em sistemas de IoT com ênfase em vulnerabilidades que podem permitir ataques perpetrados por terceiros. O trabalho é o resultado de um estudo concebido para identificar vários ataques às tecnologias que dão suporte a sistemas de IoT. Mais especificamente, o estudo identifica 66 ataques a tecnologias relacionadas a IoT, sendo 48 deles ataques relacionados a protocolos de comunicação que utilizam radiofrequência.

Palavras-chaves: segurança em redes, ataques, Internet of Things, IoT.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ARPA - Advanced Research Projects Agency

BLE - Bluetooth Low Energy

DoS - *Denial of Service*

DDoS - *Distributed Denial of Service*

IA - Inteligência Artificial

IoT - *Internet of Things*

M2M - *Machine to Machine*

NFC – *Near Field Communication*

RFID - Radio-Frequency Identification

SCM - *Supply chain management*

WSN – Wireless Sensor Network

SUMÁRIO

1 INTRODUÇÃO

O conceito de *Internet of Things* (IoT) emerge da capacidade de acoplar um computador miniaturizado a uma “coisa” (*Thing*), um objeto do mundo real, e conectá-lo a Internet [1]. Essa junção agrega novas funcionalidades ao objeto, oferecendo, porém, uma capacidade de processamento reduzida, dada a natureza miniaturizada do computador. Por esse motivo, os equipamentos IoT, chamados de dispositivos neste trabalho, usualmente se comunicam com computadores de ou com maior capacidade para processar os dados que podem produzir.

Os dispositivos de IoT comumente estão aptos a receber informações através de sensores e tomar ações através de atuadores, como: pistão, válvula, monitor, etc. [2]. Esses sensores e atuadores estão conectados a uma rede de dispositivos e possivelmente à Internet. A estrutura de rede permite que os diversos dispositivos possam ser controlados remotamente. Porém, o benefício obtido ao utilizar IoT para implementar sistemas, toma para si as vulnerabilidades de tecnologias usadas na implementação [3].

Este trabalho tem como objetivo apresentar diversos ataques às soluções de tecnologia que dão suporte a sistemas relacionados a Internet das Coisas (IoT), com foco em transmissão via radiofrequência. Para alcançar esse objetivo, foi elaborado um estudo sobre IoT, incluindo seus campos de atuação, tecnologias que dão suporte a sua implementação e questões de segurança relacionadas a essas tecnologias. O estudo foi realizado através de análise de 219 artigos científicos recentes envolvendo IoT, dos quais foram selecionados aqueles que discorriam consistentemente sobre questões de segurança. Para complementar o estudo e fundamentar conceitos básicos, também foram utilizadas bibliografias consagradas juntamente com informações colhidas na Internet.

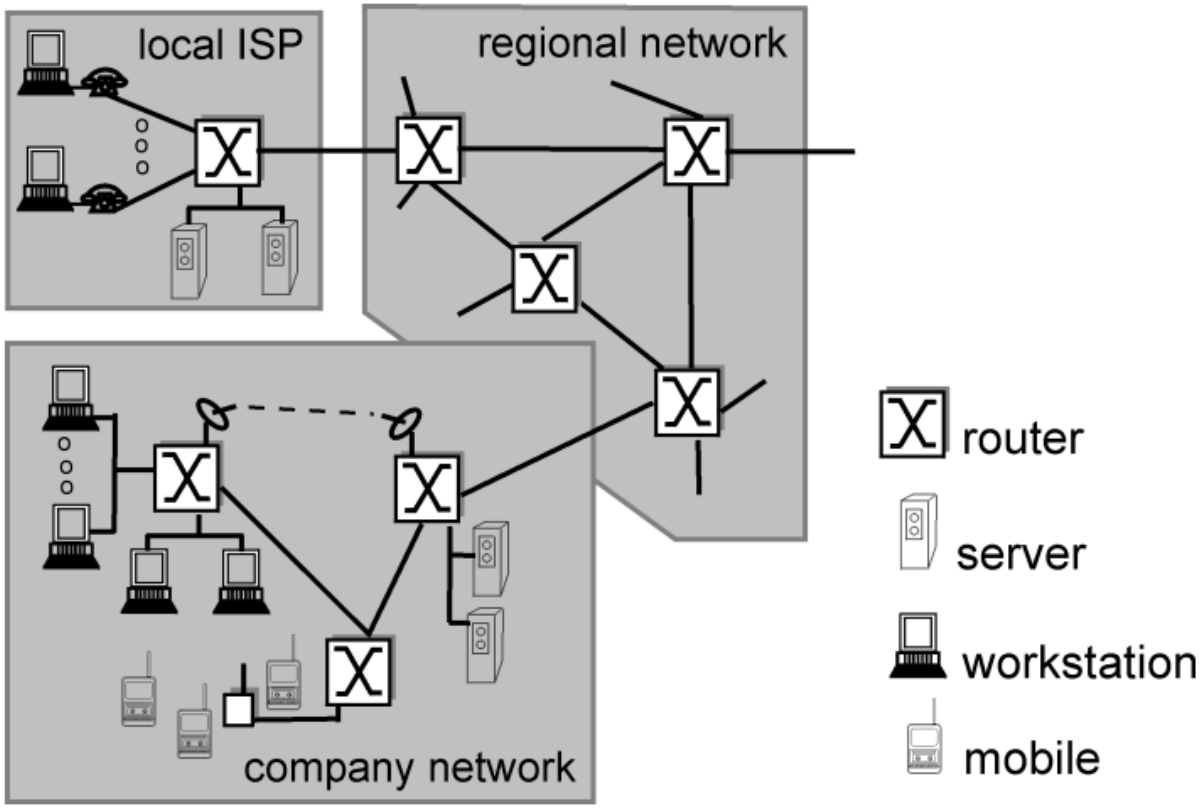
Este trabalho está organizado como descrito a seguir. O Capítulo 2 apresenta os conceitos fundamentais para o entendimento de IoT. O Capítulo 3 descreve o método de pesquisa utilizado para a realização do estudo. O Capítulo 4 apresenta

os ataques conhecidos a computares em rede, questões de segurança envolvendo softwares e outras estratégias conhecidas de ataque. O Capítulo 5 relaciona as questões de segurança envolvendo radiofrequência. O Capítulo 6 apresenta a conclusão do trabalho, incluindo oportunidades para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta uma série de conceitos necessários para compreender Internet das coisas (IoT) e Redes de computadores. O capítulo está dividido em 3 seções. A Seção 2.1 apresenta conceitos básicos de redes. A Seção 2.2 apresenta conceitos básicos sobre segurança em redes. Por fim, a Seção 2.3 discorre sobre o conceito de Internet das Coisas (IoT) e explora diversas possibilidades de utilização.

Figura 1 – Esquema do funcionamento de redes



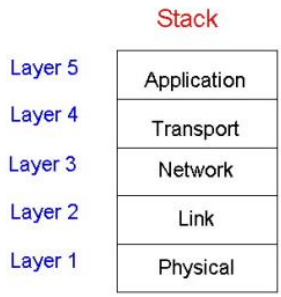
Fonte: Kurose e Ross [4]

2.1 REDES DE COMPUTADORES

Segundo Kurose e Ross [4], redes de computadores podem ser definidas como computadores que estão capacitados de se comunicar entre si através de uma infraestrutura de *hardware e software*. A Internet é um exemplo de rede global de computadores no qual diferentes aplicações podem se comunicar, trocando dados e informações diversas. Na Figura 1 são apresentados alguns componentes de *hardware* necessários para que os dados sejam transportados e a comunicação se desenvolva, como: roteadores, switch, etc. Esses componentes, juntos com as máquinas dos usuários e servidores, fazem parte do conjunto de elementos que constituem uma rede de computadores.

As arquiteturas de rede determinam como ocorre o fluxo de comunicação entre os elementos da rede [4]. Em particular, a Internet é uma rede que possui uma arquitetura baseada em camadas, onde uma camada provê serviços de comunicação para a camada adjacente. A Figura 2 ilustra a ordem de camadas utilizada pela Internet: Camada de Aplicação (*Application*), Camada de Transporte (*Transport*), Camada de Rede (*Network*), Camada de Enlace (*Link*) e Camada Física (*Physical)*.

Figura 2 - Arquitetura em camadas



Fonte: Kurose e Ross [4]

Para que a comunicação entre os elementos da rede ocorra também é necessário estabelecer, pelo lado do *software,* diversas regras de comunicação, chamadas de “protocolos”, como: TCP, UDP, IP, SMTP, etc. Os protocolos de rede têm como objetivo padronizar alguma etapa da comunicação, cumprindo uma de-

terminada função [4]. Existem diversos protocolos de rede, sendo os mais conhecidos aqueles que auxiliam na operação da Internet e dos serviços oferecidos por ela.

Numa arquitetura de redes, como a Internet, cada protocolo está vinculado à uma camada da rede. Na Camada de Aplicação encontram-se os protocolos HTTP (web), SMTP *(envio de e-mails)* e FTP (troca de arquivos). Já na Camada de Transporte, estão definidos os protocolos de comunicação de mais baixo nível, como o TCP e UDP. Num nível mais elementar, na Camada de Redes, encontram-se os protocolos IP e ICMP, que controlam o fluxo de dados entre diferentes tipos de redes locais. A penúltima camada, a Camada de Enlace, opera protocolos de troca de dados dentro de redes locais, como o protocolo Ethernet. Por fim, a Camada Física define protocolos vinculados a camada de enlace e manipula elementos “físicos”, como níveis de tensão elétrica ou sinais de luz.

Historicamente, as redes de computadores, a nível nacional, surgem no contexto da guerra fria com a Arpanet, um projeto dos Estados Unidos da América para interligação de computadores ao longo do território [5]. *Advanced Research Projects Agency (*ARPA*)* foi a instituição responsável por conectar diversos computadores dos órgãos governamentais, universidade e centros de pesquisa. Essa inovação permitiu com que o desenvolvimento de projetos tivesse considerável avanço, o que na Guerra Fria era crucial para a manutenção da paz. Após a guerra, o código aberto do projeto deu o material necessário para que usuários não militares desenvolvessem protocolos como o *World Wide Web (*WWW*)* e *Hypertext Transfer Protocol (*HTTP*).*

2.2 SEGURANÇA EM REDES

Esta seção apresenta heurísticas de segurança em redes de computadores. As questões de segurança em computadores relacionam-se a ataques que buscam violar os princípios listados a seguir.

Segurança em redes une tópicos relacionados a prevenção, mitigação e estudo de ataques em redes [6]. Os problemas de segurança em redes estão relacionados com o acesso não autorizado, modificação indevida e uso indevido dos recursos disponíveis, etc. As heurísticas de segurança em redes se baseiam em Confidencialidade, Integridade, Autorização, Identificação e outros preceitos. Os ataques

têm como alvo abalar um ou mais desses preceitos, podendo ocorrer de forma passiva ou ativa. A forma Passiva ocorre quando o objetivo se resume em coletar informação. Já a forma ativa se dá quando o atacante busca executar comandos, impossibilitar a conexão, modificar dados, etc.

Confidencialidade, Integridade, Autorização e Identificação são os princípios de segurança que sistemas seguros devem oferecer aos usuários [6], [7]. A Confidencialidade preza que os dados devem ser somente acessados por quem possui autorização. A Autorização dita que o acesso a integridade do sistema deve ser feito somente por usuários autorizados. A Integridade se resume na capacidade de fazer alterações no sistema ou nos dados somente por um usuário autorizado. Por fim, a Identificação dita quanto a confirmação da identidade do usuário.

2.3 INTERNET DAS COISAS

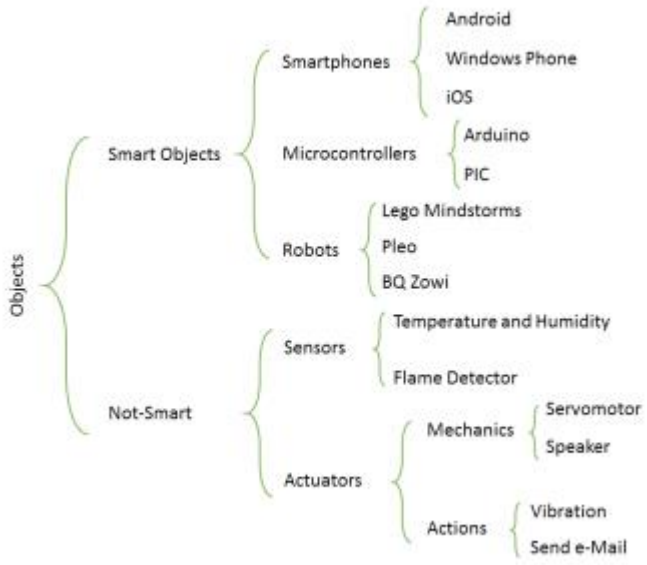
Como os termos de IoT podem variar de acordo com os com diferentes autores é conveniente estabelecer um conjunto de definições de termos básicos para o correto entendimento do texto neste trabalho. Esta seção apresenta conceitos gerais e definições acerca de Internet das coisas (IoT). São apresentados os fundamentos, sensores, atuadores e a formalização do termo "*Thing*" em IoT. Na parte final desta seção também são apresentados campos de estudos relacionados a IoT.

2.3.1 INTRODUÇÃO A IOT

O termo *Internet of Things* (IoT) é o resultado da combinação do termo "Internet", entendido como uma rede global de computadores e do termo "*Things"* entendido como objetos do cotidiano. Esses objetos podem ter tamanhos variados, como o tamanho uma caneta, de um foguete, ou com tamanhos até maiores ou menores [8]. Assim, o conceito de IoT consiste na junção de um computador miniaturizado com um objeto ("*Thing*"), de forma a agregar funcionalidades extras aos objetos. Os dispositivos IoT (ou simplesmente dispositivos) são o produto dessa junção e podem ser classificados basicamente como sensores ou atuadores. Os sensores são os dispositivos que coletam dados do mundo real, enquanto atuadores são os dispositivos que realizam ações no ambiente físico.

Segundo González [2], os dispositivos podem ser definidos de forma distinta por cada autor. A fim de entender o que está no escopo de IoT, é necessário dispor das formalidades exibidas a seguir. As coisas ("*Things"*), podem ser especializadas em duas categorias, inteligentes e não inteligentes. As coisas inteligentes são aquelas que possuem capacidade de processamento embutido. Enquanto as coisas não inteligentes são todos as outras que comporão um dispositivo junto a computador miniaturizado. Na Figura 3 é ilustrada a hierarquia dos objetos.

Figura 3 - Hierarquia de especialização de objetos no contexto de IoT



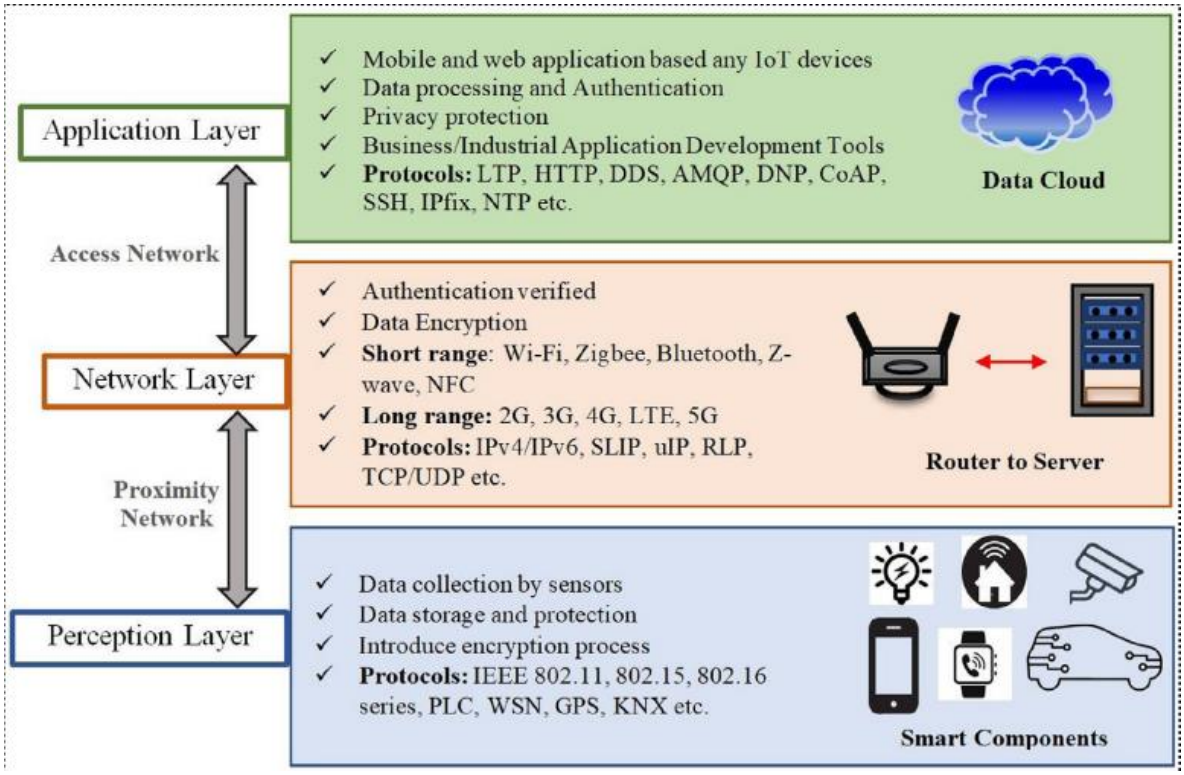
Fonte: C. González García, *et al*. [2]

A existência de sensores e atuadores são componentes vitais para a criação de sistemas IoT. Sendo assim, há necessidade em definir o que é cada um [2]. Um sensor é aquele que pode coletar informações do ambiente, quantificar e transformar em dado para ser tratado por um computador. Enquanto os atuadores são aqueles que vão tomar ações no ambiente em que estão inseridos. Eles podem ser mecânicos, como: pistões, bombas hidráulicas, etc. Há também a classe de atuadores responsável pelo controle. Os atuadores de controle podem ser exemplificados, como: monitores, lâmpadas LED ou controle de luzes.

Devido a sua variação de tamanho, os dispositivos podem possuir diversas limitações, como: armazenamento, processamento, largura de banda, etc. Uma das formas contornar essas limitações utiliza uma arquitetura denominada "Arquite-

tura em Três Camadas” [9]. Nessa arquitetura os dados são gerados pelos dispositivos numa primeira camada, denominada de “Camada de Percepção” (*Perception Layer).* Esses dados são transmitidos por uma ou mais redes de curto ou longo alcance em uma camada, denominada de “Camada de Redes” (*Network Layer)*. O fluxo dos dados tem destino a uma última camada, denominada de “Camada de Aplicação” (*Application Layer),* que tem o objetivo de processar os dados recebidos através do uso de um computador com maior poder de computação. Essa arquitetura, seus protocolos e responsabilidades de cada camada estão ilustrados na Figura 4.

Figura 4 - Arquitetura IoT



Fonte: S. M. Tahsien, *et al.* [7]

2.3.2 CAMPOS DE ESTUDOS RELACIONADOS A IOT

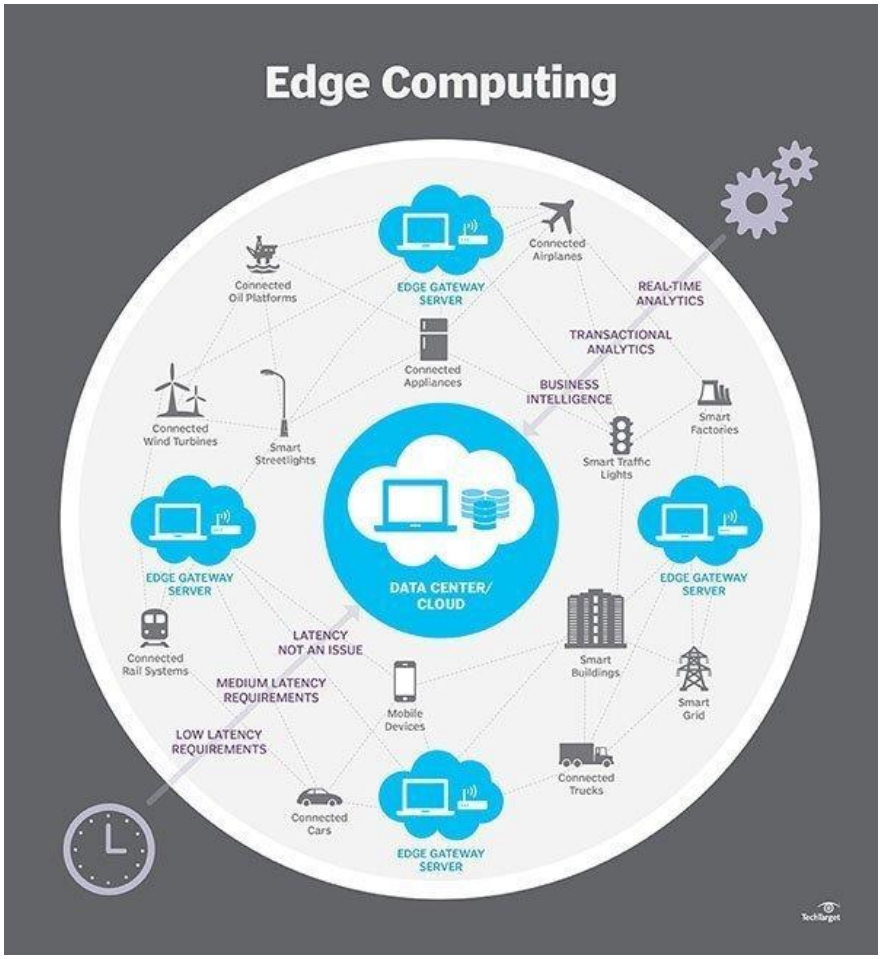
A seguir estão enumerados diversos campos de estudo relacionados a Internet das Coisas (IoT). Esses campos podem parecer desconectados entre si, mas todos podem contribuir para evolução da chamada Internet das Coisas. Essa evolu-

ção pode se dar através da ampliação do escopo de utilização ou resolvendo os problemas encontrados na implantação de sistemas IoT.

A arquitetura *Cloud Computing* é o modelo base para diversas aplicações [11]. Essa arquitetura consiste em enviar todo processamento robusto das aplicações para ser processado em um servidor centralizado e somente a informação processada é repassada ao usuário. Com isso, a responsabilidade do processamento aumenta para o lado do servidor, o que permite as aplicações funcionarem com requisições técnicas mais simples nos dispositivos finais.

Alguns sistemas de IoT podem requerer baixa latência nas suas operações e demandar um alto volume de tráfego e processamento em tempo real que não pode ser oferecido eficientemente pela arquitetura *Cloud Computing* [12]. A arquitetura de Computação de Borda (*Edge Computing*) propõe posicionar servidores intermediários que dividem o processamento com um servidor central. Como ilustrado na Figura 5, esses servidores intermediários fazem um processamento bruto dos dados e somente eles se comunicam com um servidor central para realizar o processamento final dos dados [11]. Dessa forma, o servidor principal é desafogado da enorme quantidade de dados produzidos e os servidores intermediários podem oferecer latência reduzida se comparada com o servidor central se comunicando diretamente com os dispositivos da rede.

Figura 5 - Computação de Borda



Fonte: Techtarget [10]

Big Data Analytics corresponde a um campo que estuda práticas para resolver o problema na análise de grandes volumes de dados [13]. Um grande volume de dados para esse campo deve se enquadrar em três características: volume, variedade e velocidade. Sistemas que utilizam Internet das Coisas (IoT) podem possuir milhares de sensores diferentes que estão continuamente enviando as informações do ambiente, sendo candidatos a gerar grandes volumes de dados.

Inteligência Artificial (IA) tem como objetivo simular o comportamento racional humano para resolver problemas em computação [14]. Devido a quantidade enorme de dados gerados por sistemas de IoT, pode haver a necessidade do processamento dessa massa de dados usando uma forma alternativa. Utilizando I.A, se torna possível analisar a correlação entre dados que pareceriam desconexos através dos paradigmas usuais da computação.

Ambient Inteligence é um campo de estudo que propõe utilizar sensores para sentir as necessidades das pessoas no ambiente e reagir nos objetos não inteligentes usando os atuadores [15]. Os dados gerados são processados por computadores com maior poder de computação utilizando Inteligência Artificial (IA). Após o processamento, esse computados envia comandos aos atuadores do ambiente, que realizam ações como: fechar ou abrir uma cortina, controle de iluminação, etc.

O Aprendizado de Máquina (*Machine Learning)* consiste na análise de padrões de uma massa de dados [16]. Os algoritmos no contexto de *Machine Learning* se tornam mais precisos proporcionalmente a quantidade de dados. Sistemas de IoT podem gerar uma enorme quantidade de dados que podem ser utilizados para treinar uma máquina reconhecer a um determinado padrão.

Digital Twin consiste em um modelo digital de um componente físico ou sistema [17]. Como essa tecnologia provê um modelo fiel ao sistema ou componente em tempo real, ela pode ser utilizada de forma a aprimorar a experiência do desenvolvedor e reduzir o tempo de desenvolvimento. Para garantir a atualização do estado do modelo, podem ser utilizados sensores IoT, barateando o custo quando comparado a utilização de um modelo físico real.

*Supply Chain Management (*SCM*),* pode ser descrito como a gerência de uma linha logística que utiliza tecnologias relacionadas a IoT [18]. Nesse contexto, o objeto a ser transportado é precisamente localizado com o auxílio de elementos sensores IoT. Ao mesmo tempo, os atuadores IoT permitem atuar à distância na linha logística. Tais fatos possibilitam resolver problemas remotamente, inclusive internacionalmente, reduzindo custos e tempos operacionais e burocráticos.

Com possibilidade de suporte à diversos sistemas, *Machine to Machine (M2M)* tem como objetivo realizar a integração e comunicação entre dispositivos [19]. Com base nesse objetivo, os protocolos desenvolvidos buscam generalizar os diferentes padrões de comunicação entre dispositivos. Dessa forma, os sistemas podem integrar diversas tecnologias e tirar maior proveito dos benefícios de cada uma.

O campo de *Machine-to-Human* tem como objetivo prover protocolos e interfaces de forma a facilitar a comunicação entre humano e a máquina [20]. Assim, de forma análoga a comunicação entre seres humanos, esses protocolos e interfaces acabam provendo maior inclusão digital das pessoas que os usam.

3 METODOLOGIA

Este capítulo descreve a metodologia utilizada para realização deste trabalho. O estudo foi realizado em duas etapas, uma Etapa de Preparação para o Estudo e a Etapa Principal do Estudo, por sua vez dividida em duas fases.

3.1 ETAPA DE PREPARAÇÃO DO ESTUDO

Um estudo sobre questões de segurança em Internet das Coisas é bastante amplo e envolve variadas tecnologias, como: rede de computadores, aprendizado de máquina, meta-heurísticas, etc. Desta forma, a etapa de preparação teve como objetivos principais:

- entendimento do significado técnico do termo Internet das Coisas (IoT);
- identificar a potencial amplitude do tema de segurança em IoT; e
- esclarecer limites para o estudo a ser realizado.

Além desses objetivos principais, a etapa também teve como objetivo garantir a familiarização com mecanismos de busca de artigos científicos (CAPES, SCOPUS, IEEE, Google Scholar) pelo autor do trabalho.

Nesta etapa foram examinados 52 artigos e visitados diversos *sites* explicativos na Internet. Como resultado, foi possível melhorar a compreensão do significado de Internet das Coisas, tecnologias associadas e definir limites para o estudo propriamente dito.

3.2 ETAPA PRINCIPAL DO ESTUDO

Os objetivos do estudo foram definidos ao final da etapa preliminar e são eles:

- identificar diferentes ataques a tecnologias utilizadas em Internet das Coisas (IoT) descritos em artigos de periódicos;
- selecionar os ataques mais conhecidos dentre os ataques identificados;
- identificar tecnologias que utilizam radiofrequência para dar suporte a sistemas IoT; e
- selecionar dentre os ataques identificados aqueles relacionados com tecnologias que utilizam radiofrequência para oferecer suporte a sistemas IoT.

Esta etapa principal do estudo foi realizada em duas fases. A primeira fase tomou como base o artigo “IoT Security: Ongoing Challenges and Research Opportunities” [21], um dos artigos selecionados na etapa anterior. Esse artigo foi escolhido por apresentar, na data de início dessa etapa, 226 citações na base IEEE e 439 citações na base SCOPUS. Inspirada pela técnica *forward snowballing* [22], foi criada uma lista com os 439 artigos que referenciavam esse artigo [21] na base SCOPUS. Dessa lista, foram escolhidos os 25 artigos mais citados e os 25 artigos mais recentemente publicados. Os títulos, *abstracts* e os pontos centrais dos conteúdos desses 50 artigos foram analisados, procurando por adequação ao tema. A partir dessa análise, cinco (5) artigos, os artigos [6], [23]–[26], foram selecionados por apresentarem conteúdo relacionado com os objetivos do estudo. A partir dos ataques presentes nesses cinco artigos, foi criada uma Tabela de Ataques.

Numa segunda fase, foram pesquisadas referências complementares para cada ataque identificado. Para tal, foi realizado um processo de busca semelhante à fase anterior, a partir do artigo “Sybil attacks and their defenses in the internet of Things” [27], um dos 50 artigos analisados anteriormente. Foi realizada uma busca na base IEEE por artigos que referenciavam esse artigo [27]. Os 219 artigos encontrados foram ordenados em ordem decrescente de tempo e examinados, procurando-se novos textos de referência para os ataques já presentes na Tabela de Ataques. Como efeito colateral, novos ataques foram encontrados, ao mesmo tempo que alguns ataques antigos foram referenciados. O fim da busca por artigos foi decidido quando a Tabela de Ataques passou a conter 142 ataques identificados, uma quantidade considerada adequada para a finalidade deste trabalho. Como resultado desse último processo de inspeção de artigos, foram acrescentados os artigos [28]–[31].

4 QUESTÕES DE SEGURANÇA EM IOT

Este capítulo discorre sobre questões de segurança em Internet das Coisas (IoT) que não estão obrigatoriamente relacionadas à radiofrequência. A Seção 4.1 apresenta algumas questões de segurança envolvendo software. A Seção 4.2 apresenta algumas das estratégias de ataque mais reconhecidas pela comunidade de segurança da informação. Por fim, a Seção 4.3 apresenta outras estratégias conhecidas de ataques.

4.1 QUESTÕES DE SEGURANÇA ENVOLVENDO SOFTWARE

Os dispositivos em IoT possuem um computador miniaturizado, que por sua vez é gerido por um sistema operacional. Esses dispositivos podem utilizar diferentes sistemas operacionais, tais como: Android, LiteOS, TineOS, etc. [26]. Lembrando que sistemas operacionais são *softwares* escritos por serem humanos e, portanto, estão sujeitos a mesmas questões de segurança de outros *softwares*.

Softwares são programas escritos por programadores, portanto estão sujeitos a falhas na criação da lógica desses programas, que são comumente conhecidos como *bugs* [21]. Aproveitando-se dessas falhas na programação, um atacante com ciência de um *bug* pode abusar dele para atuar indevidamente nesses programas. Um *bug* pode ser resolvido com uma atualização no programa, porém em um sistema de IoT pode ser mais atualizar todos os dispositivos. Isso ocorre devido a algumas atualizações necessitarem manipular o dispositivo fisicamente, o que pode ser complicado, pois um sistema pode conter uma quantidade muito grande de dispositivos distribuídos.

Outro fator relevante para segurança de dispositivos em IoT é que cerca de 20% dos usuários tendem a manter os dispositivos com configurações de fábrica [32]. Como configurações de fábrica tendem a ser genéricas e pouco elaboradas, elas não são capazes de restringir o acesso de forma adequada para todos os cená-

rios de uso. Isso pode gerar vulnerabilidades que podem ser exploradas por diversos tipos de ataque, que exploram justamente as deficiências das configurações de fábrica.

4.2 ESTRATÉGIAS MAIS CONHECIDAS DE ATAQUE A REDES

Esta seção apresenta estratégias comumente utilizadas para atacar redes de computadores. Essas estratégias podem ser entendidas como paradigmas que podem servir de base para diversos tipos de ataque, aplicáveis à diversas situações bem como para diversas tecnologias de comunicação.

4.2.1 PHISHING

O ataque *Phishing* consiste em falsificar algum conteúdo com objetivo de obter vantagem em cima de uma vítima, podendo obter suas informações ou instalar um *malware* em sua máquina [33]. Nesse ataque, o atacante cria um conteúdo falso de interesse geral dos usuários da Internet, como: bancos, serviços, etc. Quando a vítima acessa o conteúdo falso, o ataque pode seguir dois cursos distintos. No primeiro caso, o atacante obtém informações sigilosas da vítima, como: dados bancários, senhas de serviços *online*, etc. Já no segundo caso, o atacante pode conseguir injetar algum programa malicioso na máquina da vítima e assim obter sucessão em outros tipos de ataques.

4.2.2 SPOOFING

Spoofing consiste na falsificação da identidade de uma vítima [34]. O ataque dispõe de diversos métodos, como: Falsificação de IP, Interpretação de voz, etc. Diferente do *Phishing, Spoofing* não necessariamente precisa da atuação da vítima, pois é possível falsificar a identidade de uma vítima explorando falhas nas tecnologias, engenharia social ou utilizando outros métodos. Na atualidade, os sistemas estão colocando diferentes passos para identificação do usuário com intuito de comba-

ter o *Spoofing*. Como por exemplo: reconhecimento por voz, reconhecimento de digital, etc.

4.2.3 DOS e DDOS

Os sistemas de computação proveem os seus serviços através do uso de alguma rede, como a Internet. O ataque *Denial of Service* (DoS) tem como objetivo para o atacante tornar o serviço indisponível ou com desempenho defasado [35]. Isso pode ser feito de diferentes formas, de modo a abusar alguma peculiaridade em uma tecnologia presente no computador da vítima. Porém, um dos mais populares métodos consiste no envio massivo de pacotes SYN para uma vítima. Os pacotes SYN tem a função de estabelecer uma conexão, o que força o computador da vítima a formar e responder um pacote ACK ao remetente [36]. A quantidade massiva de respostas forçadas afeta o desempenho do computador, que no pior caso torna o serviço indisponível.

O ataque DoS pode ocorrer de forma distribuída, ou seja, com várias máquinas atacantes que utilizam alguma técnica contra uma só vítima. Quando o ataque ocorre de forma distribuída, ele recebe o nome de *Distributed Denial of Service* (DDoS).

4.2.4 EAVESDROPPING

Eavesdropping consiste em um ataque passivo, que ocorre em tempo real, com o objetivo de obter a informação trafegada através do meio de transmissão, seja ele: uma rede cabeada, ao ar livre, etc. [23]. O ataque pode ser executado de diferentes maneiras ao dispor das características da tecnologia utilizada para propagação da informação, como: fax, Internet, conversa ao ar livre, etc. Esse ataque pode ser combatido ao utilizar mensagens cifradas durante a comunicação. Esse método impede que o atacante obtenha a informação trafegada, mesmo que tenha interceptado a comunicação.

4.2.5 MAN-IN-THE-MIDDLE

O ataque Man-in-the-Middle (MitM) consiste na infiltração da comunicação entre dois elementos de uma rede [37]. Ao ter sucesso em se infiltrar na comunicação, o atacante fica responsável por receber a informação do remetente e repassar ao destinatário. Desta forma, o atacante pode não só ter acesso a informação, mas também alterar a informação. Esse ataque é difícil ser percebido pelas vítimas, pois o atacante pode garantir que as informações cheguem com sucesso, o que inibe algumas suspeitas.

4.3 OUTRAS ESTRATÉGIAS CONHECIDAS DE ATAQUES

Esta seção apresenta outros ataques conhecidos pela comunidade de segurança da informação, mas não tão mencionados fora dessa comunidade. As estratégias a seguir estão organizadas nas seguintes categorias[1]: senhas*, leak, software* e identificação.

As estratégias de ataque categorizadas como senhas têm como o objetivo quebrar a criptografia em uso e obter a senha de algum usuário para realizar um login autorizado no sistema. São exemplos desses ataques: *Brute-force* [38]*; Crypt-Analysis attacks* [39]*, Social Engineering* [40] *e Hash Colision* [41]. *Radio-Frequency Identification* (RFID) é um exemplo de uma tecnologia conectada a IoT, onde esses ataques podem ser aplicados.

Os ataques categorizados como *Leak* têm sua estratégia voltada a obter a informação trafegada entre os usuários de uma rede de computadores. Os seguintes ataques se enquadram nessa categoria: *Man in the middle* [42]*, Eavesdropping* [43]*, Traffic analysis* [44] *e Sniffing* [45]. *Wireless Sensor Network* (WSN), RFID e *Near Field Communication* (NFC) são exemplos de algumas tecnologias conectadas a IoT e que são afetas por esses ataques.

Os ataques categorizados como identificação têm como objetivo estratégico obter autorização no sistema ao utilizar uma identificação autorizada. Os métodos utilizados consistem no roubo, sequestro ou falsificação de uma identificação

[1] Definidas pelo autor.

autorizada. A seguir, alguns exemplos de ataques usados para realizar o roubo da identificação: *Hijacking* [46], *Spoofing* [47] e *Replay Attack* [48]. Esses ataques afetam as seguintes tecnologias conectadas a IoT: WSN, RFID, *Bluetooth Low Energy* (BLE), NFC.

As estratégias de ataque categorizadas como *software* têm como objetivo obter controle, prejudicar ou acessar dados de um servidor que prove suporte a um sistema. Normalmente, esses ataques exploram falhas ou infiltram algum *software* malicioso no sistema. Os seguintes ataques podem ser classificados nessa categoria: *Exploit Attack* [49], *Malware* [31], *Malicious vírus/worm* [50], *Backdoors* [51] *e Malicious Code Attack* [52], *Phishing Attack* [52] *e Denial of Service* [53]. Esses ataques afetam as seguintes tecnologias conectadas à IoT: RFID e *Cloud Computing*.

5 ATAQUES ENVOLVENDO RADIOFRÊQUENCIA

Neste capítulo são apresentados os 48 ataques relacionados a tecnologias de radiofrequência utilizadas em Internet das Coisas (IoT) que foram identificados neste estudo. Cada seção deste capítulo inicia-se com uma breve descrição da tecnologia analisada e, em seguida, apresenta uma relação de ataques que utiliza essa mesma tecnologia.

5.1 TECNOLOGIA RADIO-FREQUENCY IDENTIFICATION

Radio-Frequency Identification (RFID) é uma tecnologia de baixo custo e baixa necessidade energética, que tem como objetivo enviar informação sem necessidade de fios [54]. RFID pode ser usado como marcação de dispositivos e por isso possui aplicabilidade em IoT para diversos setores, como: Ambientes Inteligentes, *Supply-Chain Management*, etc. A popularização dessa tecnologia decorre da miniaturização dos componentes eletrônicos.

A arquitetura de RFID é composta de 3 partes: aplicação, leitor e marcação (*Tag*) [26]. A *tag* é uma marcação única do objeto, sendo ela composta por um número identificador que é obtido do protocolo IPV6. O leitor é chamado pela aplicação para ler uma *tag* e repassar para a aplicação o valor dessa *tag*. O leitor serve também para transmitir dados a uma *tag* através de uma antena que utiliza sinal de rádio do protocolo RFID. Já o componente de aplicação consiste em uma porta de acesso para que alguma aplicação se comunique com o leitor e obter o valor de uma *tag*.

Dispositivos que utilizam RFID estão sujeitos a ataques perpetrados por terceiros que visam atingir o processo de identificação ou abusar de alguma outra particularidade da tecnologia. A seguir são listados diversos tipos de ataques que abusam de características do protocolo RFID.

- *Kill Command Attack* [31], [55] - O comando *kill* em RFID é enviado por um leitor e torna uma *tag* inabilitada para receber novos comandos. O ataque *Kill Command* consiste no uso não autorizado do comando *kill* pelo atacante, o que resulta no bloqueio de futuros comandos recebidos por um dispositivo atacado.

- *Deactivation Attack* [26], [56] - O ataque *Deactivation* tem como objetivo desativar a transmissão da informação de uma *tag*. Isso pode ser feito ao danificar o dispositivo fisicamente ou a utilizar o comando *kill* no dispositivo visado.

- *Passive interference* [26], [57] - *Passive Interference* é um ataque consiste em causar interferência na comunicação de rádio usada em RFID de maneira indireta. O ataque atua de forma a causar interferência no meio de comunicação, de maneiras onde isso ocorre por uma consequência da ação e não pelo objetivo final da ação. O ataque pode ser executado de diversas formas, como geradores eletrônicos, mistura de metais, etc. No primeiro exemplo, o objetivo do gerador é gerar energia elétrica. Porém, essa forma de geração de energia elétrica tem como efeito colateral causar interferência em ondas de rádio que passam por perto do gerador.

- *Tag removal* [26], [43] - O ataque *Tag Removal* consiste na remoção não autorizada da *tag* de um dispositivo. Isso é possível pois as *tags* podem estar anexadas aos dispositivos de forma insegura. Após remover a *tag*, o dispositivo não pode mais ser identificado.

- *Tag destruction* [26], [43] – Este ataque tem como ideia danificar fisicamente a *tag*. Esse ataque impede o funcionamento de uma *tag* e também inutiliza a identificação de um dispositivo.

- *Unauthorized Tag Reading* [26], [58] - O ataque de leitura não autorizada (*Unauthorized Tag Reading*) consiste em ler, modificar ou excluir o conteúdo de uma *tag*. Esse ataque se torna possível pois o protocolo de autenticação em RFID não é aplicado durante o processo de leitura de uma *tag*.

- *Tag Modification* [26], [57] - Consiste em usar a falha de configuração da *tag* para modificar seu conteúdo. A falha consiste no administrador do dispositivo deixar a tag habilitada a modificações após a implantação dela em um sistema.

- *Detaching The Tag* [26], [59] - O ataque *Detaching The Tag* consiste em separar a *tag* de um dispositivo. Caso tenha sucesso no ataque, um atacante pode fazer algum dispositivo se passar por outro e dar início a outros ataques, como *Spoofing*.

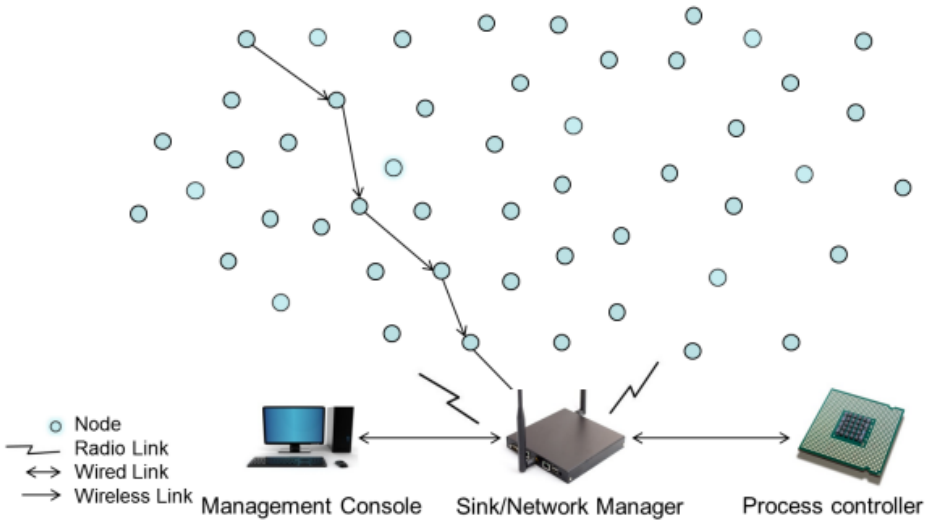
- *Tracking* [26], [60] - Tem como objetivo rastrear uma vítima através das *tags* de dispositivos que ela possui. Esse ataque tende a atingir mais vítimas a cada ano, pois a tendência é que cada vez mais os indivíduos possuam dispositivos com uma *tag*.

5.2 TECNOLOGIA WIRELESS SENSOR NETWORK

Wireless sensor network (WSN) consiste em uma rede de aparelhos micro-eletro-mecânicos, os dispositivos [61]. Como os aparelhos são miniaturizados, sua capacidade de processamento, memória e largura de banda são pequenos também. Como ilustrado na Figura 6, os dispositivos coletam as informações e se comunicam entre si para fazer o dado chegar até uma estação. Essa estação então que vai receber e redirecionar para o gerenciamento ou processamento das informações.

WSN pode ser um dos meios de rede utilizados para transmissões de informações produzidas por dispositivos IoT [7]. O uso dessa rede possibilita que ataques possam ser lançados com intenções de prejudicar o desempenho da rede ou capturar informações. A seguir são listados diversos ataques que utilizam características da arquitetura de rede WSN e uma breve descrição de cada um.

Figura 6 - Redes WSN



Fonte: A. A. Kumar S., *et al.* [61]

- *Black Hole Attack* [26], [62], [63] – Tem início quando um dispositivo malicioso envia falsas informações durante o processo criação da rota dos pacotes de dados. Isso ocorre de modo a forçar o processo de criação de rotas a incluir o dispositivo malicioso na rota de pacotes. Após inserido na rota, esse dispositivo começa a descartar todos os pacotes que passarem por ele, causando negação de serviço.

- *Grey hole Attack* [26], [62], [63] - Este é um ataque semelhante ao ataque *Black Hole*. Assim, um dispositivo malicioso é posicionado na rede e ele envia dados falsos durante o processo de criação da rota dos pacotes de dados. A partir do momento em que esse dispositivo está na rota dos pacotes, ele começa a descartar os pacotes seletivamente. Nesse caso, os pacotes de dados são descartados e passam apenas os pacotes de controle, o que causa negação de serviço e uma confusão na rede. Pois os outros dispositivos têm informações de que tudo está ocorrendo sem problemas.

- *Hello Flood Attack* [26], [64] - Quando um novo dispositivo pretende entrar em uma rede WSN, ele precisa enviar uma mensagem “*Hello*” para todos os membros da rede anunciando sua entrada. O ataque *Hello Flood* consiste em

capturar e retransmitir essa mensagem para tentar se passar por esse dispositivo perante ao máximo de dispositivos possíveis.

- *Carousel Attack* [26], [62] - O objetivo do ataque *Carousel* consiste em usar um dispositivo malicioso para enviar pacotes de controle durante o processo de criação de rotas, de modo a forçar a rota a ter o primeiro dispositivo como destino do roteamento[62]. Isso faz a rota dos pacotes ficar circular, dessa forma a informação é perdida pois os pacotes são descartados após um determinado tempo em tráfego.

- *Stretch Attack* [26], [62] - Consiste em usar um dispositivo malicioso para enviar falsas informações durante o processo de criação de rotas. O objetivo é forçar o processo a criar uma rota que passe pelo máximo de dispositivos possíveis e assim aumentar o consumo de bateria dos dispositivos na rede.

- *Jellyfish Attack* [26], [62] - O objetivo deste ataque é inserir um dispositivo malicioso na rede e atrasar os pacotes que passam por ele. Desta forma, a rede tem prejuízo no desempenho e aumenta a latência fim a fim.

- *Vampire Attack* [26], [62] - O ataque do vampiro é executado com o objetivo de causar negação de serviço na rede drenando a bateria dos dispositivos. Isso é feito reduzindo os recursos dos dispositivos.

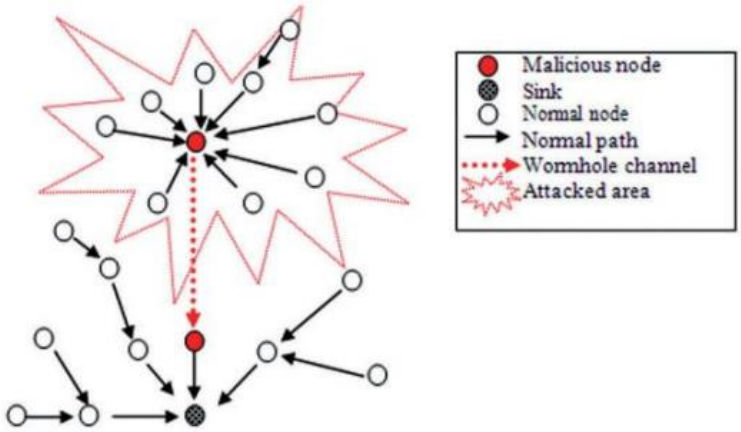
- *Collision Attack* [26], [65] – Usa um dispositivo malicioso para enviar, de forma continua, quadros de dados no enlace. Ao executar esse ataque, todos dispositivos no mesmo enlace ficam impedidos de enviar seus quadros de dados.

- *Exhausted Attack* [26], [65] – O ataque *Exhausted* tem como objetivo esgotar os recursos do receptor de uma rede. Isso é feito por um dispositivo malicioso que envia sucessivos pacotes ACK ou *Join*, dois quais o receptor deve aceitar e responder.

- *Unfairness Attack* [26], [65] – O objetivo é utilizar um dispositivo malicioso para causar prejuízo no desempenho da rede. O método utilizado consiste no uso contínuo dos serviços do enlace por esse dispositivo.

- *Wormhole Attack* [26], [66] - Visa roubar informações. A execução se baseia em utilizar dispositivos maliciosos que possuam um enlace privilegiado com alta velocidade de transferência entre eles. Quando o processo de criação de rotas for iniciar, o enlace privilegiado terá boas chances de entrar na rota dos pacotes de dados. Como ilustrado na Figura 7, os pacotes de dados que passarem por essa rota são capturados pelos dispositivos maliciosos.

Figura 7 - Ataque *Wormhole*



Fonte: M. Meghdadi, *et al.* [67]

5.3 TECNOLOGIA BLUETOOTH LOW ENERGY

*Bluetooth Low Energy (*BLE*)* é um protocolo utilizado para comunicação de dispositivos em um sistema de IoT [25]. O protocolo oferece desenvolvimento simples, baixo custo energético e boa velocidade de transferência. Porém, a simplicidade impede o desenvolvimento de soluções de segurança mais elaboradas, deixando brecha para possíveis ataques. A seguir, estão apresentados alguns dos ataques que utilizam as fragilidades do protocolo BLE.

- *Device Cloning* [25], [68], [69] - Os dispositivos que desejam se comunicar utilizando o protocolo BLE devem antes estar pareados. O ataque *Device Cloning* consiste em clonar um dispositivo. Isso é feito por um dispositivo malicioso que clona o endereço MAC de um dos dispositivos que estão se comuni-

cando. Após o dispositivo malicioso clonar o endereço MAC, ele força outros dispositivos a interromperem o pareamento. A partir deste momento, o dispositivo malicioso começa parear com o outro dispositivo da comunicação se passando pelo dispositivo clonado.

- *Device Authentication Attack* [25], [38], [70] - O ataque *Device Cloning* resume-se em capturar a chave de encriptação, podendo usar de estratégias tal como Eavesdropping. Uma vez capturada a chave de autenticação, torna-se necessário quebrar a criptografia da chave. Isso pode ser feito com o ataque *Brute-force*.

- *Offline PIN Cracking* [25], [71] Consiste no uso de técnicas, como *Brute-force,* para encontrar o número PIN de um dispositivo que utilize o protocolo BLE. Porém ao fazer o procedimento *offline*, o atacante pode tentar quantas combinações quiser, não sendo parado por algum limitador de tentativas que teria *online*.

- *Blue Smack* [25], [72] - Devido a uma falha no protocolo L2CAP, as aplicações param de funcionar caso seja for recebido um pacote malformado. O ataque *Blue Smack* abusa dessa falha para interromper o serviço de alguma aplicação. Nesse caso, um atacante envia um envia um pacote de dados malformado a uma vítima. Ao receber o pacote de dados malformado, a vítima tem seu serviço interrompido.

- *Fuzzing Attack* [25], [73] - Dispositivos que utilizam serviços GATT estão sujeitos a ter a aplicação subitamente interrompida, caso a aplicação receba um pacote malformado ou com dados aleatórios. O atacante que utiliza o ataque *Fuzzing* analisa o comportamento da aplicação ao enviar e receber dados, com intuito de enviar um pacote dados que seja aceito pela aplicação. Após a observação, o atacante gera um pacote malformado ou com dados aleatórios e envia a vítima.

- *Activity Detection* [25], [74] – Se realiza através da análise do tráfego de dados de um dispositivo que utilize o protocolo BLE. Como a criptografia é fraca,

se torna possível descobrir a ação que o dispositivo está realizando ao analisar os dados trafegados durante a comunicação com outro dispositivo.

- *Interception* [31], [75] - O ataque *Interception* consiste em capturar a comunicação entre dispositivos. Isso se torna possível e facilmente praticável, pois a criptografia do protocolo BLE é fraca e já existem ferramentas prontas para a prática.

- *Blue Printing* [25], [76] - O objetivo do ataque *Blue Printing* é coletar dados do dispositivo da vítima, como: versão do Bluetooth, IMEI e modelo do dispositivo. Essas informações ficam disponíveis publicamente, pois o protocolo *Bluetooth* especifica que os dispositivos devem anunciar publicamente (*Broadcast)* seus serviços GATT.

- *Blue Stumbling* [25], [77] - O ataque *Blue Stumbling* tem como objetivo analisar os dispositivos na área. A análise é feita de forma anônima pelo atacante e busca informações dos dispositivos na área para verificar a viabilidade de lançar outros ataques.

- *Co-Located Mobile Application Attack* [25], [78] - Para conseguir roubar informações via Bluetooth, não necessariamente o ataque precisa que visar alguma vulnerabilidade protocolo Bluetooth. Outra forma de conseguir extrair informações consiste na utilização do ataque *Co-Located Mobile Application.* Nesse ataque, o atacante obtém acesso a outra aplicação que utilize Bluetooth no mesmo dispositivo e compartilhe o mesmo canal com a aplicação desejada.

- *Bluesnarfing* [31], [79] - O ataque *Bluesnarfing* se resume em conseguir acesso a um dispositivo através do protocolo Bluetooth. Ao conseguir acesso, o atacante pode executar Eavesdropping ou redirecionar chamadas.

- *BlueBugging* [31], [79] - O objetivo do ataque *BlueBugging* é conseguir acesso a informações de um dispositivo com Bluetooth. Isso é feito por um atacante que explora vulnerabilidades em firmwares antigos e desatualizados dos dispositivos.

- *BlueJacking* [31], [79] - O ataque *BlueJacking* consiste no envio de mensagens anônimas a dispositivos na área. Esse ataque não sequestra o dispositivo ou vaza informações, porém causa preocupações pois parece que o atacante tem controle do dispositivo.

5.4 TECNOLOGIA NEAR FIELD COMMUNICATION

Near Field Communication (NFC) é uma tecnologia de comunicação sem fio e alcance curto (4cm) [80]. Para executar a comunicação entre dois diferentes dispositivos, cada um deles assume uma função, um sendo o iniciador e o outro o alvo. O iniciador gera um campo de radiofrequência que carrega eletricamente e de forma passiva o alvo o que permite a transmissão dos dados. Essa tecnologia pode ser utilizada para construção de sistemas IoT, porém o custo de energia é superior ao protocolo *Bluetooth Low Energy*. Caso utilizada, há questões de segurança que devem ser consideradas. A seguir são listados alguns ataques que abusam de características do protocolo NFC.

- *Data Corruption* [31], [81] - Consiste em corromper os dados de uma comunicação NFC. Isso é feito por um atacante que gera perturbações ativas no campo elétrico do iniciador. Isso corrompe os dados transmitidos, o que faz o dispositivo receptor descartar o pacote.

- *Data Modification* [31], [82] - Tem como objetivo interferir no meio de forma análoga ao ataque *Data Corruption*, porém o objetivo não é modificar aleatoriamente o dado. Dessa vez, a modificação é feita de modo a alterar o formato do dado transmitido ou a informação dele.

- *Data Insertion* [31], [81] - Esta estratégia consiste em inserir dados durante o processo de comunicação entre o iniciador e o alvo. Essa inserção é complicada de ser feita, pois o dispositivo que recebe os dados pode entender o dado inserido como dado corrompido e descartá-lo. Logo, o processo tem que ser feito de forma a considerar o que domínio de dados aceitos pelo receptor.

5.5 TECNOLOGIA WI-FI

Wi-Fi é uma tecnologia de comunicação entre dispositivos que não utiliza fio e corresponde ao padrão 802.11 [83]. Essa tecnologia é usada em muitos projetos IoT por conta do baixo custo de implementação e mobilidade. Porém, há diversas questões de segurança, listadas a seguir que põem em risco a informação que trafega no enlace. De modo geral, a maior parte das vulnerabilidades são encontradas no protocolo WEP.

O protocolo WEP tem seu mecanismo de criptografia baseado no algoritmo RC4[55]. O algoritmo RC4 utiliza uma cifra (chave) e executa um XOR *bit* a *bit* na mensagem. Como medida de segurança adicional para implementação do protocolo WEP, foi adicionado um outro mecanismo de segurança, chamado de vetor de inicialização [84]. O vetor de inicialização é uma sequência de 24 *bits* que muda a cada transmissão no protocolo WEP. Mesmo com a utilização de ambos métodos, o protocolo WEP é inseguro e não deve mais ser utilizado, tendo em vista que há outros protocolos mais seguros disponíveis, como WPA2. Apesar da utilização de uma chave mais protegida (maior número de *bits*), o vetor de inicialização tem sempre 24 *bits*. Devido a pequeno tamanho do vetor de inicialização, o protocolo se torna suscetível a diversos ataques, como os apresentados na categoria de senhas, disponíveis na Seção 4.3.

- FMS *Attack* [31], [85] - O ataque FMS compromete a privacidade de usuários que usam o protocolo de segurança WEP. O atacante que utiliza esse ataque tem como objetivo recuperar a chave de encriptação através dos vetores de inicialização. Para encontrar a chave pode ser usando o ataque *Brute Force*.

- Korek *Attack* [31], [86] - O ataque Korek depende do FMS para achar a chave. Um atacante que utiliza do ataque Korek tem maior eficiência para recuperar a chave de encriptação, ou seja, com número menor de tentativas.

- PTW *Attack* [31], [87] - Possui duas novas melhorias em relação ao Korek e ao FMS. A primeira consiste em conseguir realizar o ataque com um número menor ainda de tentativas em relação ao Korek e a segunda melhoria consiste em analisar um conjunto de *bytes* de uma vez ao invés de ir *byte* a *byte*.

Dessa forma, um atacante consegue quebrar a criptografia do WEP com maior facilidade.

- *Google Replay Attack* [31], [85] - Consiste em colocar em página do *Google* como página inicial de uma rede Wi-Fi. Dessa forma cada usuário que acessar a rede pode estar sujeito a ter sua "*google log"* recolhida por um atacante, onde parte da chave de encriptação está contida.

- Chop Chop *Attack* [31], [85] - O *checksum* é um mecanismo utilizado para verificar se os dados foram corrompidos durante a transmissão de um quadro de dados no enlace. O ataque *Chop Chop* tem como alvo o *checksum* do protocolo WEP. O ataque se inicia quando um atacante faz uso do ataque *Brute Force* com alvo no *checksum* de um dispositivo que utiliza o protocolo WEP. Dessa forma, se torna possível recuperar a mensagem sem utilizar a chave de encriptação.

- Ohigashi-Mor *Attack* [31], [85] - Visa o protocolo de segurança WPA, que é utilizado pelo protocolo 802.11[85]. Um atacante que faz uso desse ataque pode injetar um pacote de dados malicioso em um dispositivo com tempo de 15 minutos no melhor caso.

- Michael *Attack* [31], [88] - O ataque *Michael* consiste em fazer a reversão do algoritmo Michael, que é utilizado em um mecanismo de segurança baseado em *hash*. Esse ataque permite a um atacante injetar um pacote de dados malicioso no dispositivo alvo.

- *The Hole196 Vulnerability* [31], [89] – Baseia-se em explorar uma falha do protocolo 802.11. Essa falha que permite um atacante enviar um falso pedido para acessar o ponto de acesso *Wi-Fi* junto com seu endereço MAC. Assim a tabela ARP do ponto de acesso *Wi-Fi* é atualizada com o endereço MAC do atacante e ele passa a receber cada quadro de dados transmitido pelo ponto de acesso *Wi-Fi*.

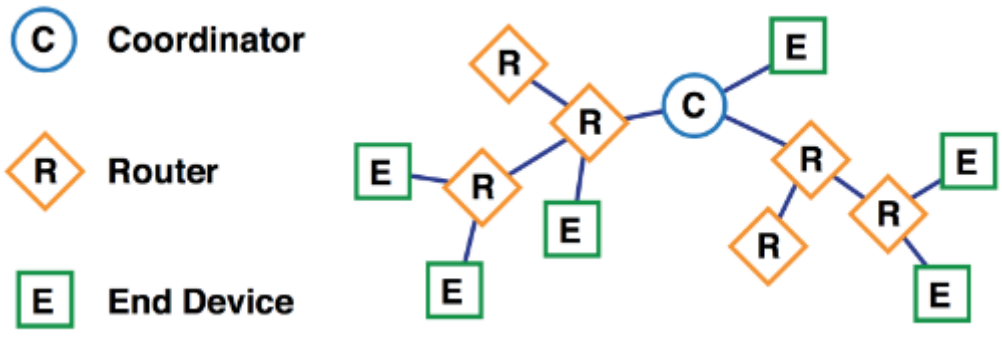
- *Dictionary Attack* [31], [85] - O ataque *Dictionary* é uma variação do ataque *Brute Force,* no qual as combinações testadas pelo atacante são palavras do

dicionário. Desta forma, o atacante tem um número de tentativas menor do que se testar todas as combinações de senhas. Isso ocorre, pois os administradores dos pontos de acesso *Wi-Fi* tendem a utilizar palavras do dicionário como senha para efetuar o *login* no ponto de acesso *Wi-Fi*.

5.6 TECNOLOGIA ZIGBEE

ZigBee é um protocolo desenvolvido para redes de dispositivos IoT [90]. Ele foi criado para fornecer comunicação segura, baixo consumo energético e com alcance de 100 metros. Diferentemente de WSN, os dispositivos não fazem parte do tráfego da rede e sim enviam seus dados para roteadores. Os roteadores ficam responsáveis por trafegar os dados e enviar ao coordenador. Os coordenadores controlam o tráfego dos dados, as questões de segurança e o envio de dados para uma rede externa. Os dispositivos finais, conhecidos como *Zigbee End Devices* (ZED), assumem as funções de sensor ou atuador em um sistema de IoT. A estrutura de coordenadores, roteadores e os dispositivos finais está ilustrada na Figura 8.

Figura 8 - Componentes ZigBee



Fonte: X. Fan, *et al.* [90]

ZigBee é um dos protocolos sem fio mais seguros para se utilizar em sistemas de IoT. Esse protocolo conta com chave de encriptação de 128 *bits*, chaves simétricas e um sistema de encriptação avançada AES[90]. As chaves de encriptação podem ser distribuídas durante a fabricação dos dispositivos, implantação do sistema ou durante funcionamento do sistema, através dos chamados "*Trust Center*" [91]. O dispositivo com permissão "*Trust Center*" fica responsável por distribuir as chaves no sistema durante o funcionamento do sistema. Porém, é possível que um usuário deixe a rede sem configuração de encriptação, deixando-a suscetível vazamento das informações. A seguir estão listados alguns ataques que abusam de vulnerabilidades encontradas no protocolo ZigBee.

- *Obtain The Key Attack* [31], [92] - Como a chave de encriptação tem que ser enviada por um "*Trust Center*" após o sistema estar em funcionamento. O ataque *Obtain The Key* consiste em um atacante usar *Eavesdropping* para capturar a chave de encriptação durante a transmissão da chave para um dispositivo. Esse ataque resulta no comprometimento de toda informação desse um dispositivo.

- *Redirecting Communication Attack* [31], [93] - Em ZigBee a comunicação pode ser redirecionada através do ataque *Redirecting Communication*. Isso permite que um atacante consiga não só obter o conteúdo confidencial transmitido, mas também alterar e redirecionar os pacotes de dados.

- ZED *Sabotage Attack* [31], [94] - O ataque ZED Sabotage pode ser entendido como uma sabotagem aos dispositivos finais em ZigBee. A sabotagem consiste em um atacante enviar sinais "*Wake Up*" periodicamente, com o fim de manter os dispositivos ligados e drenar sua bateria.

6 CONCLUSÃO

Este trabalho contém o resultado de um estudo sobre questões de segurança em Internet das Coisas (IoT), relacionando ataques às tecnologias de comunicação utilizadas, com ênfase em tecnologias que utilizam radiofrequência. O estudo utilizou 9 artigos publicados em periódicos como fonte primária de informação. Os critérios de seleção se basearem em aderência ao tema da pesquisa, número de citações do artigo e data da publicação, sendo priorizados artigos mais recentes.

Cada artigo selecionado para o estudo enumera diversos ataques a tecnologias utilizadas em Internet das Coisas. A partir dos artigos selecionados, foram identificados 142 ataques distintos, que se utilizam de variadas estratégias para obter sucesso. O estudo aplicou um critério adicional de seleção, e apenas ataques que utilizavam tecnologias baseadas em radiofrequência foram efetivamente listados. A partir desse último critério, o número de ataques identificados que atendem a esse critério é de 48 ataques, listados no Capítulo 5. No entanto, existem ataques relevantes que não envolvem radiofrequência, além de outras questões de segurança envolvendo IoT. Desta forma, o Capítulo 4 apresenta 18 ataques relevantes e três questões de segurança a se considerar.

Como oportunidades para trabalhos futuros, pode-se criar uma versão ampliada deste trabalho, incluindo os 86 ataques já identificados a partir dos 9 artigos selecionados, mas que não puderam ser incluídos neste trabalho devido a limitações de tempo. Outra possibilidade para ampliação deste trabalho consiste em aumentar o detalhamento da descrição de cada ataque identificado, incluindo exemplos e diagramas esquemáticos de funcionamento. Finalmente, uma futura versão poderia ser apresentada na forma de um dicionário de ataques, facilitando consultas realizadas por estudantes do tema "Segurança em Internet das Coisas".

REFERÊNCIAS BIBLIOGRÁFICAS

[1] S. Balaji, K. Nathani, e R. Santhakumar, “IoT Technology, Applications and Challenges: A Contemporary Survey”, *Wirel. Pers. Commun.*, vol. 108, nº 1, p. 363–388, 2019, doi: 10.1007/s11277-019-06407-w.

[2] C. González García, D. Meana-Llorián, B. Pelayo García-Bustelo, e J. Cueva Lovelle, “A review about Smart Objects, Sensors, and Actuators”, *Int. J. Interact. Multimed. Artif. Intell.*, vol. 4, p. 7–10, jan. 2017, doi: 10.9781/ijimai.2017.431.

[3] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, e N. Ghani, “Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations”, *IEEE Commun. Surv. Tutor.*, vol. 21, nº 3, p. 2702–2733, 2019, doi: 10.1109/COMST.2019.2910750.

[4] J. F. Kurose e K. W. Ross, *Computer Networking A Top-Down Approach Featuring the Internet*. Addison-Wesley, 2000.

[5] G. P. de Carvalho, “Uma reflexão sobre a rede mundial de computadores”, *Soc. E Estado*, vol. 21, p. 549–554, ago. 2006, doi: 10.1590/S0102-69922006000200010.

[6] M. V. Pawar e J. Anuradha, “Network Security and Types of Attacks in Network”, *Procedia Comput. Sci.*, vol. 48, p. 503–506, jan. 2015, doi: 10.1016/j.procs.2015.04.126.

[7] S. M. Tahsien, H. Karimipour, e P. Spachos, “Machine learning based solutions for security of Internet of Things (IoT): A survey”, *J. Netw. Comput. Appl.*, vol. 161, p. 102630, jul. 2020, doi: 10.1016/j.jnca.2020.102630.

[8] P. Suresh, J. V. Daniel, V. Parthasarathy, e R. H. Aswathy, “A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment”, em *2014 International Conference on Science Engineering and Management Research (ICSEMR)*, nov. 2014, p. 1–8. doi: 10.1109/ICSEMR.2014.7043637.

[9] M. C. Domingo, “An overview of the Internet of Things for people with disabilities”, *J. Netw. Comput. Appl.*, vol. 35, nº 2, p. 584–596, mar. 2012, doi: 10.1016/j.jnca.2011.10.015.

[10] “What Is Edge Computing? Everything You Need to Know”, *SearchDataCenter*. https://www.techtarget.com/searchdatacenter/definition/edge-computing (acessado 26 de março de 2022).

[11] K. Cao, Y. Liu, G. Meng, e Q. Sun, “An Overview on Edge Computing Research”, *IEEE Access*, vol. 8, p. 85714–85728, 2020, doi: 10.1109/ACCESS.2020.2991734.

[12] L. Jiao, R. Friedman, X. Fu, S. Secci, Z. Smoreda, e H. Tschofenig, “Cloud-based computation offloading for mobile devices: State of the art, challenges and opportunities”, *2013 Future Netw. Mob. Summit*, p. 1–11, 2013.

[13] C.-W. Tsai, C.-F. Lai, H.-C. Chao, e A. V. Vasilakos, “Big data analytics: a survey”, *J. Big Data*, vol. 2, nº 1, p. 21, out. 2015, doi: 10.1186/s40537-015-0030-3.

[14] S. Zhao, F. Blaabjerg, e H. Wang, “An Overview of Artificial Intelligence Applications for Power Electronics”, *IEEE Trans. Power Electron.*, vol. 36, nº 4, p. 4633–4658, abr. 2021, doi: 10.1109/TPEL.2020.3024914.
[15] F. Sadri, “Ambient intelligence: A survey”, *ACM Comput. Surv.*, vol. 43, nº 4, p. 1–66, out. 2011, doi: 10.1145/1978802.1978815.
[16] F. Hussain, R. Hussain, S. A. Hassan, e E. Hossain, “Machine Learning in IoT Security: Current Solutions and Future Challenges”, *IEEE Commun. Surv. Tutor.*, vol. 22, nº 3, p. 1686–1721, 2020, doi: 10.1109/COMST.2020.2986444.
[17] S. Boschert, C. Heinrich, e R. Rosen, *Next Generation Digital Twin*. 2018.
[18] M. del R. Pérez-Salazar, A. A. A. Lasserre, M. G. Cedillo-Campos, e J. C. H. González, “The role of knowledge management in supply chain management: A literature review”, *J. Ind. Eng. Manag.*, vol. 10, nº 4, Art. nº 4, out. 2017, doi: 10.3926/jiem.2144.
[19] V. Gazis, “A Survey of Standards for Machine-to-Machine and the Internet of Things”, *IEEE Commun. Surv. Tutor.*, vol. 19, nº 1, p. 482–511, 2017, doi: 10.1109/COMST.2016.2592948.
[20] J. C.T., J. Sahil, e W. Catherine I., “Effects of sentence structure and word complexity on intelligibility in machine-to-human communications”, *Comput. Speech Lang.*, vol. 58, p. 203–215, nov. 2019, doi: 10.1016/j.csl.2019.03.002.
[21] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, e S. Shieh, “IoT Security: Ongoing Challenges and Research Opportunities”, em *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, nov. 2014, p. 230–234. doi: 10.1109/SOCA.2014.58.
[22] C. Wohlin, “Guidelines for snowballing in systematic literature studies and a replication in software engineering”, em *Proceedings of the 18th international conference on evaluation and assessment in software engineering*, 2014, p. 1–10.
[23] M. Burhan, R. A. Rehman, B. Khan, e B.-S. Kim, “IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey”, *Sensors*, vol. 18, nº 9, Art. nº 9, set. 2018, doi: 10.3390/s18092796.
[24] M. A. Khan e K. Salah, “IoT security: Review, blockchain solutions, and open challenges”, *Future Gener. Comput. Syst.*, vol. 82, p. 395–411, maio 2018, doi: 10.1016/j.future.2017.11.022.
[25] A. Barua, M. A. Al Alamin, Md. S. Hossain, e E. Hossain, “Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey”, *IEEE Open J. Commun. Soc.*, vol. 3, p. 251–281, 2022, doi: 10.1109/OJCOMS.2022.3149732.
[26] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, e M. Imran, “Perception layer security in Internet of Things”, *Future Gener. Comput. Syst.*, vol. 100, p. 144–164, nov. 2019, doi: 10.1016/j.future.2019.04.038.
[27] K. Zhang, X. Liang, R. Lu, e X. Shen, “Sybil attacks and their defenses in the internet of things”, *IEEE Internet Things J.*, vol. 1, nº 5, p. 372–383, 2014.
[28] A. Raoof, A. Matrawy, e C.-H. Lung, “Routing Attacks and Mitigation Methods for RPL-Based Internet of Things”, *IEEE Commun. Surv. Tutor.*, vol. 21, nº 2, p. 1582–1606, 2019, doi: 10.1109/COMST.2018.2885894.
[29] B. K. Mohanta, D. Jena, U. Satapathy, e S. Patnaik, “Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology”, *Internet Things*, vol. 11, p. 100227, set. 2020, doi: 10.1016/j.iot.2020.100227.

[30] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, e W. Zhao, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications”, *IEEE Internet Things J.*, vol. 4, nº 5, p. 1125–1142, out. 2017, doi: 10.1109/JIOT.2017.2683200.

[31] H. Akram, D. Konstantas, e M. Mahyoub, “A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model”, *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, nº 3, 2018, doi: 10.14569/IJACSA.2018.090349.

[32] A. Cui e S. J. Stolfo, “Reflections on the engineering and operation of a large-scale embedded device vulnerability scanner”, em *Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security - BADGERS ’11*, Salzburg, Austria, 2011, p. 8–18. doi: 10.1145/1978672.1978674.

[33] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, e E. Almomani, “A Survey of Phishing Email Filtering Techniques”, *IEEE Commun. Surv. Tutor.*, vol. 15, nº 4, p. 2070–2090, 2013, doi: 10.1109/SURV.2013.030713.00020.

[34] Z. Wu, N. Evans, T. Kinnunen, J. Yamagishi, F. Alegre, e H. Li, “Spoofing and countermeasures for speaker verification: A survey”, *Speech Commun.*, vol. 66, p. 130–153, fev. 2015, doi: 10.1016/j.specom.2014.10.005.

[35] L. F. Eliyan e R. Di Pietro, “DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges”, *Future Gener. Comput. Syst.*, vol. 122, p. 149–171, set. 2021, doi: 10.1016/j.future.2021.03.011.

[36] “DoS, DDoS e Botnets”. https://www.gta.ufrj.br/grad/15_1/dos/pages/dos.html (acessado 16 de junho de 2022).

[37] N. Sivasankari e S. Kamalakkannan, “Detection and prevention of man-in-the-middle attack in iot network using regression modeling”, *Adv. Eng. Softw.*, vol. 169, p. 103126, 2022.

[38] K. J. Higgins, “Hacker’s Choice: Top Six Database Attacks”, *Dark Read.*, 2008.

[39] S. Babar, A. Stango, N. Prasad, J. Sen, e R. Prasad, “Proposed embedded security framework for Internet of Things (IoT)”, em *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE)*, fev. 2011, p. 1–5. doi: 10.1109/WIRELESSVITAE.2011.5940923.

[40] A. T. Karygiannis, B. Eydt, G. Barber, L. Bunn, e T. Phillips, “Guidelines for securing Radio Frequency Identification (RFID) systems”, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-98, 2007. doi: 10.6028/NIST.SP.800-98.

[41] M. Stevens, A. Lenstra, e B. de Weger, “Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities”, em *Advances in Cryptology - EUROCRYPT 2007*, Berlin, Heidelberg, 2007, p. 1–22. doi: 10.1007/978-3-540-72540-4_1.

[42] S. Mohite *et al.*, “RFID Security Issues”, *Int. J. Eng. Res. Technol.*, vol. Volume 2, p. 746–748, set. 2013.

[43] A. Mitrokotsa, M. R. Rieback, e A. S. Tanenbaum, “Classifying RFID attacks and defenses”, *Inf. Syst. Front.*, vol. 12, nº 5, p. 491–505, nov. 2010, doi: 10.1007/s10796-009-9210-z.

[44] A. Liu e P. Ning, “TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks”, em *2008 International Conference on In-*

formation Processing in Sensor Networks (ipsn 2008), abr. 2008, p. 245–256. doi: 10.1109/IPSN.2008.47.

[45] H. J. Tay, J. Tan, e P. Narasimhan, “A Survey of Security Vulnerabilities in Bluetooth Low Energy Beacons”, p. 9.

[46] R. T. Prapty, S. Azmin Md, S. Hossain, e H. S. Narman, “Preventing Session Hijacking using Encrypted One-Time-Cookies”, em *2020 Wireless Telecommunications Symposium (WTS)*, abr. 2020, p. 1–6. doi: 10.1109/WTS48268.2020.9198717.

[47] A. Mukaddam, I. Elhajj, A. Kayssi, e A. Chehab, “IP Spoofing Detection Using Modified Hop Count”, em *2014 IEEE 28th International Conference on Advanced Information Networking and Applications*, maio 2014, p. 512–516. doi: 10.1109/AINA.2014.62.

[48] D. Puthal, S. Nepal, R. Ranjan, e J. Chen, “Threats to networking cloud and edge datacenters in the Internet of Things. IEEE Cloud Comput”, *IEEE Cloud Comput.*, vol. 3, nº 3, p. 64–71, jun. 2016, doi: 10.1109/MCC.2016.63.

[49] “Exploit Attack in Network Layer”. http://searchsecurity.techtarget.com/definition/exploit (acessado 6 de janeiro de 2018).

[50] The OWASP Foundation, “Owasp top 10 - 2013 the ten most critical web applications security risks”.

[51] S. Hashemi e M. Zarei, “Internet of Things backdoors: Resource management issues, security challenges, and detection methods”, *Trans. Emerg. Telecommun. Technol.*, vol. 32, nº 2, fev. 2021, doi: 10.1002/ett.4142.

[52] I. Andrea, C. Chrysostomou, e G. Hadjichristofi, “Internet of Things: Security vulnerabilities and challenges”, em *2015 IEEE Symposium on Computers and Communication (ISCC)*, jul. 2015, p. 180–187. doi: 10.1109/ISCC.2015.7405513.

[53] W. Dawoud, I. Takouna, e C. Mainel, “Infrastructure as a service security: Challenges and solutions”.

[54] R. E. Spekman e P. J. Sweeney, “RFID: from concept to implementation”, *Int. J. Phys. Distrib. Logist. Manag.*, vol. 36, nº 10, p. 736–754, jan. 2006, doi: 10.1108/09600030610714571.

[55] A. T. Karygiannis, B. Eydt, G. Barber, L. Bunn, e T. Phillips, “Guidelines for securing Radio Frequency Identification (RFID) systems”, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-98, 2007. doi: 10.6028/NIST.SP.800-98.

[56] G. Kulkarni, R. Shelke, R. Sutar, e S. Mohite, “‘RFID security issues amp; challenges’”, em *2014 International Conference on Electronics and Communication Systems (ICECS)*, fev. 2014, p. 1–4. doi: 10.1109/ECS.2014.6892730.

[57] A. Mitrokotsa, M. R. Rieback, e A. S. Tanenbaum, “Classifying RFID attacks and defenses”, *Inf. Syst. Front.*, vol. 12, nº 5, p. 491–505, nov. 2010, doi: 10.1007/s10796-009-9210-z.

[58] I. Andrea, C. Chrysostomou, e G. Hadjichristofi, “Internet of Things: Security vulnerabilities and challenges”, em *2015 IEEE Symposium on Computers and Communication (ISCC)*, jul. 2015, p. 180–187. doi: 10.1109/ISCC.2015.7405513.

[59] G. Kulkarni, R. Shelke, R. Sutar, e S. Mohite, “RFID security issues & challenges”, em *2014 International Conference on Electronics and Communication Systems (ICECS)*, 2014, p. 1–4.

[60] R. Aggarwal e M. L. Das, “RFID security in the context of ‘internet of things’”, em *Proceedings of the First International Conference on Security of Internet of Things*, New York, NY, USA, ago. 2012, p. 51–56. doi: 10.1145/2490428.2490435.
[61] A. A. Kumar S., K. Ovsthus, e L. M. Kristensen., “An Industrial Perspective on Wireless Sensor Networks — A Survey of Requirements, Protocols, and Challenges”, *IEEE Commun. Surv. Tutor.*, vol. 16, nº 3, p. 1391–1412, 2014, doi: 10.1109/SURV.2014.012114.00058.
[62] M. Prabu, S. V. Rani, R. S. Kumar, e P. Venkatesh, “Dos attacks and defenses at the network layer in ad-hoc and sensor wireless networks, wireless ad-hoc sensor networks: A short survey”, *Middle-East J. Sci. Res.*, vol. 23, nº 5, p. 779–784, 2015.
[63] S. Gurung e S. Chauhan, “A dynamic threshold based approach for mitigating black-hole attack in MANET”, *Wirel. Netw.*, vol. 24, nº 8, p. 2957–2971, nov. 2018, doi: 10.1007/s11276-017-1514-1.
[64] C. Karlof e D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures”, *Ad Hoc Netw.*, vol. 1, nº 2, p. 293–315, set. 2003, doi: 10.1016/S1570-8705(03)00008-8.
[65] D. R. Raymond e S. F. Midkiff, “Denial-of-service in wireless sensor networks: Attacks and defenses”, *IEEE Pervasive Comput.*, vol. 7, nº 1, p. 74–81, 2008.
[66] A. A. Pirzada e C. McDonald, “Circumventing sinkholes and wormholes in wireless sensor networks”, em *IWWAN’05: Proceedings of International Workshop on Wireless Ad-hoc Networks*, 2005, vol. 71.
[67] M. Meghdadi, S. Ozdemir, e I. Güler, “A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks”, *IETE Tech. Rev.*, vol. 28, nº 2, p. 89, 2011, doi: 10.4103/0256-4602.78089.
[68] E. D. Cardenas, “Mac spoofing–an introduction”, *GIAC Secur. Essent. Certif. GSEC*, 2003.
[69] M. Ryan, “Bluetooth: With low energy comes low security”, 2013.
[70] T. Rosa, “Bypassing Passkey Authentication in Bluetooth Low Energy”, *Cryptol. EPrint Arch.*, 2013, Acessado: 25 de maio de 2022. [Online]. Disponível em: https://eprint.iacr.org/2013/309
[71] G. Kwon, J. Kim, J. Noh, e S. Cho, “Bluetooth low energy security vulnerability and improvement method”, em *2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*, out. 2016, p. 1–4. doi: 10.1109/ICCE-Asia.2016.7804832.
[72] S. S. Hassan, S. D. Bibon, M. S. Hossain, e M. Atiquzzaman, “Security threats in Bluetooth technology”, *Comput. Secur.*, vol. 74, p. 308–322, maio 2018, doi: 10.1016/j.cose.2017.03.008.
[73] J. Dunning, “Taming the Blue Beast: A Survey of Bluetooth Based Threats”, *IEEE Secur. Priv.*, vol. 8, nº 2, p. 20–27, mar. 2010, doi: 10.1109/MSP.2010.3.
[74] A. K. Das, P. H. Pathak, C.-N. Chuah, e P. Mohapatra, “Uncovering Privacy Leakage in BLE Network Traffic of Wearable Fitness Trackers”, em *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*, St. Augustine Florida USA, fev. 2016, p. 99–104. doi: 10.1145/2873587.2873594.
[75] “Ubertooth One - Great Scott Gadgets”. https://greatscottgadgets.com/ubertoothone/ (acessado 25 de maio de 2022).

[76] M. Herfurt e C. Mulliner, “Remote device identification based on Bluetooth fingerprinting techniques”, *Trifinite Group White Pap.*, 2004.
[77] G. Celosia e M. Cunche, “Fingerprinting bluetooth-low-energy devices based on the generic attribute profile”, em *Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things*, 2019, p. 24–31.
[78] P. Sivakumaran e J. Blasco, “A Study of the Feasibility of Co-located App Attacks against {BLE} and a {Large-Scale} Analysis of the Current {Application-Layer} Security Landscape”, em *28th USENIX Security Symposium (USENIX Security 19)*, 2019, p. 1–18.
[79] N. B.-N. I. Minar e M. Tarique, “Bluetooth security threats and solutions: a survey”, *Int. J. Distrib. Parallel Syst.*, vol. 3, nº 1, p. 127, 2012.
[80] A. Elbagoury, A. Mohsen, M. Ramadan, e M. Youssef, “Practical provably secure key sharing for near field communication devices”, em *2013 International Conference on Computing, Networking and Communications (ICNC)*, jan. 2013, p. 750–755. doi: 10.1109/ICCNC.2013.6504182.
[81] E. Haselsteiner e K. Breitfuß, *Security in Near Field Communication (NFC)-Strengths and Weaknesses (2006)*.
[82] C. H. Chen, I. C. Lin, e C. C. Yang, “NFC Attacks Analysis and Survey”, em *2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, jul. 2014, p. 458–462. doi: 10.1109/IMIS.2014.66.
[83] T. Mekhaznia e A. Zidani, “Wi-Fi Security Analysis | Elsevier Enhanced Reader”. https://reader.elsevier.com/reader/sd/pii/S1877050915034705?token=F38E917D83D82DA150AF3231E8E0F91BA35A71C8D7EDB138610096BA4E48DF858C52C419325018CE7678BD36C66BACF7&originRegion=us-east-1&originCreation=20220518020453 (acessado 17 de maio de 2022).
[84] N. Murilo, *Segurança em Redes sem fio: Aprenda a Proteger Suas Informações em Ambientes Wi-Fi e Bluetooth*. Novatec Editora.
[85] M. Caneill e J.-L. Gilis, “Attacks against the WiFi protocols WEP and WPA”, *J. No Dec.*, 2010.
[86] E. Tews e M. Beck, “Practical attacks against WEP and WPA”, em *Proceedings of the second ACM conference on Wireless network security*, 2009, p. 79–86.
[87] A. Bittau, M. Handley, e J. Lackey, “The final nail in WEP’s coffin”, em *2006 IEEE Symposium on Security and Privacy (S&P’06)*, 2006, p. 15 pp. – 400.
[88] M. Beck, “Enhanced TKIP michael attacks”, *ArXiv Prepr. ArXiv14106295*, 2014.
[89] M. S. Ahmad, “Wpa too!”, *DEF CON*, vol. 18, 2010.
[90] X. Fan, F. Susan, W. Long, e S. Li, “Security Analysis of Zigbee”, p. 18.
[91] NXP Semiconductors 2018, *ZigBee 3.0 Stack User Guide*. NXP Semiconductors, 2018.
[92] J. Wright, “KillerBee: Practical ZigBee Exploitation Framework or” Wireless Hacking and the Kinetic World””, em *Proc. 11th ToorCon Conf*, 2018, p. 1–39.
[93] P. Dowland, V. Grout, M. Knahl, e B. Humm, *SEIN2011: Proceedings of the Seventh Collaborative Research Symposium*. Lulu.com, 2011.
[94] N. Vidgren, K. Haataja, J. L. Patiño-Andres, J. J. Ramírez-Sanchis, e P. Toivanen, “Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned”, em *2013 46th Hawaii International Conference on System Sciences*, jan. 2013, p. 5132–5138. doi: 10.1109/HICSS.2013.475.