UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE MATEMÁTICA
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

OLIVER AUGUSTO ALVES SARTORI

IDENTIFICAÇÃO POR RADIOFREQUÊNCIA

Estudo teórico e prática aplicada ao controle de acesso

RIO DE JANEIRO
2020

OLIVER AUGUSTO ALVES SARTORI

IDENTIFICAÇÃO POR RADIOFREQUÊNCIA

Estudo teórico e prática aplicada ao controle de acesso

Trabalho de conclusão de curso de graduação apresentado ao Departamento de Ciência da Computação da Universidade Federal do Rio de Janeiro como parte dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. Claudio Miceli de Farias
Co-orientador: Profa. Valeria Menezes Bastos

RIO DE JANEIRO
2020

CIP - Catalogação na Publicação

S251i

Sartori, Oliver Augusto Alves
Identificação por radiofrequência: estudo teórico e prática aplicada ao controle de acesso / Oliver Augusto Alves Sartori. -- Rio de Janeiro, 2020.
96 f.

Orientador: Claudio Miceli de Farias.
Coorientador: Valeria Menezes Bastos.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Instituto de Matemática, Bacharel em Ciência da Computação, 2020.

1. Rfid. 2. Identificação por radiofrequência. 3. Controle de acesso. I. Farias, Claudio Miceli de, orient. II. Bastos, Valeria Menezes, coorient. III. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

OLIVER AUGUSTO ALVES SARTORI

IDENTIFICAÇÃO POR RADIOFREQUÊNCIA
Estudo teórico e prática aplicada ao controle de acesso

Trabalho de conclusão de curso de graduação apresentado ao Departamento de Ciência da Computação da Universidade Federal do Rio de Janeiro como parte dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Aprovado em 01 de Outubro de 2020

BANCA EXAMINADORA:

Claudio Miceli de Farias
D.Sc. (UFRJ)

Valeria Menezes Bastos
D.Sc. (UFRJ)

Participação por vídeo-conferência
Silvana Rossetto
D.Sc. (UFRJ)

Participação por vídeo-conferência
Carlos Mendes
D.Sc. (UFRJ)

AGRADECIMENTOS

Gostaria de agradecer aos meus pais, José Faria e Maria Helena, por todo amor incondicional que me deram e dão até hoje.

Agradeço a todos os professores que me acompanharam durante a graduação, em especial aos professores Severino Collier Coutinho e Valeria Menezes Bastos por me guiarem e suportarem durante todos estes anos, e ao professor Claudio Miceli de Farias pela realização desta monografia.

Por fim, mas não menos importante, agradeço aos meus amigos por toda alegria e suporte que me deram nesta reta final, em especial ao Oliveira Lima, por enxergar em mim um potencial que nem eu mesmo via; o melhor amigo e mentor que eu jamais imaginei que teria.

"Todas as vitórias ocultam uma abdicação."

Simone de Beauvoir

RESUMO

Sistemas de identificação por radiofrequência estão se tornando cada vez mais comuns e presentes no cotidiana, facilitando a vida de uma parcela cada vez maior da população. A tecnologia vem expandindo cada vez mais seus usos, não servindo mais apenas para marcação e rastreio de produtos ou animais, mas também como meio de pagamento e chave de acesso em portas e catracas. Explorando o que há de mais fundamental da tecnologia, os objetivos deste trabalho são: torna-se um material rico e sólido sobre a tecnologia de identificação por radiofrequência em língua portuguesa e implementar um sistema de identificação por radiofrequência de etiquetas passivas de alta frequência no Instituto Tércio Pacitti (NCE/UFRJ), a fim de automatizar, agilizar e controlar o fluxo de entrada e saída de docentes, alunos e funcionários do instituto.

Palavras-chave: rfid. radiofrequência. alta frequência. etiqueta passiva. controle de acesso.

ABSTRACT

Radiofrequency identification systems are becoming more and more common and present in everyday life, facilitating the life of a growing portion of the population. The technology is increasingly expanding its uses, no longer serving only for marking and screening of products or animals, but also as a means of payment and key access in doors and ratchets. Exploring what is most fundamental about technology, the objectives of this work are: it becomes a rich and solid material on the radio frequency identification technology in Portuguese and to implement a radio frequency identification system for passive high frequency tags at Instituto Tércio Pacitti (NCE / UFRJ), in order to automate, streamline and control the flow of incoming and outgoing teachers, students and institute staff.

Keywords: rfid. radiofrequency. high frequency. passive tag. access control.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

UFRJ	Universidade Federal do Rio de Janeiro
DCC	Departamento de Ciência da Computação
NCE	Núcleo de Computação Eletrônica
RFID	Radio frequency identification
LF	Low frequency
HF	High frequency
UHF	Ultra high frequency
Hz	Hertz
KHz	kiloHertz
MHz	megaHertz
GHz	gigaHertz
SI	Sistema Internacional de Unidades
DoS	Denial of Service
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
EPC	Electronic Product Code
MIT	Massachusetts Institute of Technology
Gen-1	Padrão EPCglobal Generation-1
Gen-2	Padrão EPCglobal Generation-2
TID	Tag Identifier
HDX	Half-duplex
FDX	Full-duplex
SEQ	Sequential systems
SDMA	Space Division Multiple Access

FDMA	Frequency Domain Multiple Access
TDMA	Time Domain Multiple Access
CDMA	Code Division Multiple Access
SDM	Space-division multiplexing
FDM	Frequency-division multiplexing
TDM	Time-division multiplexing
CDM	Code-division multiplexing
ASK	Amplitude Shift Keying
PSK	Phase Shift Keying
FSK	Frequency Shift Keying
GPIO	General Purpose Input/Output
HDMI	High-Definition Multimedia Interface
USB	Universal Serial Bus
A	Ampere
mA	miliampere
V	Volts
UART	Universal Asynchrounous Receiver/Transmiter
SPI	Serial Peripheral Interface
I2C	Inter-Integrated Circuit
kbit/s	kilobit por segundo
cm	centímetros
CRC	Cyclic Redundancy Check
LAN	Local Area Network
BPSK	Binary Phase Shift Keying
SGBD	Sistema de Gerenciamento de Banco de Dados
IOT	Internet of Things

LTS	Long-Term Support
UNIP	Universidade Paulista
RTC	Real Time Clock
LCD	Liquid Crystal Display

SUMÁRIO

1 INTRODUÇÃO

Ao longo das décadas o ser humano tem estudado e empregado cada vez mais tecnologias de comunicação sem fio no seu cotidiano, como o rádio, a televisão, as conexões de Internet *wi-fi*, os acessórios *bluetooth*, entre outros. Entretanto, uma nova área vem crescendo exponencialmente e ganhando cada vez mais espaço nos últimos anos, que é a tecnologia de Identificação por Radiofrequência (RFID).

RFID, sigla em inglês para *Radio-frequency identification*, ou Identificação por Radiofrequência em português, pode ser definida como um modo automático de identificação que usa ondas de rádio para detectar, rastrear, identificar e gerenciar objetos, seres ou indivíduos (XIAO; GIBBONS; LEBRUN, 2009).

Todo sistema RFID é composto por pelo menos três componentes básicos: uma antena, um transceptor (com decodificador) e um *transponder*, também conhecido como "etiqueta" (DOMDOUZIS; KUMAR; ANUMBA, 2007), e podem ser classificados quanto à frequência em que operam (baixa frequência, alta frequência, ultra-alta frequência ou micro-ondas) e quanto ao tipo de etiquetas utilizadas (passiva ou ativa).

A ideia do RFID não é nova, muito pelo contrário, os primórdios da tecnologia datam da década de 1940. Durante a Segunda Guerra Mundial os britânicos desenvolveram a tecnologia *"Identity Friend or Foe"* (Identificar Aliado ou Inimigo) que tinha como objetivo distinguir aeronaves aliadas de aeronaves inimigas durante o retorno das mesmas para a base aérea. Esta tecnologia utilizava-se de um transponder colocado em cada aeronave aliada, que, quando interrogado por um sinal oriundo das bases aéreas, respondia apropriadamente (DOMDOUZIS; KUMAR; ANUMBA, 2007). Após anos de pesquisa a tecnologia evoluiu para fins mais nobres, sendo empregada em diversas áreas, tais como: Controle de acesso, marcação de animais, pagamento, marcação em nível de item, entre outros (CHAWLA; HA, 2007).

Tão antiga quanto a tecnologia de RFID são os problemas do Instituto Tércio Pacitti, da Universidade Federal do Rio de Janeiro (UFRJ), com o seu controle de acesso. O Instituto, também conhecido como Núcleo de Computação Eletrônica (NCE), é um instituto da UFRJ que tem como objetivo: "contribuir de forma inequívoca para o domínio da tecnologia de computação no país, através de sua atuação na pesquisa e no ensino de graduação e pós-graduação de Informática." (RODRIGUES, 2019). O mesmo é responsável por abrigar grandes projetos da universidade, tais como: o supercomputador Netuno [1], o Sistema Integrado de Gestão Acadêmica (SIGA), responsável por agregar todos os sistemas de registro acadêmico [2], os grupos de extensão do Departamento de Ciência da Computação (DCC), dentre outros.

[1] <https://ufrj.br/noticia/2015/10/22/ufrj-inaugura-super-computador>
[2] <http://www.nce.ufrj.br/servicos/siga/default.asp>

Durante vários anos o controle de acesso ao NCE fora realizado através de cartões de papel e plástico com códigos de barras embutidos. No caso de professores e funcionários, o cartão tinha acesso liberado permanentemente, no caso de alunos, o acesso tinha que ser liberado manualmente e individualmente pelos seguranças ou funcionários da instituição, o que sempre gerava filas e atrasos quando o fluxo de alunos ou visitantes era muito grande. Entretanto, problemas com este sistema ocorreram e todo ele teve que ser desabilitado, permitindo assim a entrada de qualquer pessoa nas dependências do instituto sem a necessidade de identificação ou qualquer outro controle. Esta falha no controle de acesso, e consequentemente de segurança, acaba por expor alunos, professores, funcionários, bens materiais, bens intelectuais e dados da UFRJ a um maior risco.

Com o objetivo de resolver os problemas de controle de acesso do Instituto Tércio Pacitti, fomos atrás de uma solução que pudesse ser implementada de forma simples, eficaz e sem gerar grandes custos financeiros à instituição onde, após um período de pesquisas e estudos, chegamos a tecnologia de identificação por radiofrequência (RFID). Assim, utilizando os ensinamentos aprendidos durante a graduação em ciência da computação e os conceitos do RFID, esta monografia nasce com o objetivo de elaborar e implementar um sistema de identificação de usuários através da tecnologia RFID de alta frequência, que seja economicamente barato, tecnicamente viável do ponto de vista de implementação e que seja possível de ser implementada no Instituto Tércio Pacitti da UFRJ, a fim de automatizar, agilizar e melhor controlar o fluxo de passagem de docentes, alunos e funcionários nas dependências do instituto. Desta forma, esta monografia gira em torno de 3 pilares básicos: RFID, baixo custo econômico (barato), baixa complexidade técnica de implementação, sendo estes seus atrativos principais.

Para além dos nossos muros, durante a elaboração desta monografia percebemos um segundo problema: a grande maioria do material encontrado sobre o assunto encontra-se em inglês. Apesar do idioma não ser uma barreira para o autor ou seus orientadores, compreendemos que a mesma não é de domínio universal por todos os brasileiros. Entendemos também que a tecnologia de RFID é demasiada útil e versátil para ficar restrita apenas àqueles que compreendem o idioma inglês. Assim, esta monografia ganhou um segundo objetivo durante seu desenvolvimento: tornar-se um material rico e sólido sobre a tecnologia de identificação por radiofrequência em língua portuguesa. Este objetivo, que nasceu como "secundário"durante o processo, tornou-se tão sólido e interessante para o autor que acabou se tornando tão importante quanto a implementação do projeto.

O fluxo geral de funcionamento do sistema se dará da seguinte forma: uma catraca, contendo internamente um microcontrolador e 2 módulos leitores RFID, é posicionada em um ponto onde se deseja controlar o acesso. O usuário que desejar passar pela catraca deverá primeiro aproximar um cartão RFID do módulo leitor, caso o identificador do cartão esteja cadastrado no banco de dados, o acesso é liberado, caso contrário, o acesso é negado. Para realizar tal tarefa, foram escolhidos equipamentos de *hardware*, em

exceção a catraca, que possuem preço acessível e são amplamente conhecidos e documentados no meio da eletrônica, como o Raspberry Pi e o módulo RFID-RC522. De forma similar, as soluções de *software* foram desenvolvidas sob demanda, utilizando linguagens de programação fáceis e *open-source*, como Python e PHP.

Para facilitar a implementação, o sistema foi dividido em dois módulos: controle e comando, onde cada módulo foi dividida em dois submódulos: *hardware* e *software*. O módulo de controle trata dos componentes que estão diretamente ligados ao ponto de controle de acesso, como microcontrolador, módulos RFID, codificador rotativo e programa de consulta, enquanto o módulo de comando trata dos componentes do *back-end*, tais como banco de dados e aplicações de gerenciamento de usuários e operadores do sistema. Os submódulos *hardware* e *software* tratam, respectivamente, dos equipamentos físicos e das lógicas computacionais empregados em cada módulo.

Esta monografia encontra-se organizada da seguinte forma: O capítulo 1, Introdução, descreve a motivação por trás deste trabalho. O Capítulo 2, Identificação por radiofrequência, descreve diversos conceitos da tecnologia, desde a física até questões de segurança. O capítulo 3, Trabalhos acadêmicos relacionados, descreve trabalhos similares a este presentes na literatura, além de os comparar com esta monografia. O capítulo 4, Desenvolvimento, começa introduzindo a proposta do projeto, como o fluxo de funcionamento foi pensado e como a implementação que viria à seguir seria dividida para, em seguida, descrever detalhadamente o processo de implementação do projeto, desde a escolha inicial dos equipamentos e das tecnologias, dos porquês de cada uma, até os detalhes sobre a implementação. O capítulo 5, Conclusões e trabalhos futuros, descreve os resultados alcançados do projeto, o que foi possível e não foi possível fazer, além de uma seção sobre como este trabalho poderia ser melhorado e aperfeiçoado.

2 IDENTIFICAÇÃO POR RADIOFREQUÊNCIA

Abordaremos neste capítulo os conceitos que permeiam e explicam a tecnologia de identificação por radiofrequência. Começaremos pelos conceitos físicos da tecnologia, depois veremos os principais componentes de um sistema RFID e, por fim, como o sistema funciona de fato. Compreendido os conceitos básicos passaremos para alguns preceitos relevantes, como as instituições e normativas que definem e regulam a tecnologia e os problemas de segurança conhecidos.

2.1 A FÍSICA POR TRÁS DA TECNOLOGIA

Nesta seção serão abordados alguns dos princípios físicos que embasam o funcionamento da tecnologia de identificação por radiofrequência.

Identificação por radiofrequência, como o nome sugere, utiliza-se das ondas de rádio para seu funcionamento, porém, antes de explicar o que são ondas de rádio é necessário explicar o que são ondas e, posteriormente, o que são ondas eletromagnéticas pois, como ver-se-á em breve, ondas de rádio são na verdade uma parte do espectro das ondas eletromagnéticas.

2.1.1 Ondas

O que é onda? Uma onda ocorre quando um sistema é deslocado do seu equilíbrio, e a perturbação se propaga ao longo de uma região, carregando consigo energia. Assim, uma onda pode ser caracterizada como qualquer perturbação em um sistema que se propaga por um meio e onde apenas energia é transportada (YOUNG; FREEDMAN, 2008). A figura 1 exemplifica diversas ondas em uma superfície líquida.

Ondas podem ser classificadas em ondas mecânicas e ondas eletromagnéticas e esta classificação deve-se principalmente à natureza da onda e ao meio em que podem se propagar. Ondas mecânicas necessitam de um meio físico para se propagarem pois transportam energia cinética e potencial durante seu deslocamento. Já ondas eletromagnéticas não necessitam de um meio material, podendo se propagar inclusive no vácuo, isto porque são o resultado da oscilação combinada entre campo elétrico e campo magnético (SOFISICA, 2019).

Uma onda possui cinco características básicas: amplitude, comprimento de onda, período, frequência e velocidade de onda.

Amplitude pode ser definida como: o deslocamento máximo de um objeto oscilando em torno da sua posição de equilíbrio (URONE; HINRICHS, 2017). Em ondas longitudinais, por exemplo, amplitude seria a distância vertical entre o eixo horizontal da onda (ponto de equilíbrio) e o ponto mais alto ou mais baixo do movimento ondulatório. O ponto mais

Figura 1 – Exemplo de onda

Fonte: https://www.sobiologia.com.br/conteudos/oitava_serie/Ondas.php

alto de uma onda é conhecido como crista enquanto que o ponto mais baixo é conhecido como vale (URONE; HINRICHS, 2017). A figura 2 ilustra o conceito.

Comprimento de onda é definido como: a distância entre partes idênticas adjacentes de uma onda, como por exemplo, a distância entre duas cristas ou dois vales consecutivos (URONE; HINRICHS, 2017). A figura 2 ilustra o conceito.

Período é definido como: o tempo que se leva para completar uma oscilação, ou seja, é o tempo que a fonte da oscilação leva para produzir um comprimento de onda. (URONE; HINRICHS, 2017).

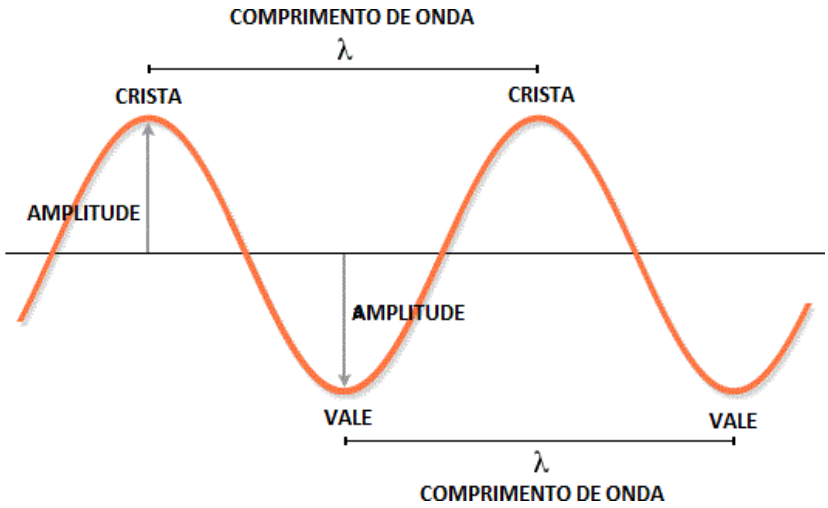
Frequência é definida como: o número de eventos por unidade de tempo, no contexto das ondas seria o número de oscilações por unidade de tempo (URONE; HINRICHS, 2017). No Sistema Internacional de Unidades (SI) a unidade da frequência é o Hertz (Hz) medida no intervalo de um segundo[1]. A frequência é uma definição muito importante para o RFID pois ela influencia diretamente em alguns aspectos da tecnologia.

Velocidade de onda, ou velocidade de propagação, é definida como: a velocidade na qual a onda se desloca, sendo o meio em que a onda se propaga influência diretamente na velocidade (URONE; HINRICHS, 2017).

Tendo claro os conceitos acima, pode-se definir o que são ondas de rádio: ondas de rádio são um tipo de onda eletromagnética que se encontra no intervalo de frequência entre $3x10^3$ Hz (3 KHz) e $3x10^8$ Hz (300 GHz) do espectro eletromagnético (AHSON; ILYAS, 2018). São o tipo de onda com maior comprimento de onda, menor frequência e menor quantidade de energia transportada de todo o espectro, além de viajar à velocidade da luz como toda onda eletromagnética (NASA, 2013). A figura 3 ilustra o espectro eletromagnético e suas diversas divisões.

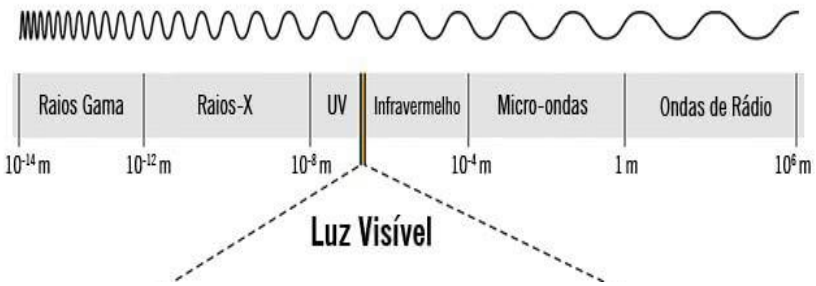
[1] <https://www.bipm.org/en/CGPM/db/11/12/>

Figura 2 – Características de onda



Fonte: https://athoselectronics.com/frequencia-como-funciona/

Figura 3 – Espectro eletromagnético



Fonte: https://www.todamateria.com.br/espectro-eletromagnetico/

A utilização de ondas de rádio para transporte de dados não é algo novo, tecnologias já estabelecidas como o *bluetooth* e o *wi-fi* são alguns dos exemplos que utilizam as ondas de rádio como princípio fundamental para seu funcionamento (ROBERTS, 2006).

2.1.2 Campos magnéticos

Um segundo conceito físico central para se compreender é o de campos magnéticos. Um campo magnético é gerador por um carga, ou um conjunto de cargas, em movimento. Embora força elétrica e magnética sejam diferentes, usa-se o conceito de campo para descrever ambos os tipos de força (YOUNG; FREEDMAN, 2009).

Conclui-se então que um campo magnético é uma força gerada pela interação entre cargas elétricas em movimento. Este conceito é considerado importante pois, como ver-se-á na seção 2.3 "Fundamentos operacionais", é através de campos magnéticos que ocorre o acoplamento, transmissão de energia e dados entre leitor e etiqueta (os principais componentes de um sistema RFID) (CHAWLA; HA, 2007).

Dentro da teoria de campos magnéticos, o conceito sobre indução magnética será útil

futuramente. A indução magnética pode ser definida como: a variação de um fluxo magnético através de um circuito, induzindo uma FEM e uma corrente elétrica no circuito (YOUNG; FREEDMAN, 2009). Conclui-se então que indução magnética é o processo de se gerar uma corrente elétrica em um circuito através da variação de um campo eletromagnético sobre o circuito. Este conceito é considerado importante pois, como ver-se-á na seção 2.3 "Fundamentos operacionais", é graças a indução magnética que etiquetas passivas (sem um aporte energético próprio) podem se energizar e funcionar (CHAWLA; HA, 2007).

2.1.3 Indução e indutância

Os últimos conceitos físicos a serem compreendidos são o de indução, indutância e indutância mútua.

Indução pode ser definida como: o processo no qual uma força eletromotriz pode ser induzida através da alteração do fluxo magnético. Já indutância é definida como a propriedade de um dispositivo que informa quão efetivamente ele induz uma força eletromotriz em outro dispositivo. Por último, indutância mútua define o quão eficaz um par de dispositivos está induzindo força eletromotriz um ao outro. (URONE; HINRICHS, 2017).

Dentro da teoria de indução há um conceito envolvendo indutância mútua que será bastante importante no decorrer deste trabalho, que é o de acoplamento indutivo ou acoplamento magnético. Define-se acoplamento como o puro ato de interação entre dois sistemas. No caso do acoplamento indutivo esta interação ocorre graças aos campos magnéticos gerados pelos circuitos participantes, por isto do acoplamento indutivo também poder ser chamado de acoplamento magnético (ZVEREV, 2005). Passando esta definição para o contexto do RFID, define-se acoplamento indutivo quando há a transferência de energia entre circuitos em virtude da indutância mútua entre os mesmos, assim, o acoplamento no RFID ocorre quando a antena da etiqueta entra na área do campo eletromagnético gerado pela antena do leitor (JOURNAL, 2019).

Este conceito é considerado importante pois, como ver-se-á na seção 2.3, Fundamentos operacionais, sistemas RFID nas faixas de baixa e alta frequência utilizam-se do acoplamento indutivo para transferência de energia e dados entre leitor e etiqueta (QING; GOH; CHEN, 2009).

2.2 COMPONENTES DE UM SISTEMA RFID

Nesta seção serão abordados os principais componentes que compõem a infraestrutura de sistemas de identificação por radiofrequência.

Sistemas RFID podem possuir diversos componentes na sua infraestrutura, sendo praticamente impossível fornecer uma lista completa destes, assim, serão abordados neste trabalho, apenas os principais destes elementos, aqueles que estão mais presentes nas

implementações da tecnologia. São eles: antena, transceptor (com decodificador) e *transponder* (DOMDOUZIS; KUMAR; ANUMBA, 2007).

Apesar da nomenclatura técnica acima, dificilmente ver-se-á estes elementos com estes nomes, até mesmo em artigos e documentações, por isto antes de se adentrar nas explicações desta seção será necessário realizar algumas correlações. Estas correlações serão usadas daqui para frente com frequência. A primeira é que o *transponder* também pode ser chamado de "etiqueta", do inglês *tag* (XIAO; GIBBONS; LEBRUN, 2009). A segunda ocorre da união de dois elementos, um transceptor com decodificador e uma antena que, quando combinados, formam um aparelho único conhecido como leitor (DOMDOUZIS; KUMAR; ANUMBA, 2007), do inglês *reader*. Ao contrário da etiqueta que é mais uma correlação de nomes, transceptor e antena são elementos distintos, mas que muito comumente são encontrados juntos.

2.2.1 Antena

Na extremidade da infraestrutura encontram-se as antenas. Uma antena RFID tem como principal função estabelecer a comunicação entre etiqueta e transceptor (DOMDOUZIS; KUMAR; ANUMBA, 2007), sendo o elemento condutor que permite que etiqueta e transceptor enviem e recebam dados entre si (RFID4U, 2016). São geralmente formadas por finos fios metálicos, geralmente de cobre, em formato de bobina circular ou retangular (GOOD; BENAISSA, 2009), como ilustrado na figura 4. Não podem ser elaboradas de qualquer modo, havendo um estudo físico-matemático para serem confeccionadas (SON; PYO, 2005), estudo este que encontra-se fora do escopo deste trabalho.

Figura 4 – Antena de etiqueta RFID

Fonte: http://dycuqybaxemabitola.mint-body.com/rfid-chip-41324132.html

Apesar da principal função ser universal, as utilidades da antena variam um pouco de acordo com a perspectiva, que pode ser do transceptor ou da etiqueta.

A antena na perspectiva do transceptor é responsável por transmitir o seu sinal de interrogação do transceptor e receber o sinal de resposta da etiqueta (RFID4U, 2016), converter a energia elétrica recebida de uma fonte (tomada, por exemplo) em ondas de rádio, ondas estas que serão propagadas no espaço tanto verticalmente quanto horizontalmente para criar uma área espacial eletromagnética onde a etiqueta poderá se acoplar (AHSON; ILYAS, 2018). A figura 5 exemplifica uma antena externa de transceptor.

Figura 5 – Antena externa de transceptor

Fonte: https://www.zebra.com/gb/en/products/rfid/rfid-reader-antennas/an480.html

A antena na perspectiva da etiqueta é responsável por captar as ondas eletromagnéticas geradas pela antena do transceptor e convertê-las novamente para energia elétrica, graças ao princípio da indução eletromagnética, energia esta que será usada para alimentar o *microchip* presente na etiqueta (CHAWLA; HA, 2007). A figura 4 ilustra dois formatos de antena de etiqueta RFID.

2.2.2 Transceptor (leitor)

No lado da infraestrutura há o transceptor. O transceptor, ou leitor, tem como principais funções se comunicar com a etiqueta, fornecer medidas anti-colisão em ambientes com múltiplas etiquetas e ser o mediador entre etiqueta e infraestrutura (RFID4U, 2016). O leitor também é responsável por fornecer energia a etiquetas passivas, converter em ondas de rádio os dados a serem enviados à etiqueta (codificação) e converter em dados as respostas recebidas da etiqueta (decodificação) (XIAO; GIBBONS; LEBRUN, 2009). A figura 6 exemplifica um leitor RFID.

Leitores RFID podem ser classificados quanto a frequência em que operam, sendo as principais: baixa frequência, alta frequência, ultra-alta frequência e micro-ondas (LOZANO-NIETO, 2010). Mais detalhes sobre as frequências utilizadas serão apresentadas mais à frente.

Figura 6 – Leitor RFID internamente

Fonte: https://www.indiamart.com/proddetail/rfid-reader-125khz-18997063655.html

2.2.3 Transponder (etiqueta)

No lado da aplicação/usuário há o *transponder*. O *transponder*, ou etiqueta, é o elemento responsável por armazenar um número de série exclusivo e/ou informações sobre um produto (XIAO; GIBBONS; LEBRUN, 2009), funcionando como elemento identificador do objeto ao qual está anexado, objeto este que pode ser uma caixa, uma peça de roupa, um animal, um ser humano, dentre outros.

Etiquetas RFID podem ser classificadas e agrupadas de algumas formas, tais como do tipo da memória de armazenamento dos dados (somente-leitura ou leitura-escrita) e do tipo aporte energético (passiva ou ativa) (DOMDOUZIS; KUMAR; ANUMBA, 2007).

Etiquetas de memória somente-leitura, na maioria das vezes, não possuem capacidade de armazenamento, tendo seu número identificador único gravado na etiqueta (DOMDOUZIS; KUMAR; ANUMBA, 2007). Se este tipo de etiqueta for interrogada por um leitor ela começará a transmitir seu número identificador de forma contínua, e somente isto. Desta forma, o fluxo de dados entre leitor e etiqueta é unidirecional, da etiqueta para o leitor (FINKENZELLER, 2010).

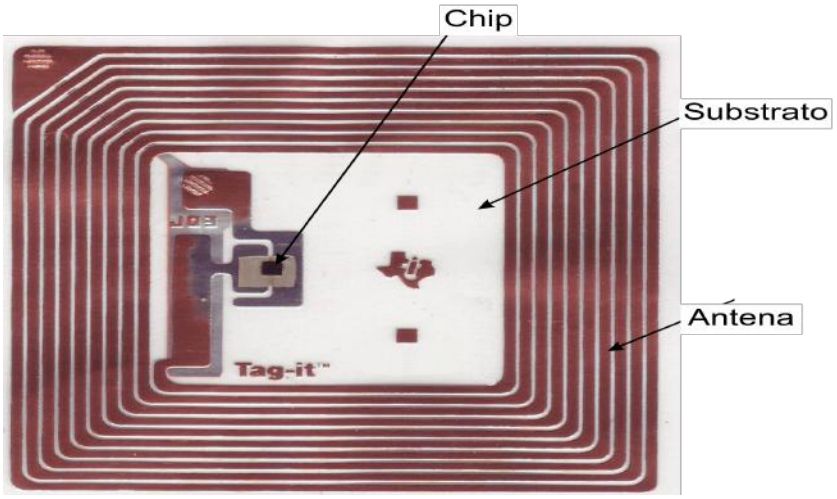
Uma das limitações das etiquetas somente-leitura é que é preciso garantir que apenas uma etiqueta deste tipo esteja no alcance de leitura do leitor, caso contrário, as etiquetas transmitindo simultaneamente levarão a uma colisão de dados e o leitor não será capaz de identificar corretamente nenhuma das etiquetas transmitindo (FINKENZELLER, 2010).

Etiquetas de memória leitura-escrita, por outro lado, possuem uma pequena memória interna que pode ser lida, escrita e reprogramada indefinidamente (AHSAN; SHAH; KINGSTON, 2010).

Uma etiqueta passiva é composta por *microchip* e antena (XIAO; GIBBONS; LEBRUN, 2009). Por precisar estar próxima do campo magnético gerado pelo leitor para

funcionar (CHAWLA; HA, 2007) possui um alcance de funcionamento relativamente curto (de apenas alguns metros) com memória de armazenamento menor e somente-leitura (XIAO; GIBBONS; LEBRUN, 2009). Em contrapartida, por ser mais simples de se fabricar, se comparada a etiqueta ativa, é consideravelmente mais barata (CHAWLA; HA, 2007) e possui um tempo de vida indefinido (WANT, 2006a). A figura 7 exemplifica uma etiqueta passiva.

Figura 7 – Exemplo de etiqueta RFID passiva



Fonte: https://endtimestruth.com/mark-of-the-beast/rfid/

Uma etiqueta ativa é composta por *microchip*, antena e bateria (XIAO; GIBBONS; LEBRUN, 2009). Por possuir aporte energético interno, pode conter uma memória de armazenamento maior, funções superiores de leitura e escrita, e não precisa estar tão perto do campo magnético do leitor para funcionar, tendo assim um alcance de funcionamento relativamente longo (FINKENZELLER, 2010). Em contrapartida, devido a bateria, o tempo de vida desta etiqueta é limitada a duração da mesma, além de ser consideravelmente mais cara de ser produzida se comparada a etiqueta passiva (WANT, 2006a). Um ponto importante a se destacar é que esta bateria interna não auxilia na transmissão de dados entre etiqueta-leitor, apenas fornece energia ao *chip* e a memória interna, sendo o campo eletromagnético gerado a única fonte utilizada para a transmissão de dados entre o etiqueta e o leitor (FINKENZELLER, 2010). A figura 8 exemplifica uma etiqueta ativa.

A tabela 1 ilustra algumas das diferenças entre etiquetas ativas e passivas.

2.3 FUNDAMENTOS OPERACIONAIS

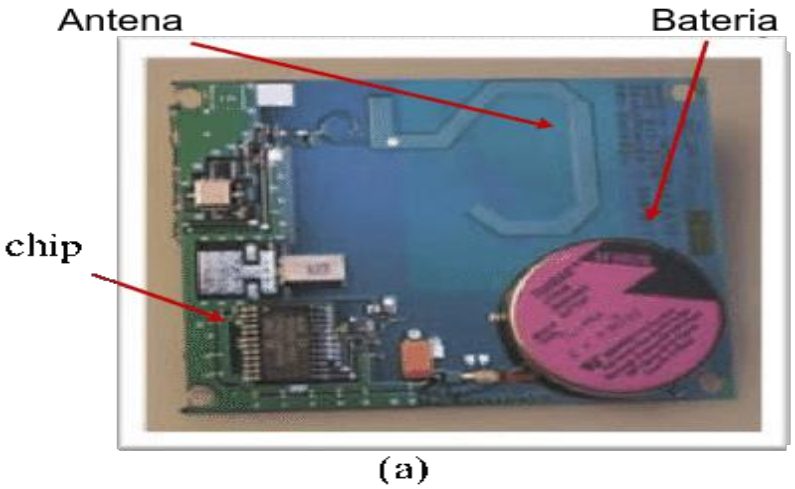
Nesta seção serão abordados detalhes de operação e implementação de sistemas de identificação por radiofrequência.

Tabela 1 – Diferenças entre etiquetas RFID ativas e passivas

	Etiquetas RFID ativas	Etiquetas RFID passivas
Fonte de energia	Interna	Proveniente do leitor
Disponibilidade de energia	Contínua	Apenas na presença do campo do leitor
Intensidade do sinal necessária do leitor para a etiqueta	Baixa	Alta
Intensidade do sinal disponível da etiqueta ao leitor	Alta	Baixa
Distância da comunicação	Longa distância	Curta distância
Armazenamento de dados	Grande	Pequena

Fonte: (DOMDOUZIS; KUMAR; ANUMBA, 2007, p.352,traduzido pelo autor)

Figura 8 – Exemplo de etiqueta RFID ativa



Fonte: https://www.researchgate.net/figure/a-Active-and-b-passive-RFID-tag-Semi-active-tags-Although-they-have-their-own-power_fig3_308167938

2.3.1 Funcionamento básico

Todo sistema RFID, independente da frequência utilizada, da distância de operação, do tipo e da quantidade de etiquetas utilizadas e do tamanho da infraestrutura, compartilha do mesmo procedimento básico de operação.

Quando em funcionamento, o leitor fica continuamente emitindo ondas eletromagnéticas através da sua antena, enquanto observa a ocorrência de interferências no campo gerado, tais como modulações e ondas eletromagnéticas contrárias, pois tais interferências podem significar que uma etiqueta entrou no seu campo de ação (SORRELLS, 1998).

Do outro lado da infraestrutura, quando uma etiqueta é posicionada dentro do campo eletromagnético de um leitor ela "acorda" e começa a transmitir suas informações internas para o leitor gerador do campo eletromagnético que a acordou. Esta parte do funcionamento varia muito de acordo com o tipo de etiqueta utilizada: nas passivas (sem aporte energético próprio) a etiqueta começa a "colher" a energia necessária para funcionar do campo magnético do leitor e, quando possui energia suficiente para habilitar o *chip* interno, começa a transmitir as informações; nas ativas (com aporte energético próprio) a etiqueta pode começar a transmitir assim que sente a presença do campo eletromagnético do leitor pois já possui a energia necessária para habilitar o *chip* interno (SORRELLS, 1998).

No momento que o leitor detecta as perturbações no seu campo eletromagnético, ele começa a decodificar e transformar as variações sentidas em um fluxo de *bits*. Esta decodificação varia de acordo com os métodos de codificação e modulação de dados utilizados. Este procedimento básico é conhecido como apresentação (*handshake*) entre leitor e etiqueta (SORRELLS, 1998).

2.3.2 Classificação de sistemas RFID

Sistemas RFID podem ser classificados de diversas formas, dependendo dos componentes utilizados na infraestrutura e das características de operação dos mesmos, entretanto, as três formas mais usuais de classificação são com relação a: frequência de operação, método de acoplamento e alcance de funcionamento (FINKENZELLER, 2010). As três formas serão abordadas brevemente aqui e posteriormente aprofundadas.

Com relação à frequência, sistemas RFID operam geralmente em quatro frequências distintas: baixa frequência, alta frequência, ultra-alta frequência e micro-ondas (LOZANO-NIETO, 2010).

Com relação ao acoplamento leitor-etiqueta, sistemas RFID podem implementar uma das quatro técnicas: acoplamento indutivo, acoplamento por retroespelhamento (*backscattering*), acoplamento por proximidade (*close-coupling*) ou acoplamento capacitivo (FINKENZELLER, 2010).

Com relação à distância de operação entre leitor e etiqueta, sistemas RFID podem ser classificados em três tipos: sistema de acoplamento próximo, sistema de acoplamento remoto e sistema de longo alcance (FINKENZELLER, 2010).

2.3.3 Frequências de operação

Sistemas RFID também podem ser classificados com relação à frequência de rádio que utilizam, sendo baixa frequência, alta frequência, ultra-alta frequência e micro-ondas as quatro principais faixas de definição(WYLD, 2006 apud XIAO; GIBBONS; LEBRUN, 2009).

Diversas fatores influenciam na escolha da melhor frequência para a aplicação, tais como: tamanho máximo da etiqueta a ser implantada, alcance de leitura do sistema, taxa de transferência de dados, resistência à interferência, entre outros (XIAO; GIBBONS; LEBRUN, 2009).

Considera-se como baixa frequência (LF) a faixa de frequência entre 30 KHz e 300 KHz, sendo entre 125 KHz e 135 KHz as tipicamente utilizadas (XIAO; GIBBONS; LEBRUN, 2009). Algumas das características desta faixa de frequência incluem: utilização do acoplamento indutivo; boa penetração das ondas em obstáculos (inclusive metal) (FINKENZELLER, 2010); boa resistência à presença de metais; baixa atenuação do sinal quando trafegando pela água (LOZANO-NIETO, 2010); baixa taxa de transferência de dados(menos de 1 kbit/s); utilização principalmente de etiquetas passivas; curta distância de operação (aproximadamente 50 cm). As áreas de aplicação incluem: controle acesso, identificação de animais e rastreamento de objetos (XIAO; GIBBONS; LEBRUN, 2009).

Considera-se como alta frequência (HF) as faixas de frequência entre 3 MHz e 30 MHz, sendo 13.56 MHz a tipicamente utilizada (XIAO; GIBBONS; LEBRUN, 2009). Algumas das características desta faixa de frequência incluem: menor resistência à presença de metais, maior atenuação do sinal na água e etiqueta com menor custo de fabricação, quando comparadas à baixa frequência (LOZANO-NIETO, 2010); utilização do acoplamento indutivo; boa penetração das ondas em obstáculos (FINKENZELLER, 2010); utilização principalmente de etiquetas passivas; taxa de transferência de dados moderada (aproximadamente 25 kbit/s); distância de operação moderada (aproximadamente 90 cm). As áreas de aplicação incluem: controle de acesso, rastreamento de objetos (livros de biblioteca, bagagens em aeroportos e etc), identificação inteligente de pessoas (e-passaporte) (XIAO; GIBBONS; LEBRUN, 2009) e bilhetagem de transporte público (Rio card).

Considera-se como ultra-alta frequência (UHF) as faixas de frequência entre 300 MHz e 1000 MHz. As faixas de frequência tipicamente utilizadas variam muito conforme a região do globo e o tipo de etiqueta, bem como a distância de operação: etiquetas passivas costumam operar na faixa entre 865 MHz e 868 MHz na Europa, entre 902 MHz e 928 MHz nos Estados Unidos e possuem distância de operação de aproximadamente 3 m (podendo chegar a 6 m), já as etiquetas ativas operam na faixa entre 315 MHz e 433 MHz e possuem distância de operação de aproximadamente 15 m (podendo chegar a 30 m) (XIAO; GIBBONS; LEBRUN, 2009). Algumas das características desta faixa de frequência incluem: utilização do acoplamento por retroespelhamento; má desempenho na presença de metais; impossibilidade de utilização através da água (LOZANO-NIETO, 2010); taxa de transferência de dados moderada (aproximadamente 30 kbit/s). A principal área de aplicação encontra-se no rastreamento global de objetos (cadeia de suprimentos) (XIAO; GIBBONS; LEBRUN, 2009).

Considera-se como micro-ondas (*microwave*) as faixas de frequência entre 2 GHz e 30 GHz, sendo 2.45 GHz e 5.8 GHz as tipicamente utilizadas (XIAO; GIBBONS; LEBRUN,

2009). Algumas das características desta faixa de frequência incluem: propagação do sinal limitado à linha direta de visão; altos custos de produção de leitores e etiquetas; altíssima imunidade a ruído (LOZANO-NIETO, 2010); utilização do acoplamento por retroespelhamento; boa resistência a interferência de campos eletromagnéticos externos (FINKENZELLER, 2010); altíssimas taxas de transferência de dados (até 100 kbit/s); impossibilidade de penetrar metal e água; boas distâncias de operação (aproximadamente 3 m para etiquetas passivas e 15 m para etiquetas ativas). As áreas de aplicação incluem: monitoramento de vagões ferroviários e cobrança automática de pedágios (XIAO; GIBBONS; LEBRUN, 2009).

De forma geral, tem-se que quanto maior a frequência da onda maior será a taxa de transferência de dados, em contrapartida, maior será o custo dos equipamentos e, consequentemente, da implantação do sistema (XIAO; GIBBONS; LEBRUN, 2009).

2.3.4 Distâncias de operação

A distância de operação pode ser definida como o alcance máximo na qual etiqueta e leitor ainda conseguem trocar informações de forma consistente. Diversas características influenciam na distância de operação, tais como: frequência utilizada, tipo de etiqueta (passiva ou ativa), modo de acoplamento e etc. Desta forma, sistemas RFID podem ser classificados em três tipos: sistema de acoplamento próximo (*close-coupling systems*), sistema de acoplamento remoto (*remote-coupling systems*) ou sistema de longo alcance (*long-range systems*) (FINKENZELLER, 2010).

Nos sistemas de acoplamento próximo a distância de operação entre leitor e etiqueta é muito curta, tipicamente na região de até 1cm. Devido a curtíssima distância de operação, estes sistemas possuem algumas peculiaridades, tais como: necessidade de se inserir a etiqueta no leitor, ou posicioná-la sobre uma superfície própria, para funcionar; fornecer grandes quantidades de energia a etiqueta, se comparado aos outros tipos; utilizar os campos elétrico e magnético para acoplamento; operar, teoricamente, em qualquer frequência desejada até 30 MHz, visto que não dependem da propagação dos campos. Sistemas de acoplamento próximo são utilizados principalmente em aplicações que necessitam da curta distância por questões de segurança, como fechaduras eletrônicas e sistemas de pagamento, porém, devido as limitações, estão sendo cada vez menos utilizados (FINKENZELLER, 2010).

Nos sistemas de acoplamento remoto a distância de operação entre leitor e etiqueta é mediana, tipicamente na região de até 1m. Todos os sistemas deste tipo operam nas faixas de baixa ou alta frequência, além de quase todos utilizarem-se do acoplamento indutivo em campo magnético para acoplagem. Sistemas de acoplamento remoto são os mais empregados atualmente no mercado, sendo utilizados nas mais diversas áreas e aplicações, tais como: cartões inteligentes sem contato, identificação de animais, automação industrial, entre outros (FINKENZELLER, 2010).

Nos sistemas de longo alcance a distância de operação entre leitor e etiqueta é longa, com alcances superiores a 1m, porém, sistemas típicos chegam a 3m com etiquetas passivas e acima de 15m com etiquetas ativas. Todos os sistemas deste tipo operam nas faixas de ultra-alta frequência ou micro-ondas, além de utilizarem-se do acoplamento por retro-espelhamento em campo eletromagnético para se acoplarem (FINKENZELLER, 2010).

2.3.5 Fluxo de comunicação

Similar a redes de computadores, o fluxo de comunicação entre etiqueta e leitor nos sistemas RFID pode ocorrer de três formas: *half-duplex* (HDX), *full-duplex* (FDX) ou sequencial (SEQ) (LOUREIRO; SOUZA; LOPES, 2015).

No modo de comunicação *half-duplex* (HDX) o canal de comunicação só pode ser utilizado para transmissão por apenas um dos participantes, ou seja, ou a etiqueta está transmitindo para o leitor (procedimento conhecido como *up-link*) e o leitor está apenas escutando, ou o leitor está transmitindo para a etiqueta (procedimento conhecido como *down-link*) e a etiqueta está apenas escutando (FINKENZELLER, 2010). Este tipo de comunicação é muito utilizada em etiquetas passivas (LOUREIRO; SOUZA; LOPES, 2015). Em sistemas RFID *half-duplex* que trabalham em frequências abaixo de 30 MHz, o procedimento de modulação de carga (*load modulation*) é o mais comumente utilizado para a transmissão de dados (FINKENZELLER, 2010).

No modo de comunicação *full-duplex* (FDX) o canal de comunicação pode ser compartilhado para transmissão por ambos os participantes, ou seja, tanto leitor quanto etiqueta podem transmitir simultaneamente um para o outro (LOUREIRO; SOUZA; LOPES, 2015).

O modo de comunicação sequencial (SEQ) difere um pouco dos dois modos acima. Enquanto que nos modos duplex a transferência de energia do leitor para etiqueta é contínua e independente da direção do fluxo de dados, no modo sequencial, por outro lado, a transferência de energia ocorre por um período delimitado de tempo. A transferência de dados do leitor para etiqueta (*down-link*) funciona em paralelo ao intervalo de tempo da transferência de energia, enquanto que a transferência de dados da etiqueta para o leitor (*up-link*) ocorre nos intervalos de não transmissão do leitor. O modo de transferência de energia dos modos duplex é conhecido como "operação de pulso", enquanto que o do modo sequencial é conhecido como "sistema pulsado" (FINKENZELLER, 2010). Devido a esta transferência de energia pulsada (e não contínua), é necessário que a etiqueta seja capaz de armazenar energia para posteriormente utilizá-la para a transmissão de dados (LOUREIRO; SOUZA; LOPES, 2015).

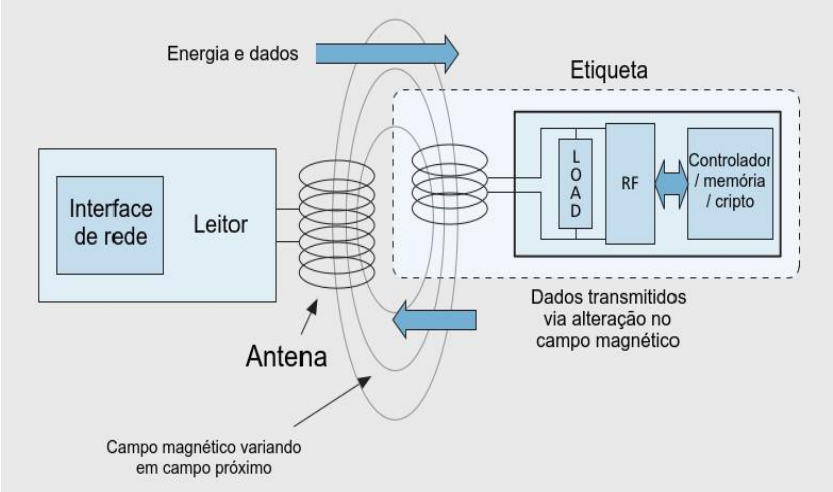
2.3.6 Métodos de acoplamento

Como visto na seção 2.1, "A física por trás da tecnologia", acoplamento é definido como o ato de interação entre dois sistemas. No contexto do RFID, os dois sistemas da composição são a etiqueta e o leitor. Desta forma, o acoplamento na tecnologia RFID é o mecanismo pelo qual ocorre a transferência de energia e dados entre leitor e etiqueta.

Sistemas RFID duplex (FDX ou HDX) possuem quatro tipos de acoplamento possíveis: indutivo, retroespelhamento, proximidade e capacitivo (ou elétrico) (FINKENZELLER, 2010). Nem todos os métodos são aplicáveis a todas as implementações da tecnologia, fatores como alcance de leitura, frequência, tipo de etiquete, dentre outros, limitam as implementações a um ou dois métodos, assim como ver-se-á nas explicações abaixo.

O acoplamento indutivo entre leitor e etiqueta baseia-se no princípio físico da indução magnética. No leitor, o fluxo de uma corrente alternada de alta frequência na antena gera um campo eletromagnético alternado de alta frequência nas proximidades. Devido ao comprimento de onda da faixa de frequência utilizada ser diversas vezes maior que a distância de operação entre leitor e etiqueta, o campo eletromagnético gerado pode ser tratado como um campo magnético alternado. Deste modo, se uma etiqueta for posicionada no campo magnético alternado do leitor, uma corrente alternada será induzida na antena da etiqueta, gerando assim a energia elétrica necessária para alimentar seu *chip* (WANT, 2006b; FINKENZELLER, 2010). A figura 9 exemplifica uma sistema de acoplamento indutivo.

Figura 9 – Acoplamento indutivo



Fonte: (CHAWLA; HA, 2007, p.12)

Três pontos a serem destacados são: Este tipo de acoplamento é utilizado geralmente em sistemas onde, a distância de operação encontra-se em uma região ao redor da antena do leitor conhecida como campo próximo (*near-field*). Etiquetas que operam através deste tipo de acoplamento quase sempre são passivas, ou seja, toda a energia necessária para

funcionar precisa vir do campo magnético do leitor (FINKENZELLER, 2010). Devido a natureza magnética do campo, as antenas de leitor e etiqueta devem ser do tipo bobina (CHAWLA; HA, 2007).

Sistemas RFID que implementam o acoplamento indutivo utilizam-se de uma técnica conhecida como modulação de carga para a transferência de dados entre etiqueta e leitor.

Como visto acima, graças ao princípio da indução magnética, uma pequena corrente elétrica é gerada na antena do leitor. Esta pequena corrente que flui pela antena da etiqueta também gera, pelos mesmos princípios físicos aplicados ao leitor, um pequeno campo magnético próprio e oposto ao campo magnético do leitor. Devido a indutância mútua entre leitor e etiqueta, o pequeno campo magnético da etiqueta gera uma pequena corrente elétrica na antena do leitor, que é capaz de identificar esta pequena variação de corrente interna. Deste modo, variando sua própria corrente interna através de um resistor de carga, a etiqueta é capaz de variar a carga que ela induz no leitor. Caso a etiqueta faça esta variação de forma controlada em relação ao tempo, um padrão pode ser criado para codificar as informações de identificação da etiqueta, que o leitor será capaz de compreender monitorando a variação da corrente, em função do tempo, na própria antena (CHAWLA; HA, 2007; WANT, 2006b; FINKENZELLER, 2010).

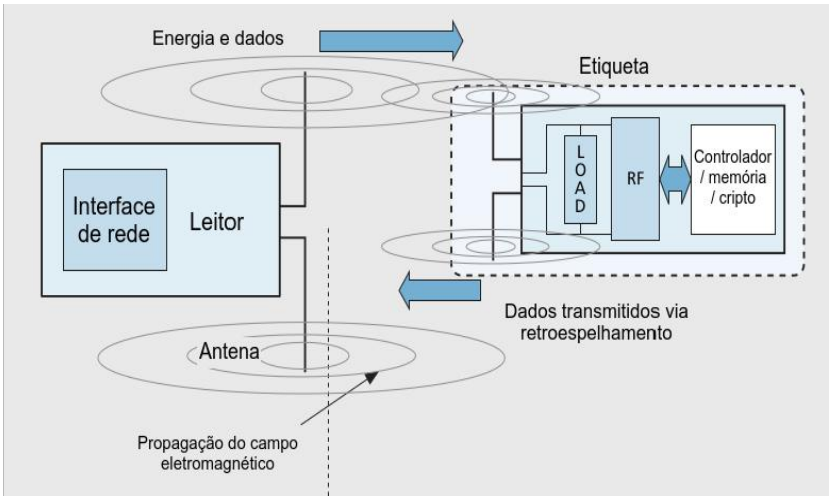
O acoplamento por retroespelhamento (*backscattering*) é empregado principalmente em sistemas onde a distância de operação encontra-se em uma região, ao redor da antena do leitor, conhecida como campo distante (*Far-Field*). O acoplamento ocorre através de ondas eletromagnéticas. O leitor, através de uma antena do tipo dipolo, emite ondas eletromagnéticas que se propagarão até a antena da etiqueta. Na antena da etiqueta, também do tipo dipolo, as ondas gerarão uma diferença de potencial alternada entre os "braços" da antena que, consequentemente, gerarão a energia necessária para alimentar o *chip* da etiqueta (CHAWLA; HA, 2007; WANT, 2006a).

Devido a distância de operação do sistema estar muito além dos limites do campo próximo, a etiqueta não pode se utilizar do princípio da modulação de carga para enviar sua identificação para o leitor, ao invés disso, emprega-se a técnica que dá nome ao acoplamento, o retroespelhamento (WANT, 2006a).

Dependendo das dimensões de fabricação de uma antena, ela pode ser utilizada para absorver grande parte da energia eletromagnética, de uma certa frequência, que chega até ela. Porém, caso alguma incompatibilidade de impedância ocorra nesta frequência, parte da energia que chegou até a antena é refletida, como pequenas ondas, de volta para o leitor. Caso o leitor esteja equipado com um receptor de rádio altamente sensível, ele será capaz de detectar estas pequenas ondas refletidas de volta pela etiqueta. Deste modo, utilizando-se da troca de impedância da antena em relação ao tempo, a etiqueta é capaz de refletir mais ou menos energia de volta para o leitor, criando assim um padrão de codificação que pode ser reconhecido pelo leitor através do monitoramento das variações de ondas refletidas. (CHAWLA; HA, 2007; WANT, 2006a). A figura 10 representa uma

sistema de acoplamento por retroespelhamento.

Figura 10 – Acoplamento por retroespelhamento



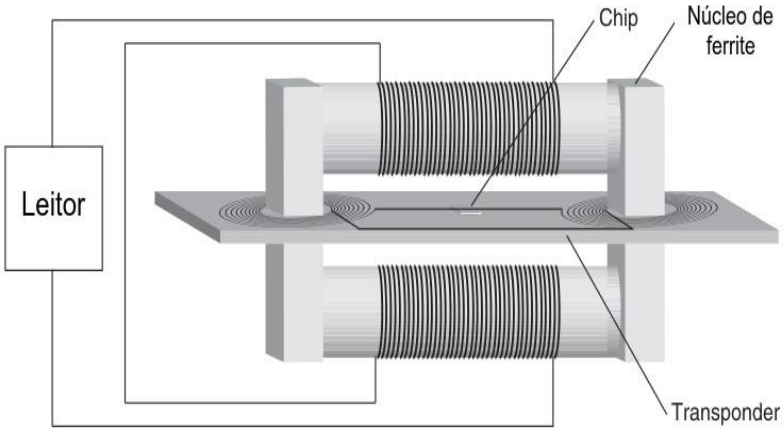
Fonte: (CHAWLA; HA, 2007, p.13)

Dois pontos a serem destacados são: Este tipo de acoplamento é utilizado geralmente em sistemas que operam nas bandas de ultra-alta frequência (UHF) e micro-ondas. Devido aos princípios de funcionamento, as antenas de leitor e etiqueta devem ser do tipo dipolo (CHAWLA; HA, 2007).

O acoplamento por proximidade (*close-coupling*) é implementado principalmente em sistemas onde a etiqueta deve tocar ou ser inserida no leitor, tendo assim um alcance de funcionamento entre 0.1cm e 1cm. Neste tipo de acoplamento as antenas do leitor devem ser precisamente elaboradas pois, ao se inserir a etiqueta no leitor, a antena da etiqueta precisa posicionar-se perfeitamente em um espaçamento existente entre as antenas do leitor, assim como exemplificado na figura 11. A disposição formada por este esquema fica similar a disposição de uma bobina elétrica, com o leitor representando a bobina primária e a etiqueta representando a bobina secundária. Após instanciada a disposição acima, uma corrente alternada de alta frequência flui pela antena do leitor, gerando um campo magnético de alta frequência no espaçamento entre suas antenas e, consequentemente, através da antena da etiqueta, gerando assim a corrente necessária para alimentar o *chip* da etiqueta (FINKENZELLER, 2010).

No acoplamento elétrico, ou capacitivo, o acoplamento ocorre através da geração de campos elétricos de alta voltagem entre a antena do leitor e o neutro (ou terra). A antena do leitor é composta por uma grande placa metálica condutora que, quando aplicada uma voltagem de alta frequência, gera um campo elétrico de alta frequência entre a placa e o neutro. De forma similar, a antena da etiqueta é formada por duas placas condutoras posicionadas paralelamente uma ao lado da outra (formando um plano), quando as antenas da etiqueta são colocadas dentro do campo elétrico gerado pela antena do leitor, uma

Figura 11 – Acoplamento por proximidade

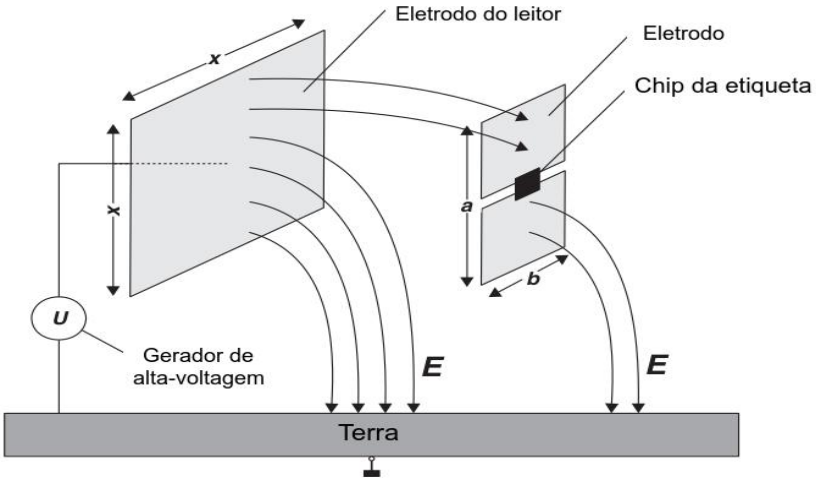


Fonte: (FINKENZELLER, 2010, p.49)

tensão elétrica é induzida entre as placas da etiqueta, gerando assim a corrente necessária para alimentar o *chip* (FINKENZELLER, 2010).

A figura 12 ajuda a compreender melhor o processo.

Figura 12 – Acoplamento elétrico/capacitivo



Fonte: (FINKENZELLER, 2010, p.51)

Um ponto observado por (NIKITIN; RAO; LAZAR, 2007) é que as características: método de acoplamento, frequência utilizada e alcance de operação, são interligadas. Sistemas RFID de baixa e alta frequências são, geralmente, de curto alcance e baseados em acoplamento indutivo através de campos magnéticos, enquanto que os sistemas de ultra-alta frequência e micro-ondas são, geralmente, de longo alcance baseados em retro-espelhamento eletromagnético através de propagação eletromagnética.

Há ainda um outro modo de se classificar os métodos de acoplamento, mas desta vez voltado para sistemas de etiquetas passivas, que é com relação a distância de operação do

sistema. Sistemas RFID onde a etiqueta precisa estar próxima ao leitor para funcionar são conhecidos como sistemas de acoplamento de campo próximo (*near-field coupling*) e utilizam-se do princípio do acoplamento indutivo e da modulação de carga para funcionar. Sistemas RFID onde a etiqueta pode estar a uma certa distância do leitor são conhecidos como sistemas de acoplamento de campo distante (*Far-Field coupling*) e utilizam-se do acoplamento por retroespelhamento para funcionar (WANT, 2006b).

Definições como "próximo" e "distante" são relativas e não podem ser utilizadas sem uma definição mais precisa, assim, considera-se campo próximo a área ao redor da antena do leitor que está a uma distância máxima de 0.16 vezes o comprimento de onda da frequência utilizada. De forma análoga, considera-se campo distante a área ao redor da antena do leitor que está distante a, pelo menos, 0.16 vezes o comprimento de onda da frequência utilizada (FINKENZELLER, 2010).

A figura 9 representa um sistema de campo próximo, enquanto a figura 10 representa um sistema de campo distante.

2.3.7 Modulação de dados

Uma das operações mais essenciais em sistemas RFID é a troca de informações entre etiqueta e leitor e, como visto anteriormente, a tecnologia utiliza-se de ondas eletromagnéticas como meio de comunicação no meio físico. Desta forma, para que a troca ocorra, é necessário que os dados em formato digital (zeros e uns) sejam transformados em formato analógico (ondas eletromagnéticas) para que possam ser emitidos e recebidos pelas antenas de etiqueta e leitor. Assim, para que a transmissão ocorra, é necessário que o fluxo de *bits* seja, de alguma forma, inserido nas ondas eletromagnéticas. Um dos modos de se fazer esta inserção é através da manipulação das mesmas.

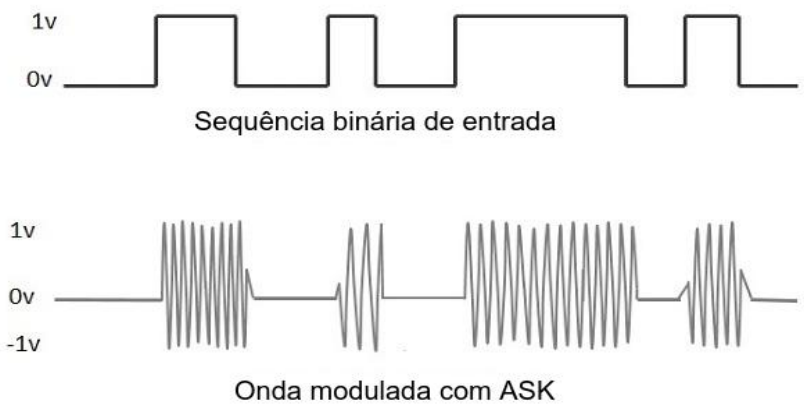
Durante o processo de manipulação de uma onda, pelo menos uma, mas geralmente apenas uma, de suas três características básicas - amplitude, frequência e fase - é alterada a fim de codificar a mensagem. À onda eletromagnética original, sem manipulação, dá-se o nome de onda portadora, ou simplesmente portadora. À troca de formato digital para analógico e ao processo de manipulação das características básicas da onda eletromagnética, com o intuito de transportar dados, dá-se o nome de modulação digital, ou simplesmente modulação (LOZANO-NIETO, 2010; FINKENZELLER, 2010). O processo inverso, de recuperação da mensagem original à partir de uma mensagem codificada, dá-se o nome de demodulação (FINKENZELLER, 2010).

À modulação realizada no âmbito da frequência dá-se o nome de Modulação por Chaveamento de Frequência. À modulação realizada no âmbito da amplitude dá-se o nome de Modulação por Chaveamento de Amplitude. À modulação realizada no âmbito da fase dá-se o nome de Modulação por Chaveamento de Fase. Todos os outros métodos de modulação existentes são derivados destes três métodos básicos (LOZANO-NIETO, 2010; FINKENZELLER, 2010).

Modulação por chaveamento de amplitude, mais conhecida pela sua sigla em inglês ASK (*Amplitude Shift Keying*), ocorre quando a amplitude da onda portadora oscila entre dois valores distintos (FINKENZELLER, 2010). Aqui, um valor de amplitude mais alto significa 1 binário, enquanto um valor de amplitude mais baixo significa 0 binário (LOZANO-NIETO, 2010). A figura 13 ilustra o formato de uma onda pós aplicação da modulação por chaveamento de amplitude.

Devido a simplicidade de modulação e demodulação, o ASK é amplamente implementado em todos os tipos de sistemas RFID (FINKENZELLER, 2010) (principalmente em sistemas *full-duplex* (KITSOS; ZHANG, 2008) e de acoplamento por retroespelhamento (WANT, 2006b)), além de oferecer as maiores taxas de transferência de dados dentre as modulações. Em contrapartida, possui a pior resistência a ruídos (LOZANO-NIETO, 2010).

Figura 13 – Formato de onda pós modulação por chaveamento de amplitude



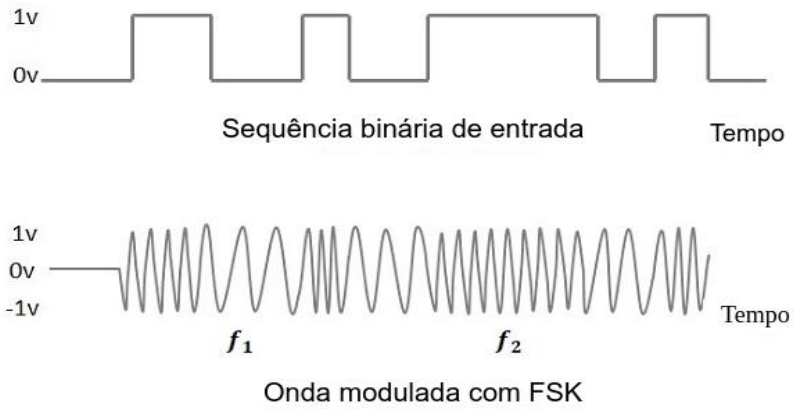
Fonte: https://www.tutorialspoint.com/digital_communication/digital_communication_amplitude_shift_keying.htm

Modulação por chaveamento de frequência, mais conhecida pela sua sigla em inglês FSK (*Frequency Shift Keying*), ocorre quando a frequência da onda portadora oscila entre dois valores distintos (FINKENZELLER, 2010). Aqui, um valor de frequência mais alto significa 1 binário, enquanto um valor de frequência mais baixo significa 0 binário. A figura 14 ilustra o formato de uma onda pós aplicação da modulação por chaveamento de frequência.

Este tipo de modulação apresenta imunidade a ruídos muito boa e pode ser implementada em leitores relativamente simples, mas sofre com taxas de transmissão inferiores dentre as modulações (SORRELLS, 1998). Sistemas half-duplex e de acoplamento por retroespelhamento são alguns dos sistemas que podem implementar o FSK (KITSOS; ZHANG, 2008; AHSON; ILYAS, 2018).

Modulação por chaveamento de fase, mais conhecida pela sua sigla em inglês PSK (*Phase Shift Keying*), ocorre através das mudanças de fase do sinal portador, entre os

Figura 14 – Formato de onda pós modulação por chaveamento de frequência

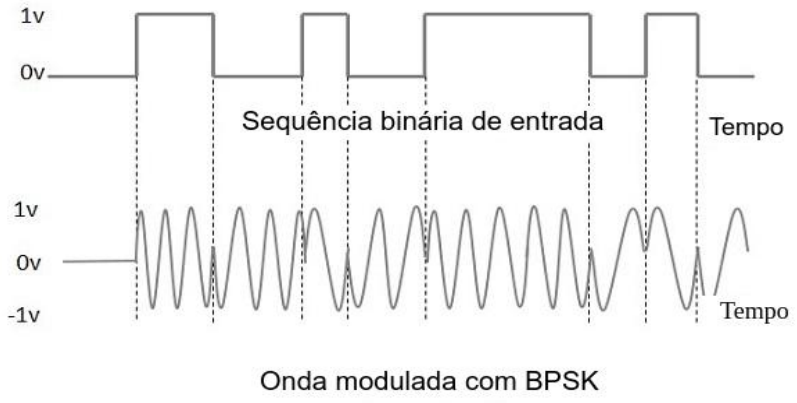


Fonte: https://www.tutorialspoint.com/digital_communication/digital_communication_frequency_shift_keying.htm

ciclos do relógio (LOZANO-NIETO, 2010). Aqui, sempre que ocorrer uma transição de valores do sinal digital, ocorrerá uma mudança de 180 graus na fase da onda portadora (FINKENZELLER, 2010), ou seja, sempre que ocorrer uma transição do *bit* 0 para o *bit* 1, ou vice-e-versa, no fluxo de *bits*, a fase da portadora será chaveada em 180 graus. A figura 15 ilustra o formato de uma onda pós aplicação da modulação por chaveamento de fase.

Como apenas a fase do sinal portador é modulada, é possível transmitir mais informações no mesmo período de tempo, resultando em uma taxa de transmissão de dados superior, se comparado ao FSK, mas ainda inferior ao ASK (LOZANO-NIETO, 2010). Este tipo de modulação apresenta imunidade a ruídos moderada e é suportada por leitores relativamente simples de serem fabricados (SORRELLS, 1998).

Figura 15 – Formato de onda pós modulação por chaveamento de fase



Fonte: https://www.tutorialspoint.com/digital_communication/digital_communication_phase_shift_keying.htm

2.3.8 Codificação de dados

Codificação de dados refere-se ao ato de processar e alterar o fluxo de *bits* (*bitstream*) (zeros e uns) para que possam trafegar de forma segura no caminho entre os componente de uma comunicação (SORRELLS, 1998).

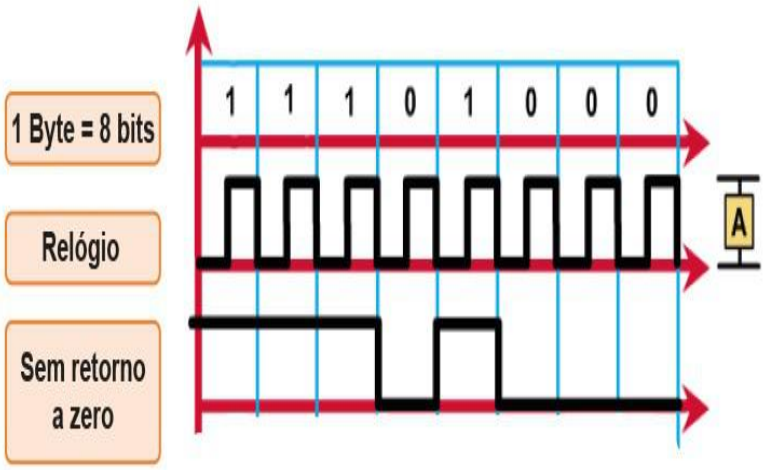
Nem todo tipo de codificação pode ser implementado em um sistema, características como: número de *bits* a serem codificados, taxa de transferência requerida, redundância necessária para recuperação de erros, entre outros, influenciam no tipo de codificação que pode ser implementado (WANT, 2006a), além de afetarem vários outros aspectos da comunicação, tais como: recuperação de erros, custo de implementação, largura de banda, capacidade de sincronização, entre outros (SORRELLS, 1998).

Codificação de dados é um tema amplamente estudado e que daria uma monografia por si só, devido a isto, serão abordados de forma não profunda, apenas alguns dos métodos mais populares utilizados em sistemas RFID atualmente, sendo eles: Não Retorno a Zero Direto (*Non-Return to Zero(NRZ) Direct*), Bifase Diferencial (*Differential Biphase*) e Bifase_L (*Biphase_L*) (Manchester) (SORRELLS, 1998).

Apesar do nome, a codificação Não Retorno a Zero não realiza qualquer tipo codificação nos dados, simplesmente sincronizando o fluxo de *bits* com o *clock* interno para transmissão. Assim, um 1 binário é enviado por um sinal "forte" enquanto um 0 binário é enviado por um sinal "fraco". Como se pode imaginar, este tipo de codificação apresenta problemas quando uma longa sequência de 0s ou de 1s precisa ser transmitida (LOZANO-NIETO, 2010). Este tipo de codificação é usada quase que exclusivamente com as modulações FSK e PSK (FINKENZELLER, 2010).

A figura 16 ilustra o formato de onda após uma codificação Não Retorno a Zero em um dado fluxo de *bits* e um relógio de sincronização.

Figura 16 – Formato de onda pós codificação Não Retorno a Zero



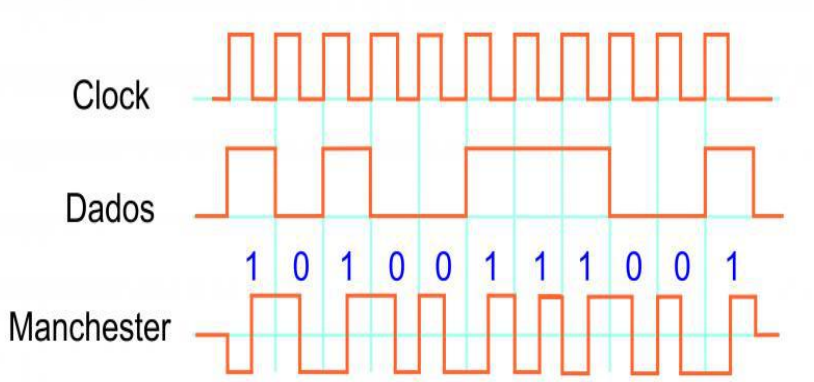
Fonte: http://estacio.webaula.com.br/cursos/go0364/aula2.html

Na codificação Bifase Diferencial, ocorre uma mudança na "força" do sinal em todo meio período do relógio. Um 1 binário é representado por uma mudança na "força" do sinal no inicio do período do relógio, enquanto um 0 binário é representado por uma permanência da "força" do sinal no inicio do período do relógio. Nesta codificação, as informações do relógio interno do emissor são mescladas aos dados enviados para que o receptor possa sincronizar-se corretamente e assim decodificar os dados recebidos (LOZANO-NIETO, 2010; AHSON; ILYAS, 2018).

A codificação Bifase_L, mais conhecida como codificação Manchester, é uma variação da codificação Bifase Diferencial. Aqui, um 1 binário é representado por uma mudança na "força", de alta para baixa, no meio do período do relógio, enquanto que um 0 binário é representado por uma mudança na "força", de baixa para alta, no meio do período do relógio. Como na Bifase Diferencial, as informações do relógio interno do emissor são mescladas aos dados enviados para que o receptor possa sincronizar-se corretamente e assim decodificar os dados recebidos (LOZANO-NIETO, 2010). Este tipo de codificação é muito utilizada em sistemas que implementam a técnica de modulação de carga para transmissão de dados (FINKENZELLER, 2010).

A figura 17 ilustra o formato de onda após uma codificação Manchester em um dado fluxo de *bits* e um relógio de sincronização.

Figura 17 – Formato de onda pós codificação Manchester



Fonte: http://www.ead.ufrpe.br/acervo-digital-eadtec/node/782

2.3.9 Colisão e anticolisão

Todo canal de comunicação, independente do meio utilizado, possui uma capacidade máxima de transporte, que é a taxa máxima de dados que o canal suporta transportar por um período de tempo. No contexto do RFID, quando há apenas uma etiqueta querendo transmitir, toda a capacidade do canal disponível pode ser cedida a esta única etiqueta,

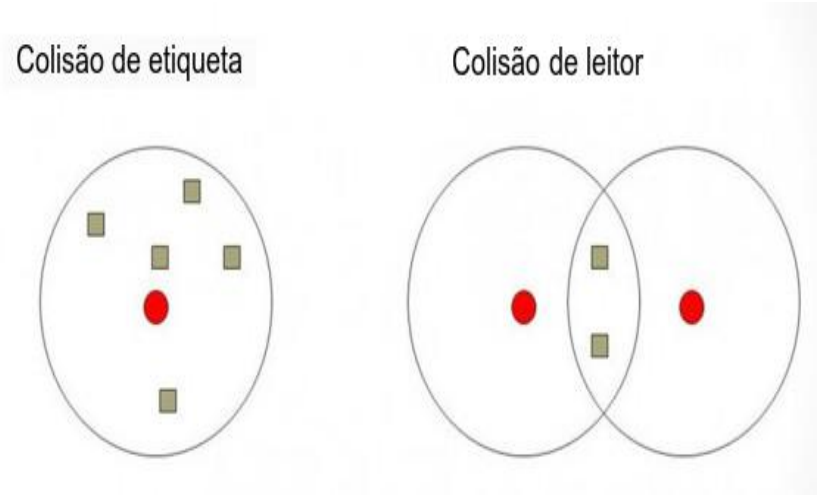
entretanto, quando há múltiplas etiquetas querendo transmitir, a capacidade do canal precisa ser dividida de tal modo que todas as etiquetas consigam transmitir seus dados para o leitor sem que uma etiqueta interfira na comunicação da outra (FINKENZELLER, 2010). Quando a interferência ocorre pode-se dizer que houve uma colisão entre pacotes no canal de comunicação.

Colisões geram saturação no canal, o que pode acarretar em sobrecarga na comunicação e grandes atrasos de transmissão, fazendo com que o leitor possa não reconhecer todas as etiquetas que deveria e, consequentemente, não identificar e rastrear todos os objetos adequadamente (LOZANO-NIETO, 2010).

Colisões em sistemas RFID podem ser classificadas em dois grupos: colisão de leitores e colisão de etiquetas. Colisão de leitores ocorre quando dois ou mais leitores vizinhos tentam ler uma mesma etiqueta simultaneamente, fazendo com que seus sinais colidam entre si e a etiqueta não consiga identificar e responder a nenhum dos sinais. De forma análoga, uma colisão de etiquetas ocorre quando duas ou mais etiquetas tentam transmitir simultaneamente, fazendo com que seus sinais colidam e o leitor não consiga identificar corretamente nenhum dos sinais (AHSON; ILYAS, 2018). A este tipo de comunicação, onde múltiplas etiquetas tentam transmitir para o mesmo leitor, dá-se o nome de "acesso múltiplo" (*multi-access*) (FINKENZELLER, 2010) e é uma das formas mais comuns de colisão em sistemas RFID.

A figura 18 ilustra os dois tipos de colisão supracitados.

Figura 18 – Colisão de leitores e colisão de etiquetas



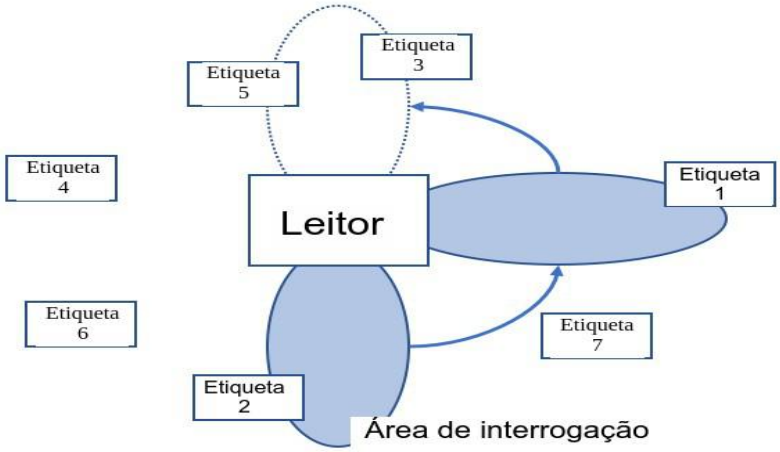
Fonte: http://www.cxjrfidfactory.com/what-is-rfid-tag-and-reader-collision/

Problemas de acesso múltiplo em sistemas de comunicação sem fio já são amplamente conhecidos e estudados nas áreas de telecomunicação e redes de computadores. Devido a isto, diversas técnicas já existem para lidar com o problema e tentar separar, ou identificar, o sinal de cada participante da comunicação. Os quatro métodos principais empregados atualmente são: Acesso Múltiplo por Divisão Espacial (*Space Division Multiple*

Access (SDMA)), Acesso Múltiplo por Divisão de Frequência (*Frequency Division Multiple Access (FDMA)*), Acesso Múltiplo por Divisão de Tempo (*Time Domain Multiple Access (TDMA)*) e Acesso Múltiplo por Divisão de Código (*Code Division Multiple Access(CDMA)*) (FINKENZELLER, 2010).

No Acesso Múltiplo por Divisão Espacial, o enlace é totalmente utilizado em uma determinada área espacial por um determinado período de tempo, ou seja, uma área do espaço é englobada pelo enlace por um determinado período de tempo (FINKENZELLER, 2010). A figura 19 exemplifica a técnica.

Figura 19 – Multiplexação por Divisão de Espaço



Fonte: http://azhar-paperpresentation.blogspot.com/2010/04/code-division-multiple-access.html

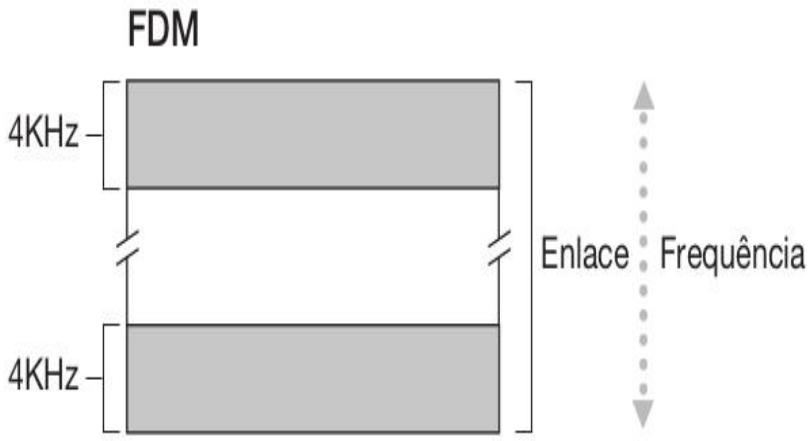
No Acesso Múltiplo por Divisão de Frequência, o espectro de frequência de um enlace é compartilhado entre todas as conexões estabelecidas através deste enlace, ou seja, o enlace reserva uma banda de frequência para cada conexão durante o período da ligação (KUROSE; ROSS, 2014). A figura 20 exemplifica a técnica.

No Acesso Múltiplo por Divisão de Tempo, o tempo é dividido em quadros de duração fixa, e cada quadro é dividido em um número fixo de compartimentos (*slots*). Quando estabelece uma conexão por meio de um enlace, a rede dedica à conexão um compartimento de tempo em cada quadro. Esses compartimentos são reservados para o uso exclusivo dessa conexão, e um dos compartimentos de tempo (em cada quadro) fica disponível para transmitir os dados dela (KUROSE; ROSS, 2014). A figura 21 exemplifica a técnica.

No Acesso Múltiplo por Divisão de Código, ao invés de se atribuir faixas de frequência ou tempo para os participantes, atribui-se um código exclusivo para cada um. Assim, cada participante usará seu código único para codificar as informações que envia (KUROSE; ROSS, 2014).

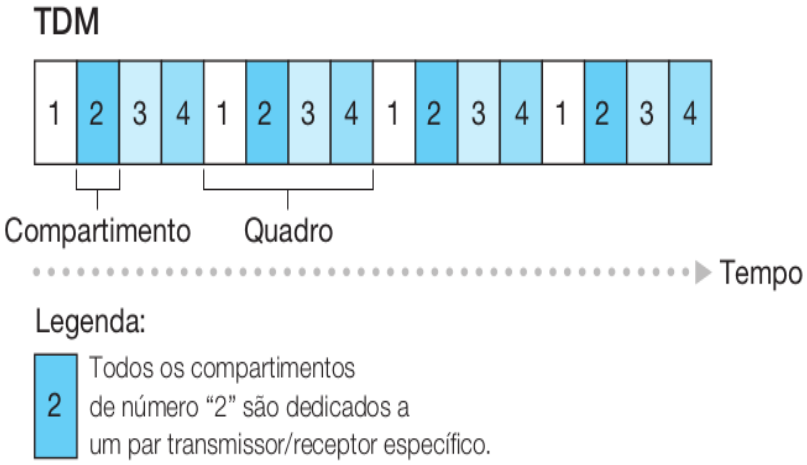
A figura 22 ilustra a diferença de comportamento dos diferentes métodos de acesso múltiplo ao meio no intervalo frequência-tempo.

Figura 20 – Multiplexação por Divisão de Frequência



Fonte: (KUROSE; ROSS, 2014, p.22)

Figura 21 – Multiplexação por Divisão de Tempo

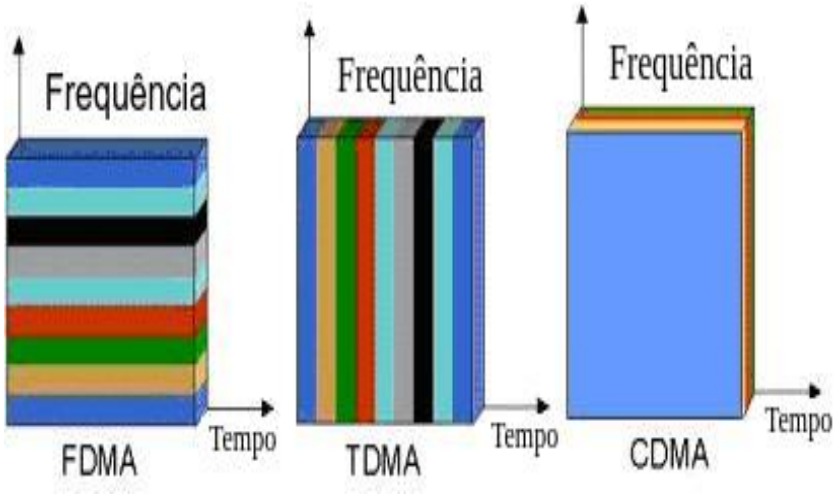


Fonte: (KUROSE; ROSS, 2014, p.22)

A implementação de procedimentos que permitam que um leitor seja capaz de identificar e receber dados de múltiplas etiquetas simultaneamente pode ser particularmente desafiador, visto que tal procedimento deve prevenir colisões entre os pacotes sem que isso cause um atraso detectável nas operações entre leitor e etiqueta. Assim, um protocolo que facilita a manipulação de múltiplos acessos pelo leitor sem causar grandes atrasos recebe o nome de "sistema de anticolisão" (FINKENZELLER, 2010) ou "protocolo de anticolisão".

Protocolos de anticolisão podem ser agrupados em duas categorias (dependendo do procedimento em que são baseados): Aloha (*aloha-based*) ou Árvore (*tree-based*). Implementar protocolos de anticolisão em sistemas passivos pode ser um desafio a mais, visto que etiquetas passivas de baixo poder computacional e memória não conseguem detectar

Figura 22 – FDMA vs TDMA vs CDMA no intervalo frequência-tempo



Fonte: http://azhar-paperpresentation.blogspot.com/2010/04/code-division-multiple-access.html

colisões nem etiquetas vizinhas ativas, ou seja, qualquer colisão gera a necessidade de retransmissão por parte da etiqueta. Assim, um protocolo de anticolisão deve permitir o reconhecimento de etiquetas passivas com poucas colisões e com execução em tempo real (AHSON; ILYAS, 2018).

2.4 PADRÕES E NORMATIVAS

Nesta seção serão abordadas as instituições que estudam e regulamentam a tecnologia de identificação por radiofrequência, bem como as normas e padrões que regem o RFID de baixa de frequência e as etiquetas passivas.

Primeiro precisa-se explicar o que é um padrão. Segundo a (ISO, 2019a, traduzido pelo autor): "Um padrão fornece especificações de classe mundial para produtos, serviços e sistemas, para garantir qualidade, segurança e eficiência.".

As normas, no contexto do RFID, foram elaboradas para padronizar quatro áreas principais:

- Interface aérea: para a comunicação básica entre etiqueta e leitor.
- Conteúdo de dados e codificação: esquemas de numeração.
- Conformidade: teste de sistemas RFID.
- Interoperabilidade entre aplicações e sistemas RFID.

(WARD; KRANENBURG, 2006)

Uma das maiores vantagens da padronização do RFID é com relação a interoperabilidade entre aplicações e sistemas, pois, como visto acima, padrões fornecem um meio

de trafegar, definir, usar e interpretar dados, independentemente de quem ou onde estes dados estejam sendo usados. Padrões permitem que, por exemplo, etiquetas sejam compradas de um fornecedor X enquanto leitores sejam comprados de um fornecedor Y, tendo garantido que etiqueta e leitor se comunicarão entre si devido aos padrões que ambos tiveram que seguir durante sua concepção e fabricação.

Dentre as instituições regulamentadoras mundiais, duas vem trabalhando com mais sucesso e destaque para a padronização do RFID: ISO/IEC e EPCglobal (MONTEIRO; PACHECO; LIMA, 2010).

2.4.1 ISO/IEC

ISO, acrônimo do inglês para *International Organization for Standardization*, é uma organização internacional independente e não governamental que tem como objetivo: "compartilhar conhecimento e desenvolver normas internacionais relevantes, voluntárias, baseadas em consenso e relevantes para o mercado, que apoiem a inovação e forneçam soluções para os desafios globais" (ISO, 2019a). A organização é responsável por: "elaborar documentos que forneçam requisitos, especificações, diretrizes ou características que podem ser usadas consistentemente para garantir que materiais, produtos, processos e serviços sejam adequados ao seu propósito" (ISO, 2019b).

IEC, acrônimo do inglês para *International Electrotechnical Commission*, é uma organização sem fins lucrativos, quase governamental (IEC, 2019b) que tem como objetivo: "preparar e publicar normas internacionais para todas as tecnologias elétricas, eletrônicas e relacionadas" (IEC, 2019a).

A alguns anos ISO e IEC se uniram em um subcomitê para juntos estabelecerem os padrões da tecnologia RFID. Este subcomitê ficou conhecido como ISO/IEC JTC1 ou apenas ISO/IEC (MONTEIRO; PACHECO; LIMA, 2010).

Algumas das principais normas ISO/IEC que regem a tecnologia de identificação por radiofrequência são:

- ISO 11784: Identificação por radiofrequência de animais - Estrutura do código.[2]
- ISO 11785: Identificação por radiofrequência de animais - Conceito técnico.[3]
- ISO 14223: Identificação por radiofrequência de animais - *transponders* avançados.[4]
- ISO/IEC 14443: Cartões e dispositivos de segurança para identificação pessoal - Objetos de proximidade sem contato.
  - ISO/IEC 14443-1: Características físicas.[5]

[2] https://www.iso.org/standard/25881.html
[3] https://www.iso.org/standard/19982.html
[4] https://www.iso.org/standard/50979.html
[5] https://www.iso.org/standard/73596.html

  - ISO/IEC 14443-2: Potência de rádio-frequência e interface de sinal.[6]
  - ISO/IEC 14443-3: Inicialização e anticolisão.[7]
  - ISO/IEC 14443-4: Protocolo de transmissão.[8]

- ISO/IEC 15961: Identificação por radiofrequência (RFID) para gerenciamento de itens - Protocolo de dados: interface do aplicativo.[9]

- ISO/IEC 15962: Identificação por radiofrequência (RFID) para gerenciamento de itens - Protocolo de dados: regras de codificação de dados e funções de memória lógica.[10]

- ISO/IEC 15963: Identificação por radiofrequência para gerenciamento de itens - identificação exclusiva para etiquetas RF.[11]

- ISO/IEC 18000: Tecnologia da informação - Identificação por radiofrequência para gerenciamento de itens

  - ISO/IEC 18000-1: Arquitetura de referência e definição de parâmetros a serem padronizados.[12]
  - ISO/IEC 18000-2: Parâmetros para comunicações de interface aérea abaixo de 135 kHz.[13]
  - ISO/IEC 18000-3: Parâmetros para comunicações de interface aérea a 13,56 MHz.[14]
  - ISO/IEC 18000-4: Parâmetros para comunicações de interface aérea a 2,45 GH.[15]
  - ISO/IEC 18000-6: Parâmetros para comunicações de interface aérea a 860 MHz a 960 MHz Geral.[16]
  - ISO/IEC 18000-7: Parâmetros para comunicações de interface aérea ativa a 433 MHz.[17]

(CHAWLA; HA, 2007; RFID4U, 2019)

[6] https://www.iso.org/standard/66288.html
[7] https://www.iso.org/standard/73598.html
[8] https://www.iso.org/standard/73599.html
[9] https://www.iso.org/standard/30528.html
[10] https://www.iso.org/standard/43459.html
[11] https://www.iso.org/standard/52124.html
[12] https://www.iso.org/standard/46145.html
[13] https://www.iso.org/standard/46146.html
[14] https://www.iso.org/standard/53424.html
[15] https://www.iso.org/standard/68145.html
[16] https://www.iso.org/standard/59644.html
[17] https://www.iso.org/standard/57336.html

2.4.2 EPCglobal

EPCglobal é uma iniciativa da organização GS1 (organização sem fins lucrativos que desenvolve e mantém padrões globais para comunicação empresarial) que tem como objetivo: "[...] inovar e desenvolver padrões voltados a indústria no setor de Código Eletrônico de Produto (*Electronic Product Code (EPC)*), apoiar o uso da tecnologia de identificação por radiofrequência (RFID) e permitir a visibilidade global de itens (EPCIS) nos dias atuais." (GS1, 2019).

EPC, acrônimo do inglês para *Electronic Product Code*, é um valor numérico único gravado na memória das etiquetas RFID (que seguem as normas da EPCglobal) e que funciona como identificador universal único para objetos físicos. O código EPC possui 96-bits de informação e é estruturado como na figura 23 (WARD; KRANENBURG, 2006).

Figura 23 – Estrutura EPC

Fonte: (WARD; KRANENBURG, 2006, p.13)

O *header* define qual codificação está em uso, o *EPC Manager* identifica a empresa/-fabricante do produto, o *Object Class* define o produto em si e o *Serial Number* define uma entidade do produto (WARD; KRANENBURG, 2006). Assim, os 96-bits de informação podem fornecer identificadores exclusivos para aproximadamente 268 milhões 2^28 de empresas, onde cada empresa pode ter aproximadamente 16 milhões 2^24 de tipos de produtos e aproximadamente 68 bilhões 2^36 de números de série em cada classe (BROCK, 2010).

O consórcio EPCglobal, em conjunto com o *Media Lab* do Instituto de Tecnologia de Massachusetts (*Institute of Technology*), decidiu criar um novo padrão para sistemas RFID de ultra-alta frequência (UHF). O primeiro conjunto de padrões e etiquetas resultante desta parceria ficou conhecido como *Generation-1* (Gen-1) (WANT, 2006b)

Devido ao sucesso e a algumas limitações relacionadas a escalabilidade global da Gen-1, a EPCglobal, em conjunto com a ISO, trabalharam para elaborar a próxima geração deste padrão que ficou conhecido como *Generation-2* (Gen-2) (WANT, 2006b). A *joint-venture* entre EPCglobal e ISO fez com que o Gen-2 também fosse incluído como um padrão ISO, similar ao padrão ISO 18000-6 tipo C (LOUREIRO; SOUZA; LOPES, 2015).

Uma das principais alterações da Gen-1 para a Gen-2 foi a adição de um *bit* no *header* do EPC, permitindo assim que leitores RFID possam distinguir etiquetas ISO de etiquetas EPCglobal na hora da leitura (WANT, 2006b).

O padrão Gen-2 define cinco classes de etiquetas RFID que vão sendo incrementadas progressivamente sobre as classes anteriores:

- Classe 0 ou Classe 1: Etiqueta passiva
  - Etiqueta simples, utilizada como base para todas as outras etiquetas passivas;
  - identificador de etiqueta (*tag identifier* - TID): armazena informações sobre o fabricante da etiqueta;
  - Memória somente-leitura estilo escreva-uma-leia-muitas (*write-once-read-many*);
  - controle de acesso protegido por senha;
  - botão de desligamento (*kill switch*) para desabilitar a etiqueta no ponto de venda;
  - memória do usuário (opcional).
- Classe 2: Etiqueta passiva com funcionalidade estendida
  - memória regravável;
  - identificador de etiqueta (TID) estendido;
  - memória do usuário estendida;
  - controle de acesso autenticado.
- Classe 3: Etiqueta semi-passiva
  - Etiqueta semi-passiva com bateria interna abrangendo funcionalidades da classe 3;
  - fonte de energia integral para suplementar a energia capturada;
  - circuito de sensoriamento integrado.
- Classe 4: Etiqueta ativa *ad-hoc*
  - Etiqueta ativa abrangendo funcionalidades da classe 3;
  - Capacidade de se comunicar com outras etiquetas da mesma classe;
  - Capacidade de formar redes *ad-hoc*.
- Classe 5: Etiqueta-leitor ativa
  - Etiqueta-leitor abrangendo funcionalidades da classe 4;
  - Capacidade de energizar etiquetas das classes 1 e 2;
  - Capacidade de estabelecer comunicação passiva com etiquetas da classe 3.

(WANT, 2006b; ADHIARNA; RHO, 2009)

Apesar de ambas as iniciativas, ISO/IEC e EPCglobal, estarem trabalhando na padronização do RFID isto não significa que estejam convergindo para o mesmo ponto. Enquanto ISO/IEC tem como foco padronizar protocolos de interface aérea, estrutura e formatação de dados em etiquetas, testes de conformidade, testes de performance e outros para toda a indústria, independente da frequência utilizada; a EPCglobal tem como foco padronizar o desenvolvimento e utilização do EPC e do próprio protocolo de interface aérea para rastreio de produtos através de uma cadeia internacional de fornecimento, com enfoque nas frequências ultra-altas (VIOLINO, 2005).

Um ponto importante a se destacar é que os padrões da ISO/IEC e EPCglobal não regulamentam as faixas de frequência utilizáveis em cada região, ou seja, cada país é responsável por definir e regulamentar o uso e as faixas de frequências permitidas para dispositivos de rádio, como é o caso do RFID (RFID4U, 2019).

2.5 NEAR FIELD COMMUNICATION (NFC)

NFC, sigla em inglês para *Near Field Communication*, ou Comunicação de Campo Próximo em português, é um protocolo de comunicação sem fio de curto alcance fortemente baseado nos padrões RFID, desenvolvido inicialmente pelas empresas Philips e Sony no final de 2002 (COSKUN; OZDENIZCI; OK, 2013) com o objetivo de proporcionar, a dispositivos móveis sem fio, um meio seguro de comunicação com outros dispositivos similares que estivessem nas redondezas imediatamente próximas, sem que houvesse qualquer esforço na configuração da rede por parte do usuário (AHSON; ILYAS, 2018; WANT, 2006b).

Devido ao forte embasamento no RFID, o NFC possui diversas similaridades com este. Algumas das características da tecnologia incluem: ser um protocolo de comunicação de curta distância (até 10cm), *half-duplex*, utilizar-se do acoplamento indutivo entre dispositivos, operar na frequência de 13.56 MHz, possuir uma taxa de transferência de até 424 kbps, operar de forma um-para-um, dentre outras (COSKUN; OZDENIZCI; OK, 2013; COSKUN; OZDENIZCI; OK, 2012).

Apesar das semelhanças, NFC e RFID também possuem algumas diferenças entre si:

A primeira diferença diz respeito ao modo de comunicação entre os dispositivos. Enquanto que no RFID o sentido de comunicação é unilateral, ou seja, o leitor interroga a etiqueta e a etiqueta depois simplesmente responde, no NFC o sentido da comunicação pode ser tanto unilateral quanto bilateral (SAB; FERREIRA; ROZENDO, 2013). Esta bilateralidade deve-se ao fato de que dispositivos NFC podem ser construídos para trabalhar tanto como leitor quanto como etiqueta, possuindo para isto tanto um transceptor quanto um transponder de 13.56 MHz conectados à antena (FINKENZELLER, 2010). Devido a esta bilateralidade, dispositivos NFC podem realizar uma comunicação *Peer-to-*

Peer entre si, sendo uma das características que auxilia na implementação e popularização da tecnologia nos *smartphones* mais atuais.

A segunda diferença diz respeito à distância de comunicação entre os dispositivos. Enquanto o RFID pode possuir diversas distâncias de operação, de alguns centímetros até dezenas de metros dependendo da implementação, o NFC possui uma distância de operação prática de até 10 cm. A curta distância possui algumas vantagens, tais como: maior segurança e menor geração de interferência ao redor da comunicação (SAB; FERREIRA; ROZENDO, 2013).

O protocolo NFC define três tipos de dispositivos: celular habilitado com NFC, etiqueta NFC e leitor NFC. Um celular habilitado com NFC, como o próprio nome sugere, é um celular tradicional ou um *smartphone* contendo os protocolos de comunicação NFC inclusos. Uma etiqueta NFC nada mais é do que uma etiqueta RFID passiva, com uma pequena memória para armazenamento de dados, que assim como uma etiqueta RFID passiva, necessita do campo magnético gerado por um dispositivo ativo, como um leitor ou um celular, para poder operar e transmitir seus dados. Um leitor NFC é um dispositivo ativo capaz de se comunicar de forma bidirecional com outros dispositivos NFC. Uma associação interessante que pode ser realizada é a de um celular NFC com um leitor NFC, dando ao celular a capacidade de ler e escrever etiquetas NFC (COSKUN; OZDENIZCI; OK, 2012).

O protocolo NFC apresenta dois modos de operação: ativo e passivo. No modo ativo, os dois dispositivos da comunicação possuem uma fonte de energia interna própria, sendo ambos capazes de gerar um campo magnético para a transmissão dos dados. No modo passivo, apenas um dos dispositivos da comunicação é capaz de gerar um campo magnético, ficando este conhecido como "iniciador" e sendo responsável por iniciar a troca de informações, enquanto o segundo dispositivo apenas utiliza o campo gerado pelo primeiro para funcionar (COSKUN; OZDENIZCI; OK, 2012).

O protocolo NFC define três formas possíveis de operação para os dispositivos: leitor/escritor, *peer-to-peer* e emulação de cartão. Cada modo possui um requisito técnico, operacional e de projeto diferente, bem como uma interface de radiofrequência distinta (ISO/IEC 14443, FeliCa, NFCIP-1, NFCIP-2) (COSKUN; OZDENIZCI; OK, 2013).

Com relação à padronização, a tecnologia também possui seu conjunto de padrões. O NFC é definido principalmente nas normas ISO/IEC 18092[18] NFCIP-1 (ECMA 340) e ISO/IEC 21481[19] NFCIP-2 (ECMA 352) (FINKENZELLER, 2010). Na camada física de radiofrequência, por outro lado, temos um conjunto de protocolos que são compatíveis

[18] https://www.iso.org/standard/56692.html
[19] https://www.iso.org/standard/56855.html

com as normas ISO/IEC 14443, JIS X 6319[20,21,22,23] (padrão de cartão inteligente de proximidade sem contato da Sony conhecido como FeliCa) e ISO/IEC 15693[24,25,26] (outro padrão de cartão inteligente de proximidade sem contato) (COSKUN; OZDENIZCI; OK, 2012).

Um ponto importante a se destacar aqui é sobre a ISO/IEC 14443 e seus dois subtipos: ISO/IEC 14443 Tipo A (ISO/IEC 14443-A) e ISO/IEC 14443 Tipo B (ISO/IEC 14443-B). Devido a falta de acordo entre as partes durante a elaboração da norma ISO/IEC 14443, com relação à interface de comunicação e como a transferência de dados entre leitor e etiqueta deveria funcionar, dois procedimentos distintos de transferência foram criados, gerando as sub-normas Tipo A e Tipo B (FINKENZELLER, 2010).

No Tipo A, 100% da modulação ASK, com um Miller modificado para codificação dos dados, é utilizado como procedimento de modulação para transferência de dados leitor-etiqueta. Na comunicação etiqueta-leitor, a subportadora OOK de 847.5 kHz (13.56 MHz / 16) é utilizada para a comunicação, com Modulação de Carga (*Load Modulation*) e codificação de dados Manchester (COSKUN; OZDENIZCI; OK, 2012; FINKENZELLER, 2010).

No Tipo B, 10% da modulação ASK, com o NRZ-L para codificação dos dados, é utilizado como procedimento de modulação para transferência de dados leitor-etiqueta. Na comunicação etiqueta-leitor, a subportadora OOK de 847.5 kHz (13.56 MHz / 16) é utilizada para a comunicação, com modulação de sinal de 180º BPSK (*Binary Phase Shift Keying*) e codificação de dados NRZ-L (COSKUN; OZDENIZCI; OK, 2012; FINKENZELLER, 2010).

Apesar desta dupla existência, etiquetas e cartões inteligentes só precisam implementar um dos dois procedimentos para estarem em conformidade com a ISO. Os leitores, por outro lado, precisam suportar completamente e simultaneamente os dois procedimentos, chaveando entre um e outro periodicamente durante a fase de espera de um cartão, para estarem em conformidade com a ISO (FINKENZELLER, 2010).

2.5.1 NFC Forum

Assim como o RFID, o NFC também possui suas organizações e associações que ajudam a desenvolver e promover o uso da tecnologia. No caso do NFC temos o "NFC Forum", uma das instituições mais atuantes e importantes neste segmento.

[20] https://standards.globalspec.com/std/1281338/jis-x-6319-1
[21] https://standards.globalspec.com/std/1548443/jis-x-6319-2
[22] https://standards.globalspec.com/std/1360369/jis-x-6319-3
[23] https://standards.globalspec.com/std/10070623/jis-x-6319-4
[24] https://www.iso.org/standard/70837.html
[25] https://www.iso.org/standard/73601.html
[26] https://www.iso.org/standard/73602.html

Segundo a própria instituição, o NFC Forum é uma associação industrial sem fins lucrativos cujos membros advém de todas os setores do universo NFC. Trabalhando em conjunto com o NFC Forum, as organizações membros compartilham experiência em desenvolvimento, aplicação e *marketing*, a fim de desenvolver as melhores soluções possíveis para promover o uso da tecnologia de NFC, melhorando a vida dos consumidores em todo o mundo e avançando nos objetivos de negócios das organizações membros (FORUM, 2019a).

O fórum tem como missão: promover o uso do NFC através do desenvolvimento de especificações, garantindo a interoperabilidade entre dispositivos e serviços e educando o mercado sobre a tecnologia NFC (COSKUN; OZDENIZCI; OK, 2012). Além disso, a associação possui como principais objetivos:

- Desenvolver especificações NFC que definam uma arquitetura modular para dispositivos NFC.
- Definir protocolos de interoperabilidade e entrega de serviços independente do dispositivo utilizado.
- Definir protocolos para descoberta de dispositivos.
- Incentivar os provedores de tecnologia a desenvolver e implantar produtos habilitados para NFC em torno de um conjunto comum de especificações.
- Estabelecer um programa de certificação que garanta produtos compatíveis de acordo com as especificações do NFC Forum.
- Promover o uso global da tecnologia NFC educando consumidores e usuários corporativos sobre os aplicativos e benefícios da tecnologia.

(COSKUN; OZDENIZCI; OK, 2012)

Um dos trabalhos realizados pelo NFC Fórum, por exemplo, foi a definição de quatro tipos distintos de etiquetas NFC, da etiqueta tipo 1 até a etiqueta tipo 4. Cada tipo possui diferentes características e é baseado em pelo menos um dos padrões: ISO/IEC 1444-A, ISO/IEC 14443-B ou JIS X 6319 (Sony FeliCa) (COSKUN; OZDENIZCI; OK, 2012):

- Tipo 1: A etiqueta NFC tipo 1 é baseada na norma ISO/IEC 14443 Tipo A, é tanto gravável (*writable*) quanto somente-leitura (mas pode ser configurada como somente-leitura pelo usuário), possui capacidade de armazenamento expansível até 2 kb e velocidade de comunicação de 106 kbps.
- Tipo 2: A etiqueta NFC tipo 2 é baseada na norma ISO/IEC 14443 Tipo A, é tanto gravável quanto somente-leitura (mas pode ser configurada como somente-

leitura pelo usuário), possui capacidade de armazenamento expansível até 2 kb e velocidade de comunicação de 106 kbps.

- Tipo 3: A etiqueta NFC tipo 3 é baseada na norma JIS X 6319, possui capacidade de armazenamento de 2 kb e velocidade de comunicação de 212 kbps.

- Tipo 4: A etiqueta NFC tipo 4 é compatível com os dois subtipos (A e B) da norma ISO/IEC 14443, pode ser gravável ou somente-leitura, possui capacidade de armazenamento de até 32 kB e velocidade de comunicação entre 106 kbps e 424 kbps.

Apesar de não muito conhecido pelo publico em geral, o NFC Forum possui grandes nomes da indústria de tecnologia e de pagamento como membros principais, tais como: Apple, Google, Mastercard, Visa, NXP, QUALCOMM, Samsung, Sony, entre outros (FORUM, 2019b).

2.6 FALHAS DE SEGURANÇA

Nesta seção serão abordados os principais pontos fracos da tecnologia de identificação por radiofrequência na área da segurança da informação.

Assim como qualquer outro sistema computacional, sistemas RFID também são passíveis de serem afetados por problemas de segurança, tais como falhas, vulnerabilidades e ataques em vários pontos da infraestrutura.(FINKENZELLER, 2010).

Ataques a sistemas RFID podem ser direcionados a três pontos da infraestrutura: etiqueta, leitor ou interface aérea leitor-etiqueta (FINKENZELLER, 2010), podem ser caracterizadas em quatro grupos: ataques à autenticidade, integridade, confidencialidade e/ou disponibilidade (XIAO; GIBBONS; LEBRUN, 2009) e podem ser realizados por diversos motivos, mas agrupáveis em uma das quatro categorias:

- : Espionagem: o atacante tenta obter acesso não autorizado a informações e dados do arquivo ativo e passivo.:

- : Fraude: o atacante tenta fornecer informações incorretas ao sistema RFID para enganar a parte ativa, ou seja, o operador do sistema RFID ou a parte passiva, ou seja, o usuário do sistema RFID.:

- : Negação de serviço: esse tipo de ataque afeta a disponibilidade de funções do sistema RFID.:

- : Proteção a privacidade: O atacante considera o sistema RFID uma ameaça à sua privacidade e tenta se proteger com ataques ao sistema RFID.

(FINKENZELLER, 2010):

(XIAO; GIBBONS; LEBRUN, 2009, p.365-371,traduzido pelo autor) definem os seguintes ataques em seu artigo: "Engenharia reversa, análise de consumo energético, *eavesdropping*, ataque de *man-in-the-middle*, negação de Serviço (DoS), *spoofing*, clonagem, reenvio, vírus, rastreamento, abordagem matar etiqueta e bloqueio de etiqueta.". Apesar de todos serem considerados ataques a sistemas RFID, alguns são mais específicos e danosos para certas implementações, como por exemplo, a abordagem "matar etiqueta" pode ser muito mais nociva a implementações de controle de estoque do que de controle de acesso. Desta forma, serão abordados nesta seção apenas os ataques mais nocivos a implementações de controle de acesso.

Eavesdropping (escuta): Como todo sistema de comunicação sem fio, onde os dados viajam pelo ar em múltiplas direções, sistemas RFID também podem sofrer de interceptações e escutas não autorizados. Assim, um ataque de *eavesdrop* ocorre quando um agente terceiro externo consegue interceptar a comunicação entre etiqueta e leitor enquanto ambos trocam dados e comandos. Devido a falta de capacidade, ou elevados custos de implementação, a maioria das etiquetas RFID não possuem um sistema criptográfico implementado, consequentemente durante as comunicações, informações e comandos trafegados entre leitor e etiqueta são feitos em texto claro, tornando este tipo de ataque relativamente simples mas efetivo. As informações obtidas neste ataque podem gerar outros ataques à infraestrutura RFID (XIAO; GIBBONS; LEBRUN, 2009).

Man-in-the-middle (homem-no-meio): Ataques de *man-in-the-middle* (MITM) são um velho conhecido na segurança de redes de computadores e redes sem fio. Este tipo de ataque ocorre quando um agente terceiro externo consegue se posicionar no meio da comunicação entre dois componentes, no cenário do RFID entre etiqueta e leitor, podendo desta forma observar e manipular as informações que e vem e vão sem que os comunicantes tenham ciência do ataque (CAPEC, 2019). Sistemas RFID são particularmente vulneráveis a este tipo de ataque devido ao tamanho e baixíssimo preço das etiquetas, o que significa que geralmente há falta de circuitos sofisticados de proteção ou criptografia (XIAO; GIBBONS; LEBRUN, 2009).

Clonagem: Clonagem é o processo de copiar os dados de uma etiqueta válida e inseri-los em uma outra etiqueta, criando assim uma cópia não-autorizada idêntica a original (XIAO; GIBBONS; LEBRUN, 2009). Um exemplo deste ataque são os resultados obtidos pelos pesquisadores da Universidade Johns Hopkins e da RSA Labs, que publicaram resultados experimentais da clonagem de uma etiqueta criptograficamente protegida da Texas Instruments, a *digital signature transponder (DST)*,que foi utilizada para comprar gasolina e dar a partida em um carro (TANENBAUM; RIEBACK; CRISPO, 2006; XIAO; GIBBONS; LEBRUN, 2009).

Spoofing: Um ataque de *spoof* ocorre quando uma etiqueta forjada, através de clonagem por exemplo, se passa por uma etiqueta válida para um leitor RFID, ganhando assim

acesso ou vantagem ilegítimos. O processo de *spoofing* e clonagem estão intrinsecamente ligados, primeiro usando-se a clonagem para se obter uma etiqueta válida e depois utilizando a etiqueta clonada para se obter vantagens indevidas (XIAO; GIBBONS; LEBRUN, 2009).

Reenvio (*replay*): Neste tipo de ataque um agente mal-intencionado intercepta as comunicações entre leitor e etiqueta (seja por MITM, *eavesdrop* ou outros), grava um sinal válido, seja comando do leitor ou resposta da etiqueta, e posteriormente reproduz este sinal para algum fim (XIAO; GIBBONS; LEBRUN, 2009). Este ataque pode ser utilizando, por exemplo, para interceptar a resposta da etiqueta ao leitor e posteriormente reproduzi-la para conseguir acesso a algum lugar.

Negação de serviço (DoS): Os ataques descritos até aqui tinham, como objetivo, alterar ou obter informações a fim de burlar sistemas de identificação. A negação de serviço, entretanto, possui como principal objetivo desabilitar ou inutilizar o sistema, seja atacando a etiqueta, a interface aérea de comunicação ou o *backend*. Um dos ataques de DoS mais simples e eficientes que podem ser realizados contra sistemas RFID é sobre a interface sem fio, mais precisamente sobre a camada física da aplicação, através de *jamming* e interferência (XIAO; GIBBONS; LEBRUN, 2009). *Jamming* ocorre quando um dispositivo transmite ativamente sinais de rádio pode congestionar o canal de comunicação, e com isso interromper o funcionamento de todos os leitores ao seu redor (EGLI, 2006 apud XIAO; GIBBONS; LEBRUN, 2009). Para funcionar, entretanto, um dispositivo de *jamming* precisa estar perto o suficiente do leitor ou usar antenas suficientemente grandes ou operar em alta potência de transmissão (FINKENZELLER, 2010).

Como visto acima, diversas formas e caminhos podem ser tomados para atacar sistemas RFID e, apesar desta seção não ter entrado em detalhes sobre contramedidas para as vulnerabilidades apresentadas, diversos esforços tem sido feitos para combater tais problemas.

3 TRABALHOS ACADÊMICOS RELACIONADOS

Uma das principais aplicações do RFID, no mundo prático, é o de controle automático de estoque de mercadorias e bens, porém, apesar de principal, ela não é a única. A ideia de se criar e utilizar um sistema de identificação por radiofrequência que, ao invés de identificar e controlar objetos, identifique e valide pessoas e controle seu acesso a salas e prédios não é nova. Existem diversas citações, exemplos e experimentações na literatura sobre como o RFID pode ser utilizado para tal finalidade.

Para começar e mostrar que, de fato, a ideia não é nova, pode-se citar o livro (KITSOS; ZHANG, 2008), que nas seções "3.1.3 Personal Identification and Access Control" e "2.3.2 Access Control", os autores abordam a utilização do RFID no controles de acesso. A obra destaca as vantagens dos cartões de acesso RFID em comparação às chaves tradicionais; tais como o fato de serem mais difíceis de serem copiados, mais fáceis de serem substituídos em caso de perda, fornecerem mais controle e registro da sua utilização; e como o RFID já é implementado em diversas companhias e hotéis para tal finalidade (KITSOS; ZHANG, 2008).

Um segundo ponto abordado é que, assim como uma catraca é um ponto de acesso para um prédio, um aeroporto pode ser considerado um ponto de acesso para um país. Assim, os autores discutem brevemente a utilização do RFID, tanto para o lado positivo, como aumentar a integridade do passaporte e diminuir falsificações, quanto para o lado negativo, como verificação de antecedentes não autorizada, roubo de identidade e rastreamento ilegal. Um exemplo de caso de uso de RFID em passaportes é o governo dos EUA, que emitiu passaportes incluindo um chip RFID de 64 kilobytes contendo as informações pessoais do portador do passaporte (KITSOS; ZHANG, 2008).

O trabalho (RAVI et al., 2013), propõe um sistema de segurança de identificação de pessoas através da tecnologia de RFID, provendo controle de acesso a áreas restritas através da implementação do sistema em um ponto de controle de acesso, como uma porta. Os autores destacam que tal sistema ajuda a melhorar os níveis de segurança por só permitir a entrada de pessoas autorizadas nos ambientes em que o sistema encontra-se instalado.

O funcionamento do sistema dá-se da seguinte maneira: O processo começa quando uma etiqueta RFID entra no campo de atuação do leitor RFID. O leitor então interroga a etiqueta para obter seus dados e enviá-los ao microcontrolador, onde ocorrerá o resto da validação. O microcontrolador, de posse dos dados, faz uma comparação dos mesmos com sua base de dados interna, a fim de validar se a etiqueta apresentada possui ou não autorização de entrada. Caso esteja tudo correto, o microcontrolador libera o acesso do usuário pela porta, caso contrário, a porta continua travada (RAVI et al., 2013).

Tanto o trabalho em destaque quanto esta monografia possuem um esquema geral

de funcionamento parecidos, entretanto, alguns detalhes fazem a diferença. O primeiro deles é o fato de que, no trabalho em destaque, a base de dados de usuários encontra-se na memória do microcontrolador que, como veremos a seguir, possui apenas 4K bytes. No projeto desta monografia, por outro lado, a base de dados de usuários encontra-se em um sistema de gerenciamento de banco de dados em um servidor central apartado, garantindo assim todas as vantagens de tal sistema, como: escalabilidade, confiabilidade, simplicidade de manuseio, desempenho, flexibilidade e etc. O segundo detalhe é o fato do microcontrolador escolhido, um 89c51, ser muito antigo, limitado em processamento e capacidade e não mais recomendado pela própria fabricante, o que pode limitar futuras expansões. No projeto desta monografia, por outro lado, o microcontrolador escolhido, um Raspberry Pi Zero W, apesar de um pouco mais caro, possibilita mais flexibilidade por ser mais moderno, possuir mais poder de processamento, armazenamento, portas de conexões serial e sem fio, além de um sistema operacional completo como Linux. O terceiro detalhe é que não há, no trabalho em destaque, a menção de um *software* de gerenciamento do sistema, ou seja, não há um *software* onde um operador externo possa realizar alterações ou consultas no banco de dados de usuários. No projeto desta monografia, por outro lado, uma aplicação *web* foi construída especialmente para este projeto, para que um operador externo possa interagir com o sistema sem a necessidade de conhecimento prévio sobre a arquitetura do projeto.

Os principais componentes utilizados pelos autores para o projeto foram: Etiqueta RFID, leitor RFID, microcontrolador 89c51 e motor para controle da porta (RAVI et al., 2013). O 89c51 "[...] é um microcomputador CMOS de 8 bits de baixo consumo e alto desempenho com 4K bytes de memória Flash somente-leitura programável e apagável [...]" (CORPORATION, 2000, traduzido pelo autor). Comparado ao microcontrolador utilizado nesta monografia, o Raspberry Pi Zero W, o 89c51 é inferior em quase todos os aspectos, desde o número de portar *GPIO* e tipos de conexões com o mundo externo até processamento, armazenamento e flexibilidade. Não há especificações com relação ao tipo da etiqueta e do leitor, sendo assim não há como se fazer uma correlação com os mesmos componentes presentes nesta monografia.

O projeto apresentado acima mostra-se extremamente simples, um dos mais simples que serão apresentados aqui, sendo exatamente por este motivo que ele é um dos primeiros desta seção, para mostrar o quão simples um sistema de segurança de identificação por radiofrequência pode ser.

No livro (GRAAFSTRA, 2006), capítulo 2 "Getting in the Front Door", o autor desenvolve o projeto de implementação de uma fechadura eletrônica contendo RFID, teclado e chave física em uma porta convencional. O capítulo trata tanto da parte teórica, mostrando e explicando os componentes utilizados, quanto da parte prática, explicando de forma macro os passos a serem adotados. O autor se preocupa com aspectos de segurança que poderiam passar despercebidos por outros, como a não exposição de cabos para fora

da caixa da fechadura e a possibilidade de se usar uma chave convencional no caso de falhas no sistema ou ausência de energia elétrica para operação do mesmo (GRAAFSTRA, 2006).

Por se tratar de uma fechadura com certos aspectos convencionais, em uma porta convencional, alguns componentes assemelham-se aos já encontrados em fechaduras tradicionais, já outros são mais específicos para a parte elétrica, assim, o projeto lista como componentes: placas de circuito de uso geral, relés, batedor de porta eletrônico (*electronic door strike*), leitor USB RFID, trinco eletrônico com teclado e caixa plástica de proteção (GRAAFSTRA, 2006). Por se tratar de uma implementação para portas tradicionais, alguns dos equipamentos listados não se encaixam no projeto proposto por este trabalho, tais como o batedor de porta eletrônico e o trinco eletrônico com teclado, visto que este trabalho visa ser implementado em um ponto como uma catraca, onde não há portas, trincos ou batedores. Os outros componentes, apesar de plausíveis de serem utilizados, não acarretariam em ganhos significativos de funcionalidade, controle, preço ou praticidade ao projeto e aos componentes propostos nesta monografia. O leitor USB RFID proposto no livro, por exemplo, necessita estar conectado a um computador para funcionar e bibliotecas proprietárias para a leitura/escrita das etiquetas, além de ser mais caro que os componentes utilizados para o mesmo fim nesta monografia, um microcontrolador e um módulo RFID.

Apesar do projeto ser interessante e mostra-se bem estruturado e explicado, o mesmo trata de uma implementação para uso pessoal em portas tradicionais, enquanto que a proposta mostrada nesta monografia visa ambientes maiores, mais heterogêneos, com um fluxo de uso maior e uma escalabilidade mais fácil, graças ao modo como a parte física e lógica foram separadas e elaborados.

O trabalho de iniciação científica (SILVA, 2018) propõe a criação de um sistema para automatizar o controle de frequência dos alunos nas aulas da Universidade Paulista (UNIP). Como motivação, o autor destaca o processo manual de controle de frequência realizada por instituições de ensino e professores através das conhecidas "chamadas"[1] em sala de aula, como este processo é dispendioso em questão de tempo de aula, redundante por ser necessário inseri-lo posteriormente em um sistema digital da instituição e passível de falhas. Assim, para tentar sanar tais problemas, o autor propõe o uso da IOT e do RFID na elaboração de um sistema informatizado capaz de automatizar a coleta e armazenamento em nuvem da presença dos alunos em sala de aula, bem como facilitar o acompanhamento desta frequência por parte dos professores através de um aplicativo de celular.

Os principais materiais e *softwares* utilizados pelo autor foram: NodeMCU com microcontrolador ESP8266, módulo RFID-RC522, etiquetas RFID e NFC, arquitetura de

[1] Processo em que o professor chama, em voz alta e durante a aula, o nome de cada aluno inscrito na matéria e, quando chamado, o aluno deve confirmar presença ao professor

servidor WAMP (*Windows, Apache, MySQL, PHP*) e plataforma de desenvolvimento *mobile* "MIT App Inventor 2"[2] (SILVA, 2018). Apesar do NodeMCU com ESP8266 ser um microcontrolador pequeno e muito barato, o mesmo é mais limitado e complexo de se manusear se comparado ao microcontrolador escolhido nesta monografia, o Raspberry Pi Zero W. O NodeMCU pode ser considerado mais limitado por não possuir tanto poder de processamento ou um sistema operacional completo como o Raspberry Pi, além de ser mais complexo de se programar por utilizar uma linguagem de programação própria, enquanto que, exatamente por possuir um sistema operacional completo, o Raspberry Pi suporta uma infinidade de linguagens de programação. Em contrapartida, ambos os trabalhos, a iniciação científica e esta monografia, escolheram o módulo RFID-RC522 como módulo RFID, sendo este o módulo de escolha para vários projetos que lidam com RFID de alta frequência.

Com relação a arquitetura de servidor, o autor utilizou-se do conjunto conhecido como WAMP, composto por: Windows como sistema operacional, Apache como servidor *web*, MySQL como banco de dados e PHP como linguagem de programação no servidor. Apesar de ser uma arquitetura conhecida e sólida, ela tem o problema de se basear no Windows, um sistema operacional proprietário pago, assim, para a realização do projeto desta monografia, deu-se preferência a utilização do Linux, um sistema operacional livre e sem custos, ao invés do Windows. Outra mudança é a substituição do banco de dados MySQL pelo MariaDB, entretanto, ambos são muito parecidos entre si, sendo o MariaDB um *fork* do MySQL.

O trabalho apresentado mostra-se interessante pois aborda um problema real enfrentado em praticamente todas as instituições de ensino brasileiras. Apesar da solução proposta ser de difícil implementação por necessitar de investimento em infraestrutura e equipamentos, a mesma não deixa de ser factível e relativamente simples em termos técnicos. Ambos os trabalhos, a iniciação científica e esta monografia, são similares em sua proposta e implementação, pois ambos propõem-se em implementar um sistema de controle de presença/acesso, utilizando a tecnologia RFID com microcontroladores e módulos baratos e aplicações criadas especialmente para o projeto. Apesar de algumas diferenças, como a escolha por servidores locais ao invés da computação em nuvem como proposto no trabalho acima, as semelhanças sobressaem-se as diferenças.

O trabalho (DEVECCHI; UNIFACCAMP, 2015) propõe a criação de um sistema embarcado de ponto eletrônico digital com tecnologia RFID, um banco de dados para armazenamento e um sistema *web* para exibição do fluxo (entrada e saída) gerado pelas passagens no ponto eletrônico.

Os principais materiais e *softwares* utilizados pelo autor foram: placa Arduino Duemilanove, placa Arduino Ethernet Shield, módulo RTC (*Real Time Clock*), módulo RFID-RC522, módulo LCD (*Liquid Crystal Display*), servidor *web* Apache, banco de dados

[2] http://ai2.appinventor.mit.edu/

MySQL 5.5 e linguagem de programação de servidor PHP 5.4 (DEVECCHI; UNIFACCAMP, 2015). O módulo RFID-RC522 escolhido pelo autor é o mesmo utilizado nesta monografia, sendo este o módulo padrão para vários projetos que lidam com RFID de alta frequência. Apesar do Arduino escolhido ser um microcontrolador sólido e bastante utilizado, o mesmo mostra-se incompleto para o projeto proposto pelo autor, visto que houve a necessidade de se acoplar um módulo *Ethernet* para que o conjunto pudesse se comunicar com um servidor *web* externo. Outro ponto que pode se tornar um problema é a escolha por um módulo de conexão a Internet via cabo, o que torna necessário uma infraestrutura de cabeamento Ethernet de um roteador ou *switch* até o Arduino. Ambos os problemas foram contornados nesta monografia com a escolha do Raspberry Pi Zero W como microcontrolador, pois o mesmo possui um módulo de comunicação sem fio já acoplado à placa. Outro ponto positivo do Raspberry Pi sobre o Arduino é o sistema operacional completo que roda sobre ele, conferindo uma customização e facilidade de uso maior se comparado ao Arduino.

Com relação a arquitetura de servidor, todos os *softwares* escolhidos pelo autor do trabalho acima são similares aos utilizados nesta monografia, sendo a única diferença, excluindo-se as versões, é a utilização do MariaDB ao invés do MySQL como sistema de gerenciamento de banco de dados.

O trabalho apresentado, apesar de simples, possui alguns problemas arquiteturais, como a escolha de um microcontrolador sem meios próprios de acesso a Internet, quando a funcionalidade mostra-se necessária. Independente disto, ambos os projetos, o trabalho acima e esta monografia, possuem objetivos similares, enquanto o primeiro registra o fluxo de passagem (entrada e saída) de funcionários pelo ponto eletrônico, o segundo registra e controla o fluxo de pessoas por um ponto de controle de acesso, ambos utilizando-se da tecnologia de identificação por radiofrequência para identificar os usuários dos sistema.

O trabalho (ONONIWU; NWAJI, 2012) desenvolve um sistema de gerenciamento automático de presença, um ponto eletrônico de presença, com controle automático da porta de entrada, utilizando-se do RFID de baixa frequência como meio identificador do funcionário. O sistema fica responsável por verificar se a etiqueta apresentada pelo usuário está cadastrada no sistema, validando assim se o mesmo é realmente um funcionário, e, caso esteja, anotar as horas de entrada e saída do funcionário e liberar automaticamente a porta de acesso para passagem. O objetivo do sistema proposto neste trabalho é automatizar o processo de ponto de controle de presença em empresas, diminuindo com isso as fraudes, agilizando o processo e tornando-o mais dinâmico e seguro se comparado ao processo manual.

O projeto foi divido em duas partes: *hardware* e *software*. No quesito *hardware*, os autores optaram por utilizar um microcontrolador ATMEL AT89S52, um módulo leitor RFID SEEED de 125 KHz, etiquetas RFID UME4100, um computador, um motor e uma porta automática. Apesar do RFID de baixa frequência ser uma opção viável e

muito utilizada em diversos projetos deste tipo, muitas das etiquetas RFID nesta faixa de frequência, inclusive as utilizadas no projeto em questão, sofrem com a falta de um sistema de segurança e privacidade sólidos, capazes de efetivamente proteger os dados internos de seus portadores. Etiquetas RFID de alta frequência e NFC, como as utilizadas nesta monografia, por outro lado, podem possuir um forte sistema criptográfico embutido, como 3DES e AES de 128bits, aumentando assim consideravelmente a segurança geral do projeto. Apesar desta monografia em específico não utilizar tais etiquetas, os outros componentes de *hardware* utilizados, Raspberry Pi Zero e módulo RFID-RC522, são totalmente compatíveis com tais cartões mais robustos e seguros, abrindo possibilidades futuras de melhorias.

Outro ponto de discussão é com relação a arquitetura do projeto e como o microcontrolador é utilizado. Os autores utilizaram um computador pessoal como centro de processamento e o microcontrolador fica responsável por intermediar a comunicação entre o computador e o motor que controla a abertura da porta, tudo interligado por conexões seriais. Apesar de possível, não é a configuração mais prática, visto que os componentes devem estar próximos um do outro para se conectarem, além da necessidade de um computador pessoal como centro de processamento. O microcontrolador utilizado nesta monografia, por outro lado, serve tanto como centro de processamento quanto para se conectar ao ponto de controle de acesso, controlando a liberação da catraca.

No quesito *software*, os autores optaram por utilizar o Microsoft visual studio, o .Microsoft .Net framework e o Microsoft Access. O visual studio e o .Net framework foram utilizados para criar uma aplicação *desktop* para facilitar o gerenciamento da aplicação por operadores externos. Apesar de ser uma opção válida, é uma opção voltada exclusivamente para o sistema operacional Windows e que exige uma instalação prévia na máquina alvo. Já a aplicação *web* criada nesta monografia é independente de sistema operacional alvo, necessitando apenas de um navegador *web* para ser utilizada. Independente da plataforma escolhida, *desktop* ou *web*, é interessante perceber a preocupação dos dois trabalhos em criar uma aplicação amigável para realizar a intermediação entre operadores da aplicação e a parte lógico-operacional do projeto, permitindo assim que os operadores possam interagir com a aplicação sem que haja um conhecimento prévio técnico sobre a mesma.

Já o Microsoft Access, o sistema de banco de dados escolhido pelos autores, possui alguns empecilhos, como o fato de ser um programa proprietário pago e que executa somente no sistema operacional Windows. Já o MariaDB, o sistema de banco de dados utilizado nesta monografia, é livre, de código-aberto e pode ser utilizado em diversos sistemas operacionais, como Windows, Linux e MacOS.

O trabalho apresentado mostra-se bem embasado do ponto de vista teórico, passando parte dele dissertando sobre as definições da tecnologia de identificação por radiofrequência. Ambos os projetos, o trabalho acima e esta monografia, possuem objetivos, e algu-

mas implementações, similares, como a implementação do sistema de identificação em um ponto de passagem real, a criação de uma interface amigável de gerenciamento para operadores externos e o uso do RFID para a identificação de pessoas. Apesar das semelhanças, também há diferenças, enquanto o primeiro utiliza-se do RFID de baixa frequência, de um microcontrolador simples como "centro de controle" e uma aplicação *desktop* para os operadores, o segundo utiliza-se do RFID de alta frequência, de um microcontrolador mais completo e uma aplicação *web* para os operadores, independente disto, ambos os projetos são bem similares nas suas intenções e objetivos.

O trabalho (FAROOQ et al., 2014) elabora um sistema de segurança e controle de acesso para os albergues localizados no interior da Univerisade de Punjab, Paquistão, envolvendo princialmente as tecnologias de identificação por radiofrequência, identificação por biometria facial e redes neurais. Os autores defendem que o sistema ajuda a melhorar o nível de segurança não somente da universidade, mas como de qualquer organização que o utilize.

O sistema foi dividido em duas fases: registro e reconhecimento. Na fase de registro, uma etiqueta RFID de baixa frequência é emitido e 10 fotos são tiradas do usuário. As fotos são utilizadas para treinar uma rede neural *FeedForward* com algoritmo de treinamento de propagação reversa. As informações do usuário, o número de identificação da etiqueta RFID e os resultados da rede neural são armazenadas para consultas futuras. Na fase de reconhecimento, o usuário utiliza-se da etiqueta RFID como um primeiro fator de autenticação. Caso a etiqueta não esteja registrada, o sistema realiza uma chamada de emergência via modem GSM para a segurança local, aciona o alarme e a câmera para captura de imagens do suspeito. Caso a etiqueta esteja registrada, o sistema inicia a câmera para capturar uma imagem do usuário para enviá-la a rede neural para validação. Caso a combinação etiqueta e pessoa esteja registrada, o acesso é liberado. Caso não haja combinação, o sistema bloqueia a etiqueta RFID utilizada, cobra uma multa do dono original da mesma e não libera o acesso, mas não aciona o alarme ou faz uma chamada à segurança local.

Com relação aos materiais utilizados, abordaremos nesta análise apenas aqueles relativos ao RFID, visto que esta monografia não possui uma vertente para biometria ou redes neurais. Assim, os principais materiais e *softwares* utilizados pelos autores foram: etiqueta RFID IPC80[3] de 125 KHz, leitor RFID IP10[4] de 125 KHz, microcontrolador AT89C52 e um computador central para processamentos pesados (FAROOQ et al., 2014).

Como discutido acima, no trabalho "Radio Frequency Identification (RFID) Based Attendance System With Automatic Door Unit", as etiquetas RFID de baixa frequência possuem algumas deficiências com relação a segurança, entretanto, estas deficiências são contornadas no trabalho em questão graças ao modo como os autores desenvolveram o

[3] http://www.idteck.com/en/products/view/ipc80
[4] http://www.idteck.com/en/products/view/ip10

sistema com um duplo fator de autenticação, sendo a etiqueta RFID o primeiro fator e a biometria facial o segundo fator. Deste modo, no quesito segurança, este trabalho mostra-se superior à esta monografia, que utiliza-se apenas do número de identificação da etiqueta RFID. Como o sistema utiliza redes neurais para análise de imagens, todo o processamento das informações fica centralizado em um computador mais robusto, assim, a utilização de um microcontrolador simples, que lida apenas como o controle dos periféricos externos como: leitor RFID, modem GSM, alarme e outros, torna-se uma boa escolha.

O trabalho discutido acima mostra-se interessantes por utilizar uma combinação de diversas tecnologias, como: RFID, biometria facial e redes neurais, para compor um sistema de segurança e controle de acesso sólido, robusto e muito bem desenhado e estruturado. Apesar das ideias apresentadas acima serem passíveis de implementação, as mesmas tornam-se inviáveis de serem implementadas nesta monografia, pois quase todo o projeto precisaria ser alterado para acomodar tais pontos, pois o mesmo baseia-se em um Raspberry Pi Zero W como microcontrolador e centro de processamento, algo que não teria poder computacional suficiente para processamento de imagem e cálculo de redes neurais.

O trabalho (HUNG; BAI; REN, 2015) propõe o *design* de um sistema de controle de acesso que utiliza-se do NFC presente em alguns *smartphones* ao invés das tradicionais etiquetas NFC em formato de cartão, em conjunto com um aplicativo dedicado no aparelho do usuário. A utilização do sistema foi dividida em dois passos: *"sensing"* e *"Enter Password"*. No primeiro passo, o usuário utiliza-se do NFC do seu *smartphone* para fazer uma primeira validação de acesso. Caso o " *smartphones* ID", como chamado pelos autores, esteja correto, um teclado numérico é liberado, em um aplicativo próprio no *smartphone* do usuário, para que o mesmo entre com a sua senha. Caso a senha esteja correta a porta é destravada, caso a senha esteja incorreta, uma alarme é acionado.

Na questão de arquitetura de *hardware*, os autores optaram por uma abordagem genérica, não especificando equipamentos específicos, desta forma, comparações com a arquitetura de *hardware* utilizada nesta monografia também serão genéricas. Assim, os autores definiram a arquitetura de *hardware* como: microcontrolador, trava magnética para a porta, módulo de relógio em tempo real, indicador de estado do sistema e módulo leitor NFC. Ambos os projetos, o trabalho em foco e esta monografia, utilizam-se de um microcontrolador para controlar os módulos externos, ao invés de um computador mais robusto. A trava magnética para a porta é substituída por uma catraca com circuito interno, independente disto, o objetivo de ambos é o mesmo, ser o ponto que controla fisicamente a passagem dos usuários. O módulo leitor NFC torna-se necessário pelo fato de ambos utilizarem um microcontrolador como componente central na arquitetura de *hardware*. O módulo de relógio em tempo real é substituído pela hora interna do microcontrolador. O indicador de estado do sistema é substituído pelos indicadores da própria catraca que é utilizada como ponto de acesso.

Com relação ao arquitetura de *software*, os autores dividiram o projeto em dois módulos: *"smartphone"* e *"Door Lock System Operation Module"*. O primeiro módulo lida com o aplicativo no *smartphone* e suas funções, como armazenar os dados do usuário, servir de etiqueta NFC e teclado numérico para a digitação da senha. Esta monografia não utiliza um aplicativo para *smartphones*, ao invés disso, usa um aplicação *web* acessível por qualquer navegador, exonerando assim o usuário de instalar qualquer aplicativo em seu celular. O Segundo módulo lida com a liberação da porta e os processamentos internos da aplicação, como codificação dos dados e validação. Algo similar ocorre no microcontrolador desta monografia.

O projeto possui alguns pontos interessantes que melhoram, em algum aspecto, os sistemas de controle de acesso no geral. O primeiro ponto diz respeito a economia financeira, por parte da instituição que aplicar o sistema proposto, em relação à compra de etiquetas NFC para distribuição aos usuários, uma vez que o próprio *smartphone* do indivíduo foi pensado para ocupar tal lugar. O segundo ponto diz respeito a praticidade e comodidade para o usuário, uma vez que grande parte das pessoas que utilizam um *smartphone* raramente não o estão carregando consigo, diminuindo assim importunos com esquecimento da etiqueta. O terceiro ponto é a utilização de um segundo fator de autenticação, a senha informada pelo usuário. Este segundo fator é responsável por aumentar consideravelmente a segurança geral do projeto, permitindo que haja maiores garantias de que, quem está passando pelo ponto de controle é de fato quem diz ser, e não alguém que conseguiu clonar a identificação do usuário.

Apesar dos pontos positivos, o projeto também possui alguns pontos negativos que precisam ser resolvidos, para que o mesmo possa ser aplicado em cenários maiores e com um público alvo mais heterogêneo, como é o caso do cenário abordado nesta monografia. O primeiro ponto é o fato do projeto basear-se unicamente em *smartphones* com NFC embutido. Por mais que a adesão de NFC em celulares esteja crescendo, a tecnologia ainda não pode ser considerada universal, principalmente em aparelhos baratos e simples, onde há a remoção de funcionalidades e *hardwares* não essenciais para o funcionamento do aparelho. Assim, seria necessário que o sistema aceitasse tanto o *smartphone* com NFC quanto a etiqueta NFC física. O segundo ponto é a necessidade de se instalar, no *smartphone* do usuário, um aplicativo especialmente desenvolvido para utilizar o sistema. Devido a heterogeneidade de tipos e versões de sistemas operacionais de *smartphones*, criar e manter diversas versões de um aplicativo, além do suporte contínuo para as futuras verões de sistemas operacionais, torna-se um trabalho constante e complexo de gerenciamento, desenvolvimento e arquitetura.

Independente dos pontos positivos e negativos, os autores do projeto elaboraram um *design* de sistema interessante e inovador, mesclando uma tecnologia cada vez mais presente na vida das pessoas, como o controle de acesso via RFID, com uma tecnologia pouco aproveitada nos *smartphones* modernos, como o NFC. Apesar de ambos os projetos, o

trabalho acima e esta monografia, abordarem o controle de acesso via RFID, os mesmos fazem isto de formas distintas, um via *smartphones* e o outro via etiquetas físicas, e, apesar das ideias inovadoras apresentadas, as mesmas não se encaixariam tão bem no contexto desta monografia, visto que os pontos negativos abordados acima impactam diretamente sobre o cenário e o contexto abordados nesta monografia.

O trabalho (SHAFIN et al., 2015) propõe a construção de um sistema de segurança de controle de acesso que se baseia na tecnologia de RFID e de uma senha individual pré-conhecida para autenticar e validar um usuário, a fim de permitir ou não sua passagem ponto de controle. O principal objetivo deste trabalho, segundo os autores, é que o mesmo seja um documento descritivo de como projetar, desenvolver, implementar e instalar uma solução de segurança relativamente barata e com uma certa garantia do nível de segurança da mesma.

O sistema desenvolve-se da seguinte forma: Uma porta encontra-se fechada por uma trava magnética que encontra-se ligada a um microcontrolador. O microcontrolador, por sua vez, é o centro que interliga os demais componentes como: leitor RFID, teclado numérico, sistema central de processamento, dentre outros. Quando um usuário aproxima sua etiqueta RFID do leitor, o mesmo é responsável por interrogar e repassar as informações lidas da etiqueta. Em seguida, o sistema pede que o usuário informe sua senha de acesso. Caso as informações fornecidas (etiqueta e senha) estejam corretas, o microcontrolador libera a trava magnética que libera a porta. Em paralelo, um registro da passagem do usuário é armazenada no banco do servidor central.

Os autores dividiram o projeto em dois módulos: *hardware* e *software*. Os principais componentes de *hardware* listados são: etiqueta RFID passiva de baixa frequência, leitor RFID de 125 kHz, microcontrolador PIC16F877A, teclado numérico, motor de controle L293D e trava magnética da porta. Em relação a etiqueta de baixa frequência, sua desvantagem em relação a etiqueta de alta frequência (o tipo utilizada nesta monografia), já foi discutida mais acima, entretanto, os autores do projeto conseguiram contornar tal défice implementando um segundo fator de autenticação através da senha de acesso, o que acaba por deixar o sistema como um todo mais seguro do que o sistema desta monografia. O microcontrolador, por sua vez, funciona basicamente como uma ponte de interligação entre os demais componentes. Neste ponto, o microcontrolador utilizado nesta monografia é muito mais completo e robusto, sendo capaz de realizar a maioria das funções de controle e gerenciamento do projeto, só não sendo utilizado para armazenar o banco de dados global do sistema e as aplicações web, apesar de ser possível. O motor de controle utilizado acima, que é responsável por comandar a trava magnética, é substituído pelo próprio sistema interno da catraca utilizada nesta monografia, não havendo uma escolha melhor ou pior do que a outra, apenas contextos diferentes.

Ao contrário do módulo de *hardware*, não há especificações detalhadas sobre os blocos de construção do sistema do módulo de *software*. O que há, entretanto, é algumas infor-

mações relativas a funcionalidades do mesmo, como: listagem de usuários cadastrados, geração e armazenamento de registros de passagem pelo ponto de controle, possibilidade de interferência manual no processo de liberação o não de uma requisição de acesso e geração de relatórios de utilização do sistema. Das funcionalidades acima, apenas a geração de registros de passagem pelo ponto de controle e uma consulta dos usuários foram implementadas no sistema desta monografia.

Ambos os projetos, o em destaque e esta monografia, possuem pontos de funcionamento em comuns, como a utilização do RFID passivo como método de autenticação do usuário, a implementação do sistema na vida real e a geração e armazenamento de registro para cada entrada ou saída realizada pelo sistema. Outros pontos, entretanto, divergem, como o fato do sistema apresentado nesta monografia não possuir um segundo fator de autenticação de usuário, baseando-se única e exclusivamente na etiqueta RFID.

O projeto apresentado acima mostra-se simples do ponto de vista técnico e de implementação, mas completo do ponto de vista de funcionalidades apresentadas. Os autores implementaram algumas funções muito interessantes e que aumentam a segurança geral do sistema, tais como o segundo fator de autenticação via senha e a possibilidade de intervenção humana para negar um acesso. Apesar de tratarem do mesmo assunto, o projeto apresentado acima e esta monografia, o primeiro possui ideias interessantes e plausíveis de implementação no segundo, sendo uma boa fonte para melhorias e atualizações futuras.

No decorrer desta seção, foram apresentados diversos artigos e trabalhos relacionados ao contexto do RFID, mostrando como a tecnologia já é amplamente estudada e implementada para o controle de acesso. Pôde-se ver como o tema é abrangente e pode ser implementado das mais diversas maneiras, desde um simples microcontrolador com um leitor embutido até um sistema de reconhecimento facial e redes neurais, sendo interessante ver como uma implementação pode seguir caminhos tão distintos, mesmo que todos acabem convergindo para o mesmo propósito.

4 DESENVOLVIMENTO

Este capítulo destina-se a descrever a implementação do projeto, desde a descrição da proposta, passando pelos porquês das escolha dos componentes de *software* e *hardware* até a efetiva implementação do projeto em um ponto de controle de acesso.

4.1 PROPOSTA DE PROJETO

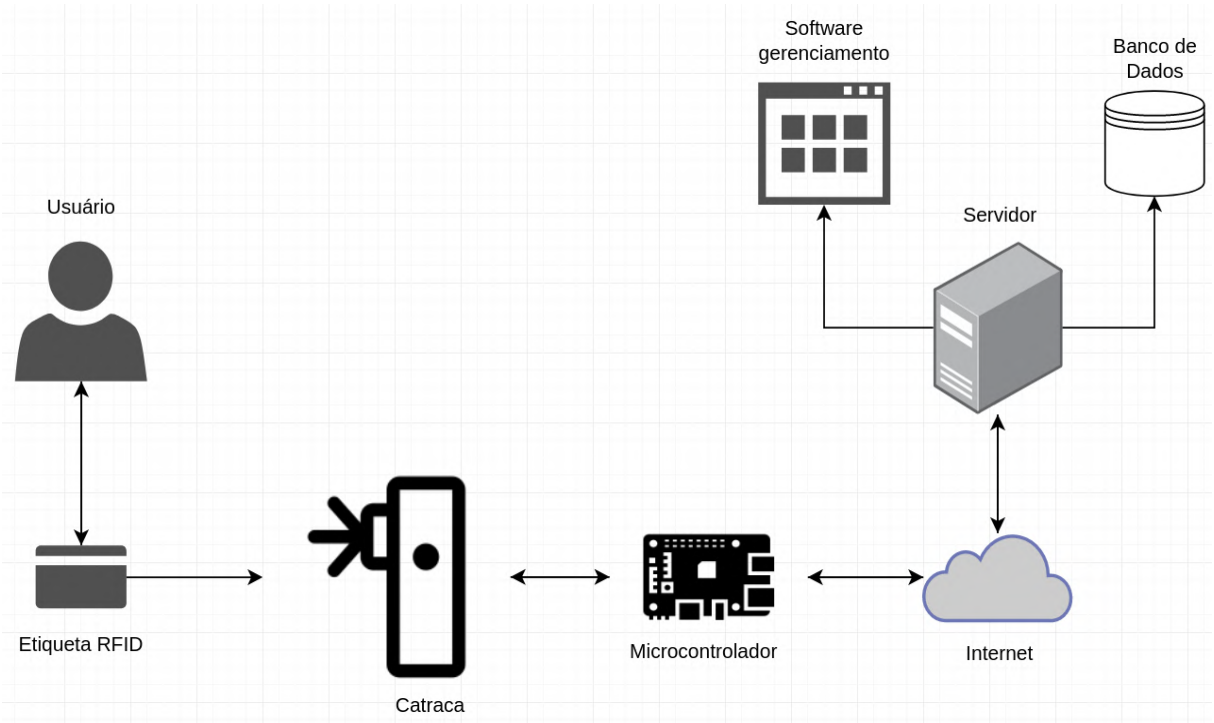
Esta monografia nasceu com o objetivo de elaborar e implementar um sistema de segurança de identificação de usuários através da tecnologia de RFID de alta frequência, que fosse economicamente e tecnicamente viáveis do ponto de vista da implementação, utilizando-se para isto equipamentos de *hardware* amplamente conhecidos e sistemas computacionais não-complexos elaborados sob demanda, e que fosse possível de ser implementada no Instituto Tércio Pacitti, da Universidade Federal do Rio de Janeiro (NCE/UFRJ), a fim de automatizar, agilizar e melhor controlar o fluxo passagem de docentes, alunos e funcionários nas dependências do instituto.

O fluxo de funcionamento traçado do sistema dá-se da seguinte forma: o processo se inicia quando um usuário aproxima uma etiqueta RFID de alta frequência do leitor RFID, localizado no ponto de controle de acesso. O leitor então interroga a etiqueta a fim de obter seu identificador único (UID) e enviá-lo ao microcontrolador. De posse do UID da etiqueta, o microcontrolador realiza uma consulta ao banco de dados central a fim de verificar se o UID informado encontra-se cadastrado e se o usuário possui permissão de acesso para a direção desejada, ou seja, o sistema verifica se o usuário está tentando entrar/sair novamente quando o mesmo já consta como dentro/fora das dependências da instituição. Caso a etiqueta não esteja presente no banco de dados, o acesso é negada e o ponto de controle de acesso permanece bloqueado. Caso a etiqueta esteja presente no banco de dados, mas o usuário não possua permissão de acesso para a direção desejada, o acesso é negado, o ponto de controle de acesso permanece bloqueado e um *e-mail* de alerta é enviado ao usuário dono da etiqueta informando-o que um comportamento anômalo foi detectado. Caso a etiqueta esteja presente no banco de dados e o usuário possua permissão de acesso para a direção desejada, o acesso é permitido e o ponto de controle de acesso é liberado, em concomitância, um registro da passagem do usuário é armazenado no banco de dados central. O codificador rotativo inicialmente citado, encontra-se conectado a parte rotatória da catraca e é responsável por verificar em que sentido, horário ou anti-horário, a catraca foi girada.

Na outra ponta do sistema encontra-se o servidor central, responsável por armazenar o banco de dados e o *software* de gerenciamento do mesmo. O banco de dados é responsável por armazenar todas as informações referentes a operadores externos, usuários do

sistema (aqueles que possuem liberação de passagem pelo ponto de controle de acesso) e registros de passagens. O *software* de gerenciamento é a aplicação responsável por fazer a interligação entre operadores externos e banco de dados, possibilitando que os operadores realizem consultas e alterações no banco sem que haja necessidade de conhecimento prévio sobre o sistema. A figura 24 ilustra superficialmente este fluxo de funcionamento, enquanto a figura 25 ilustra o diagrama de componentes.

Figura 24 – Diagrama de funcionamento

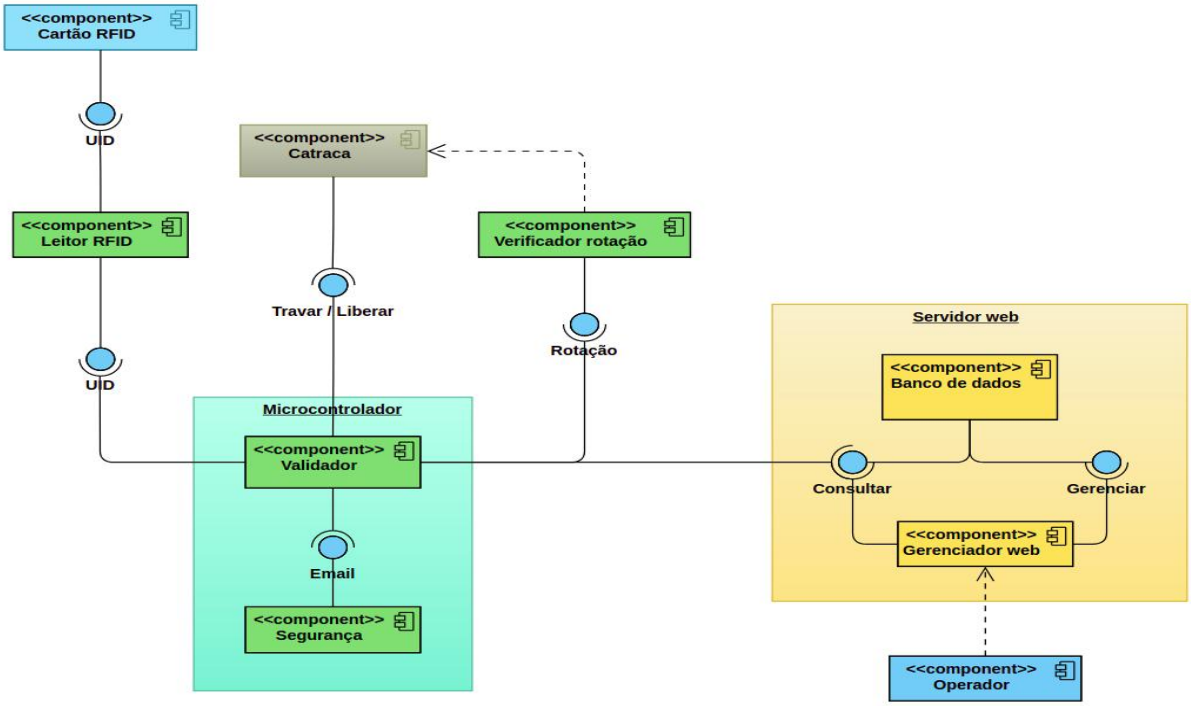


Fonte: Reprodução do autor

Para tornar este trabalho realidade, usaremos alguns componentes de *hardware* e *software* escolhidos especialmente para este projeto, prezando por certas qualidades na hora da escolha dos materiais, tais como: preço, facilidade de aquisição, facilidade de utilização, amplo acervo de documentação, casos de uso e exemplos disponíveis na Internet.

Além disso, para facilitar a implementação, o sistema foi dividido em dois módulos: controle e comando, onde cada módulo foi dividida em dois submódulos: *hardware* e *software*. O módulo de controle trata dos componentes que estão diretamente ligados ao ponto de controle de acesso, como microcontrolador, módulos RFID, codificador rotativo e programa de consulta, enquanto o módulo de comando trata dos componentes do *back-end*, tais como banco de dados e aplicações de gerenciamento de usuários e operadores do sistema. Os submódulos *hardware* e *software* tratam, respectivamente, dos equipamentos físicos e das lógicas computacionais empregados em cada módulo.

Figura 25 – Diagrama de componentes



Fonte: Reprodução do autor

4.2 PREPARAÇÃO

Nesta seção discute-se os passos preparatórios para a realização do projeto, tais como a escolha dos componentes de *software* e *hardware*, das explicações de cada um destes e os motivos que levaram à estas escolhas.

4.2.1 Controle

O elementos centrais na frente de controle são o microcontrolador e o ponto de controle de acesso. O microcontrolador é responsável por se conectar aos módulos externos (RFID e codificador rotativo), ao ponto de controle de acesso e ao banco de dados externo, além de realizar alguns outros controles e verificações. O ponto de controle de acesso (catraca) é responsável por barrar fisicamente a entrada de pessoas não-autorizadas.

4.2.1.1 Hardware

Os equipamentos de *hardware* utilizados nesta frente foram:

- Raspberry Pi Zero W
- 2 x Módulo RFID-RC522
- Codificador rotativo KY-040

- Etiqueta MIFARE Classic EV1 1k
- Cartão de memória micro SD SanDisk SDSQUAR-032G-GN6MA
- Barras de pinos
- Cabos conectores (*jumpers*)
- Catraca mecânica
- Módulo relé 3.3V
- Fonte de alimentação ATX 450W

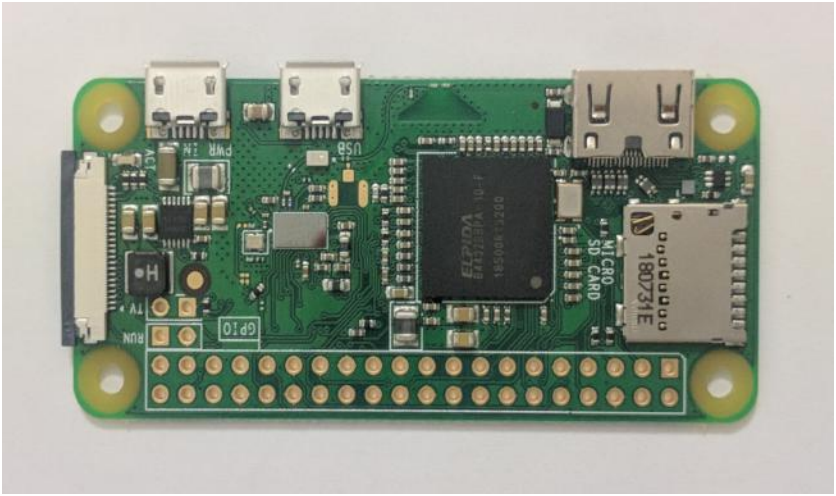
Para microcontrolador, o equipamento escolhido foi um Raspberry Pi Zero W. Um Raspberry Pi é um pequeno computador (geralmente do tamanho de um cartão de crédito), de baixo custo e alta performance, capaz de se conectar ao mundo externo de várias formas, seja através das tradicionais portas USB e HDMI, seja através dos pinos GPIO (*General Purpose Input/Output*) presentes na placa (RASPBERRYPI.ORG, 2019c). O projeto Raspberry, criado pela Fundação Raspberry Pi, foi pensado para ser um dispositivo capaz de permitir que pessoas de todas as idades explorem computação e aprendam a programar em linguagens como Scratch e Python, além de ser capaz de fazer tudo o que um computador de mesa faz, como navegação na Internet, reprodução multimídia, edição de documentos e até pequenos jogos (RASPBERRYPI.ORG, 2019c).

O Raspberry Pi Zero W é uma versão estendida do Raspberry Pi Zero, contendo módulos de conectividade sem fio como wi-fi e *bluetooth*. A placa possui, como especificações técnicas, as seguintes configurações: protocolos de comunicação sem fio 802.11 b/g/n, *bluetooth* 4.1 e *Bluetooth Low Energy* (BLE), processador Broadcom BCM2835[1] núcleo-único (*single-core*) de 1GHz, memória RAM de 512MB, portas de conexão Mini HDMI e USB *On-The-Go*, 40 pinos GPIO, dentre outras (RASPBERRYPI.ORG, 2019a). A figura 26 exibe o dispositivo utilizado.

O Raspberry Pi Zero W foi escolhido devido a algumas características e qualidades: O modelo pode ser considerado relativamente barato. Apesar do mesmo ser vendido no Brasil a um preço relativamente alto, aproximadamente 110,00 reais[2], o mesmo modelo pode ser encontrado nos Estados Unidos a 10 dólares[3], aproximadamente 38,50 reais em conversão direta[4,5]. Possui módulos de comunicação sem fio embutidos na placa, como wi-fi e *bluetooth*. Estes módulos nativos eliminam a necessidade de se comprar, conectar e configurar módulos externos, algo que aumenta muito a simplicidade do projeto, visto

[1] https://www.raspberrypi.org/documentation/hardware/raspberrypi/bcm2835/README.md
[2] https://www.filipeflop.com/produto/raspberry-pi-zero-w/
[3] https://www.adafruit.com/product/3400
[4] Cotação do 29 de junho de 2019, onde 1 dólar = 3,85 reais
[5] Preços retirados de revendedores autorizados pela própria Raspberry

Figura 26 – Raspberry Pi Zero W



Fonte: Reprodução do autor

que o Raspberry Pi precisará se conectar com um banco de dados externo para realizar as consultas necessárias. Além de ser energeticamente econômico, consumindo entre 120mA a 250mA em estado ocioso (MATT, 2018; PIDRAMBLE, 2019). Esta característica torna-se útil caso queira-se conectar o sistema a uma bateria ou fonte finita de energia.

Para gerir a comunicação de radiofrequência entre o microcontrolador e as etiquetas RFID foi escolhido o módulo RFID-RC522. Este módulo de comunicação sem contato atua na frequência de 13,56MHz (alta frequência), baseia-se no *chip* MFRC522 da empresa NXP semicondutores, a mesma empresa responsável pela marca MIFARE, possui baixo consumo energético, fornece suporte a todos os níveis do padrão ISO 14443-A, possui capacidade de leitura e escrita em cartões RFID e NFC (HONGZHI et al., 2011), distância de operação máxima teórica de até 4cm (SHAARI; NOR, 2017), taxa de transmissão de dados bidirecional máxima de até 424kbit/s (GUO; ZHAO, 2015) e funções de verificação de paridade e detecção de CRC (ZENG et al., 2010).

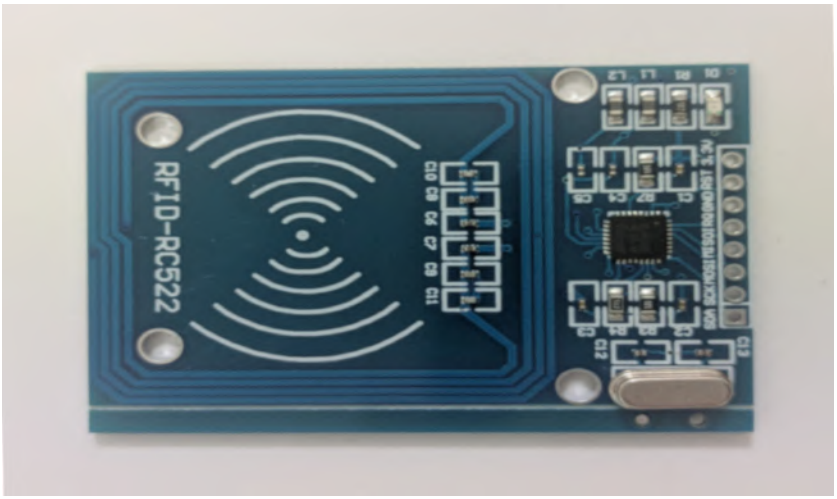
Outra importante característica do *chip* MFRC522 é seu grande suporte aos diversos modelos de cartões MIFARE. Segundo a documentação, o *chip* suporta todas as variantes dos protocolos de identificação MIFARE Mini, MIFARE 1K, MIFARE 4K, MIFARE Ultralight, MIFARE DESFire EV1 e MIFARE Plus RF (NXP SEMICONDUTORES, 2016). A figura 27 exibe um dos módulos utilizados.

O módulo RFID-RC522 pode se conectar a uma grande variedade de microcontroladores e computadores graças as suas diversas interfaces de comunicação: UART (*Universal Asynchrounous Receiver/Transmiter*), SPI (*Serial Peripheral Interface*) e I2C (*Inter-Integrated Circuit*) (HONGZHI et al., 2011). Foram utilizadas as interfaces SPI para conectar os módulos RFID ao microcontrolador.

Para este projeto, foram utilizados dois módulos RFID, um voltado para a entrada e um voltado para a saída. A utilização de dois módulos permitirá implementar funções

que aumentarão o controle e a precisão sobre as entradas e as saídas, permitindo-nos desenvolver, a nível de *software*, algumas medidas extras de segurança.

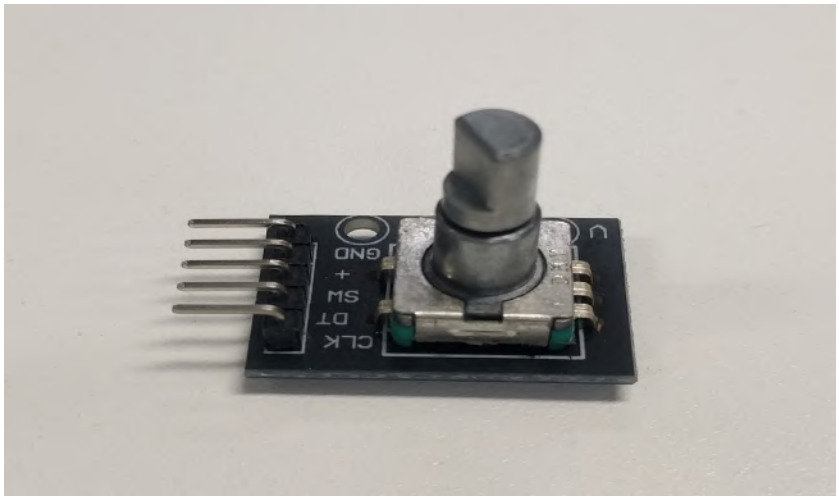
Figura 27 – Módulo RFID-RC522



Fonte: Reprodução do autor

Para verificar o sentido de rotação da catraca (horário ou anti-horário), utilizou-se um codificador rotativo KY-040, que é um codificador de rotação simples, composto por um botão de rotação contínua que indica quanto, e em qual sentido, o botão está sendo girado. A figura 28 exibe o codificador utilizado.

Figura 28 – codificador rotativo KY-040

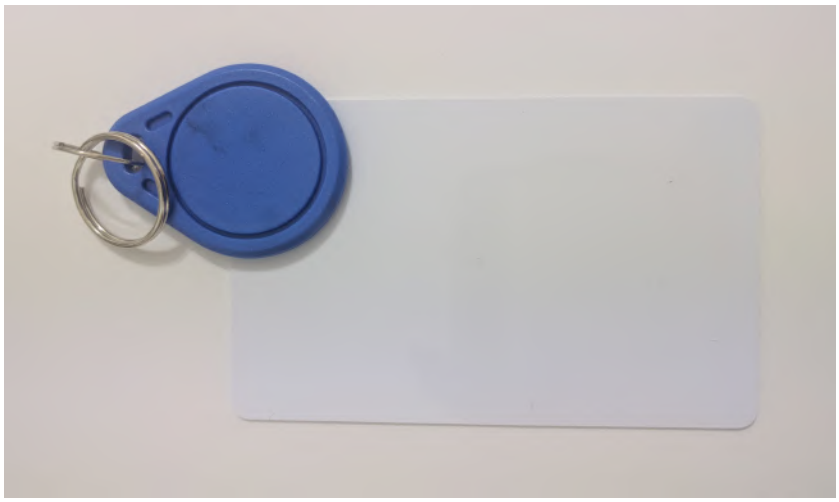


Fonte: Reprodução do autor

Como cartão de acesso para o usuário, foi escolhido a etiqueta MIFARE Classic EV1 1k, também conhecido como MIFARE Classic 1k ou MIFARE S50. Mais do que uma simples etiqueta, este modelo é considerado um cartão inteligente sem contato que opera na frequência de 13,56MHz (alta frequência), possui 1024 bytes de espaço de armazenamento

interno, permite tanto leitura quanto escrita da memória interna, opera em conformidade com a ISO/IEC 14443 Tipo A e possui criptografia de cifra de fluxo Crypto-1 para autenticação e troca de dados (NXP SEMICONDUTORES, 2018). A figura 29 exibe duas das etiquetas utilizadas.

Figura 29 – Etiqueta RFID MIFARE Classic EV1 1k



Fonte: Reprodução do autor

Para armazenamento interno do microcontrolador, foi escolhido o cartão de memória micro SD SanDisk SDSQUAR-032G-GN6MA. Este cartão é utilizado como memória secundária pelo Raspberry Pi, armazenando o sistema operacional Raspbian e os demais arquivos do projeto. Este modelo de cartão foi escolhido principalmente pela sua alta performance, possuindo características como: classe 10[6], UHS-I[7] e A1[8]. A figura 30 exibe o cartão utilizado.

As barras de pinos e os cabos conectores, também conhecidos como *jumpers*, são componentes genéricos, sem um critério de escolha específico, utilizados para realizar a conexão física entre as portas GPIO do microcontrolador e os outros componentes. As figuras 31 e 32 exibem as barras e cabos utilizados, respectivamente.

Para controlar fisicamente a passagem dos usuários, foi escolhida uma catraca mecânica de 3 braços da Bruson metalúrgica. Esta foi escolhida por ser a catraca disponível para a implementação deste trabalho, não tendo sido necessário gastos extras para aquisição ou restauração da mesma.

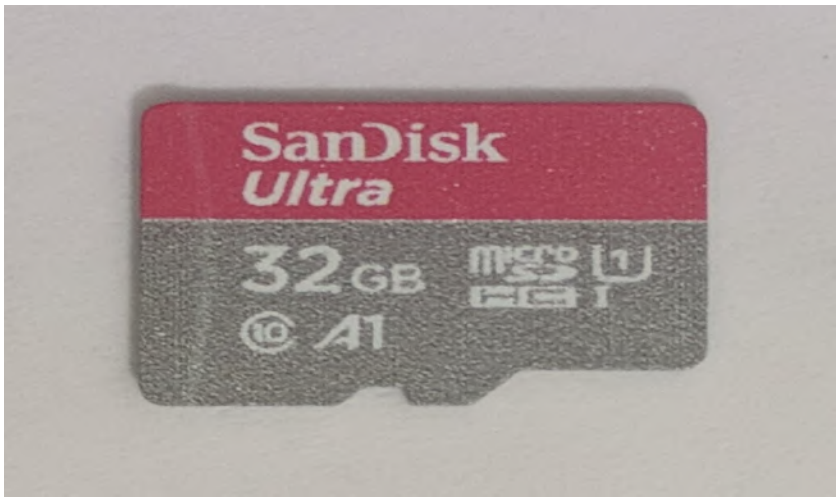
A catraca possui o sistema de travamento baseado em um solenoide de 12V. Esta voltagem de operação é muito maior do que os 5V capazes de serem gerados pelo microcontrolador, assim, foi necessário ligar a catraca diretamente à fonte de alimentação. Desta forma, para que o microcontrolador pudesse controlar a liberação da catraca foi

[6] https://kb.sandisk.com/app/answers/detail/a_id/1996/

[7] 6

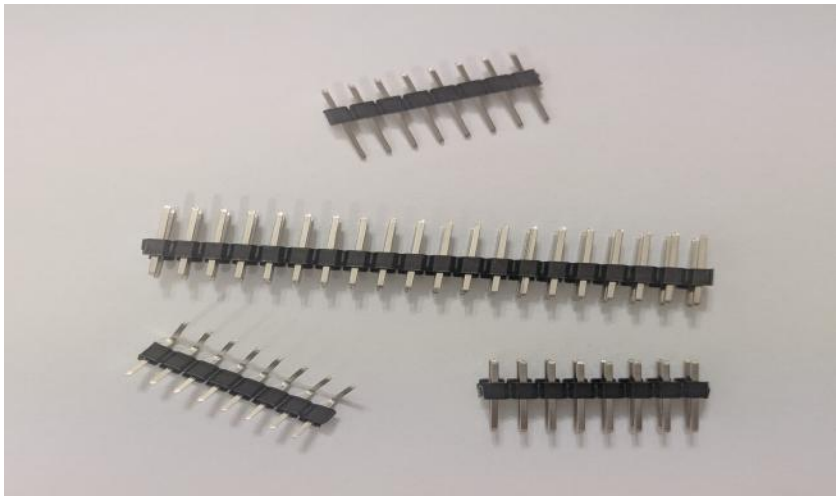
[8] https://www.sdcard.org/developers/overview/application/index.html

Figura 30 – Cartão de memória micro SD



Fonte: Reprodução do autor

Figura 31 – Barras de pinos



Fonte: Reprodução do autor

preciso adicionar um módulo relé 3.3V à composição. Uma observação importante é que o módulo deve operar em 3.3V, pois esta é a maior voltagem que pode ser gerada pelos pinos GPIO do microcontrolador. A figura 34 exibe o relé utilizado.

Para alimentar todos os componentes supracitados, foi escolhida uma fonte de alimentação ATX 450W, a mesma encontrada em computadores de mesa. Não há características ou qualidades específicas que levaram para a escolha desta fonte em particular, podendo a mesma ser substituída por outras, devendo-se apenas observar as recomendações da própria Raspberry Pi com relação a tensão e amperagem, que podem variar de modelo para modelo[9]. A figura 35 exibe a fonte utilizada.

Tendo escolhido os equipamentos de *hardware*, o próximo passo foi adquiri-los. Al-

[9] https://www.raspberrypi.org/documentation/faqs/#pi-power

Figura 32 – Cabos conectores

Fonte: Reprodução do autor

Figura 33 – Catraca mecânica

Fonte: Reprodução do autor

guns dos componentes foram comprados em diferentes épocas e diferentes fornecedores, enquanto outros, como a fonte e a catraca, já estavam previamente disponíveis para utilização. Assim, a tabela 2 detalha os preços pagos por cada componente e o valor total gasto.

4.2.1.2 Software

Os componentes de *software* utilizados nesta frente foram:

- Sistema operacional: Raspbian Buster
- Linguagem de programação: Python 3.7.3

Figura 34 – Módulo relé

Fonte: Reprodução do autor

Figura 35 – Fonte de alimentação ATX

Fonte: Reprodução do autor

- Bibliotecas: SPI-Py[10], MFRC522-python[11], RPi.GPIO[12], mysql-connector-python[13], evdev[14]

Um Raspberry Pi é um pequeno computador e, assim como todo computador, o mesmo precisa de um sistema operacional para se tornar funcional, assim, para tal função, foi utilizado o Raspbian Buster. Raspbian é um sistema operacional livre baseado no Debian, de arquitetura armhf, otimizado especialmente para o *hardware* do Raspberry Pi (RASPBIAN.ORG, 2019) e considerado o sistema operacional oficial da Fundação Raspberry

[10] https://github.com/lthiery/SPI-Py
[11] https://github.com/mxgxw/MFRC522-python
[12] https://pypi.org/project/RPi.GPIO/
[13] https://pypi.org/project/mysql-connector-python/
[14] https://pypi.org/project/evdev/

Tabela 2 – Preço dos equipamentos

Peça	Preço
Raspberry Pi Zero W	R$109,90
2 x Módulo RFID-RC522	R$47.80
Codificador rotativo KY-040	R$12,90
Cartão de memória micro SD SanDisk SDSQUAR-032G-GN6MA	R$49,00
Barra de pinos	R$3,40
Cabos conectores (*jumpers*)	R$11,90
Catraca mecânica	R$00,00
módulo relé 3.3V	R$9,90
Fonte de alimentação ATX 450W	R$00,00
Total	R$244,80

Fonte: Reprodução do autor

Pi para seus computadores (RASPBERRYPI.ORG, 2019b). Buster é apenas o codinome da versão do Raspbian, assim como o "Buster" em "Debian Buster". Esta versão foi a escolhida por ser a versão estável mais recente do Raspbian até a data de elaboração deste projeto.

Para o desenvolvimento dos programas necessários, a linguagem escolhida foi o Python 3.7.3. Python é uma linguagem de programação de alto nível, interpretada, orientada a objeto, de semântica dinâmica e sintaxe simples (PYTHON.ORG, 2019). A linguagem foi escolhida por ser simples, de fácil compreensão, fácil manutenção, completa e vir instalada por padrão (ou ser de fácil instalação) em praticamente todas as distribuições Linux atualmente existentes. Esta versão foi a escolhida por ser a versão estável mais recente do Python 3, nos repositórios oficiais do Raspbian Buster, até a data de elaboração deste projeto.

Algumas bibliotecas externas ao Python foram utilizadas para facilitar a elaboração dos sistemas desenvolvidos, sendo elas: SPI-Py, MFRC522-python, RPi.GPIO, MySQL-python e evdev.

4.2.2 Comando

O elemento central na frente de comando é o Sistema de Gerenciamento de Banco de Dados (SGBD), ou servidor de banco de dados. O mesmo é responsável por armazenar todas as informações importantes do projeto, tais como usuários cadastrados, operadores do sistema e registro de passagens, entrada e saída, pelo ponto de controle de acesso.

4.2.2.1 Hardware

Na frente de comando, o *hardware* necessário é uma máquina servidora para armazenar o banco de dados e os programas de gerenciamento do projeto. O servidor pode ser tanto uma máquina local quanto uma máquina em servidor remoto, como a nuvem. Por se tratar de um projeto piloto, foi utilizado como servidor o computador pessoal do autor desta monografia, um *notebook* Lenovo IdeaPad G400S touch.

4.2.2.2 Software

Os componentes de *software* utilizados nesta frente foram:

- Sistema operacional: Ubuntu Server 18.04.3 LTS
- Servidor de banco de dados: MariaDB Server 10.1.40
- Servidor *web*: Apache 2.4.29
- Linguagens de programação: Python 3.6.8 e PHP 7.2.19
- Bibliotecas: mysql-connector-python

Para sistema operacional do servidor escolhemos o Ubuntu Server 18.04.3 LTS (*Long-Term Support*), que é um sistema operacional Linux, livre, de código-aberto (*open-source*), baseado no Debian e mantido pela Canonical (UBUNTU.COM, 2019). É uma das distribuições Linux mais utilizadas no mundo, sendo escolhida para este projeto pela sua estabilidade, por ser livre de custos, possuir grande suporte da comunidade Linux, suporte estendido da Canonical até 2023 (QUIGLEY, 2019) e boa compatibilidade de *drivers* a uma diversa gama de *hardwares*.

Para servidor de banco de dados escolhemos o MariaDB 10.1.40, que é um banco de dados de código-aberto nascido de um *fork* do MySQL e mantido pelos desenvolvedores originais do MySQL. O MariaDB é um dos SGBDs mais populares do mundo e usado por grandes nomes da indústria de tecnologia, como Wikipedia, WordPress.com e Google (MARIADB.ORG, 2019). Esta versão foi a escolhida por ser a versão estável mais recente do MariaDB.

Para servidor *web* escolhemos o Apache 2.4.29, que é um servidor *web* colaborativo, livre, de código-aberto, robusto, repleto de funcionalidades, de nível comercial e mantido

pela Apache Software Foundation (APACHE.ORG, 2019). O Apache é um dos servidores HTTP mais utilizados no mundo e esta versão foi a escolhida por ser a versão estável mais recente do Apache.

Para linguagens de programação escolhemos o Python 3.6.8 e o PHP 7.2.19. PHP é uma linguagem de programação de *script*, de código-aberto, de uso geral, adequada para o desenvolvimento de aplicações *web* e que pode ser incorporada em conjunto com código HTML (PHP.NET, 2019). O PHP é uma das linguagens de programação mais utilizadas no mundo no lado do servidor para desenvolver aplicações *web* e páginas HTTP, e esta versão foi escolhida por ser a versão estável mais recente do PHP, o mesmo valendo para a versão escolhida do Python.

Algumas bibliotecas externas ao Python foram utilizadas para facilitar a elaboração dos sistemas desenvolvidos, sendo ela: MySQL-python.

4.3 IMPLEMENTAÇÃO

Nesta seção discute-se os passos dados para a implementação do projeto, desde os pontos de solda realizados nos componentes de *hardware*, passando pela codificação dos *softwares* de controle, até a junção de todos os componentes para formar um sistema funcional.

Vale ressaltar que não serão mostrados "tutoriais" dos procedimentos aqui aplicados, e sim o que deve ser feito, em uma perspectiva macro, para se implementar tal sistema. O "passo-a-passo" de cada procedimento encontra-se fora do escopo desta monografia.

4.3.1 Controle

Nesta seção discute-se os passos de implementação da frente de controle. Como dito anteriormente, esta frente trata dos componentes que estão ligados diretamente ao ponto de controle de acesso, como microcontrolador, módulos RFID, codificador rotativo e programa de consulta. Desta forma, esta seção cobre os seguintes itens:

- Soldagem dos componentes eletrônicos.
- Instalação do sistema operacional.
- Conexões entre componentes eletrônicos.
- Planejamento e desenvolvimento de *software*.
- Integração dos componentes e validação.

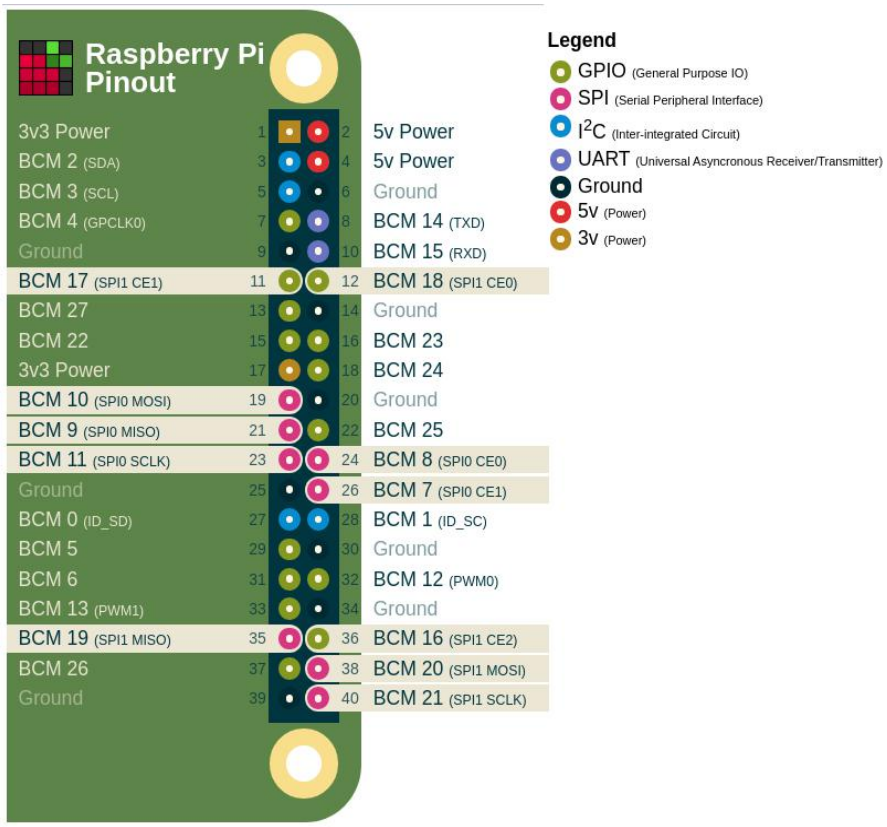
4.3.1.1 1º passo - Soldagem

O primeiro passo na frente de controle foi soldar as barras de pinos nas entradas GPIO do microcontrolador e dos módulos RFID. Como pode-se ver pelas figuras 26 e 27,

as placas possuem pequenos "furos" agrupados em linha em suas estruturas, 40 no caso do Raspberry Pi e 8 no caso do RC522. Estes "furos" são as entradas GPIO de cada placa.

GPIO, sigla em inglês para *General Purpose Input/Output*, é um sinal digital controlado por software, ou seja, uma porta GPIO funciona como uma interface programável que possibilita o acesso a propriedades e dados internos da placa via *software* (KEDLAYA; BHAGYALAKSHMI, 2014). A figura 36 exibe com mais detalhes as portas GPIO do Raspberry Pi, destacando as portas especialmente pré-programadas para se comunicar via interfaces SPI.

Figura 36 – Raspberry Pi *pinout*



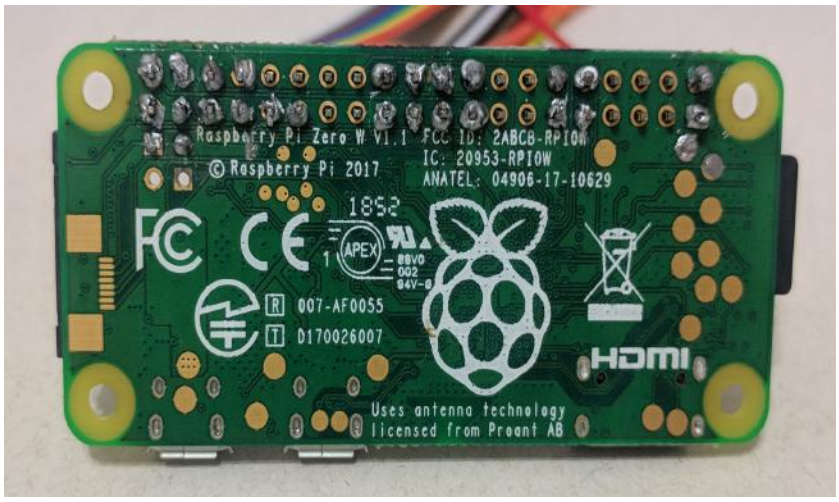
Fonte: https://pinout.xyz/pinout/spi

A solda torna-se necessária para que se tenha uma maior segurança de que realmente há contato entre os pinos e as entradas, entretanto ela não elimina a possibilidade de mal contato entre os componentes, apenas diminui sua possibilidade. As figuras 37 e 38 exibem as soldas realizadas no Raspberry Pi e no módulo RC522, respectivamente.

4.3.1.2 2º passo - Sistema operacional

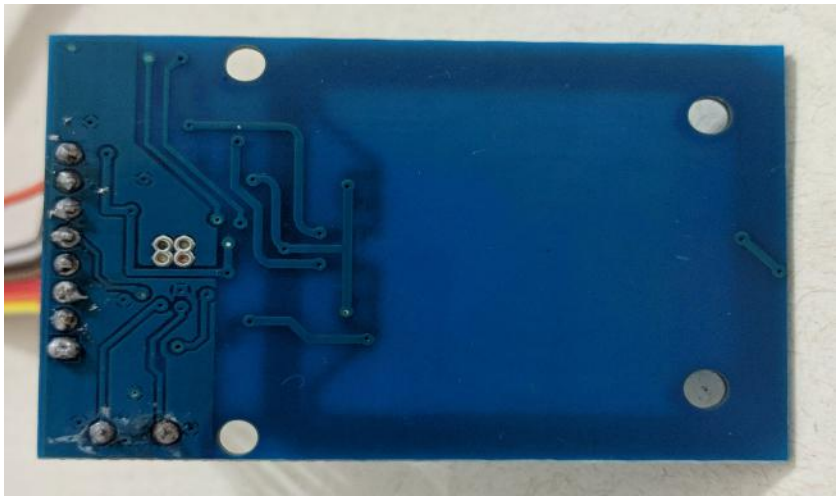
O segundo passo foi instalar o sistema operacional Raspbian Buster no cartão de memória micro SD e realizar certas configurações iniciais, como: atualização do sistema

Figura 37 – Portas GPIO do Raspberry Pi soldadas



Fonte: Reprodução do autor

Figura 38 – Portas GPIO do módulo RC522 soldadas



Fonte: Reprodução do autor

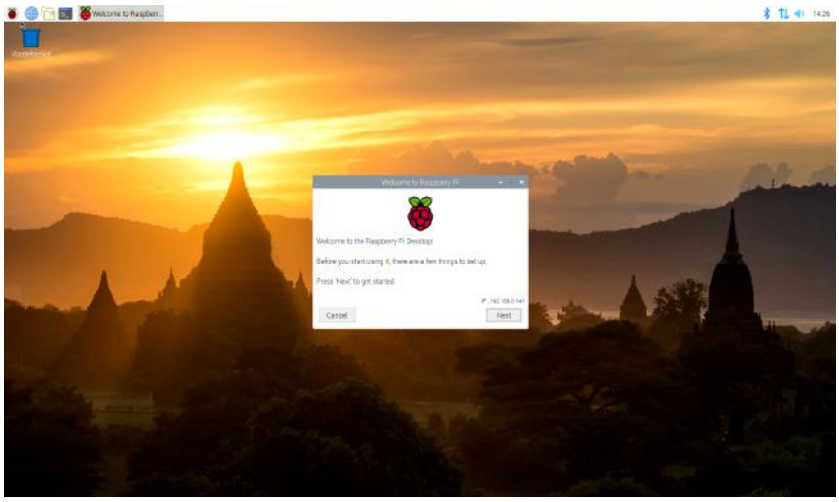
operacional, instalação das aplicações e das bibliotecas necessárias e habilitação do SSH para acesso remoto. A figura 39 exibe a tela inicial do sistema.

4.3.1.3 3º passo - Conexões

O terceiro passo foi escolher as interfaces de comunicação que seriam utilizadas pelos dispositivos do arranjo, habilitar as interfaces escolhidas no microcontrolador e conectar fisicamente os dispositivos. Aqui, foi utilizado o padrão SPI para conectar fisicamente os módulos RFID ao microcontrolador.

SPI, sigla em inglês para *Serial Peripheral Interface*, "[...] é um protocolo de dados serial síncrono usado por microcontroladores para comunicação rápida com um ou mais dispositivos periféricos em curtas distâncias." (ARDUINO.CC, 2019, traduzido pelo au-

Figura 39 – Tela principal do Raspbian Buster



Fonte: https://www.tomshardware.com/news/raspbian-buster-upgrade,39735.html

tor). Arquiteturalmente, os dispositivos do arranjo se dividem em um mestre e vários escravos, sendo geralmente o microcontrolador o mestre e os periféricos os escravos. Há 4 portas principais de comunicação entre mestre e escravos no SPI: SS, SCK, MOSI, MISO.

- SS (*Slave Select*): Porta utilizada pelo mestre para ativar ou desativar dispositivos específicos. Identificada no módulo RC522 como "SDA".
- SCK (*Serial Clock*): Porta utilizada para sincronizar o relógio do escravo com o do mestre para as transmissões de informação.
- MOSI (*Master Out Slave In*): Porta utilizada para enviar informações do mestre para o escravo.
- MISO (*Master In Slave Out*): Porta utilizada para enviar informações do escravo para o mestre.

Enquanto que as portas SCK, MOSI e MISO podem ser compartilhadas por diversos periféricos, a porta SS deve ser única para cada periférico, isto porque é esta porta que define se o escravo deve escutar ou ignorar as comunicações do mestre. É graças a isto que diversos periféricos podem compartilhar as outras 3 portas principais (ARDUINO.CC, 2019).

Como podemos ver pela figura 36, o Raspberry Pi possui duas interfaces SPI (SPI0 e SPI1), e cada interface suporta até dois dispositivos em paralelo (SPIx CE0 e SPIx CE1) enquanto compartilha as outras portas da mesma interface (SPIx SCLK, SPIx MISO, SPIx MOSI). Por questões de praticidade, escolhemos utilizar as duas interfaces SPI, cada uma com um módulo RFID. Assim, o mapa de conexões entre Raspberry Pi e módulo RC522 ficou como definido na tabela 3.

Tabela 3 – Mapa de conexões Raspberry Pi e módulos RC522

Porta de comunicação (RC522)	Porta GPIO (SPI0)	Porta GPIO (SPI1)
SDA (SS)	BCM 8 (SPI0 CE0)	BCM 18 (SPI1 CE0)
SCK	BCM 11 (SPI0 SCLK)	BCM 21 (SPI1 SCLK)
MOSI	BCM 10 (SPI0 MOSI)	BCM 20 (SPI1 MOSI)
MISO	BCM 9 (SPI0 MISO)	BCM 19 (SPI1 MISO)
IRQ	BCM 24	BCM 26
GND	Ground	Ground
RST	BCM 25	BCM 13
3.3V	3.3V Power	3.3V Power

Fonte: Reprodução do autor

Um ponto importante a se destacar sobre a utilização das duas interfaces SPI no Raspberry Pi é que, por padrão, ambas vem desabilitadas e precisam ser ativadas manualmente, entretanto, o modo mais difundido pelos tutoriais presentes na Internet, via menu de configurações "raspi-config", ativa somente a interface SPI0. Para se ativar também a interface SPI1 é necessário realizar alterações no arquivo "/boot/config.txt" e desativar o módulo *Bluetooth*. Isto se deve a uma aparente interferência interna entre o módulo *Bluetooth* e a interface SPI1[15].

Com relação ao codificador rotativo, existem algumas formas de conectá-lo ao microcontrolador. Para este projeto utilizou-se um *driver* de dispositivo do Linux específico para codificadores rotativos[16].

Tanto o codificador rotativo quanto o módulo relé não exigem uma interface de comunicação específica, assim, o mapa de conexões entre o microcontrolador e estes componentes, especificamente, ficou como definido nas tabelas 4 e 5.

4.3.1.4 4º passo - Aplicações de *software*

O quarto passo foi planejar e implementar as aplicações responsáveis por: receber as informações de leitura dos módulos RFID, verificar se o identificador da etiqueta lida possui permissão de passagem pelo ponto de controle de acesso, liberar o ponto de controle

[15] https://www.raspberrypi.org/forums/viewtopic.php?t=146291
[16] https://blog.ploetzli.ch/2018/ky-040-rotary-encoder-linux-raspberry-pi/

Tabela 4 – Mapa de conexões Raspberry Pi e codificador rotativo KY-040

Porta de comunicação	Porta GPIO
CLK	BCM 2
DT	BCM 3
+	BCM 4
GND	Ground

Fonte: Reprodução do autor

Tabela 5 – Mapa de conexões Raspberry Pi e módulo relé

Porta de comunicação	Porta GPIO
VCC	5V
GND	Ground
IN	BCM 18

Fonte: Reprodução do autor

de acesso em caso de identificação positiva, verificar o sentido de rotação do ponto de controle de acesso através do codificador rotativo, atualizar o banco de dados da presença ou ausência do usuário nas dependências da instituição, registrar no banco de dados informações referentes à passagem do usuário pelo ponto de controle, como: identificação do usuário, dia, hora e sentido (entrando ou saindo), e informar via *e-mail* qualquer ação considerada suspeita no sistema, como: tentativa de passagem de cartão RFID inexistente, tentativa de passagem para o mesmo sentido (ex: entrar quando já se encontra presente).

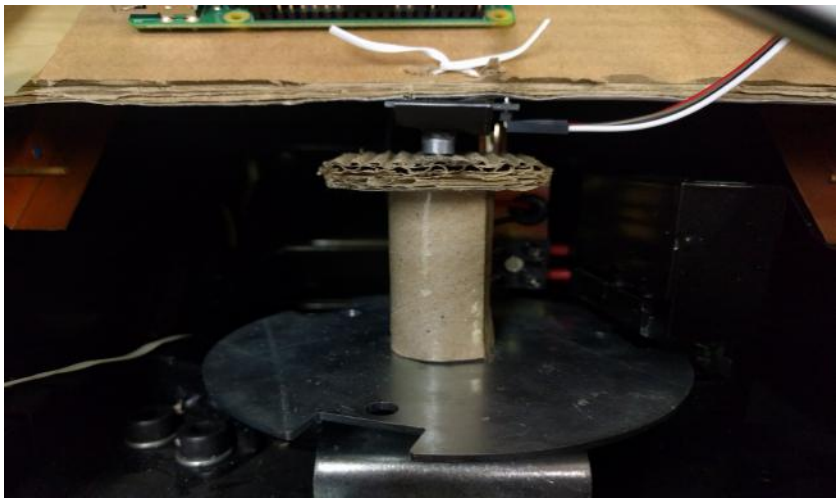
4.3.1.5 5º passo - Integração e validação

O quinto passo foi integrar microcontrolador, módulos RC522, codificador rotativo, módulo relé e aplicações desenvolvidas a um ponto de controle de acesso, além de testar e validar se tudo estava funcionando conforme o elaborado. O ponto de controle de acesso escolhido foi uma catraca mecânica de 3 braços, como ilustrado na figura 33.

Devido ao modo como os componentes internos da catraca estão estruturados, foi necessário elaborar algumas peças extras para que os equipamentos pudessem ser acoplados e acomodados na parte interna, sendo estes um cilindro oco e um disco com um furo no centro, como ilustrado na figura 40. Estes componentes serviram para fazer a transferência

de rotação entre o disco interno da catraca e o codificador rotativo.

Figura 40 – Peças



Fonte: Reprodução do autor

As figuras 41, 42 e 43 exibem o resultado da integração, com todos os componentes desta seção posicionados e configurados na catraca. Após a montagem, foi realizado uma bateria de testes para validar se o sistema estava funcionando corretamente, tais como: passagem de etiqueta não cadastrada, passagem de etiqueta cadastrada, tentativa de saída quando usuário não consta como presente na instituição, tentativa de entrada quando usuário consta como presente na instituição, atualização do banco de dados quando entrada/saída bem sucedida e ausência de atualização quando entrada/saída falha.

4.3.2 Comando

Nesta seção discute-se os passos de implementação da frente de comando. Como dito anteriormente, esta frente trata dos componentes do *back-end*, tais como banco de dados e aplicações de gerenciamento de usuários e operadores do sistema. Desta forma, esta seção cobre os seguintes itens:

- Configuração do servidor.
- Planejamento e implementação do banco de dados.
- Planejamento e desenvolvimento da aplicação *web*.

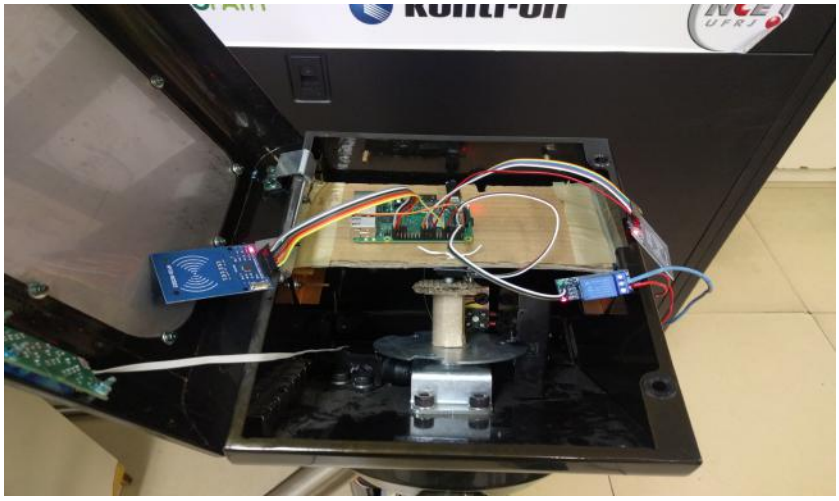
4.3.2.1 1º passo - Configuração de servidor

O primeiro passo na frente de comando foi preparar o servidor, e o ambiente, para o desenvolvimento do projeto. Ações como instalação e atualização do sistema operacional, instalação dos *softwares* e bibliotecas necessários, realização das configurações básicas iniciais e validação de funcionamento, foram todas realizadas nesta primeira etapa.

Figura 41 – Ponto de controle implementado

Fonte: Reprodução do autor

Figura 42 – Ponto de controle implementado



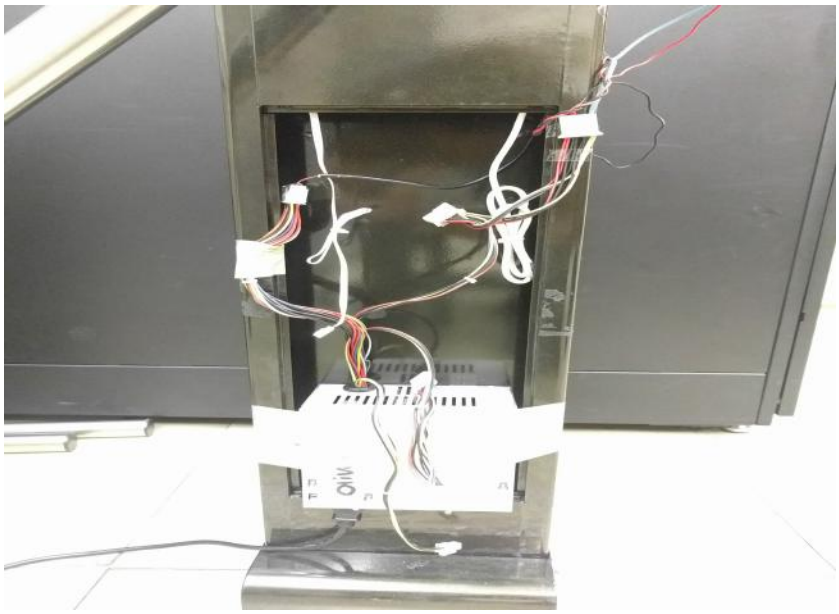
Fonte: Reprodução do autor

4.3.2.2 2º passo - Banco de dados

O segundo passo foi planejar e implementar o esquema do banco de dados, que ficou definido como no modelo da figura 44.

A tabela "Usuario" é a tabela básica do esquema, ela armazena os dados de todas as pessoas que desejam adentrar no instituto, seja ela funcionário, professor, terceirizado, aluno ou visitante. A coluna "cpf" é a chave primária, enquanto a coluna "email" é uma chave única. A tabela "Operador" armazena alguns dados extras necessários para que

Figura 43 – Ponto de controle implementado



Fonte: Reprodução do autor

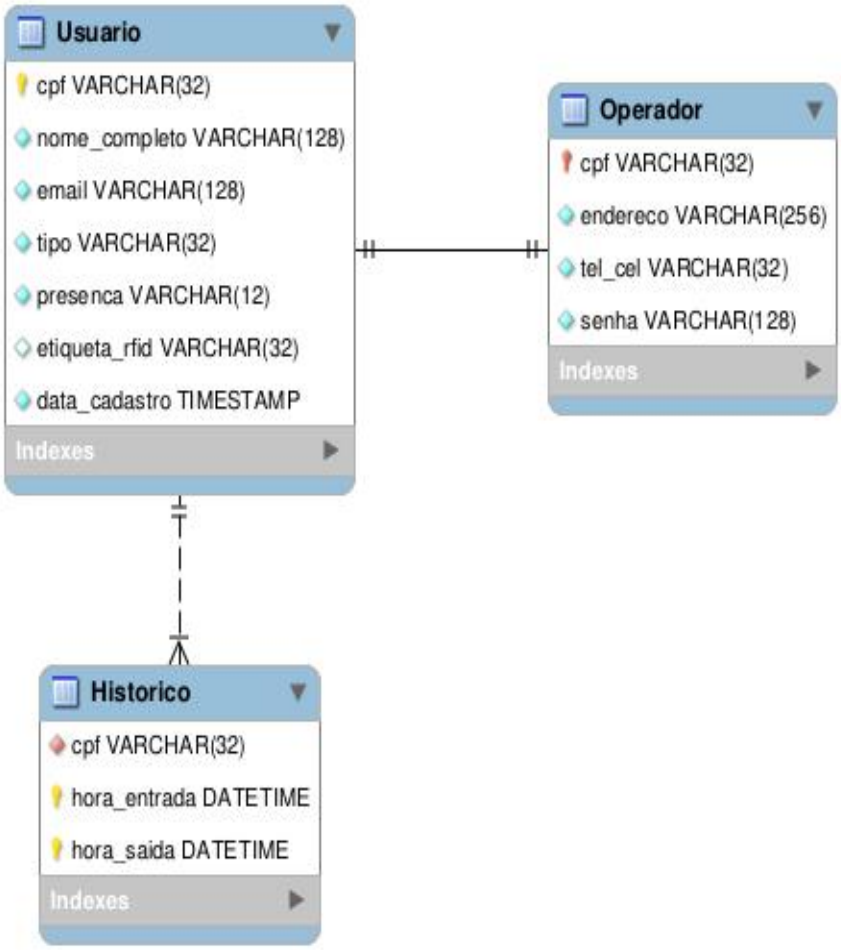
um usuário seja elevado a operador. Um operador é um usuário capaz de se autenticar na aplicação *web* para gerenciar outros usuários do sistema. A coluna "cpf" é a chave primária-estrangeira que correlaciona os registros com a tabela "Usuario". A tabela "Historico" armazena todos os eventos de uso do ponto de controle de acesso, seja para entrada ou saída. A coluna "cpf" é a chave primária-estrangeira que correlaciona os registros com a tabela "Usuario".

Além das tabelas, três usuários são criados no MariaDB para gerenciamento do banco. O usuário "admin", apenas via acesso local, possui todas as permissões para o banco de dados do projeto. O usuário "operador", apenas via acesso local, possui permissões de consulta na tabela "Operador" e de alteração na tabela "Usuario", sendo este o usuário utilizado pela aplicação PHP para realizar as operações dos operadores autenticados na aplicação *web*. O usuário "raspberry", com acesso remoto apenas da mesma sub-rede do MariaDB, possui permissões de consulta na tabela "Usuario" e de inserção na tabela "Historico", sendo este o usuário utilizado pelo microcontrolador para realizar consultas de usuários e inserções de históricos no banco de dados.

4.3.2.3 3º passo - Aplicação *web*

O terceiro passo foi planejar e implementar uma aplicação *web* em PHP onde operadores externos podem se autenticar para cadastrar novos usuários e gerenciar os existentes. A aplicação utiliza o usuário "operador" do MariaDB para realizar as operações no banco. A mesma possui apenas duas telas, uma de autenticação, que valida se o usuário e a senha informados estão presentes na tabela "Operador", e uma de cadastro de novos usuários

Figura 44 – Modelo entidade-relacionamento



Fonte: Reprodução do autor

(e consulta dos já existentes), onde o operador entra com as informações necessárias de cadastro da pessoa que deseja utilizar o ponto de controle de acesso. As figuras 45 e 46 exibem as telas da aplicação desenvolvida.

Figura 45 – Página de autenticação

Fonte: Reprodução do autor

Figura 46 – Página principal

Fonte: Reprodução do autor

5 CONCLUSÕES E TRABALHOS FUTUROS

5.1 CONCLUSÕES

Esta monografia nasceu com o objetivo de elaborar e implementar um sistema de segurança de identificação de usuários através da tecnologia de RFID de alta frequência, que fosse economicamente barato e tecnicamente simples de ser implementado, e que fosse possível de ser implementada no Instituto Tércio Pacitti, da Universidade Federal do Rio de Janeiro (NCE/UFRJ), a fim de automatizar, agilizar e melhor controlar o fluxo passagem de docentes, alunos e funcionários nas dependências do instituto.

Após o embasamento teórico das seções iniciais, descreveu-se através do capítulo 4 os passos dados durante o processo de implementação do projeto, desde a escolha dos equipamentos e seus porquês, até a sua implementação e validação. Das várias soluções empregadas, algumas merecem destaque pelo seu desempenho acima do esperado.

A primeira delas refere-se ao módulo RFID-RC522, um leitor que se mostrou muito capaz e correto nas leituras, com uma ótima abrangência de etiquetas suportadas, diversas interfaces de comunicação com o microcontrolador, barato, ampla documentação na Internet e fácil de ser utilizado, não trazendo qualquer dificuldade extra na hora da implementação.

A segunda refere-se ao Raspberry Pi Zero W, que apesar de não ser a versão mais potente de todos os modelos disponíveis, mostrou-se a versão ideal para um microcontrolador de funções simples, sendo econômico tanto financeiramente quanto energeticamente, excelente documentação disponível e de construção sólida, aguentando diversos impactos leves e soldas quentes.

A terceira refere-se as linguagens de programação, Python e PHP, que são muito amigáveis a novos usuários, mesmo àqueles que nunca programaram na vida, sendo poderosas o suficiente para elaborar grandes projetos ao mesmo tempo que são simples e rápidas para pequenas implementações, excelente documentação e milhares de tutoriais e exemplos na Internet.

Assim, ao final desta monografia, dois importantes marcos foram alcançados: mostrar que é possível elaborar um sistema de controle de acesso baseado em RFID economicamente barato e tecnicamente simples, e elaborar um material rico e sólido sobre a tecnologia de identificação por radiofrequência em língua portuguesa.

Há, entretanto, alguns poréns. Devido ao modo como o sistema foi pensado, simples e barato, existem pontos que podem precisar de atenção especial dependendo das necessidades e especificações de cada implementação. O primeiro deles encontra-se no modo como a autenticação foi elaborada, dependendo única e exclusivamente do número identificador (UID) do cartão de acesso, número este que pode ser clonado por um agente

mal-intencionado caso o mesmo obtenha acesso ao cartão.

O segundo ponto encontra-se no modelo de etiqueta utilizado, o MIFARE *Classic* 1K, que possui uma cifra criptográfica própria (Crypto1) para proteger a memória interna do cartão, cifra esta que possui algumas vulnerabilidades publicamente conhecidas (GRüLL, 2015).

O terceiro ponto encontra-se no codificador rotativo, que apresenta algumas incoerências com relação a precisão e corretude das leituras de rotação da catraca, fazendo com que a mesma não fosse bloqueada corretamente após uma rotação.

Outro ponto importante a ser levantado, mas que não está diretamente relacionado ao projeto em si, diz respeito ao sistema de alimentação de energia elétrica e suas constantes falhas. Todos os dispositivos envolvidos neste projeto funcionam a base de energia elétrica, caso o suprimento de energia seja cortado, todo o sistema para de funcionar. Como medida de segurança, o ponto de controle de acesso não pode ficar no estado bloqueado caso ocorra uma falta de energia, devendo ficar no estado livre em caso de queda de energia, deixando assim a instituição mais vulnerável.

Os pontos supracitados possuem similaridades com relação aos seus motivos, todos feriram de alguma forma pelo menos um dos três pilares propostos inicialmente, um sistema de controle de acesso baseado em RFID, economicamente barato e tecnicamente simples de ser implementado. Entretanto, estes pontos não diminuem o valor final deste trabalho.

5.2 TRABALHOS FUTUROS

Apesar de completo e funcional no estado atual, este trabalho não implementa o estado da arte possível para as tecnologias aqui utilizadas, havendo espaço para expansão, a começar pelos pontos citados na seção 5.1.

Com relação a autenticação, implementar um sistema que utilize mais do que apenas o número identificador (UID) do cartão para autenticar o usuário, como armazenar algum dado extra na memória interna da etiqueta e posteriormente validar este valor. De todas as melhorias a serem vistas nesta seção, esta é a mais simples e sem custos adicionais de ser implementada, entretanto, devido ao modelo de etiqueta utilizada (MIFARE *Classic* 1k), qualquer solução para este ponto que envolva a memória interna da etiqueta esbarra na frágil função criptográfica implementada para protegê-la.

Com relação a etiqueta Mifare Classic 1k, implementar modelos de cartões com cifras criptográficas mais seguras, como os modelos MIFARE Plus e MIFARE DESFire que possuem cifras AES-128bits e 3DES (NXP, 2016b; NXP, 2016a). Solucionando-se este ponto desta forma, o questão de se utilizar apenas o UID da etiqueta para autenticação passa a ser mais facilmente solucionada, visto que agora a memória interna das etiquetas estaria devidamente cifrada e segura. Esta melhoria, apesar de ser a mais recomendada,

também significa um aumento no preço do projeto, visto que cartões com tecnologias mais avançadas tendem a ser mais caros, e na complexidade do projeto, visto que será necessário gerenciar as chaves de acesso as áreas protegidas das etiquetas.

Com relação ao codificador rotativo, implementar métodos mais precisos na medição da rotação, como através de um sensor de luminosidade e cor que identifica a rotação através de códigos de cores posicionados em diferentes pontos da catraca. Apesar da sugestão dada ser cara e aumentar consideravelmente o preço final do projeto, este ponto de melhoria é o que permite as soluções mais criativas, sendo a própria solução utilizada nesta monografia uma forma não ortodoxa de conectar catraca e codificador.

Com relação a energia elétrica, implementar um sistema de alimentação auxiliar que entrasse em ação quando o principal falhasse, garantindo assim o funcionando dos sistemas do projeto. Vale ressaltar que os sistemas do projeto constituem tanto da catraca e do microcontrolador quanto do servidor de banco de dados e gerenciamento. Um exemplo prático de solução seria o *nobreak*, um regulador de tensão com bateria interna, que manteria os sistemas funcionando mesmo que por um breve período de tempo. Em um segundo caso de esgotamento do *nobreak*, a solução mais viável é a liberação da catraca e controle de acesso manual por um segurança.

Todas as ideias alternativas de implementação aqui apresentadas são apenas sugestões, havendo diversos outros meios de se aprimorar este trabalho.

REFERÊNCIAS

ADHIARNA, N.; RHO, J.-J. Standardization and global adoption of radio frequency identification (rfid): Strategic issues for developing countries. p. 1461–1468, 2009.

AHSAN, K.; SHAH, H.; KINGSTON, P. Rfid applications: An introductory and exploratory study. **International Journal of Computer Science Issues**, v. 7, n. 3, 2010.

AHSON, S. A.; ILYAS, M. **RFID Handbook: Applications, Technology, Security, and Privacy**. 1. ed. Florida: CRC Press, 2018.

APACHE.ORG. **About the Apache HTTP Server Project - The Apache HTTP Server Project**. 2019. Acessado em: 11/08/2019. Disponível em: <https://httpd.apache.org/ABOUT_APACHE.html>.

ARDUINO.CC. **Arduino - SPI**. 2019. Acessado em: 02/09/2019. Disponível em: <https://www.arduino.cc/en/reference/SPI>.

BROCK, D. L. The electronic product code (epc) a naming scheme for physical objects. MIT Auto-ID Center, 2010.

CAPEC. **CAPEC - CAPEC-94: Man in the Middle Attack (Version 3.1)**. 2019. Acessado em: 09/04/2019. Disponível em: <https://capec.mitre.org/data/definitions/94.html>.

CHAWLA, V.; HA, D. S. An overview of passive rfid. **IEEE Communications Magazine**, v. 45, n. 9, p. 11–17, 2007.

CORPORATION, A. **AT89C51**. 2000. Acessado em: 22/09/2019. Disponível em: <http://ww1.microchip.com/downloads/en/DeviceDoc/doc0265.pdf>.

COSKUN, V.; OZDENIZCI, B.; OK, K. **Near Field Communication (NFC): From Theory to Practice 1st Edition**. 1. ed. Nova Jersey: John Wiley & Sons, Ltd., 2012.

COSKUN, V.; OZDENIZCI, B.; OK, K. A survey on near field communication (nfc) technology. **Wireless Personal Communications**, v. 71, n. 3, p. 2259–2294, 2013.

DEVECCHI, A.; UNIFACCAMP, P. Um sistema de ponto eletrônico digital: projeto e implementação de hardware e software (atividade prática de desenvolvimento de software). 06 2015. Disponível em: <https://www.researchgate.net/publication/280835505>.

DOMDOUZIS, K.; KUMAR, B.; ANUMBA, C. Radio-frequency identification (rfid) applications: A brief introduction. **Advanced Engineering Informatics**, v. 21, n. 4, p. 350–355, 2007.

EGLI. 2006.

FAROOQ, U. et al. Rfid based security and access control system. **International Journal of Engineering and Technology**, p. 309–314, 01 2014.

FINKENZELLER, K. **RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near–Field Communication**. 3. ed. Chichester: John Wiley & Sons, Ltd., 2010.

FORUM, N. **About Us | NFC Forum**. 2019. Acessado em: 17/06/2019. Disponível em: <https://nfc-forum.org/about-us/>.

FORUM, N. **Our Members NFC | NFC Forum**. 2019. Acessado em: 17/06/2019. Disponível em: <https://nfc-forum.org/about-us/our-members/>.

GOOD, T.; BENAISSA, M. A low-frequency rfid to challenge security and privacy concerns. p. 856–863, 2009.

GRAAFSTRA, A. **RFID Toys: Cool Projects for Home, Office, and Entertainment**. 1. ed. Indiana: Wiley Publishing, Inc., 2006.

GRüLL, J. **Security Statement on Crypto1 Implementations**. 2015. Acessado em: 01/07/2019. Disponível em: <https://www.mifare.net/en/products/chip-card-ics/mifare-classic/security-statement-on-crypto1-implementations/>.

GS1. **EPCglobal | GS1**. 2019. Acessado em: 10/04/2019. Disponível em: <https://www.gs1.org/epcglobal>.

GUO, Y.; ZHAO, Z. Design of school bus passengers' identity authentication system based on rfid. p. 412–415, 10 2015.

HONGZHI, O. et al. Design of auto-guard system based on rfid and network. p. 1292–1295, 04 2011.

HUNG, C.-H.; BAI, Y.-W.; REN, J.-H. Design and implementation of a door lock control based on a near field communication of a smartphone. p. 45–46, June 2015.

IEC. **IEC - About IEC > What we do**. 2019. Acessado em: 10/04/2019. Disponível em: <https://www.iec.ch/about/activities/?ref=menu>.

IEC. **IEC - About the IEC > Who we are**. 2019. Acessado em: 10/04/2019. Disponível em: <https://www.iec.ch/about/profile/?ref=menu>.

ISO. **About Us**. 2019. Acessado em: 10/04/2019. Disponível em: <https://www.iso.org/about-us.html>.

ISO. **Standards**. 2019. Acessado em: 10/04/2019. Disponível em: <https://www.iso.org/standards.html>.

JOURNAL, R. **Inductive coupling - Glossary Term - RFID Journal**. 2019. Acessado em: 07/04/2019. Disponível em: <https://www.rfidjournal.com/glossary/term?81>.

KEDLAYA, S. G.; BHAGYALAKSHMI, H. R. Design and implementation of gpio enumeration library and application for uefi-bios. **International Journal of Scientific Engineering and Technology**, v. 3, p. 524–528, 05 2014.

KITSOS, P.; ZHANG, Y. **RFID Security: Techniques, Protocols and System-on-Chip Design**. 1. ed. New York: Springer US, 2008.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet - uma abordagem top-down**. 6. ed. São Paulo: Pearson Education do Brasil Ltda., 2014.

LOUREIRO, G. d. S. M.; SOUZA, I. Q. d.; LOPES, M. G. d. M. **RFID Identificação por Rádio Frequência**. 2015. Acessado em: 14/04/2019. Disponível em: <https://www.gta.ufrj.br/grad/15_1/rfid/index.html>.

LOZANO-NIETO, A. **RFID Design Fundamentals and Applications**. 1. ed. Florida: CRC Press, 2010.

MARIADB.ORG. **About MariaDB - MariaDB.org**. 2019. Acessado em: 21/07/2019. Disponível em: <https://mariadb.org/about/>.

MATT. **Raspberry Pi Power Consumption Data**. 2018. Acessado em: 29/06/2019. Disponível em: <https://www.raspberrypi-spy.co.uk/2018/11/raspberry-pi-power-consumption-data/>.

MONTEIRO, F. V.; PACHECO, G. F. d. C.; LIMA, L. C. de. **RFID - Radio Frequency Identification**. 2010. Acessado em: 10/04/2019. Disponível em: <https://www.gta.ufrj.br/grad/10_1/rfid/comunicacao.html>.

NASA. **Electromagnetic Spectrum - Introduction**. 2013. Acessado em: 06/04/2019. Disponível em: <https://imagine.gsfc.nasa.gov/science/toolbox/emspectrum1.html>.

NIKITIN, P. V.; RAO, K. V. S.; LAZAR, S. An overview of near field uhf rfid. p. 167–174, 2007.

NXP. **MIFARE DESFire | NXP**. 2016. Acessado em: 02/07/2019. Disponível em: <https://www.nxp.com/products/identification-security/rfid/mifare-hf/mifare-desfire:MC_53450>.

NXP. **MIFARE Plus | NXP**. 2016. Acessado em: 02/07/2019. Disponível em: <https://www.nxp.com/products/identification-security/rfid/mifare-hf/mifare-plus:MC_57609>.

NXP SEMICONDUTORES. **MFRC522 - Standard performance MIFARE and NTAG frontend**. 2016. Rev. 3.9; Acessado em: 07/07/2019. Disponível em: <https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf>.

NXP SEMICONDUTORES. **MF1S50YYX_V1 - MIFARE Classic EV1 1K - Mainstream contactless smart card IC for fast and easy solution development**. 2018. Rev. 3.2; Acessado em: 07/07/2019. Disponível em: <https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf>.

ONONIWU, G.; NWAJI, O. Radio frequency identification (rfid) based attendance system withautomatic door unit. **Academic Research International**, v. 2, p. 168–183, 03 2012.

PHP.NET. **PHP: What is PHP? - Manual**. 2019. Acessado em: 11/08/2019. Disponível em: <https://www.php.net/manual/en/intro-whatis.php>.

PIDRAMBLE. **Power Consumption Benchmarks**. 2019. Acessado em: 29/06/2019. Disponível em: <https://www.pidramble.com/wiki/benchmarks/power-consumption>.

PYTHON.ORG. **What is Python? Executive Summary | Python.org**. 2019. Acessado em: 23/07/2019. Disponível em: <https://www.python.org/doc/essays/blurb/>.

QING, X.; GOH, C.; CHEN, Z. Segmented loop antenna for uhf near-field rfid applications. **Electronics Letters**, v. 45, n. 17, p. 872–873, 2009.

QUIGLEY, B. **Releases - Ubuntu Wiki**. 2019. Acessado em: 11/08/2019. Disponível em: <https://wiki.ubuntu.com/Releases>.

RASPBERRYPI.ORG. **Buy a Raspberry Pi Zero W – Raspberry Pi**. 2019. Acessado em: 04/07/2019. Disponível em: <https://www.raspberrypi.org/products/raspberry-pi-zero-w/>.

RASPBERRYPI.ORG. **Download Raspbian for Raspberry Pi**. 2019. Acessado em: 21/07/2019. Disponível em: <https://www.raspberrypi.org/downloads/raspbian/>.

RASPBERRYPI.ORG. **What is a Raspberry Pi?** 2019. Acessado em: 29/06/2019. Disponível em: <https://www.raspberrypi.org/help/what-\%20is-a-raspberry-pi/>.

RASPBIAN.ORG. **FrontPage - Raspbian**. 2019. Acessado em: 21/07/2019. Disponível em: <https://www.raspbian.org/>.

RAVI, K. S. et al. Rfid based security system. **International Journal of Innovative Technology and Exploring Engineering (IJITEE)**, v. 2, 04 2013.

RFID4U. **RFID Architecture Components | RFID4U**. 2016. Acessado em: 06/04/2019. Disponível em: <https://rfid4u.com/explore/rfid-certification-prep/cheat-sheet-rfid-architecture-components/>.

RFID4U. **Global RFID Standards and Regulations | RFID4U**. 2019. Acessado em: 10/04/2019. Disponível em: <https://rfid4u.com/explore/rfid-certification-prep/cheat-sheet-standards-and-regulations/>.

ROBERTS, C. M. Radio frequency identification (rfid). **Computers & Security**, v. 25, n. 1, p. 18–26, 2006.

RODRIGUES, A. L. F. d. C. **Apresentação**. 2019. Acessado em: 06/04/2019. Disponível em: <http://portal.nce.ufrj.br/index.php?option=com_content&view=article&id=90&Itemid=66>.

SAB, G. A. A.; FERREIRA, R. C.; ROZENDO, R. G. **Near Field Communication**. 2013. Acessado em: 17/06/2019. Disponível em: <https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2013_2/nfc/index.html>.

SHAARI, A. M.; NOR, N. S. M. Position and orientation detection of stored object using rfid tags. **Procedia Engineering**, v. 184, p. 708–715, 2017.

SHAFIN, M. K. et al. Development of an rfid based access control system in the context of bangladesh. p. 1–5, 03 2015.

SILVA, B. A. J. O uso da iot no controle de frequência dos alunos da unip. **CONIC-Semesp - 18º Congresso Nacional de Iniciação Científica**, v. 6, 2018. Acessado em: 04/08/2019. Disponível em: <http://conic-semesp.org.br/anais/files/2018/trabalho-1000002627.pdf>.

SOFISICA. **Ondas**. 2019. Acessado em: 31/03/2019. Disponível em: <https://www.sofisica.com.br/conteudos/Ondulatoria/Ondas/classificacao.php>.

SON, H.-W.; PYO, C.-S. Design of rfid tag antennas using an inductively coupled feed. **Electronics Letters**, v. 41, n. 18, p. 994–996, 2005.

SORRELLS, P. Passive rfid basics. p. 1–7, 1998. Disponível em: <http://ww1.microchip.com/downloads/en/appnotes/00680b.pdf>.

TANENBAUM, A. S.; RIEBACK, M. R.; CRISPO, B. The evolution of rfid security. **IEEE Pervasive Computing**, IEEE Computer Society, v. 5, n. 1, p. 62–69, 2006.

UBUNTU.COM. **1.1. What is Ubuntu?** 2019. Acessado em: 11/08/2019. Disponível em: <https://help.ubuntu.com/lts/installation-guide/s390x/ch01s01.html>.

URONE, P. P.; HINRICHS, R. **College Physics**. Texas: OpenStax, 2017. Disponível em: <https://openstax.org/details/books/College-Physics>.

VIOLINO, B. **A Summary of RFID Standards**. 2005. Acessado em: 10/04/2019. Disponível em: <https://www.rfidjournal.com/articles/view?1335/>.

WANT, R. An introduction to rfid technology. **IEEE Pervasive Computing**, v. 5, n. 1, p. 25–33, 2006.

WANT, R. **RFID Explained: A Primer on Radio Frequency Identification Technologies**. Vermont: Morgan & Claypool, 2006.

WARD, M.; KRANENBURG, R. v. Rfid: frequency, standards, adoption and innovation. **Series: JISC Technology and Standards Watch**, Middlesex University London, 2006. Disponível em: <https://eprints.mdx.ac.uk/id/eprint/2990>.

WYLD, D. Rfid 101: The next big thing for management. **Management Research News**, v. 29, p. 154–173, 04 2006.

XIAO, Q.; GIBBONS, T.; LEBRUN, H. Rfid technology, security vulnerabilities, and countermeasures. 2009.

YOUNG, H. D.; FREEDMAN, R. A. **Física II: Termodinâmica e Ondas**. 12. ed. São Paulo: Pearson Education do Brasil, 2008.

YOUNG, H. D.; FREEDMAN, R. A. **Física III: Eletromagnetismo**. 12. ed. São Paulo: Pearson Education do Brasil, 2009.

ZENG, J. et al. Development of multilanguage selected automatic voice playing system based on rfid technology. p. 332–335, 08 2010.

ZVEREV, A. I. **Handbook of Filter Synthesis**. Revised edition. New York: Wiley-Interscience, 2005.