UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

JABES CANDIDO DA SILVA

APLICAÇÃO DA TECNOLOGIA LORA NA AUTOMAÇÃO DE AMBIENTES PARA CONTROLE DE ACESSO

CAMPO MOURÃO

2022

JABES CANDIDO DA SILVA

APLICAÇÃO DA TECNOLOGIA LORA NA AUTOMAÇÃO DE AMBIENTES PARA CONTROLE DE ACESSO

Application of LoRa technology in environment automation for access control

Trabalho de conclusão de curso de graduação apresentado como requisito para obtenção do título de Bacharel em Engenharia Eletrônica da Universidade Tecnológica Federal do Paraná (UTFPR).

Orientador: Prof. Marcio Rodrigues da Cunha

CAMPO MOURÃO

2022

JABES CANDIDO DA SILVA

APLICAÇÃO DA TECNOLOGIA LORA NA AUTOMAÇÃO DE AMBIENTES PARA CONTROLE DE ACESSO

Trabalho de conclusão de curso de graduação apresentado como requisito para obtenção do título de Bacharel em Engenharia Eletrônica da Universidade Tecnológica Federal do Paraná (UTFPR).

Orientador: Prof. Marcio Rodrigues da Cunha

Data de aprovação: 31/maio/2022

Leandro Castilho Brolin
Doutorado em Engenharia Elétrica
Universidade Tecnológica Federal do Paraná

Roberto Wilhelm Krauss Martinez
Doutorado em Engenharia Elétrica e Informática Industrial
Universidade Tecnológica Federal do Paraná

Marcio Rodrigues da Cunha
Doutorado em Engenharia Elétrica
Universidade Tecnológica Federal do Paraná

CAMPO MOURÃO

2022

Dedico este trabalho ao meu amado pai, que infelizmente não poderá desfrutar comigo das minhas conquistas.

AGRADECIMENTOS

Meu ser se transborda pela satisfação de ter tantas pessoas à minha volta que tanto me influenciaram positivamente a buscar e a alcançar esta grande conquista. Não podendo citar todas, deixo aqui o agradecimento ao meu pai Genivaldo Malaquias da Silva, cujo exemplo moldou o meu caráter, minha mãe Rosemeire Candido da Silva, que tanto almejou um filho vitorioso, que inspirou a força de vontade em meu ser. Agradeço ao meu orientador Marcio Rodrigues da Cunha, que acreditou e confiou em minhas capacidades. Agradeço também aos professores Paulo Gonçalvez, Eduardo Giometti Bertogna e Luiz Arthur Feitosa Santos que marcaram minha trajetória, sendo verdadeiros pilares nessa reta final de minha graduação. Agradeço à minha esposa Josiane da Silva Ribeiro, a quem sou grado por todo o apoio. Declaro toda a minha gratidão ao meu grande amigo Yuri.

RESUMO

Há uma grande gama de tecnologias sendo lançadas a cada instante. Entre elas, a tecnologia LoRa, que permite a comunicação de dispositivos simples com sistemas complexos. Uma aplicação dessa tecnologia é um sistema de trancas eletrônicas que possibilitam aos administradores de um dado ambiente o controle e o monitoramento de acessos por terceiros a esse ambiente, com custos relativamente pequenos. Neste trabalho, é elaborado um sistema composto por tranca eletrônica, gateway e um servidor web. Esse sistema controla o acesso através de trancas eletrônicas que realizam leituras de etiquetas RFID para identificação individual. Os dados são transmitidos através de um módulo de tecnologia LoRa que faz a transmissão por rádio frequência para um gateway. O gateway é o responsável por encaminhar os dados transmitidos para uma aplicação web. O gateway atua como ponte entre a transmissão via radiofrequência LoRa e a transmissão ethernet. Os dados fluem em ambos os sentidos no gateway, tanto da fechadura para o servidor, como do servidor para a fechadura. O servidor é responsável por manter uma relação de usuários cadastrados, permitindo sua consulta para a liberação do acesso. Os resultados obtidos foram razoáveis, obtendo-se um sistema funcional, porém com limitações quanto ao alcance e quantidade de fechaduras para um mesmo gateway.

Palavras-chave: LoRa; ESP32; RFID; tranca eletrônica.

ABSTRACT

There is a wide range of technologies being launched every time. Among them the LoRa technology, which allows the communication of simple devices with complex systems. An application of this technology is an electronic lock system that allows the administrators of a given environment to control and monitor the accesses by third parties to this environment with relatively low costs. In this work we elaborated a system composed by electronic lock, gateway and an application in a web server. This system controls access through electronic locks that perform RFID tag readings for individual identification. The data is transmitted through a LoRa technology module that transmits radio frequency to a gateway. The gateway is responsible for forwarding the transmitted data to a web application. The gateway acts as a bridge between the LoRa radio frequency transmission and the ethernet transmission. The data flows in both directions at the gateway, both from the latch to the web application and from the web application to the latch. The web application is responsible for accessing the data sent from the gateway to a server in the cloud and displaying the access data as reports and also controlling the access authorizations either by adding new users or by withdrawing access to others. The results obtained were reasonable, obtaining a functional system but with limitations in terms of reach and number of locks for the same gateway.

Keywords: LoRa; ESP32; RFID; electronic lock.

LISTA DE ILUSTRAÇÕES

Figura 1- Ilustração de uma rede LoRaWAN.....17
Figura 2 - Elementos da arquitetura de uma rede Wifi 20
Figura 3 - Comparação entre as tecnologias de comunicação.....22
Figura 4 - Módulo LoRa baseado no ESP32. 26
Figura 5 - Diversas tags RFID. 28
Figura 6 Diagrama de blocos 30
Figura 7 Esquemático da Tranca 31
Figura 8: Leitor MFRC522. 32
Figura 10 Módulo Gateway de 8 canais. 34
Figura 11 Adaptador Necessário.....35
Figura 12 Ligação dos pinos 36
Figura 13 *Gateway* baseado no ESP 32 37
Figura 14 Fluxograma de funcionamento do gateway.....38
Figura 15 Organização dos dados na base de dados 39
Figura 16: Fechadura Elétrica FX-500 40
Figura 17 Diagrama em blocos do funcionamento da fechadura eletrônica.....41
Figura 18 Fechadura Eletrônica montada para Testes 42
Figura 19 Localização do emissor (a esquerda) e receptor (a direita) na posição de maior alcance em área aberta.....43
Figura 20 Alcance da transmissão em área aberta sem obstáculos 44
Figura 21 Potência do sinal na mensagem com maior alcance 44
Figura 22 Transmissão sem obstáculos a um metro.....45
Figura 23 Teste de transmissão com um livro como obstáculo.....46
Figura 24 Aparelho celular como obstáculo no percurso 46
Figura 25 Palma da mão como obstáculo 47
Figura 26 Tempo em milissegundos para transmitir via LoRa.....47
Figura 27 Saída serial mostrando o tempo em milissegundos da execução do processo de validação.....48
Figura 28 Saída serial mostrando o tempo total para o acionamento do mecanismo eletromecânico da fechadura 48
Figura 29 *Tags* utilizadas neste projeto.....49

Figura 30 Tranca em estado de aguarde 52
Figura 31 Tela Inicial do *gateway*.....53
Figura 32 Tranca com a mensagem “acesso autorizado” 53
Figura 33 Tranca com a mensagem “acesso negado” 54

LISTA DE TABELAS

TABELA 1 - Composição da Mensagem Transmitida em LoRa.....33

LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

ADC	Automated Data Collection – Coleta Automática de Dados
ANATEL	Agência Nacional de Telecomunicações
AP	Access Point – Ponto de Acesso
BLE	Bluetooth Low Energy – Bluetooth de Baixo Consumo
BPS	Bits por Segundo
BSS	Basic Service Set – Configuração de Serviços Básicos
BW	Band Width – Largura de Banda
DS	Distribution System – Sistema de Distribuição
DS	Direct Sequence – Sequência Direta
EPC	Electronic Product Code – Codigo Eletrônico de Produto
ESS	Extended Service Set – Conjunto de Serviço
FH	Frequency Hopping – Salto de Frequência
GPIO	General Purpose Input/Output – Entradas e Saídas de Propósito Geral
HDMI	High-Definition Multimedia Interface – Interface de Multimídia de Alta Definição
HF RFID	High-Frequency Radio Frequency Identification – Identificação por Radiofrequência em Altas Frequências
IP	Internet Protocol – Protocolo de Internet
ISM	Instrumental - Scientific - Medical – Instrumental, Científico, Médico.
ISO	International Organization for Standardization – Organização Internacional para Padronização
LAN	Local Area Network – Rede Local
LORA	Long Range – Longo Alcance
LORAWAN	Long Range Wide Area Network – Rede de Longo Alcance
LPWAN	Low Power Wide Area Network – Rede de Longo Alcance e Baixo Consumo
MIT	Massachusetts Institute of Technology – Instituto de Tecnologia de Massachusetts
M2M	Machine to Machine – Máquina para Máquina

OLED	Organic Light-Emitting Diode – Diodo Orgânico Emissor de Luz
PLC	Power Line Carrier – Comunicação Via Rede
RCA	Radio Corporation of America – Corporação de Rádio da América
RFID	Radio Frequency Identification – Identificação por Radiofrequência
SF	Spreading factor – Fator de Espalhamento
SOC	System on Chip – Sistema em um Chip
SP	Spread Spectrum – Espectro de Difusão
STA	Station – Estação
TCP	Transmission Control Protocol – Protocolo de Controle de Transmissão
UHF RFID	Ultra High-Frequency Radio Frequency Identification – Identificação por Ultra Alta Frequência
USB	Universal Serial Bus – Barramento Serial Universal
WIFI	Wireless Fidelity – Fidelidade Wireless
WIRELESS	Wire Less – Sem fio

SUMÁRIO

1. INTRODUÇÃO 13
1.1 OBJETIVO GERAL 16
1.2 OBJETIVOS ESPECÍFICOS 16
1.3 JUSTIFICATIVA 17
2. FUNDAMENTAÇÃO TEÓRICA 18
3. METODOLOGIA 30
3.1 LEITURA DA TAG RFID 31
3.2 ENVIANDO DADOS PARA O *GATEWAY* 32
3.3 VALIDAÇÃO DO ACESSO 33
3.4 FINALIZAÇÃO DO PROCESSO 40
3.5 PLANEJAMENTO EXPERIMENTAL E DIAGNÓSTICO 42
3.5.1 Alcance 42
3.5.2 Gastos de tempo do sistema 47
3.5.3 Teste com as Tags 49
4. RESULTADOS E DISCUSSÕES 50
5. CONCLUSÕES 55
REFERÊNCIAS 58

1. INTRODUÇÃO

Com o avanço da tecnologia e as mudanças contextuais, o homem tem buscado melhorias visando qualidade de vida, lucro ou facilidades. Essa busca fomentou o desenvolvimento da tecnologia, partindo de invenções básicas, como a roda, até as mais atuais como os sistemas embarcados.

Alguns sistemas que antes eram implementados apenas em ambientes industriais, passaram a ser utilizados em residências, comumente em atividades que muitas vezes passam desapercebidas, fornecendo maior segurança, economia, conforto e tempo livre para realizar outras atividades (RAMOS e SANTOS, 2015).

Inicialmente, a automação residencial, ou domótica, era vista como algo do futuro, com alto grau de tecnologia limitada para poucas pessoas, o que garantia um certo *status* (TEZA, 2002). Porém, com o barateamento e a difusão de novas tecnologias, sistemas mais elaborados se tornaram mais acessíveis, o que impulsionou a difusão da domótica.

A domótica se baseia na integração de vários elementos eletrônicos que fornecem as mais diversas funções, que partem de simples sistemas de medição, como a temperatura de um cômodo, a complexos sistemas de controle e operações, como o acesso a um ambiente mediante uma identificação.

Atualmente, o conceito de domótica vai além de dispositivos cujos sistemas de controle são independentes e isolados dos demais, passando a dar ênfase na integração de todos os dispositivos em um sistema único, unindo meios eletrônicos com informáticos (PALMA e PINTO, 2007).

Segundo Teza (2002) os sistemas que compõe um sistema de domótica podem ser classificados em três grupos de acordo com o grau de dependência de um sistema de interação humana ou de outros sistemas. Sendo eles:

- Sistemas autônomos – São sistemas que não dependem de outros sistemas para atuarem. Geralmente, controlam dispositivos específicos com funções simples como ligar ou desligar de acordo com ajustes pré-definidos
- Integração de Sistemas – Vários subsistemas integrados a um único controlador. De certa forma, é uma extensão de controle remoto para

diversos dispositivos que operam unicamente da forma para a qual foram projetados para operar.

- Residência Inteligente – o produto pode ser personalizado para atender as necessidades de seu proprietário. Nesse perfil, o sistema assume o papel de gestor e não de controlador.

Nos níveis de integração de Sistemas e Residência Inteligente é necessária a comunicação entre os dispositivos. Entretanto, em sistemas autônomos a comunicação pode ser vista como comandos para desligar ou ligar, enquanto que para sistemas integrados e residências inteligentes a comunicação recebe uma maior relevância, uma vez que são transmitidos dados e informações mais complexas e importantes.

Com isso em vista, muitas tecnologias e protocolos de comunicação foram desenvolvidos ao longo do tempo para aplicações em domótica, como o protocolo X-10 e UPB que permitem controlar iluminação e outros dispositivos através da instalação elétrica existente e INSTEON que utiliza radiofrequência e a rede elétrica. Mas há também padrões e protocolos para comunicação, muito utilizados em domótica, que incorporaram novas funcionalidades aos sistemas: HomePlug, Home PNA, Ethernet, Fire Wire, Wi-Fi, EnOcean, Bluetooth, ZigBee, infravermelho, entre outras tecnologias (MIZUSAKI, 2009).

O protocolo IEEE 802.11, conhecido como WiFi (*Wireless Fidelity* – fidelidade sem fio), é o protocolo de rede sem fio mais conhecido e difundido para utilização em sistemas de domótica. Isto se deve pela facilidade de implementação e baixo custo em relação a outras tecnologias, já que grande parte das residências e ambientes a serem automatizados já possuem estrutura instalada.

A arquitetura do WiFi é composta de vários elementos como: o cliente ou estação (STA), o ponto de acesso (AP), o conjunto básico de serviços (BSS), o sistema de distribuição (DS) e o conjunto estendido de serviços (ESS) (O'HARA e PETRICK, 2004 apud RAMOS e SANTOS, 2015, p.20).

Uma das principais vantagens da utilização de redes WiFi é que possuem uma alta taxa de transmissão, que é necessária em certas aplicações, como *stream* (transmissão em tempo real) de vídeo, além de permitir a utilização de celular e tablet para interface. No entanto, o número de equipamentos utilizando a mesma faixa de frequência (2,4Ghz) influencia diretamente no funcionamento da sua própria rede, de

forma que quanto mais dispositivos maior o tráfego de dados e menores são as taxas de transferências (RAMOS e SANTOS, 2015).

De modo geral, a tecnologia WiFi é sempre uma boa solução para casos de comunicação de alta velocidade e alta confiabilidade. Porém, se for necessária a comunicação entre dois pontos remotos, a tecnologia WiFi se mostra limitada quanto à distância, sendo necessário o uso de equipamentos adicionais que ampliam o alcance da rede ou de equipamentos com melhor eficiência e, consequentemente, maior custo. Nesses termos, tecnologias baseadas em radiofrequência se destacam, entre elas, a LoRa (*Long Range* – Grande Alcance), uma tecnologia de longo alcance e baixo consumo.

A LoRa é uma tecnologia de comunicação por radiofrequência do tipo LPWAN (*Low Power Wide Area Networks* – Rede de grande alcance e baixo consumo) e a LoRaWAN, segundo Junior (2016), é o nome dado ao protocolo que define a arquitetura do sistema, bem como os parâmetros de comunicação usando a tecnologia LoRa. Ainda segundo Junior (2016), a arquitetura da rede LoRaWAN é composta pelos seguintes elementos:

- Módulos: São os *end-points* (pontos finais) ou *end-devices* (dispositivos finais) tais como sensores de temperatura, movimento, *on-off* (ligado ou desligado), leitores de consumo de energia, de gás, de água, entre outros diversos tipos de sensores;
- Gateways: Elementos de conexão entre os módulos e os servidores de rede. Podem receber os dados de milhares de dispositivos, cobrindo um raio estimado de 2 km até 15 km, dependendo das condições de topologia;
- Servidores de rede: São os elementos responsáveis pelo gerenciamento das informações enviadas pelos gateways;
- Servidores de aplicações: São as aplicações que recebem os pacotes dos servidores de rede e, de acordo com a informação, executam uma ou mais ações específicas.

É importante frisar que o uso de uma rede local envolvendo apenas comunicação M2M (*Machine to machine* – Máquina para máquina), ou seja, comunicação entre máquinas sem a leitura humana, não requer a aplicação do

protocolo LoRaWAN, e consequentemente, não se torna necessária a utilização de um *gateway* específico (SILVA NETO, 2017b).

Para implementação de uma rede de comunicação, é fundamental analisar o custo computacional que os subsistemas irão ter. Pois dada a complexidade da operação e da comunicação com a rede, cada dispositivo necessita de um certo desempenho de processamento. Para simplificar e baratear um projeto de domótica, é comumente utilizado um modelo centralizado, de forma que apenas um dispositivo fique com a maior carga computacional. Esse dispositivo central geralmente possui uma interface de comunicação com os dispositivos e outra interface com a rede ethernet, que possibilita uma interface amigável para o usuário, além de serviços como armazenamento de dados, banco de dados, *cloud*, entre outros.

1.1 Objetivo Geral

O objetivo deste trabalho é implementar um sistema de controle de acesso que utilize a comunicação LoRa como método de transmissão de mensagens entre um concentrador e as fechaduras de um ambiente externo com um raio de ação de até 2 quilômetros, permitindo o monitoramento em tempo real do fluxo de acessos a diversos ambientes.

1.2 Objetivos Específicos

Para atingir o objetivo principal, é necessário desenvolver elementos menores que juntos compõem a rede LoRa aplicada a automação de ambientes. Para agregar a função de automatização de ambiente, será elaborado um mecanismo para controle de acessos.

Esse mecanismo irá se comunicar com um dispositivo que será denominado *gateway*, que por sua vez irá se comunicar com uma base de dados através de uma rede WiFi, onde buscará as informações de um usuário. Para isso, neste projeto será necessário:

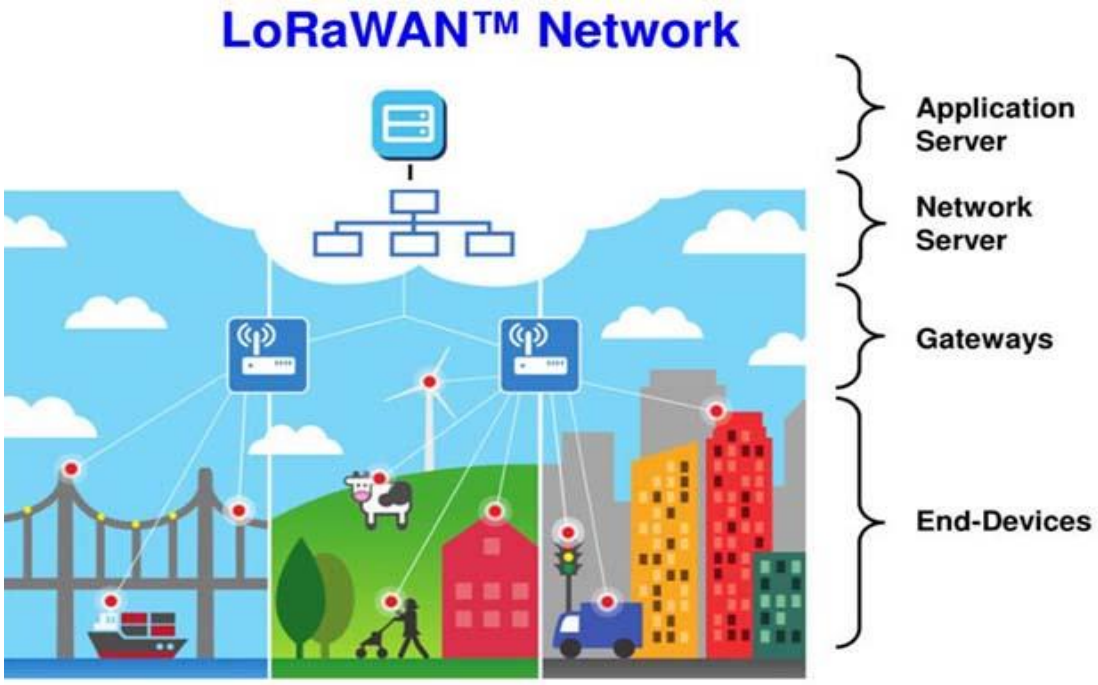
- Desenvolver um dispositivo para controle de acessos com interface de comunicação LoRa;

- Projetar um dispositivo para atuar como *gateway*;
- Integrar um serviço web de base de dados para armazenamento do histórico dos acessos e localização de usuário para autenticação.

1.3 Justificativa

A maior parte dos sistemas de automação residencial e principalmente de internet das coisas se encontra consolidada na tecnologia WiFi, que possui limitações quanto a distância e infraestrutura. Nesses aspectos, automatizar ambientes que contenham dispositivos distantes uns dos outros ou que não disponham de infraestrutura se torna impraticável ou pouco atraente frente outros métodos. Para esse contexto, torna-se necessário o uso de outras tecnologias alternativas. A tecnologia LoRa se mostra promissora para esse contexto, não apenas pela grande distância e baixo consumo, mas também por possibilitar a aplicação de protocolos como o LoRaWAN, que possibilita a comunicação dos dispositivos *end-point* com aplicações remotas através de *gateways*, como é mostrado na Figura 1.

Figura 1- Ilustração de uma rede LoRaWAN.



Fonte: JUNIOR (2016)

2. FUNDAMENTAÇÃO TEÓRICA

A automação residencial no contexto atual, não se limita mais a dispositivos executando tarefas pré-determinadas, mas sim, trata de dispositivos inteligentes comunicando-se entre si e tomando decisões através de informações vindas de outros dispositivos ou de sistemas de interface homem-máquina.

A comunicação de dados independente do protocolo ou padrão podendo ser descrita e analisada através de um modelo. O modelo mais utilizado se chama modelo de referência ISO OSI, ou simplesmente modelo ISO, que é a abreviação de *open systems interconnection*. Nesse modelo, toda a comunicação é modelada através de 7 camadas, sendo elas descritas em ordem crescente: física, enlace de dados, rede, transporte, sessão, apresentação e aplicação.

A comunicação entre dispositivos, com a finalidade de automação residencial, teve início com o X-10 PLC (*Power Line Carrier* – Transmissão sob linhas de Energia Elétrica), que, segundo Teza (2002), foi originalmente desenvolvido nos anos 70 pela Pico Electronics, na Escócia.

Os primeiros produtos baseados nessa tecnologia começaram a circular em 1979. O X-10 é uma linguagem de comunicação que permite a comunicação de dados entre equipamentos elétricos através de linhas existentes de 127 volts e com o cabeamento já existente.

No protocolo X-10, mais de um dispositivo pode ser representado pelo mesmo endereço, de forma que eles respondam igualmente a uma operação simultânea em um limite de até 256 endereços. Analisando no contexto da automação de ambientes, esse protocolo, possui a vantagem de não necessitar da instalação de toda uma infraestrutura, bastando apenas que o ambiente já possua rede elétrica e que os dispositivos a serem automatizados tenham conexão à rede de energia.

Porém, esse protocolo é muito suscetível a ruídos, uma vez que utiliza a própria rede elétrica e é limitada apenas a 256 endereços. Além disso, não é viável utilizar um mesmo endereço para mais de um dispositivo para o contexto deste trabalho, pois cada ponto de controle de acesso não pode ser aberto por ações de um segundo ponto.

Após o início da automação residencial com o sistema X-10, outros protocolos, sistemas e padrões de comunicação foram desenvolvidos. Alguns

específicos para automação residencial e outros com propósitos distintos, porém, por suas características, passaram a ser empregados na automação.

O padrão ethernet é, segundo Mizusaki (2009), um dos padrões mais utilizados para comunicação entre computadores pessoais. Esse padrão utiliza o cabo Cat5, que é o mais comum, constituído por quatro pares de fios trançados para a transmissão de dados, oferecendo alta taxa de transferência de dados e rejeição a ruído.

No entanto, são cabos que conectam todos os dispositivos na rede, ocasionando problemas de mobilidade. Logo, os dispositivos conectados à rede deverão manter suas posições físicas, o que limita a quantidade de dispositivos aptos para se conectarem. Outro ponto importante é o alcance. A rede cabeada tem um alcance máximo de 100 metros, podendo variar conforme a qualidade do cabo.

Para que dispositivos se comuniquem entre si em uma rede local, também chamada de *local area network* (LAN) é necessário um comutador (*switch*) que é um dispositivo centralizado na rede, que gerencia a comunicação entre os dispositivos (MUNDOMAX, 2010).

Além do switch, há também o roteador que é o componente que organiza como os dados vão trafegar pela rede, identificando quando um dispositivo se conecta à rede e fornecendo a esse dispositivo um número de protocolo de internet – *internet protocol* (IP), que é um identificador para o dispositivo dentro da rede (NZN, 2009).

A maior vantagem de se utilizar o padrão ethernet, segundo Mizusaki (2009), é que todos os aparelhos poderiam ser controlados usando o protocolo de controle de transmissão – *Transmission Control Protocol* (TCP), isso é, utilizando a internet, o que garante acesso aos dispositivos em qualquer local do mundo.

Porém, com todas as exigências de infraestrutura, a automação de ambientes comumente não utiliza o padrão ethernet. Porém, se a rigidez da rede for algo a ser contornado, assim como pouca exigência quanto ao alcance, o padrão IEEE 802.11 surge como uma alternativa atrativa.

O padrão IEEE 802.11, popularmente chamado de WiFi, foi criado para substituir as redes cabeadas. Esse protocolo, de acordo com Ramos e Santos (2015), se encontra no grupo das redes sem fio, juntamente com outras redes famosas tais como a ZigBee e Bluetooth.

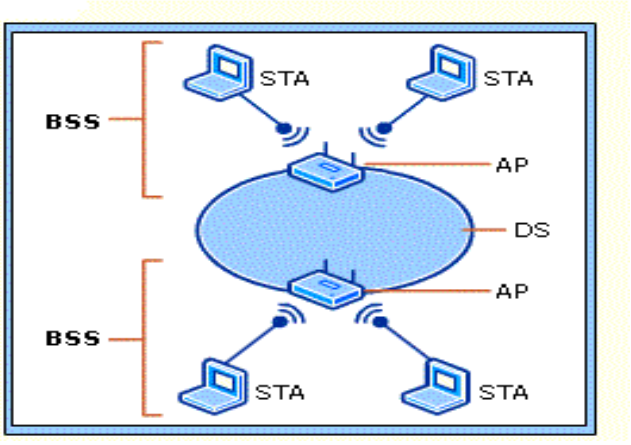
A arquitetura de uma rede WiFi é composta por elementos tais como: o cliente ou estação (STA), o ponto de acesso (AP), o conjunto básico de serviços (BSS), o sistema de distribuição (DS) e o conjunto estendido de serviços (ESS). Esses elementos são mostrados na Figura 2.

O padrão WiFi traz consigo todas as vantagens das redes cabeadas, mas com o diferencial de não necessitar de cabos para conectar os dispositivos, além de permitir a conexão de *tablets, smartphones* e outros dispositivos que melhoram a interação com o sistema.

No entanto, o alcance dessa rede é limitado. Segundo Morimoto (2011), o padrão 802.11n tem um alcance máximo de 250 metros em campo aberto e de até 70 metros em ambientes fechados. Esse alcance é suficiente para grande parte das aplicações, mas se for necessário um maior alcance, é possível utilizar repetidores de sinal.

Caso a distância seja suficientemente grande a ponto de inviabilizar uma rede LAN, ainda é possível conectar dois dispositivos através da internet, mas, para isso, ambos os locais deverão contar com conexão à internet.

Figura 2 - Elementos da arquitetura de uma rede Wifi



Fonte: VASCONCELOS; ALVES (2015)

Havendo a necessidade de comunicação entre muitos dispositivos que possam estar a uma grande distância entre si e sabendo que é um pequeno volume de informações a serem transmitidas, a conexão à rede WiFi deixa de apresentar um bom custo benefício já que para isso, seriam necessários à utilização de repetidores de sinal ou equipamentos com maior potência para transmissão em cada ponto a ser

conectado. Neste contexto outras redes baseadas na comunicação via radiofrequência passam a ser mais interessantes. Esse é o caso da tecnologia LoRa cujo nome deriva do termo *longo alcance*, em inglês: *long range*.

A tecnologia de rede LoRa é do tipo rede de grande alcance e baixo consumo – *low power wide área network* (LPWAN) que permite conectar pontos distantes com um baixo consumo de energia e de baixa largura de banda (*bandwidth)* fornecendo uma comunicação bidirecional.

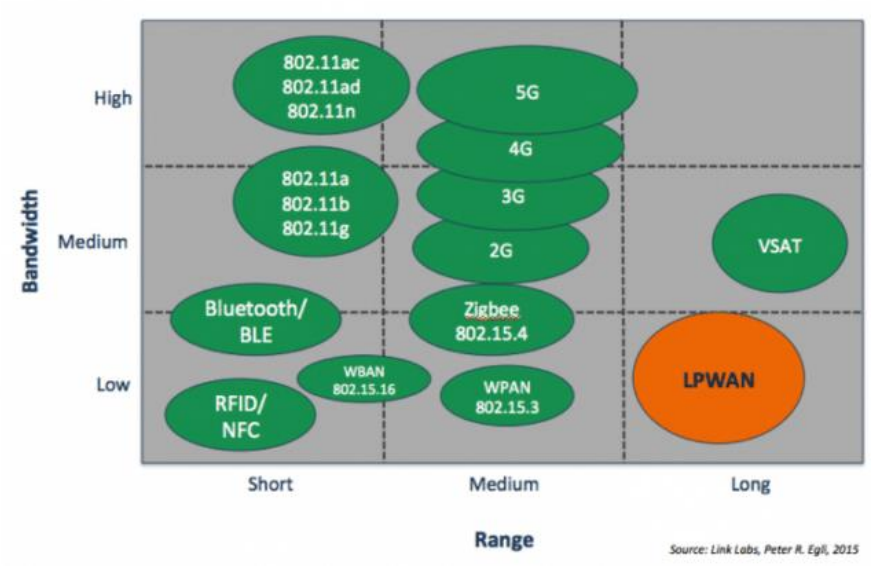
A largura de banda é a faixa de valores que um dado sistema de telecomunicações utiliza para transmissão relacionando-se com a taxa de transmissão de dados, uma breve comparação com outras tecnologias pode ser vista na Figura 3.

Para a implementação de protocolos como o LoRaWAN é necessária a utilização de *gateways* específicos. O *gateway* é compreendido, segundo Moreschi (2011), como o nó que distribui o tráfego de uma estação de trabalho a outro segmento de rede.

De uma forma simples, o *gateway* é o elemento que age como intermediário de um dispositivo e uma rede, pois ambos podem operar com protocolos diferentes sendo necessário algum dispositivo para traduzir essa comunicação. Assim sendo, comumente em uma rede com topologia estrela, os dispositivos se comunicam com o *gateway* que organiza a comunicação com outras redes, como é o caso de uma rede de computadores locais acessando a internet (JUNIOR, 2016).

Os dispositivos baseados na tecnologia LoRa podem se comunicar entre si e com o(s) *gateway*(s), que, por sua vez, realiza a comunicação com servidores web, que recebem, armazenam, processam e transmitem mensagens e permitem uma interface através de aplicativos (JUNIOR, 2016).

Figura 3 - Comparação entre as tecnologias de comunicação.



Fonte: MELO (2017)

Na camada física, que trata da transmissão de bits por um canal físico, tem-se a tecnologia LoRa, que faz uso do hardware produzido pela empresa Semtech, sendo eles os circuitos integrados sx1301, sx1272 e sx1276, esses circuitos são os módulos responsáveis por converter os bits de dados em sinais de radiofrequência.

Com a tecnologia LoRa, teoricamente, um *gateway* pode receber requisições de um número ilimitado de dispositivos. Vale ressaltar que, se a comunicação for entre dois dispositivos, não é necessário o *gateway*, que é utilizado na topologia estrela como um centralizador (SILVA NETO, 2017a).

É importante ressaltar que a LoRa opera nas seguintes faixas: rádio amador, que é de 433MHz, e também na faixa de frequência ISM (*Industrial – Scientific – medical*), porém, apenas as faixas ISM são reguladas pela ANATEL (ANATEL, 2019). As faixas de frequência ISM são as faixas livres, onde qualquer equipamento poderá realizar transmissões sem o licenciamento de órgãos de fiscalização desde que respeitem a legislação vigente que irá determinar os limites de potência e os tipos de modulação. Quanto à transmissão LoRa, as faixas ISM são, em sua grande maioria, compreendidas entre as frequências de 890 MHz até 928 MHz. É importante ressaltar que cada país possui uma resolução própria sobre a regulação dessas frequências. No Brasil, as faixas de frequência ISM que se adequam na transmissão LoRa vão de 915 MHz até 928 MHz (ANATEL, 2018).

Os dispositivos importados geralmente vêm configurados para operar de acordo com as normas americanas, que são de 902 MHz a 928MHz, que é parecida com a faixa ISM do Brasil, exceto por um trecho da faixa de frequência situada entre 907,5 MHz até 915 MHz, que é destinada a telefonia, e, portanto, deve se configurar os dispositivos para pularem essa faixa. As faixas de frequência não licenciadas no Brasil que seguem a Resolução n° 680/2017 (Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita) são as seguintes: 902-907,5 MHz e 915-928 MHz (ANATEL, 2019).

O método mais prático para realizar esta configuração é utilizar dispositivos para trabalharem na faixa de frequência ISM da Austrália, que é idêntica à do Brasil e que já está pré-configurado em diversas bibliotecas criadas para estabelecer a comunicação através de LoRa (JUNIOR, 2017).

É importante ressaltar que a faixa de frequência ISM é chamada livre, porém equipamentos que operem nessa faixa de frequência devem obedecer às resoluções da ANATEL (Agência Nacional de Telecomunicações), e, portanto, devem ser homologados ou certificados junto à ANATEL.

A tecnologia LoRa está sob duas patentes: EP2763321 de 2013 e US7791415 de 2008. Foi inicialmente desenvolvida pela Cycleo, em Grenoble na França, e depois comprada pela Semtech em 2012 (PRAJZLER, 2015).

A patente EP2766321 intitulada "*Low Power Long Range Transmitter*" sob o número de publicação: EP2763321 A1, foi publicada em 6 de agosto de 2014, também publicada como CN103973626A, US9252834 e US20140219329, pertence atualmente a Semtech Comporation e foi inventada por: Olivier Bernard André Seller e Nicolas Sornin (SELLER e SORNIN, 2014).

Já a patente US7791415, é intitulada "*Fractional –n synthesized chirp generator*", sob o número de aplicação: USS20080122635 20080516. Inventada por HornBuckle Craig. Também foi publicada como: EP2153522, EP213522, US2008284531, WO2008144579 e WO2008144579 (HORNBUCKLE, 2010).

A modulação da tecnologia LoRa é do tipo pulsos de radar comprimidos de alta intensidade com espalhamento no espectro – *compressed high intensity radar pulse spread spectrum* (CSS). Esse tipo de modulação é utilizado quando múltiplos usuários têm que compartilhar a mesma banda de frequências, por exemplo, telefones celulares, centrais de cooperativas de táxis e comunicações de controle de tráfego aéreo. A modulação faz com que a transmissão ocupe todo o espectro, mas ainda permitindo mais de um usuário transmitir simultaneamente (JUNIOR, 2016).

Existem duas técnicas básicas de espalhamento espectral: sequenciamento direto - *Direct Sequence* (DS) e salto de frequência - *Frequency Hopping* (FH), além de algumas técnicas híbridas. Com o espalhamento por frequência direta, o sinal é multiplicado por um sinal conhecido e de uma largura de banda muito maior. Já com o espalhamento por salto em frequência, a frequência central do sinal transmitido sofre uma variação pseudoaleatória, saltando entre as diversas frequências do espectro alocado (JUNIOR, 2017).

As técnicas de espalhamento espectral possuem algumas vantagens, tais como: maior tolerância a interferência; baixa probabilidade de detecção ou interceptação; maior tolerância a multipercursos e maior capacidade de alcance (HAYKIN e MOHER, 2008). Com esse tipo de modulação, obtém-se maior alcance pela diminuição do pacote de dados (JUNIOR, 2017).

Na modulação, o fator de espalhamento - *spreading fator* (SF) é programável, podendo ser: 7, 8, 9, 10, 11 e 12. Esse fator determina o tempo em que ocorre a transmissão, sendo que a informação será a mesma. Com um SF programado para 7 a transmissão será rápida, enquanto que com SF igual a 12 a transmissão será a mais lenta. A largura de banda - *Band Width* (BW) é ajustável nos valores: 125, 250 e 500 KHz. Quanto menor a BW, mais sensibilidade a interferências e mais tempo para transmissão (JUNIOR, 2017).

Segundo Junior (2016), quanto maior o alcance, menor será a carga útil - *payload*, que é a informação útil a ser transmitida, ou seja, sem as informações de endereçamento. Considerando um *payload* de 11 bytes, a taxa de transmissão é de 976 bps (bits por segundo) e a BW é de 125 KHz com *spreading factor* (SF) igual a 10. Já se a rede for configurada para ter um alcance menor, com um SF igual a 8 e BW de 500 KHz, é obtido uma taxa de transmissão de 12500 bps com um *payload* máximo de 242 bytes.

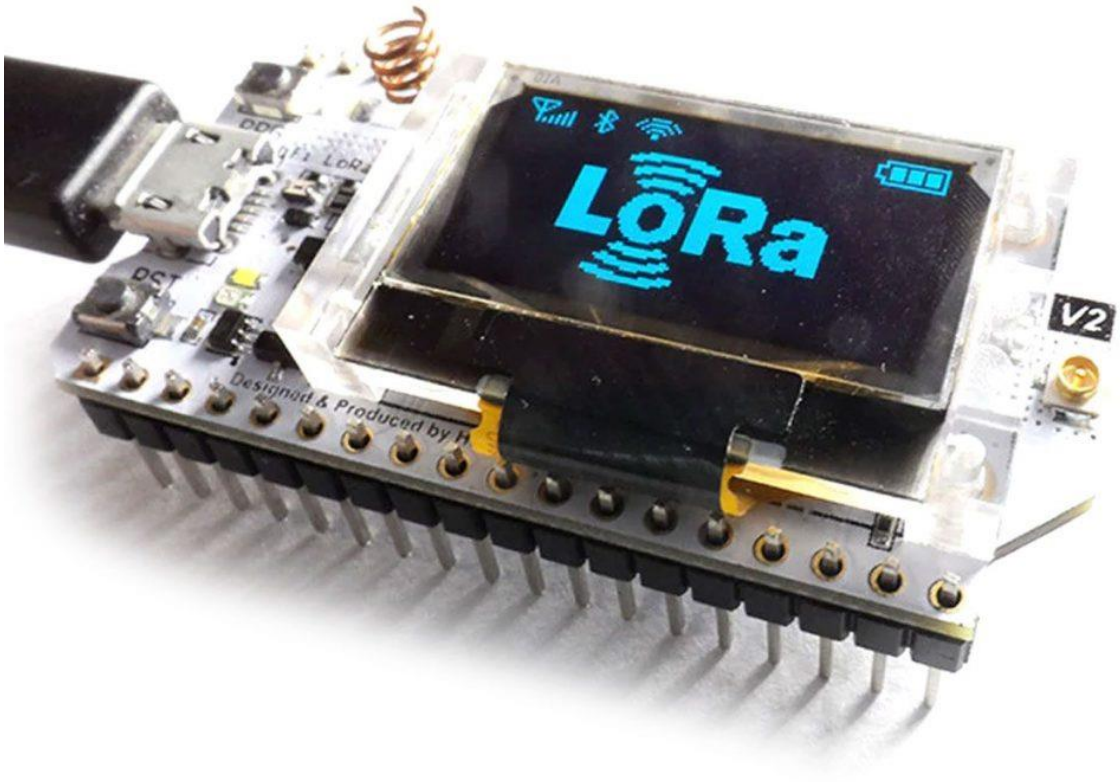
De acordo com esses parâmetros, fica evidente que a tecnologia LoRa não é compatível com aplicações que requerem transmissão de grandes volumes de dados, como imagens, voz, áudio, dentre outras. Porém, para troca de informações entre máquinas – *machine to machine* (M2M), ela apresenta um rendimento satisfatório.

Para se utilizar o padrão LoRa, é necessário utilizar componentes que possuam suporte a esse padrão. Atualmente, há diversos módulos no mercado que implementam esse padrão, a saber, o microchip RN2903, que integra um microcontrolador PIC com suporte a comunicação LoRa, o RFM95W, desenvolvido pela empresa HOPERF, e há também os módulos baseados no transceptor sx1278 da Semtech, que são o ESP32, o Atmel Atmega 32u4 – Feather 32u4, o Atmel ATSAMD21G18 – Feather M0, o STM – ST B-L072Z-LRWAN1 STM32 LoRaWAN Discovery, Adafruit LoRa breakout e LoRa Dragino Shield, entre outros (SILVA NETO, 2017a),

O ESP32, segundo Minatel (2015), é um Sistema em um chip - *System on Chip* (*SoC*), que integra uma CPU de dois núcleos – *dual core* Tensilica L108, WiFi, Bluetooth de baixo consumo - *Bluetooth Low Energy* (BLE) e uma memória RAM de aproximadamente 400 Kb. Esse SoC pode ser configurado para implementar o protocolo LoRaWAN, com um baixo custo.

O ESP32 é um componente consideravelmente novo, tendo sido lançado no mercado no dia 6 de setembro de 2016 pela empresa Chinesa Epressif (ESPRESSIF, 2016). O módulo mais comum que integra o ESP32 com o sx1278 para fornecer a comunicação no padrão LoRa é o apresentado na Figura 4, que além dos recursos já supracitados, integra um display de diodo orgânico emissor de luz – *organic light-emitting diode* (OLED) azul de 0,96 polegadas (2,4384 centímetros).

Figura 4 - Módulo LoRa baseado no ESP32.



Fonte: AISLAN (2021)

Com esse módulo, implementam-se os dispositivos *end-points*, que são aqueles dispositivos que possuem periféricos que estarão exercendo medidas ou atuações e se comunicando com o elemento centralizador da rede LoRa.

O elemento centralizador da rede LoRa, requer poder computacional para atender aos chamados dos dispositivos da rede. Com o módulo LoRa baseado no ESP32, um dispositivo de considerável poder computacional capaz de estabelecer comunicação com a rede LoRa e com o WiFi, é aceitável o seu uso como um centralizador da rede LoRa que permite a comunicação entre as redes LoRa e WiFi, possibilitando o armazenamento de dados coletados pelos *end-points* em servidores e serviços de base de dados online (SILVA NETO, 2017).

Os servidores são computadores poderosos, utilizados para centralizar um volume de informações, segundo Tanenbaum (2011). Os servidores se estabelecem em um arranjo chamado modelo cliente-servidor, onde um dispositivo na rede (cliente)

faz uma requisição ao servidor, que a processa com base nas informações contidas em suas bases de dados e devolve uma mensagem para o cliente.

Ainda segundo Tanenbaum (2011), esse arranjo cliente-servidor é muito empregado nas aplicações web, onde a resposta a um cliente consiste em uma página web, como por exemplo, um navegador solicitando uma página web em um fórum. Porém, a resposta de um servidor não precisa necessariamente ser uma página web.

Por exemplo, em um sistema de controle de acessos, os dispositivos que controlam uma fechadura podem conter recursos limitados para armazenar todos os dados dos usuários e, portanto, precisam acessar essas informações em um servidor a fim de garantir o acesso ou não.

O servidor se baseia em uma base de dados em tempo real – *real time database* que armazenará as identificações de cada usuário para realização das buscas por parte do *gateway* e também armazenará todos os registros de autenticação de usuários, permitindo um histórico de acesso dos usuários ao local da tranca eletrônica.

Nos dispositivos que controlam a fechadura, deve-se ter um mecanismo que identifique o usuário e envie para o servidor sua identificação, a fim de se checar a autorização de acesso.

Há muitos mecanismos que permitem a identificação de usuários ou objetos, como códigos de barra, biometria, cartões magnéticos, leitura de íris, etiquetas magnéticas, dentre outros. Todos os mecanismos apresentam vantagens e desvantagens, sendo necessário avaliar a aplicação para escolher o que melhor se adapta ao problema em questão.

Para uma aplicação de controle de acessos, mecanismos de leitura biométrica ou de íris garantem maior segurança contra fraudes, no entanto, exigem maiores custos. Já as etiquetas de identificação por radiofrequência - *Radio Frequency Identification* (RFID), podem garantir uma segurança mediana por uma faixa de custos muito atrativa.

O RFID de acordo com Miguel (2011), pertence ao grupo de tecnologias de Coleta Automatizada de dados - *Automated Data Collection* (ADC), juntamente com os leitores de códigos de barras e leitores biométricos.

Essa tecnologia surgiu em 1980, como uma solução para os sistemas de rastreamento e controle de acesso. Em 1999, o Instituto de Tecnologia Massachusetts

- *Massachusetts Institute of Technology* (MIT), juntamente com outros centros de pesquisa, desenvolveu estudos para elaborar uma arquitetura baseada na tecnologia de radiofrequência para servir como referência no desenvolvimento de novas aplicações de rastreamento e localização de produtos.

Desse estudo nasceu o Código Eletrônico de Produtos - *Eletronic Product Code* (EPC), que definiu a arquitetura de identificação de produtos que utilizavam os recursos proporcionados pelos sinais de radiofrequência, posteriormente chamado de RFID (PINHEIRO, 2004).

Existem muitos tipos de RFID, cada um com diferentes características, mas todos podem ser classificados em dois tipos: RFID passivo e RFID ativo. O RFID passivo não tem a necessidade de fontes, pilhas ou baterias para funcionar, toda energia que precisa vem na forma de ondas de rádio do leitor. Já os ativos, precisam de uma fonte para alimentá-los (TANENBAUM, 2011).

As etiquetas RFID ou *tags* RFID passivas são compostas por um circuito muito simples, constituído por uma antena embutida e um microchip, e assumem diversos formatos, como botões, cartões, chaveiros, adesivos, entre outros, como pode ser visto na Figura 5.

Figura 5 - Diversas tags RFID.

Fonte: CRIACORE (CA. 2022)

Segundo Tanenbaum (2011), um tipo comum de RFID é o RFID de frequência ultra alta - *Ultra-High-Frequency* RFID (UHF RFID) que pode alcançar até 15 metros, dependendo do objeto e de outros fatores a serem avaliados (DIAS e DE PIERI, 2019). Os leitores enviam sinais na banda de 902 a 928 MHZ nos Estados Unidos. As etiquetas RFID se comunicam em uma distância de poucos metros, mudando o modo como refletem os sinais do leitor, que é capaz de apanhar essas reflexões. Este modo de operação é chamado refletor ou *backscatter*.

Outro tipo popular é o RFID de alta frequência – *high frequency RFID* (HF RFID), que opera a 13,56 MHz. Seu alcance é limitado, chegando até a 2 metros, pois seus mecanismos físicos são baseados em indução.

De acordo com Tanenbaum (2011), os leitores de RFID precisam solucionar de alguma forma o problema de lidar com várias etiquetas dentro do alcance de leitura. Pois, se duas ou mais etiquetas RFID, ao escutarem um leitor, o respondem imediatamente, haverá colisão de informações.

Para tanto, a solução encontrada é fazer com que cada etiqueta espere por um pequeno intervalo aleatório antes de responder com sua identificação, permitindo que o leitor focalize etiquetas individuais e as interrogue mais a fundo.

Outro problema apresentado por Tanenbaum (2011) é a falta de segurança, pois se uma etiqueta pode ser lida por um policial em uma fronteira, nada impede que esta etiqueta seja lida por outra pessoa mal intencionada.

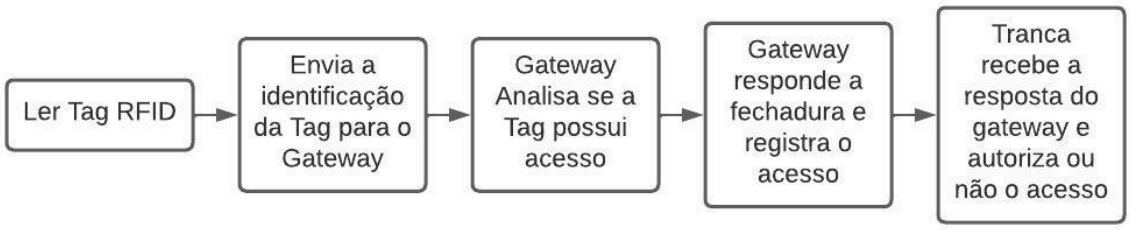
Segundo Miguel (2011), os maiores fabricantes de RFID oferecem sistemas próprios de RFID, o que resulta em diferentes características quanto ao protocolo de comunicação RFID, gerando incompatibilidades entre sistemas. Muitas organizações estão envolvidas na tentativa de padronização destes protocolos, entre elas, as principais são: a Organização Internacional para padronização - *International Organization for Standardization* (ISO) e a EPC Global.

3. METODOLOGIA

Para a produção deste projeto, deve-se considerar dois blocos distintos que trabalharão juntos para permitir o funcionamento pleno. Sendo eles o *gateway* e a tranca. Ambos os blocos usam o SOC Heltec ESP 32 como elemento central, sendo que o *gateway* utiliza apenas o SOC, sem acrescentar nenhum periférico, enquanto a tranca utiliza os periféricos de leitor RFID e circuito para comutação do relé. Ambos usam fontes de alimentação externa do tipo USB comum, podendo ser alimentados por fontes de celulares, computadores, power bank ou quaisquer outros dispositivos que forneçam alimentação via USB. No entanto, a tranca ainda necessita de uma fonte de alimentação extra de 12 volts capaz de fornecer ao menos 3 amperes para a comutação da tranca eletromecânica.

Com o sistema alimentado, pode-se considerar o funcionamento do sistema conforme o diagrama apresentado na Figura 6.

Figura 6 Diagrama de blocos



Fonte: Autoria Própria (2022)

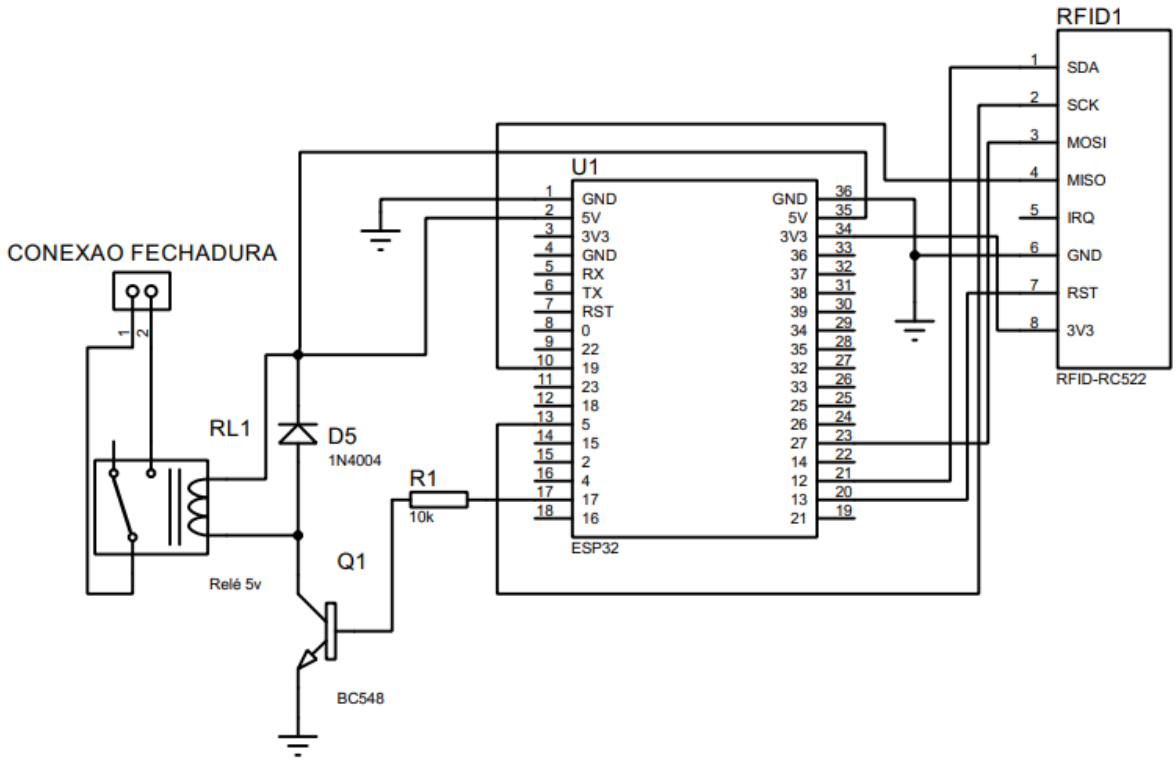
Todo o sistema fica em *Stand by* até o momento em que a tranca realiza a leitura de uma tag RFID, dando início ao processo com o envio da identificação lida da tag para o gateway através de uma transmissão via LoRa para o *gateway*. Após o envio da mensagem, a tranca exibe a mensagem de “aguarde” no display e passa a aguardar uma resposta do *gateway*. O *gateway*, ao receber uma mensagem contendo a identificação da tranca que enviou e o código da tag que foi lido, inicia um acesso à base de dados Firebase, através de uma rede WiFi, e passa a analisar, no nó de usuários cadastrados daquela tranca, se está cadastrada a identificação que a tranca enviou. Ao confirmar se há ou não cadastro do código de identificação da tag, o *gateway* responde para a tranca uma mensagem indicando se pode ou não liberar o acesso. Após o envio da mensagem, o *gateway* acessa um servidor NTP para adquirir

o horário naquele instante e grava junto à base de dados no nó referente àquela tranca se houve ou não a liberação do acesso, o horário e a identificação de quem acessou.

3.1 Leitura da Tag RFID

Dos dois blocos principais, a tranca eletrônica é o único que exigiu acréscimo de periféricos e desenvolvimento de circuito eletrônico conforme o da Figura 7:

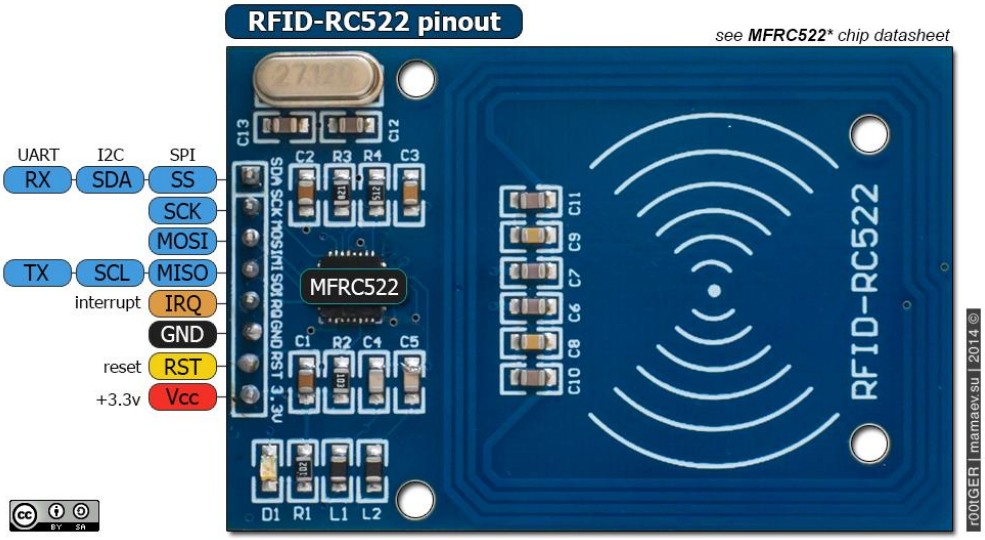
Figura 7 Esquemático da Tranca



Fonte: Autoria Própria (2022)

Nesse circuito há o leitor RFID (RFID1), um relé com tensão de controle de 5 V (RL1), circuito de comutação do relé que é composto por um transistor BC548 (Q1), um resistor de 10 kilo-ohm (R1), um diodo 1N4004 que exerce a função de roda livre (D5) e alimentação externa de 12 V e 3 A. Deve-se notar que há um bloco de conexão externa, pois a tranca possui um borne de duas conexões para conectarem a saída do relé com o circuito externo. O elemento que inicia toda a cadeia de processos é o leitor RFID do modelo MFRC522, que apresenta uma ótima relação custo/benefício e uma grande gama de bibliotecas que facilitam no desenvolvimento. O leitor MFRC522 pode ser visto na Figura 8.

Figura 8: Leitor MFRC522.



Fonte: MICROCONTROLLERSLAB (2016)

Esse leitor RFID utiliza o protocolo SPI para comunicação com microcontroladores e periféricos. Portanto, os pinos MOSI e MISO são utilizados para transmitir do *Master* para o *Slave* e do *Slave* para o *Master*, respectivamente. Já o pino SS serve para selecionar qual *Slave* irá transmitir e o SCK serve para sincronizar transmissor com receptor. O ESP 32 da Heltec já possui os pinos dedicados para comunicação SPI interconectados ao circuito integrado SX1276, o circuito que realiza a modulação LoRa. Com isso, é necessário configurar um barramento SPI tendo o ESP 32 como mestre e os módulos SX1276 e o MFRC522 como escravos. Para selecionar qual dos escravos irá utilizar o barramento, o pino 12 do ESP 32 serve como controle do módulo MFRC522 e o pino 18 para controle do SX1276.

3.2 Enviando dados para o *Gateway*

Após a leitura da *tag* RFID, é obtido um valor numérico no formato de *String* que corresponde ao código de identificação da *tag*. O processo a seguir é o envio desse código para o gateway analisar se possui permissão de acesso.

O SOC da Heltec possui um display OLED embutido para facilitar a interação com o usuário. Ao entrar no processo de validação da *tag*, a tranca irá exibir a mensagem de “aguarde” para o usuário e irá iniciar a transmissão da mensagem via

LoRa para o *gateway*. Essa mensagem é composta pelos seguintes campos: destino, origem, contagem, tamanho da mensagem, mensagem. Conforme é visto na Tabela1.

Tabela 1: Composição da Mensagem Transmitida em LoRa.

Destino	Origem	Contagem	Tamanho da Mensagem	Mensagem
0x00	0XFF	inteiro	tamanho em caracteres	código da tag RFID

Fonte: Autoria própria (2022)

Note que os dois primeiros campos são de endereçamento, sendo o primeiro de destino, que será do *gateway*, e o segundo de origem, que é a tranca que está realizando a transmissão. Existem 256 endereços possíveis, porém o último endereço (0xFF) é dedicado para abertura de todas as portas, para o caso de uma emergência.

A topologia da rede é do tipo *mesh* ou na terminologia em português: malha, onde todos podem se comunicar entre si, de forma que uma mensagem enviada pelo *gateway* ou pela tranca é recebida por todas as trancas e *gateways* no raio de alcance. Uma vez recebida a mensagem, cada dispositivo irá analisar se a mensagem é endereçada para ele, caso não seja, irá descartá-la. Na prática, a topologia se assemelha ao tipo estrela pois, mesmo recebendo a mensagem de outras fechaduras, cada tranca irá apenas receber mensagens enviadas pelo *gateway*, que se torna o elemento central da topologia. Há uma opção de desenvolver o sistema através de uma topologia mesh (malha), o que foge do escopo deste projeto.

3.3 Validação do Acesso

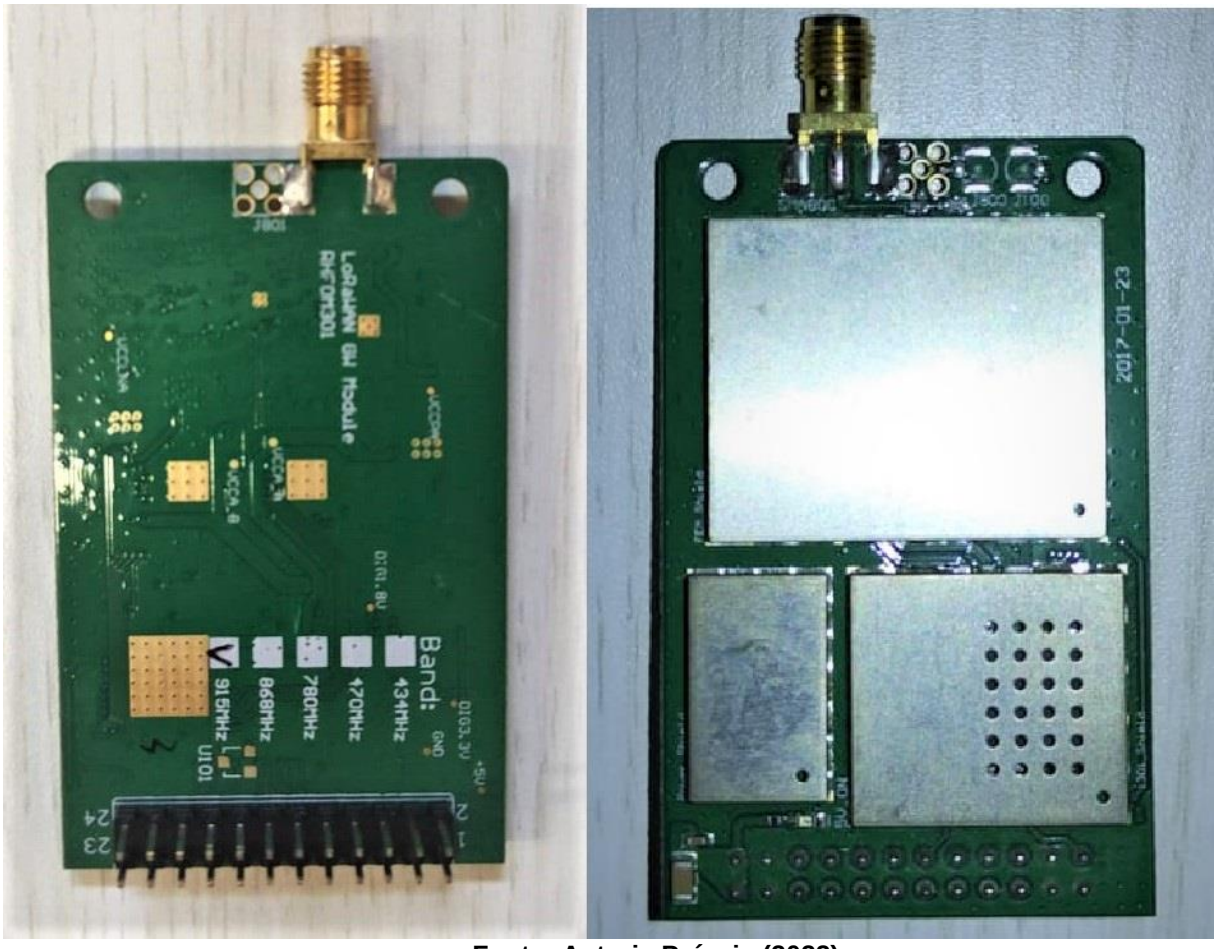
O *gateway* é o elemento central da comunicação do sistema, sendo o responsável por realizar a troca de mensagens por LoRa e também por ler e armazenar informações em uma base de dados através de comunicação WiFi. Esse elemento requer considerável poder de processamento, uma vez que é necessário para cumprir os protocolos de comunicação na rede WiFi.

Para a função de *gateway* neste trabalho, cogitou-se em duas opções: módulo RHF0M301 e ESP 32. O módulo RHF0M301 da RISINGHF é baseado no circuito integrado SX1301, que é o modulador projetado para atender a até 8 canais simultâneos de comunicação LoRa. No entanto, esse módulo requer um elemento adicional para realizar o processamento dos dados e a comunicação com a rede WiFi,

esse elemento é o Raspberry Pi. Nessa configuração, o Raspberry Pi passa a ser o elemento central do *gateway*, pois ele irá realizar as comunicações com a rede WiFi, processar as mensagens, ler e gravar na base de dados e implementar o protocolo LoRaWAN, o que abre um leque de recursos disponíveis gratuitamente na rede, como por exemplo, o thethingsnetwork.org. Enquanto o módulo RHF0310 passa a ser um periférico responsável apenas pela comunicação LoRa. Já a segunda opção de utilizar um ESP 32 para a função de *gateway* foi a optada para este trabalho e será melhor explanada a diante.

Para o funcionamento correto do *gateway* baseado no Raspberry Pi e RHF0M310, é necessária uma placa que consiga adaptar a conexão dos pinos de ambos, além de fornecer uma fonte de alimentação dedicada apenas ao módulo LoRa. Pois a corrente que ele pode consumir supera aquela fornecida pelos terminais do Raspberry Pi. A Figura 10 mostra o módulo RHF0M310; a Figura 11 mostra o adaptador necessário.

Figura 9 Módulo Gateway de 8 canais.



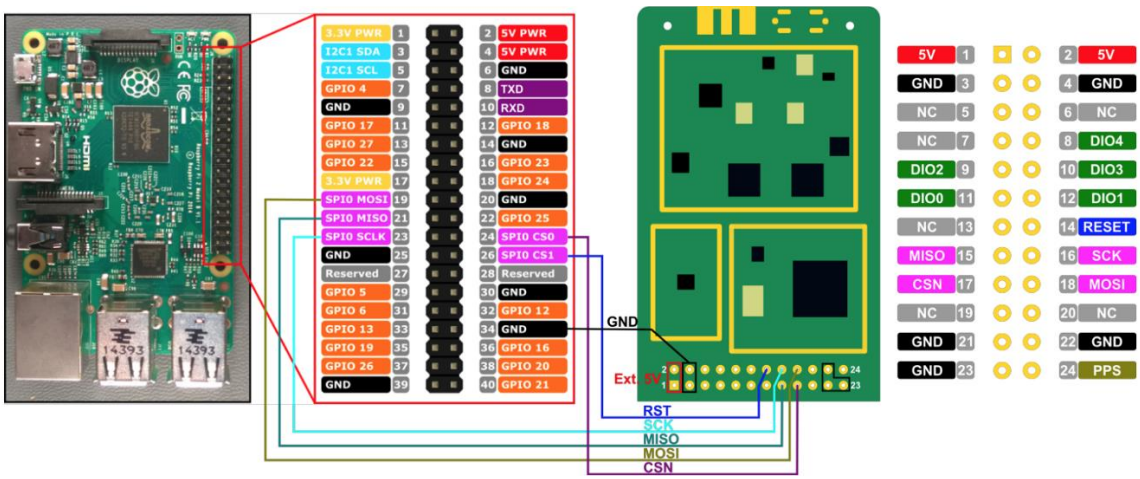
Fonte: Autoria Própria (2022)

Figura 10 Adaptador Necessário

Fonte: Autoria Própria (2022)

Na Figura 12, observa-se a ligação correta entre o Raspberry Pi e o módulo LoRa. Note que os pinos utilizados são aqueles dedicados para a comunicação SPI, onde o pino RST serve para reset do gateway, o pino SCK serve para sincronia da frequência de processamento conhecida (*clock*), Miso é por onde trafega a informação do escravo para o mestre, Mosi é por onde trafega a informação do mestre para o escravo e CSN é utilizado para selecionar o escravo que irá se comunicar com o mestre no barramento.

Figura 11 Ligação dos pinos

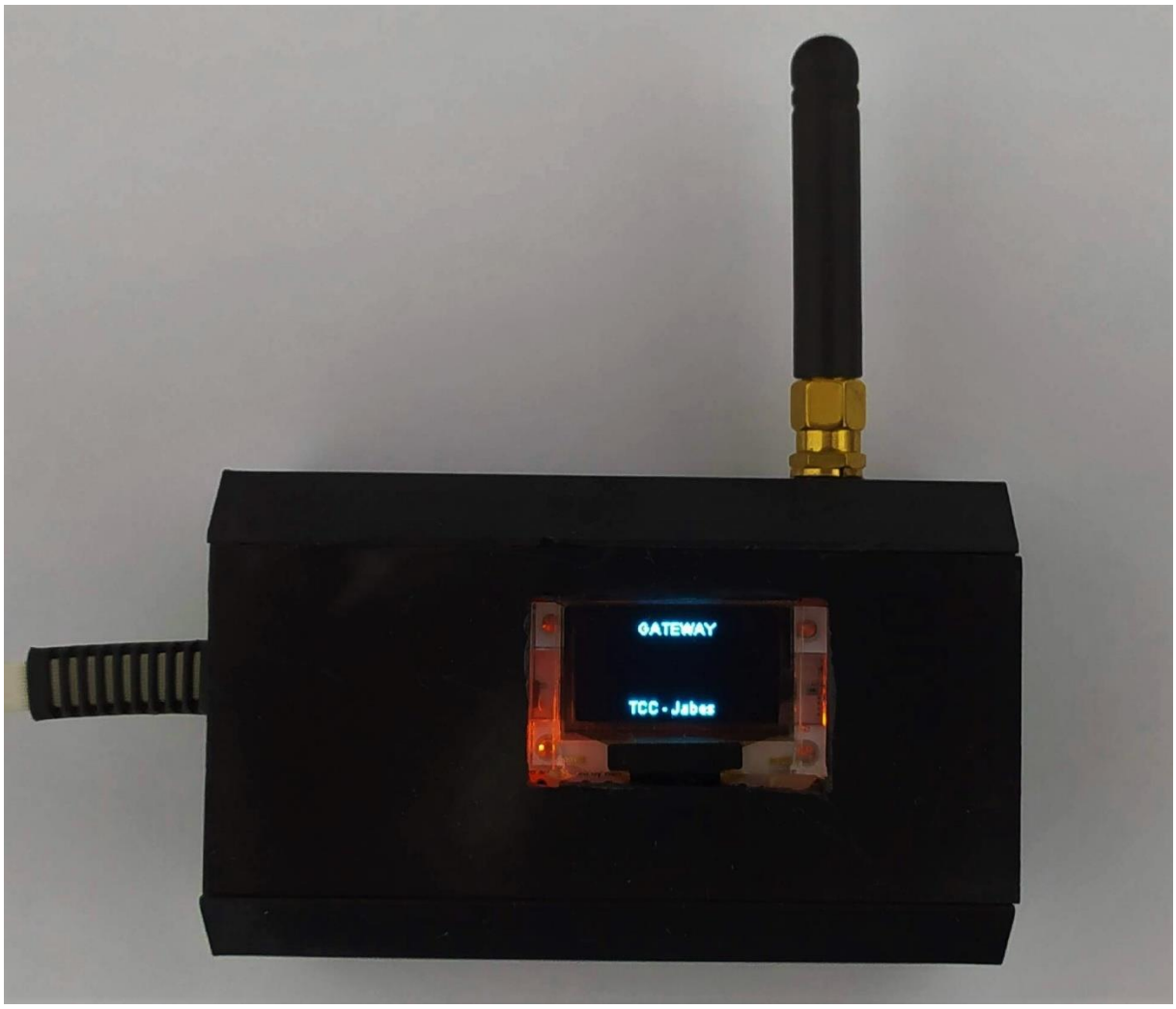


Fonte: BANKOLE (2018)

Outra opção é o uso de um transmissor LoRa baseado no ESP 32, que é de fácil implementação, porém não permite a integração com recursos da internet como faz o *gateway* baseado no Raspberry Pi. Dessa forma, a exibição dos dados e toda a interação com o sistema deverá ser feita manualmente.

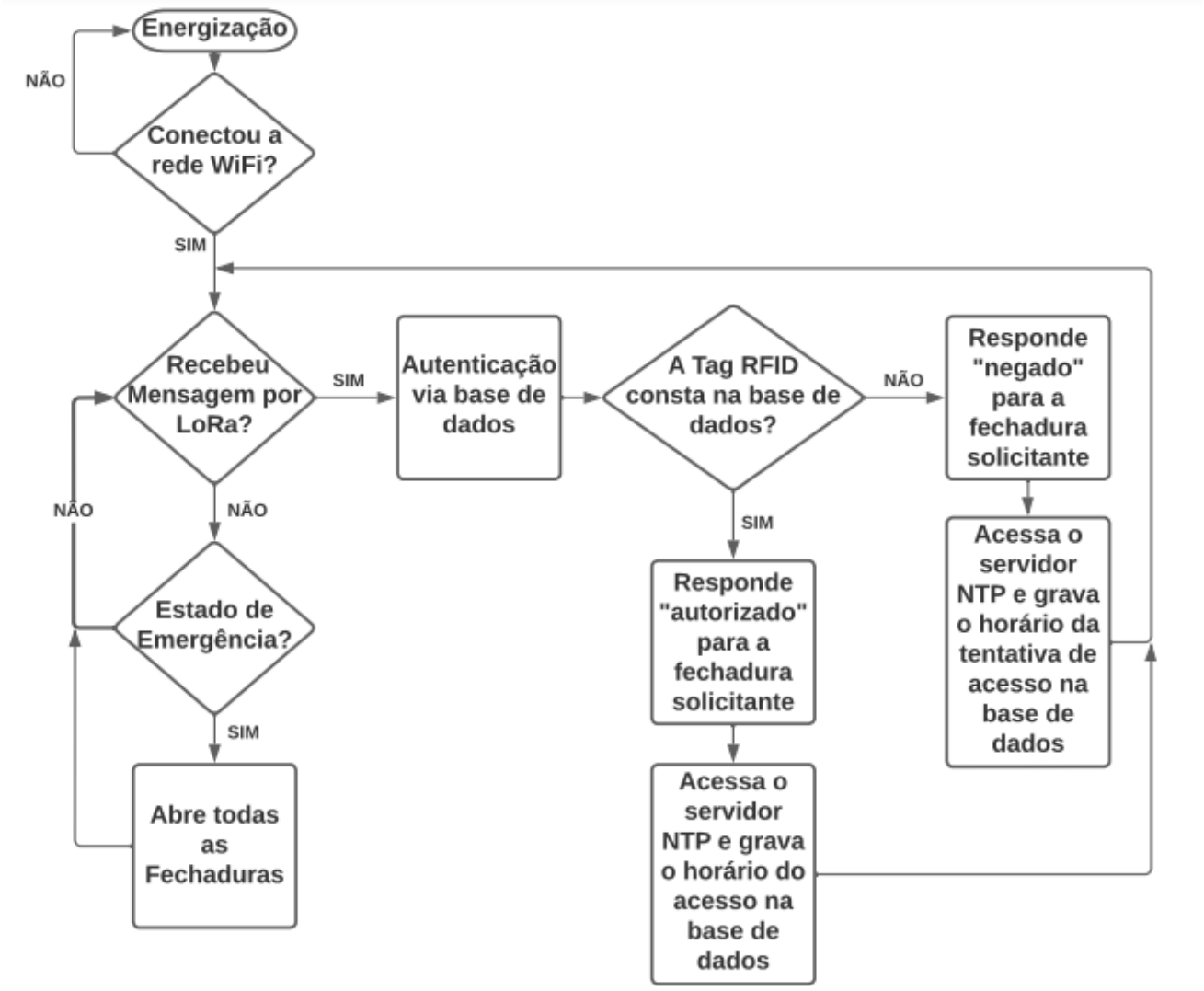
Para o *gateway* deste projeto foi optado pelo módulo ESP 32 LoRa da Heltec, que já possui o hardware necessário para comunicação LoRa e acesso à internet através da rede WiFi. O *gateway* baseado no ESP 32 pode ser visto na Figura 13 e o fluxograma da programação do *gateway* pode ser visto na Figura 14.

Figura 12 *Gateway* baseado no ESP 32



Fonte: Autoria Própria (2022)

Figura 13 Fluxograma de funcionamento do gateway



Fonte: Autoria Própria (2022)

Quando o *gateway* é energizado, ele busca se conectar a uma rede WiFi programada previamente, ficando preso neste processo até que uma conexão seja estabelecida.

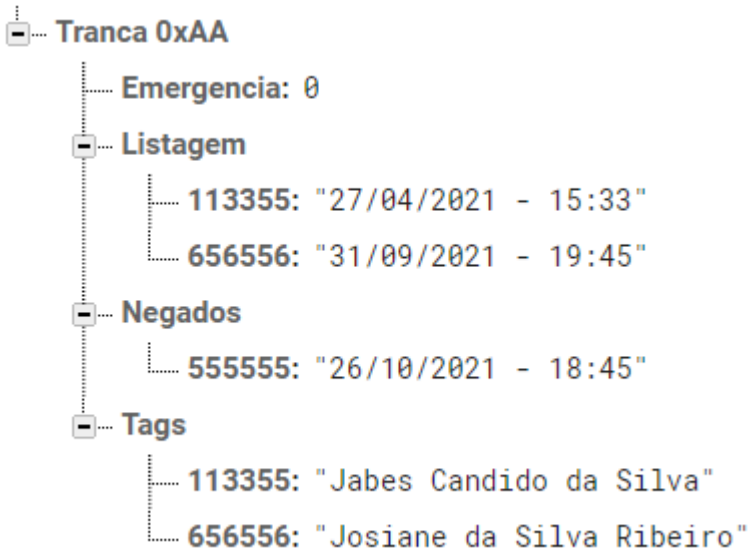
No instante em que se conecta à rede WiFi, ele passa a executar um *loop*, aguardando a recepção de alguma mensagem enviada via LoRa ou algum comando de abertura de emergência de todas as portas. O comando de abertura de todas as portas nada mais é do que a transmissão de uma mensagem com destinatário 0xFF, que é o endereço comum a todas as trancas. Para a abertura de emergência, basta realizar a alteração de uma variável na base de dados.

Ao receber uma mensagem via LoRa, o *gateway* irá analisar se o endereço de origem consta na base de dados e conferir se a tag que foi enviada consta na lista

de tags que têm autorização para acesso. Se a tag não tiver autorização para acesso, o *gateway* irá retornar uma mensagem endereçada para aquela tranca dizendo que o acesso foi negado. Noutro caso, se a tag tiver permissão de acesso, o *gateway* irá retornar uma mensagem liberando o acesso. Em ambas as situações, o *gateway* irá acessar um servidor NTP para estar registrando o horário da tentativa de acesso junto à listagem na base de dados.

A base de dados a ser utilizada é o *real time database*, que é um dos serviços da plataforma de desenvolvimento de aplicativos móveis Firebase, promovido pela Google. Essa base de dados em tempo real permite a interação com dados em tempo real por parte de dispositivos IoT, aplicações móveis, aplicações web, entre outros. O que facilita a interação de diversos sistemas de monitoramento e controle em tempo real de diferentes plataformas, tendo em comum uma base de dados consolidada e muito versátil. A estrutura do Firebase é chamada de noSQL, uma alusão a “não relacional”, já que não trata os dados como registros relacionados, mas como uma árvore de dados, onde novos dados formam nós a partir da estrutura. Essa forma permite uma menor latência e, por consequência, maior dinâmica na manipulação e na leitura dos dados. A organização dos dados de cada tranca pode ser vista na Figura 15.

Figura 14 Organização dos dados na base de dados



Fonte: Autoria própria (2022)

3.4 Finalização do processo

Ao obter uma resposta sobre a permissão de acesso, o *gateway* envia a mensagem para a fechadura e registra na base de dados o horário da tentativa de acesso e a identificação da *tag*. Terminado esse passo, o *gateway* retorna ao *loop*.

Se a fechadura receber na resposta a autorização para o acesso, ela irá acionar o relé que acionará o mecanismo eletromecânico da fechadura.

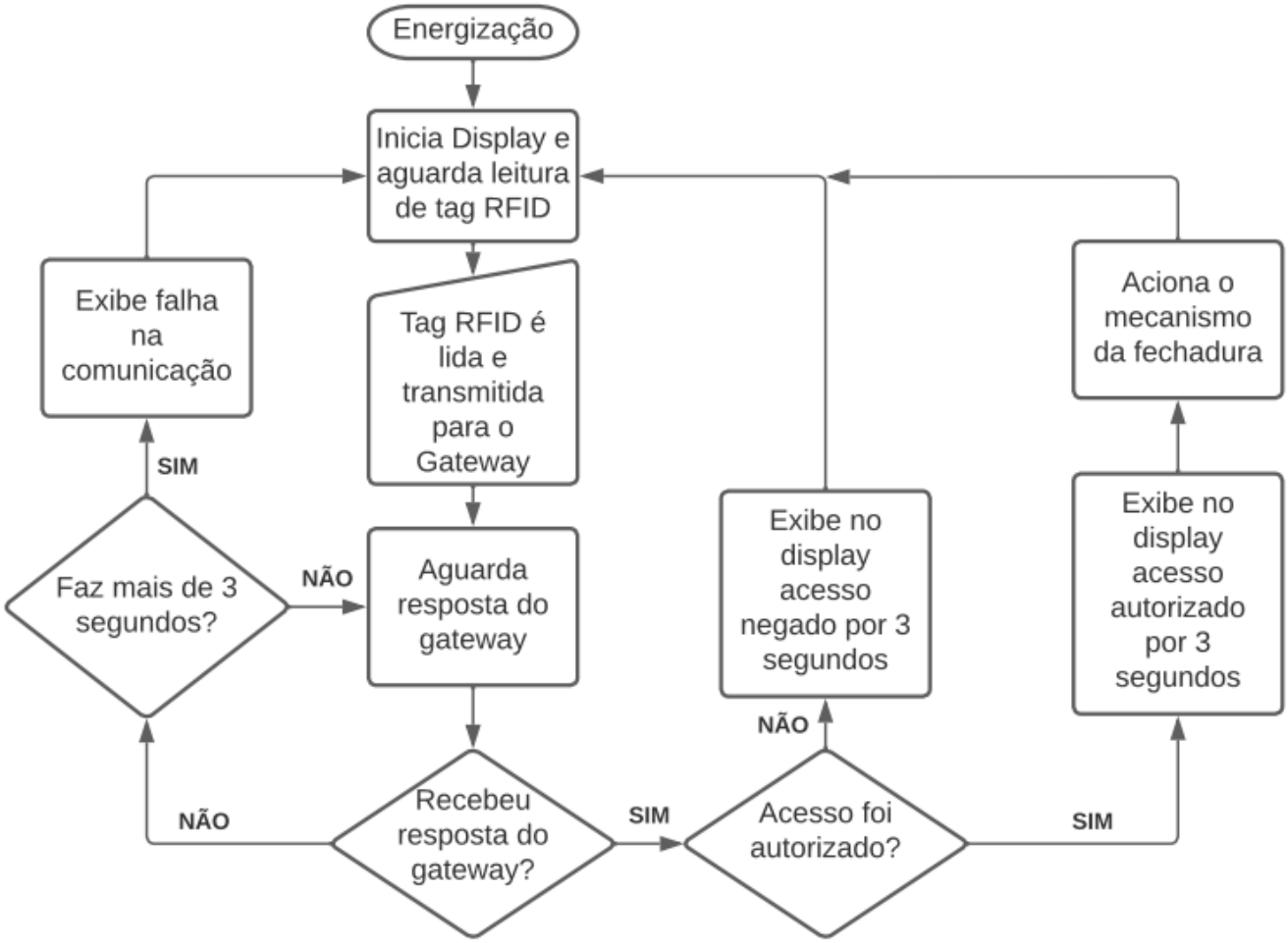
Para acionar o mecanismo eletromecânico, o pino 17 do ESP 32 é ligado a um transistor que atua como chave responsável por comutar o relé com tensão de controle de 5 volts. Já o mecanismo da fechadura pode ser de diversas tensões, de acordo com o modelo utilizado. Para esta aplicação, será utilizada uma fechadura modelo FX-500 da Intelbras que é comutada com uma tensão de 12 volts em corrente contínua, que pode ser vista na Figura 16.

Figura 15: Fechadura Elétrica FX-500

Fonte: Autoria Própria (2022)

O fluxograma completo de funcionamento da fechadura eletrônica pode ser visto na Figura 17.

Figura 16 Diagrama em blocos do funcionamento da fechadura eletrônica



Fonte: Autoria própria (2022).

Na Figura 18 pode se ver a fechadura eletrônica junto ao mecanismo eletromecânico montados sob a base de madeira que simula a abertura de uma porta.

Figura 17 Fechadura Eletrônica montada para Testes

Fonte: Autoria própria (2022)

3.5 Planejamento Experimental e Diagnóstico

Neste sistema, diversos pontos devem ser observados para garantir a aplicabilidade do sistema, tais como: latência na comunicação entre fechadura e *gateway*, tempo de processamento para/do *gateway*, capacidade de operar em modo contínuo, alcance da comunicação, entre outros.

A fim de estabelecer os parâmetros de operação do sistema, assim como seu potencial e suas limitações, aplicam-se uma série de testes para determinar suas métricas.

3.5.1 Alcance

O alcance por parte do *gateway* à rede WiFi depende em grande parte do roteador utilizado, podendo variar de metros até algumas dezenas de metros. No entanto, o alcance do *gateway* para a rede WiFi não é dos mais relevantes, mas sim

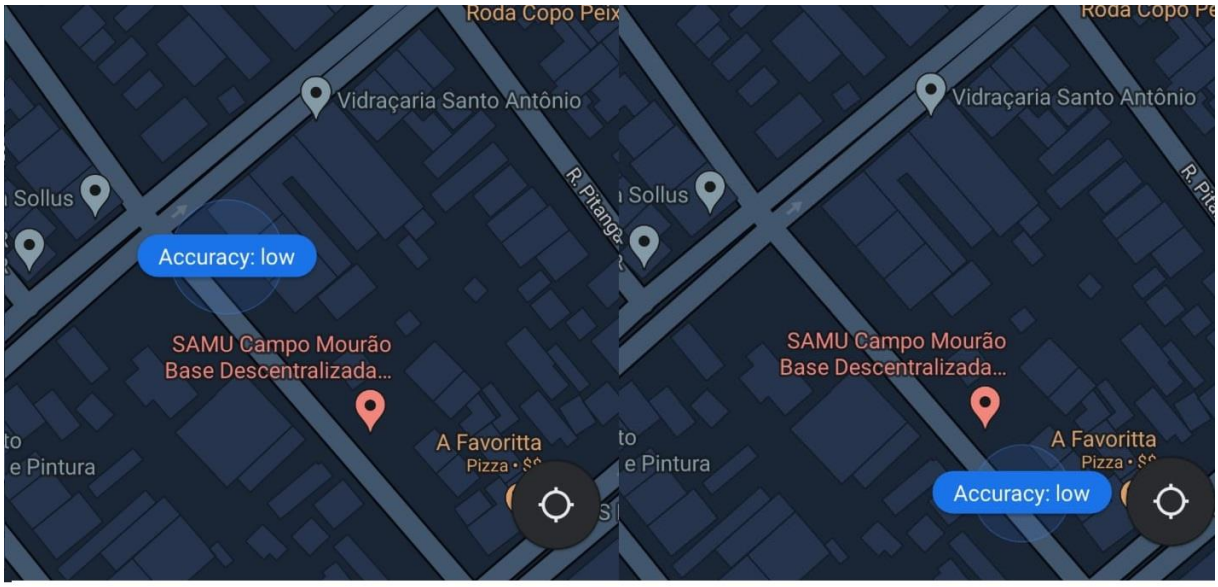
o alcance da comunicação LoRa. Para determinar o alcance da comunicação entre *gateway* e a fechadura foram realizados dois testes.

O Teste 1 foi realizado para estimar o alcance com área aberta. Nesse teste observou-se o quão longe a comunicação ocorre sem objetos no percurso.

Com emissor e receptor a uma distância de 1 m, a potência do sinal é de -95 dB, o que é consideravelmente baixo, uma vez que a sensibilidade do receptor LoRa é de -136 dB em média.

Para testar o alcance máximo, o transmissor foi posicionado com a antena omnidirecional de forma a ter visão limpa para o trajeto ao qual o receptor iria percorrer. A localização do transmissor e do receptor no instante da última mensagem recebida estão marcados na Figura 19.

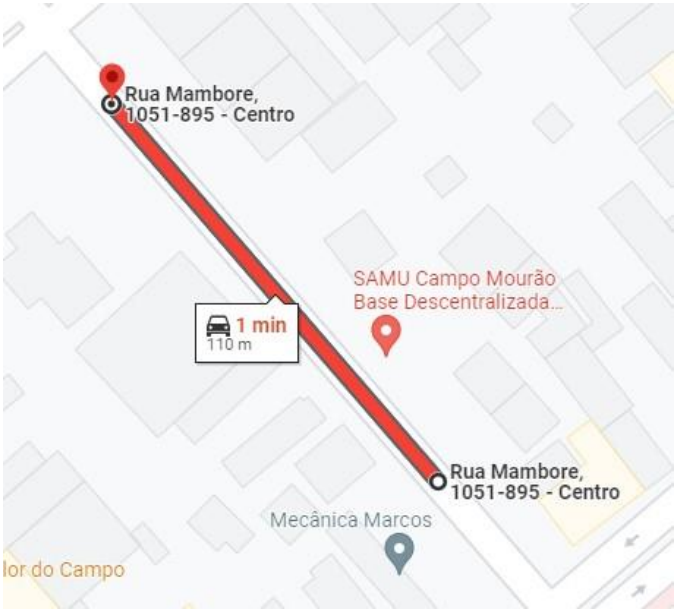
Figura 18 Localização do emissor (a esquerda) e receptor (a direita) na posição de maior alcance em área aberta



Fonte: Autoria Própria (2022)

Ao tentar mensurar a distância entre os pontos, pode-se definir aproximadamente o alcance de 110 metros para transmissão em área aberta sem obstáculos com uma margem de erro de 10 metros, conforme a Figura 20.

Figura 19 Alcance da transmissão em área aberta sem obstáculos



Fonte: Autoria Própria (2022)

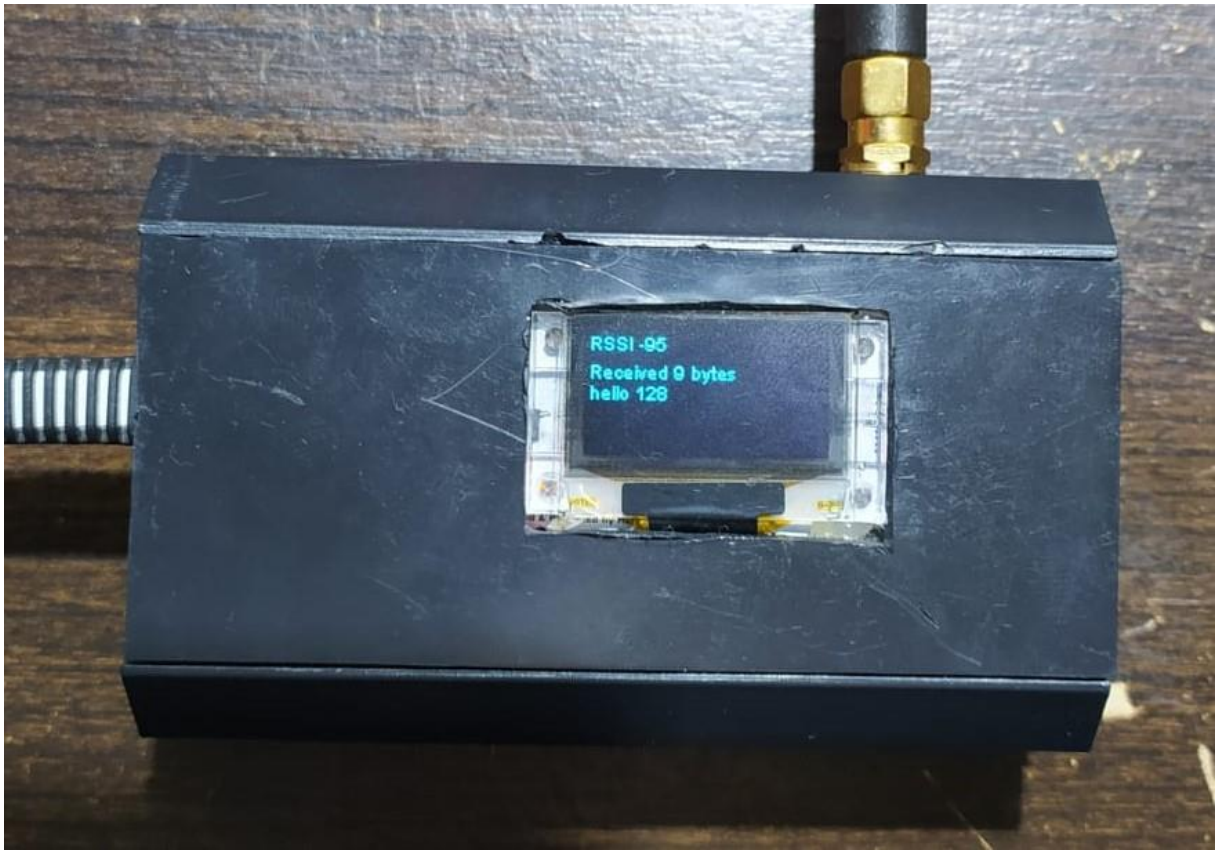
A potência do sinal recebido na transmissão na distância máxima foi de -130 dB. Um valor próximo àquela informada pelo fabricante de -136 dB. A mensagem recebida e a potência do sinal podem ser observadas na Figura 21.

Figura 20 Potência do sinal na mensagem com maior alcance

Fonte: Autoria Própria (2022)

O Teste 2 foi realizado para estimar o alcance considerando obstáculos, ou seja, com objetos. Para realizar este teste, posicionaram-se emissor e receptor a uma distância de 1 metro entre ambos. A potência do sinal recebido, conforme já foi visto, ficou em torno de -95 dB, conforme observa-se na Figura 22.

Figura 21 Transmissão sem obstáculos a um metro



Fonte: Autoria Própria (2022)

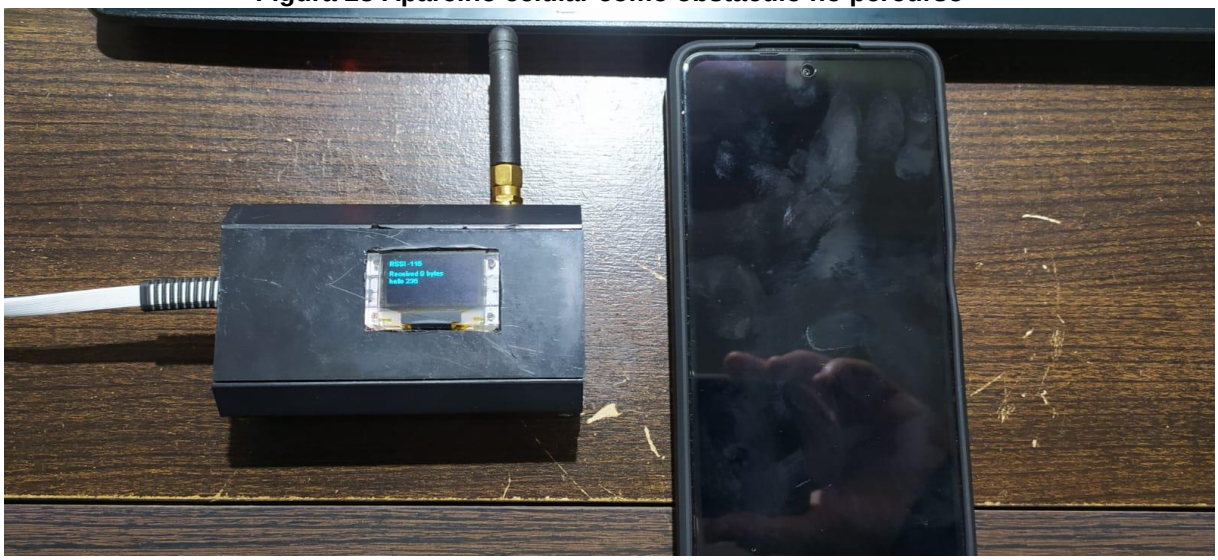
Ao inserir objetos entre o percurso, obtiveram-se diferentes comportamentos do sistema, de acordo com a natureza do objeto. O primeiro objeto a ser testado foi um livro, que foi posto próximo ao receptor de forma a ficar entre receptor e transmissor, conforme a Figura 23. A potência do sinal obtido pelo receptor não apresentou alterações, continuando em -95 dB.

Figura 22 Teste de transmissão com um livro como obstáculo

Fonte: Autoria Própria (2022)

Para o próximo teste foi utilizado um aparelho celular que ficou no percurso. Nota-se que fisicamente o aparelho celular fica abaixo do nível da antena do transmissor, no entanto, a potência do sinal recebido caiu consideravelmente: para -110 dB, conforme pode ser visto na Figura 24.

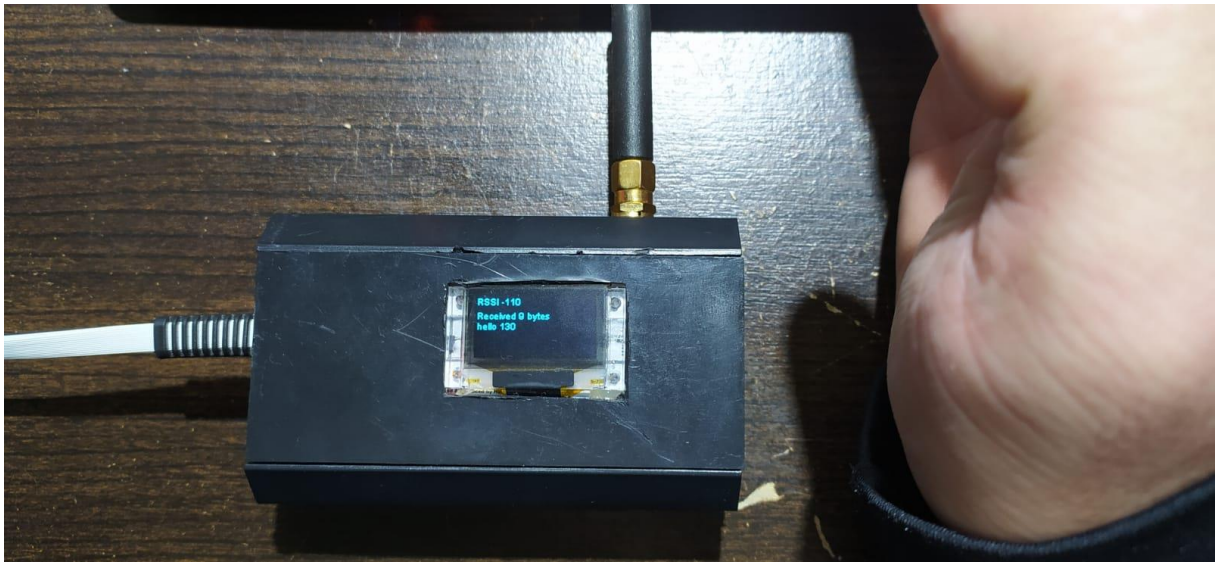
Figura 23 Aparelho celular como obstáculo no percurso



Fonte: Autoria Própria (2022)

Por fim, para o último teste utilizou-se da palma da mão para fornecer um obstáculo entre transmissor e receptor, o que também provocou uma queda na potência do sinal para -110dB, conforme a Figura 25.

Figura 24 Palma da mão como obstáculo



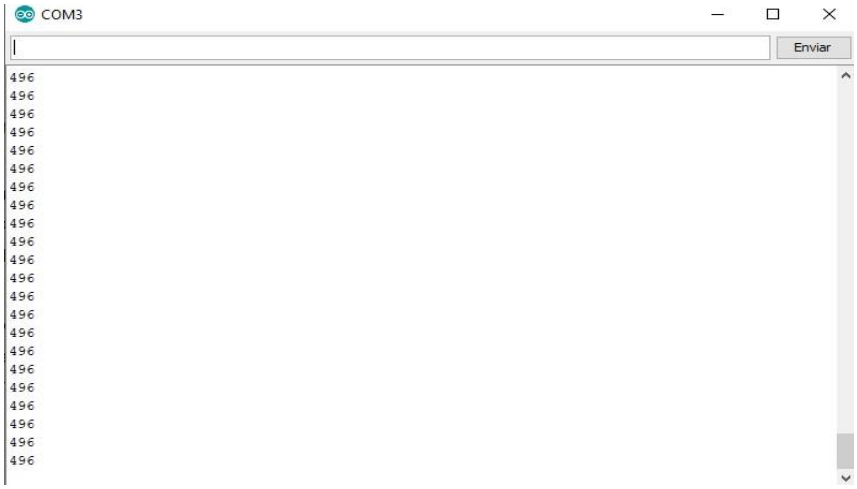
Fonte: Autoria Própria (2022)

3.5.2 Gastos de tempo do sistema

O processo de transmitir uma mensagem utilizado LoRa pode ser estimado ao utilizar a função millis(), que retorna o valor em milésimos de segundo, desde quando o sistema do ESP 32 foi iniciado, permitindo, dessa forma, o cálculo de tempo entre os processos das operações.

Neste caso, para testar a velocidade com que o ESP realiza a transmissão, criou-se uma função em loop que envia um pacote, realiza uma operação de conta referente ao millis() e exibe o valor na serial. Obtendo-se o resultado da Figura 26.

Figura 25 Tempo em milissegundos para transmitir via LoRa



Fonte: Autoria Própria (2022)

O processo completo para confirmação do *gateway* e envio da resposta para a fechadura é muito variado, devido a fatores como distância entre o gateway e a fechadura e velocidade da conexão WiFi.

Ao testar com emissor e receptor distantes em um metro, o tempo médio do processo de validação é de 1,2 até 4 segundos, conforme pode ser visto nas Figuras 27 e 28.

Figura 26 Saída serial mostrando o tempo em milissegundos da execução do processo de validação

```
Received from: 0xbb
Sent to: 0xbf
Message ID: 0
Message length: 9
Message: 113200988
RSSI: -99
Snr: 6.00

confirmando firebase
valor recebido: 113200988
endereço recebido bb
187
Valor recebido pela tranca: 113200988
valor recebido em endereço: 187

Tamanho do arquivo0
Nega acesso
envinando mensagem para a tranca
0
tempo em mili segundos para confirmação completa
2761
```

Fonte: Autoria Própria (2022)

Figura 27 Saída serial mostrando o tempo total para o acionamento do mecanismo eletromecânico da fechadura

```
2 room 4
load:0x40078000,len:9720
ho 0 tail 12 room 4
load:0x40080400,len:6364
entry 0x400806b8
Serial initial done
you can see OLED printed OLED initial done!
LoRa Initial success!
3351182enviando mensagem
3351182
enviando para gateway
Tempo total para abertura da tranca:
3443
3351182enviando mensagem
3351182
enviando para gateway
Tempo total para abertura da tranca:
1205
3351182enviando mensagem
3351182
enviando para gateway
Tempo total para abertura da tranca:
1485
```

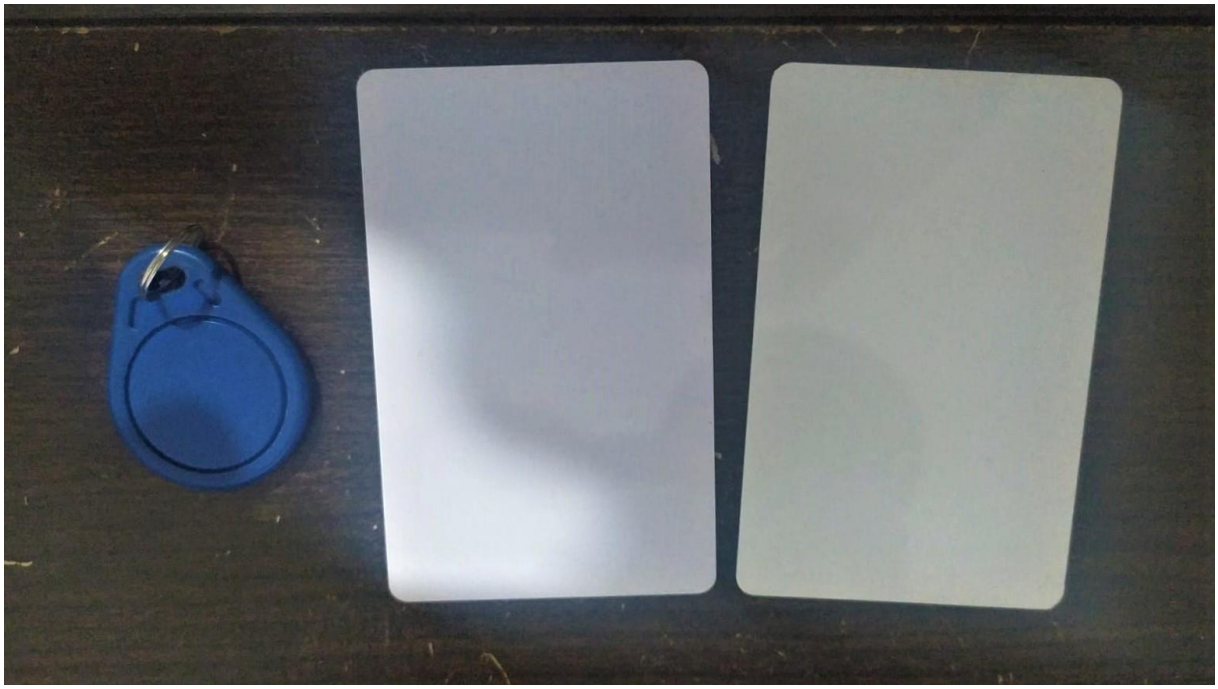
Fonte: Autoria Própria (2022)

Conforme pode ser visto na Figura 28, os tempos necessários para a execução completa partindo da leitura da tag RFID até o acionamento da fechadura eletromecânica podem variar drasticamente de acordo com a velocidade de conexão WiFi e as condições de transmissão LoRa, variando de 1205 até 3443 milésimos de segundos.

3.5.3 Teste com as Tags

O leitor RFID consegue ler as *tags* a uma distância de até 3 centímetros, com uma barreira de plástico (parede da caixa onde se aloca o leitor). Ao aproximar mais de uma tag RFID, não é realizada a leitura, pois há conflito de informações no ato da leitura. Na Figura 29 são apresentadas as *tags* utilizadas neste projeto.

Figura 28 *Tags* utilizadas neste projeto



Fonte: Autoria Própria (2022)

4. RESULTADOS E DISCUSSÕES

O protótipo apresenta um funcionamento muito bom para distâncias curtas, no entanto, com o aumento da distância e obstáculos entre receptor e transmissor, eles passam a deixar de receber as mensagens. Esse comportamento foi detectado nos primeiros testes, onde a fechadura enviava a mensagem para o *gateway*, exibia “aguarde” no display, porém não recebia a resposta do *gateway*, enquanto no *gateway* mostrava que a resposta havia sido enviada. Para contornar essa situação, toda vez que o *gateway* vai transmitir uma resposta para as fechaduras, ele executa um loop onde envia a resposta 5 vezes, de forma a garantir que a fechadura receba. Vale ressaltar que não foi implementado o protocolo LoRaWAN e que portanto executar a transmissão de forma repetida em um loop é uma maneira primitiva de buscar garantir a comunicação entre as partes mesmo que para isso aumente o tráfego e diminua consideravelmente a quantidade de *end-points*.

No lado da fechadura, ao enviar a mensagem para o *gateway*, inicia-se uma contagem de 5 segundos que, ao término, caso não seja obtida resposta do *gateway*, será exibida uma mensagem de erro na transmissão.

O mecanismo mecânico da fechadura possibilita o acesso por uma chave física que acompanha este modelo da tranca. Através do uso da chave não há registro do acesso, caracterizando-se como uma possível falha de segurança ou recurso para casos de mal funcionamento do sistema.

Ao se tratar de segurança, outro ponto deve ser considerado: a tranca pode ser ativada manualmente ao conectar um fio aos terminais do relé. Para tanto, seria necessário danificar a estrutura da caixa que contém o circuito eletrônico.

Ao realizar a leitura da *tag*, deve-se tomar os cuidados para não aproximar simultaneamente duas ou mais *tags*, pois o leitor de RFID modelo MFRC522 não é capaz de ler duas *tags* simultaneamente, devido à interferência que uma *tag* provoca na outra, causando uma confusão na leitura pelo MFRC522.

Em testes de comunicação entre a tranca e o *gateway*, obteve-se um alcance máximo de aproximadamente 110 metros, o que diverge muito do alcance de 2,4 quilômetros pronunciado pela heltec. Uma das possíveis causas dessa discrepância são danos causados ao circuito integrado responsável pela transmissão LoRa provocados pela tentativa de transmissão sem possuir uma antena adequada, o que

faz com que haja uma grande dissipação de potência no pino do circuito responsável pela comutação, por não haver um método ou instrumento que possibilite a constatação do dano ao transmissor, assume-se a premissa de que o transmissor fora danificado. Observa-se que foram adquiridas novas antenas, com maior capacidade, posteriormente aos testes, no entanto, não houve melhoras significativas no alcance, o que pode indicar que os módulos foram danificados.

A latência entre a comunicação LoRa entre os módulos foi entre 0,406 e 0,496 segundo para uma distância de aproximadamente 1 metro, e de 0,5 a 2 segundos nos limites do alcance ou com obstáculos. Já todo o processo de comunicação, que compreende da leitura da *tag* até a obtenção da resposta da fechadura, levou tempos em torno de 1 segundo a até 5 segundos, devido à velocidade de comunicação com a rede WiFi do local do *gateway*.

A estrutura geral na qual este projeto se baseia permite a utilização de até 254 trancas e um *gateway*. Nesse cenário, há a possibilidade de inúmeras colisões de informações, como por exemplo, duas ou mais fechaduras transmitindo enquanto o *gateway* está executando um processo de validação. Em testes, concluiu-se que o *gateway* não armazena leituras enquanto executa outros processos. Uma possível solução para isso é a utilização de um sistema operacional de tempo real (RTOS) aliado a uma distribuição esquematizada das tarefas para os dois núcleos do ESP 32, de forma que, enquanto um núcleo lida com as mensagens que está recebendo via LoRa, o outro núcleo executa as funções referentes à validação dos dados na rede.

Outro ponto que torna o sistema mais lento e que será crítico para o uso com diversas fechaduras é que o *gateway* realiza a transmissão de 5 mensagens para a fechadura para autorizar ou negar o acesso. Se considerar que cada transmissão demore aproximadamente 500 milissegundos, o *gateway* fica preso em um loop de transmissão por aproximadamente 2,5 segundos, tempo em que uma fechadura pode estar enviando uma mensagem que está sendo ignorada pelo *gateway*.

Este modelo pode permitir que haja a confirmação de recebimento de mensagens. Dessa forma, a fechadura envia uma mensagem contendo a *tag*, o *gateway* recebe a mensagem, executa os processos e a responde. A fechadura, ao receber a resposta do *gateway*, envia uma nova mensagem para ele dizendo que recebeu a mensagem e assim finaliza-se a comunicação. O problema dessa comunicação está no tempo de transmissão para uma única fechadura, já que haverá

ao menos três comunicações do tipo LoRa, cujo tempo mínimo é de 0,406 a 0,496 segundo, dependendo da mensagem, o que tomaria no mínimo 1,218 segundos para transmissão apenas LoRa em um processo, tornando-o mais lento.

Ao considerar a ausência de conexão da rede WiFi, seja por falta de estrutura ou por queda no fornecimento do serviço, o sistema deixará de atuar, impossibilitando os acessos e a abertura das fechaduras em situação de emergência.

Uma possibilidade para situações como essas, e até mesmo para deixar o sistema mais rápido, é a utilização do sistema SPIFFS, que nada mais é do que um recurso do ESP 32 que permite a criação de arquivos de texto de até 3 Mb. Este arquivo poderia conter uma cópia da relação de *tags* permitidas, de forma que, não havendo resposta do *gateway* após sucessivas tentativas, ele passa a analisar nos arquivos se há a possibilidade de liberação do acesso ou não.

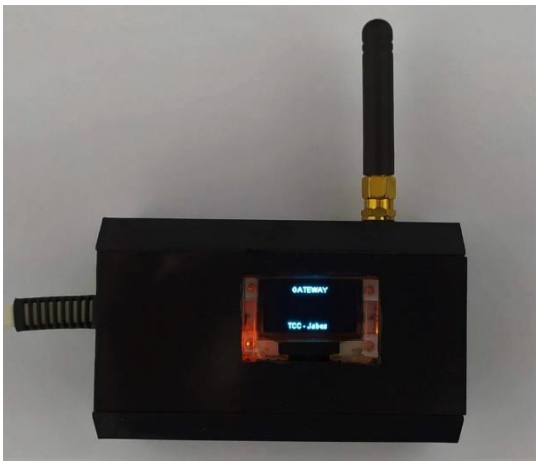
Referente ao funcionamento do sistema, ao enviar para o *gateway* o código referente à *tag* que foi lida, a tranca passa a exibir uma mensagem dizendo “aguarde”. Conforme a Figura 30.

Figura 29 Tranca em estado de aguarde

Fonte: Autoria Própria (2022)

O *gateway* foi construído em uma base de plástico com abertura para o visor, que auxilia na verificação do status de seu funcionamento. O *gateway* pode ser visto na Figura 31.

Figura 30 Tela Inicial do *gateway*



Fonte: Autoria própria (2022)

Ao receber do *gateway* a resposta, a tranca pode passar a exibir uma das seguintes mensagens no visor: “acesso autorizado” ou “acesso negado”, conforme as Figuras 32 e 33, respectivamente.

Figura 31 Tranca com a mensagem “acesso autorizado”

Fonte: Autoria Própria (2022)

Figura 32 Tranca com a mensagem “acesso negado”

Fonte: Autoria Própria (2022)

5. CONCLUSÕES

Com o presente trabalho, obteve-se um sistema capaz de controlar o acesso a ambientes, comutando uma fechadura eletromecânica, mediante a apresentação de uma tag RFID com o código previamente registrado em uma base de dados para autorização do acesso. Para isso, utiliza-se da comunicação LoRa para enviar os dados da tag e a resposta do *gateway*, caracterizando assim um sistema de automação através do uso da tecnologia LoRa.

Não se obteve um alcance excepcional conforme os anúncios dos vendedores e de demais fontes de informações, no entanto, é errado pressupor que houve uma disseminação de informações falsas referentes aos módulos LoRa, uma vez que há outras razões para a obtenção baixa na qualidade da transmissão, como antenas inadequadas, danos causados ao circuito de transmissão devido ao manuseio incorreto do mesmo, entre outros.

O ESP 32 demonstrou uma ótima eficiência, realizando tarefas relacionadas à rede WiFi, tais como leitura e gravação na base de dados Firebase, além de permitir o uso de diversas bibliotecas que facilitaram no desenvolvimento deste projeto. Vale destacar que, ao programar o ESP 32 utilizando a plataforma arduino, muitas bibliotecas focadas em outras arquiteturas de microcontroladores podem acusar incompatibilidade com o ESP 32, que é o caso da biblioteca utilizada para a interação do ESP 32 com o leitor RFID. No entanto, não houve sequer um problema ou falha no uso desse periférico.

Entre as dificuldades encontradas, a principal foi a dificuldade de identificar onde há a falha de comunicação quando um elemento está transmitindo e o outro não está recebendo. Situação essa que foi o estopim para a desistência do uso do módulo LoRa da Semtech RHF0M301, pois o *gateway* se mostrava corretamente configurado, inclusive com a frequência de trabalho correta, porém os módulos LoRa do ESP 32, que seriam os *end-points*, mostravam que estavam transmitindo de acordo com o protocolo LoRaWAN, porém não havia o recebimento de nenhuma mensagem. Sem saber onde estava o erro, foram exaustas as tentativas com o módulo RHF0M301.

Referente ao módulo RFID, houve a necessidade de uma pequena alteração na biblioteca para a configuração do pino SDA (que no protocolo SPI é chamado SS), que é responsável por selecionar o leitor RFID para realizar a escrita no barramento de comunicação SPI.

Quanto a leitura e escrita no Firebase, houve uma relativa dificuldade em encontrar uma biblioteca que funcionasse bem. A que foi utilizada se caracteriza por ser uma biblioteca de alto nível, permitindo que funções complexas sejam realizadas com relativa facilidade, sem ter que definir parâmetros de baixo nível, como estruturar mensagens JSON para configurarem uma conexão entre o ESP 32 e o backend do Firebase.

O sistema da forma como foi construído possui limitações quanto à quantidade de elementos na rede LoRa, uma vez que um grande número de elementos pode causar inúmeras colisões de transmissões e também limitações quanto a distâncias entre o *gateway* e as fechaduras.

Uma grande potencialidade deste sistema é que, com pequenas alterações nos códigos do *gateway* e, principalmente, da fechadura, é possível obter outros sistemas que variam deste como os exemplos que se seguem. Controle de luminosidade ou temperatura de um ambiente: Em uma sala de aula, o controle de luminosidade baseado no ESP 32 pode atuar junto a relés desligando ou ligando a iluminação da sala, de acordo com o horário da aula, evitando que as luzes fiquem acesas em períodos desnecessários; ou um controlador de temperatura que realiza as medições de temperatura ou umidade grava essas informações em uma base de dados e pode também atuar no controle dessas características. Contador de pessoas na entrada de uma sala ou ambiente: um sistema baseado no ESP 32 com LoRa pode auxiliar na contagem de pessoas que trafegam por algum determinado ponto, ou até mesmo para determinar se há pessoas em algum ambiente, caso seja local ou horário indevido.

Há inúmeras melhorias possíveis neste sistema, das quais serão citadas as mais relevantes:

- Desenvolver uma interface para leitura dos dados através de um aplicativo Android ou IOs.

- Desenvolver o sistema utilizando o módulo LoRa da Semtech RHF0M301. Utilizar o *gateway* da Semtech iria acrescentar uma nova gama de possibilidades a este sistema, permitindo o desenvolvimento de projetos mais elaborados e complexos, além de permitir a integração com recursos já disponíveis na web.

- Utilizar dois leitores RFID para uma só fechadura, de forma a ter controle de quem acessa e quem deixa o local. Uma vez que, havendo um só leitor, só é possível realizar a leitura de apenas um sentido do fluxo de pessoas.

- Remodelar a arquitetura do sistema utilizando o sistema de arquivos do ESP 32 para agilizar os acessos, uma vez que a validação seria totalmente interna ao ESP 32, sem depender da transmissão de informações para a validação do acesso.

- Implementar este sistema com diferentes módulos LoRa, não apenas os da Heltec, para analisar e comparar as diferenças quanto ao alcance da transmissão LoRa.

- Analisar a viabilidade de implementar o protocolo LoRaWAN utilizando um *gateway* e um end-point baseados no ESP 32.

Muitas são as melhorias e possibilidades que partem deste projeto. De forma que, satisfatoriamente, ele venha a servir de base para a elaboração de projetos futuros.

REFERÊNCIAS

AISLAN, S. **Monitoramento de Temperatura com Heltec ESP32 LoRa**. [*S. l.*], 22 dez. 2021. Disponível em: https://blog.eletrogate.com/monitoramento-remoto-de-temperatura-utilizando-a-heltec-esp32-lora/. Acesso em: 17 jun. 2022.

ALMEIDA, A. G. D. **Conhecendo o Raspberry Pi: Possibilidades de uso em contextos educacionais e profissionais**. Instituto Federal de Educação, Ciência e tecnologia, Parnamirim, 2013.

ANATEL. **CARTILHA ORIENTATIVA INTERNET DAS COISAS IoT/M2M**. [S.l.]: [s.n.]. 2019. p. 15.

BANKOLE, K. **Tutorial: Build an open source smart city with LoRaWAN**. [*S. l.*], 5 fev. 2018. Disponível em: https://medium.com/kkbankol-events/tutorial-build-a-open-source-smart-city-based-on-lora-7ca76b9a098. Acesso em: 15 fev. 2022.

DIAS, R. R. D. F.; PIERI, B. de. **Diferenças entre as frequências do sistema RFID passivo**. RFID Journal Brasil, [*S. l.*], p. 1, 20 fev. 2019. Disponível em: https://brasil.rfidjournal.com/artigos/vision?9591/2. Acesso em: 23 maio 2019

JUNIOR, V. P. **Conheça a tecnologia LoRa® e o protocolo LoRaWAN™**. [*S. l.*], 6 abr. 2016. Disponível em: https://www.embarcados.com.br/conheca-tecnologia-lora-e-o-protocolo-lorawan/. Acesso em: 22 out. 2017.

ESPRESSIF (SHANGHAI, CHINA). **Espressif Announces the Launch of ESP32 Cloud on Chip and Funding by Fosun GroupEspressif Announces the Launch of ESP32 Cloud on Chip and Funding by Fosun Group**. ESPRESSIF, SHANGHAI, CHINA, p. 1, 7 set. 2016. Disponível em: https://www.espressif.com/en/media_overview/news/20160907-esp32briefing#:~:text=Sep%207%2C%202016,MCU%20at%20Shanghai%20Parkyard%20Hotel. Acesso em: 24 out. 2017.

FRUETT, F. **Introdução ao Raspiberry Pi**, 11 setembro 2013.

HAYKIN, S.; MOHER, M. **Sistemas Modernos de Comunicações Wireless**. Porto Alegre: Bookman, 2008.

HORNBUCKLE, C. **Fractional-N Synthesized Chirp Generator**. US20080122635 20080516, 07 Setembro 2010.

MELO, P. **Introdução ao LPWAN (Low Power Wide Area Network)**. [*S. l.*], 27 jan. 2017. Disponível em: https://www.embarcados.com.br/introducao-ao-lpwan/. Acesso em: 24 out. 2017.

MICROCONTROLLERSLAB. **RC522 RFID Reader Module**. [*S. l.*], CA. 2016. Disponível em: https://microcontrollerslab.com/rc522-rfid-reader-pinout-arduino-interfacing-examples-features/. Acesso em: 24 out. 2017.

MIGUEL, A. J. H. **A Aplicação da tecnologia RFID nas Diferentes Áreas do Corpo de Bombeiros Militar de Santa Catarina** - CBMSC. CEBM - Centro de Ensino Bombeiro Militar de Santa Catarina, 2011.

MINATEL, P. **ESP32, O QUE JÁ SABEMOS SOBRE O NOVO MÓDULO**. [*S. l.*], 15 jul. 2015. Disponível em: http://pedrominatel.com.br/pt/esp32/esp32-o-que-ja-sabemos-sobre-o-novo-esp8266/. Acesso em: 22 out. 2017.

MIZUSAKI, L. E. P. **Comparação de Mecanismos de Comunicação para a Casa Inteligente**. Universidade Federal do Rio Grande do Sul, Porto Alegre, Junho 2009.

MORESCHI, K. C. **Comparação Entre Protocolos de Gateways Redundantes Utilizando Roteadores Dedicados**. Universidade Tecnológica Federal do Paraná, Campo Mourão, 2011.

MORIMOTO, MORIMOTO. **Entendendo a questão do alcance em redes wireless**. [*S. l.*], 23 fev. 2009. Disponível em: https://www.hardware.com.br/dicas/alcance-redes-wireless.html. Acesso em: 23 out. 2017.

MUNDOMAX. **O que é um Switch e para que serve?**. [*S. l.*], 10 fev. 2010. Disponível em: http://www.mundomax.com.br/blog/informatica/o-que-e-um-switch-e-para-que-serve/. Acesso em: 25 out. 2017.

SILVA NETO, E. da. **Plataformas de desenvolvimento baseadas em LoRa**. [*S. l.*], 24 ago. 2017. Disponível em: https://www.embarcados.com.br/plataformas-baseadas-em-lora/. Acesso em: 25 out. 2017.

SILVA NETO, E. da. **Criando end-devices LoRa: arquitetura e especificações**. [*S. l.*], 20 out. 2017. Disponível em: https://www.embarcados.com.br/end-devices-lora-arquitetura/. Acesso em: 22 out. 2017.

NZX, **O que é roteador?**. [*S. l.*], 2 jan. 2009. Disponível em: https://www.tecmundo.com.br/conexao/1258-o-que-e-roteador-.htm. Acesso em: 23 out. 2017. PALMA, D. S. D. C.;

PALMA, D. S. D. C.; PINTO, D. G. **DOMOITECH - Domótica com o Protocolo EIB**. Universidade do Porto, Porto , Julho 2007.

PINHEIRO, J. M. S. **RFID - Identificação por Radiofreqüência**. [*S. l.*], 11 maio 2004. Disponível em: https://www.projetoderedes.com.br/artigos/artigo_identificacao_por_radiofrequencia.php. Acesso em: 26 out. 2017.

PRAJZLER, V. **LoRa, LoRaWAN and LORIOT**. [*S. l.*], 12 nov. 2015. Disponível em: https://www.loriot.io/lorawan.html. Acesso em: 22 out. 2017. RAMOS, A. L. C.;

SANTOS, J. E. L. D. **Sistema Integrado de Automação Residencial com Comunicação sem Fio**, 2015.

RICHARDSON, M.; WALLACE, S. **Primeiros Passos com o Raspberry Pi**. 1. ed. [S.l.]: Novatec, 2013.

SEI/ANATEL. ANATEL. **Requisitos Técnicos de Certificação. Ato número 14448, de 04 de dezembro de 2017**. ATO Nº 14448, DE 04 DE DEZEMBRO DE 2017, [*S. l.*], ano 2018, n. 2184849, p. 1-30, 2 jan. 2018. Disponível em: http://www.ncc.org.br/img/Ato%2014448.pdf. Acesso em: 23 maio 2019

SELLER, O. B. A.; SORNIN, N. **Low Power Long Range Transmitter**. EP2763321 A1, 6 agosto 2014.

VASCONCELOS, T. L.; ALVES, F. M. A. **IEEE 802.11**: IEEE 802.11 a,b,g,n. [*S. l.*], CA. 2015. Disponível em: https://www.gta.ufrj.br/grad/15_1/802.11abgn/index.html. Acesso em: 17 out. 2017.

CRIACORE. **TAGS e Pulseiras RFID ou NFC - Qual a diferença?** [*S. l.*], CA. 2022. Disponível em: https://www.criacore.com/index.php/portfolio/11-projetos-interativos/19-rfid-e-nfc. Acesso em: 17 jun. 2022.

TANENBAUM, A. S. **Redes de Computadores**. 5. ed. São Paulo: Pearson, 2011.

TEZA, V. R. **Alguns Aspectos Sobre a Automação Residencial** - Domótica. Universidade Federal De Santa Catarina, Florianópolis, Maio 2002.