UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS, TECNOLOGIAS E SAÚDE

Everaldo Selau Scandolara Junior

SISTEMA ELETRÔNICO INTEGRADO PARA CONTROLE DE ACESSO - UM ESTUDO DE CASO PARA A UNIVERSIDADE FEDERAL DE SANTA CATARINA

Araranguá, Julho de 2018.

Everaldo Selau Scandolara Junior

SISTEMA ELETRÔNICO INTEGRADO PARA CONTROLE DE ACESSO - UM ESTUDO DE CASO PARA A UNIVERSIDADE FEDERAL DE SANTA CATARINA

Trabalho de Conclusão de Curso submetido à Universidade Federal de Santa Catarina, como parte dos requisitos necessários para a obtenção do Grau de Bacharel em Engenharia de Computação.
Orientador: Prof. Fábio Rodrigues de la Rocha, Dr.

Araranguá, Julho de 2018.

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Scandolara Junior, Everaldo Selau
Sistema eletrônico integrado para controle de acesso - um estudo de caso para a Universidade Federal de Santa Catarina / Everaldo Selau Scandolara Junior ; orientador, Fábio Rodrigues de La Rocha, 2018.
72 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Campus Araranguá, Graduação em Engenharia de Computação, Araranguá, 2018.

Inclui referências.

1. Engenharia de Computação. 2. Controle de Acesso. 3. Fechadura Inteligente. 4. Redes Mesh. I. de La Rocha, Fábio Rodrigues. II. Universidade Federal de Santa Catarina. Graduação em Engenharia de Computação. III. Título.

Everaldo Selau Scandolara Junior

SISTEMA ELETRÔNICO INTEGRADO PARA CONTROLE DE ACESSO - UM ESTUDO DE CASO PARA A UNIVERSIDADE FEDERAL DE SANTA CATARINA

Este Trabalho de Conclusão de Curso foi julgado aprovado para a obtenção do Título de "Bacharel em Engenharia de Computação", e aprovado em sua forma final pela Universidade Federal de Santa Catarina.

Araranguá, Julho de 2018.

Eliane Pozzebon
Assinado de forma digital por Eliane Pozzebon
Dados: 2018.07.24 11:48:56 -03'00'

Profª. Drª. Eliane Pozzebon
Coordenadora do Curso

Banca Examinadora:

***Assinado digitalmente por ***
Fábio Rodrigues de la Rocha
2018.07.17 10:31:50 BRT SIAPE: 1781774
96300752020 fabio.rocha@gmail.com

Prof. Dr. Fábio de la Rocha
Orientador

Anderson Luiz Fernandes Perez
Assinado de forma digital por Anderson Luiz Fernandes Perez
Dados: 2018.07.17 10:19:26 -03'00'

Prof. Dr. Anderson Luiz Fernandes Perez

Marcelo Daniel Berejuck
Assinado de forma digital por Marcelo Daniel Berejuck
Dados: 2018.07.19 18:22:18 -03'00'

Prof. Dr. Marcelo Daniel Berejuck

Aos meus pais, responsáveis por pavimentar o caminho até aqui.

AGRADECIMENTOS

Ao meu pai, Everaldo Selau Scandolara e à minha mãe, Josiane Guimarães dos Passos, por jamais mediram esforços para que eu chegasse até aqui e me darem todo o suporte financeiro e emocional, sendo as razões de todas as minhas conquistas. Aos meus amigos, que tornaram esta jornada acadêmica o mais divertida e proveitosa possível. À Roberta Ribas Mocelin por ser a melhor companheira para todos os momentos importantes. Ao professor e orientador Fábio Rodrigues de La Rocha, por todo o conhecimento compartilhado e, principalmente, pela paciência com um jovem tentando decifrar a "vida real". Aos professores da Universidade Federal de Santa Catarina, campus Araranguá, com destaque para o professor Anderson Luiz Fernandes Perez, o qual sempre esteve empenhado a ajudar no meu desenvolvimento profissional e pessoal, sendo um exemplo a ser seguido. Enfim, à todos que fizeram parte, deixaram suas marcas e tornaram este capítulo único em minha vida.

The only place success comes before work is in the dictionary.

Vince Lombardi

RESUMO

O controle de acesso, tipicamente, é implementado por fechaduras com chaves convencionais, sistema este criado há séculos. A utilização deste artifício em ambientes onde muitas pessoas necessitam ter acesso, pode causar transtornos, como o extravio das cópias das chaves e o agrupamento de muitas chaves para usuários que têm acesso à múltiplas salas. Para amenizar estes problemas, existem fechaduras eletrônicas disponíveis no mercado. Contudo, a maioria dos modelos são do tipo *standalone*, ou seja, sem conexão com outras fechaduras ou com um computador administrador, necessitando assim serem programadas individualmente, o quê não é uma tarefa desejada, especialmente em ambientes com várias salas e com várias fechaduras. Outro fator limitante às opções atuais no mercado é o preço elevado. Este trabalho têm o intuito de desenvolver uma solução para controle de acesso de baixo custo, utilizando identificação por rádio frequência (RFID) e que permita a atualização dos dados de acesso via rede *wireless*. O foco do trabalho é resolver o problema da Universidade Federal de Santa Catarina no controle de seus laboratórios e salas. Entretanto, o sistema pode ser adaptado para a utilização em aplicações de automação residencial e predial, sendo um produto potencialmente comercial.

Palavras-chave: controle de acesso, RFID, *wireless*, fecho eletrônico.

ABSTRACT

Access control typically is implemented by door locks with traditional keys, a system that was created centuries ago. The use of this system in environments where many people need access may cause inconveniences, like key loss and the gathering of too many keys by users who have access to multiple rooms. To settle these problems, there are electronic door locks available on the market. However, most of the models are built in a standalone way, in other words, are built without connection with other locks or an administrator computer, thus needed to be individually programmed, which is not a desired task, especially in environments with several rooms and several locks. Another limiting factor to the current options in the market is the high price. This undergraduate thesis aims to develop a low cost access control solution, using radio frequency identification (RFID), that allows the update of access data through wireless network. The focus here is to solve the University of Santa Catarina control access problems in its rooms and laboratories. However, the system can be adapted to be used in applications like residential and building automation, being a potentially commercial product.

Keywords: access control, RFID, wireless, electronic lock

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

SUMÁRIO

1 INTRODUÇÃO

O cuidado com controle de acesso não é uma novidade da sociedade moderna. Aproximadamente 4000 anos atrás, o conceito de tranca e chave foram inventados por diversas civilizações ao mesmo tempo, utilizando materiais primitivos como a madeira. Salvo algumas mínimas variações, fechaduras ainda são instaladas e utilizadas com o mesmo princípio. Ou seja, para a fechadura ser destravada é necessário o estímulo mecânico com a chave correta (KASSEM et al., 2016). Esta necessidade por controle de acesso ainda é presente e crescente na sociedade atual. A realização deste controle pode ser implementada por meio de recursos humanos, criando-se assim profissões como as de recepcionista, guarda ou porteiro. Além desta, a maneira de controle mais comum são dispositivos mecânicos como fechaduras e chaves.

Uma preocupação relevante da sociedade em geral atualmente está relacionada com a falta de segurança, tanto pessoal quanto para bens materiais. Este tipo de preocupação acaba levando a um aumento de gastos voltados à área de serviços de vigilância e monitoramento. O problema aumenta quando leva-se em consideração lugares que um grupo maior de pessoas têm a necessidade de acesso, demandando assim de um maior número de chaves, facilitando o possível extravio de algumas delas. Sem falar que, com a necessidade de uma chave para cada porta ou portão dos ambientes corriqueiramente utilizados por um indivíduo, acaba gerando um acúmulo e embaralhamento de chaves, causando desconforto e perda de tempo nas tarefas do dia-a-dia (TEH; LING; CHEONG, 2013).

A automação, termo muito utilizado atualmente, busca a resolução de alguns destes problemas, bem como a facilitação de processos, geralmente completando tarefas básicas como ligar e desligar dispositivos automaticamente. Um fator que ajuda no desenvolvimento de sistemas de automação é o baixo custo de componentes eletrônicos, possibilitando o uso da automação não somente na área industrial, setor este que demanda automação mesmo de alto custo, mas também nas áreas residencial, predial, agrícola, etc (ALKAR; BUHUR, 2005).

O uso da automação para controle de acesso é bastante utilizada em indústrias e companhias que necessitam controlar as áreas específicas que cada funcionário pode ter acesso ou não. Atualmente existem tecnologias utilizadas neste tipo de aplicação com o intuito de facilitar este controle e ainda melhorar o nível de segurança nas dependências das organizações. Porém, a maioria destes sistemas são do

tipo *standalone*, ou seja, não são conectados com um dispositivo central para a atualização dos dados de acesso. Para a realização desta tarefa, tipicamente é necessário o deslocamento de algum responsável para a atualização das informações individualmente para cada fechadura de controle de acesso.

Os microcontroladores, hoje sendo eles empregados nas mais diversas áreas, podem ser utilizados para a agregação de inteligência nos sistemas voltados ao controle de acesso, possibilitando a criação do conceito de fechaduras inteligentes (*smart locks*).

Uma fechadura inteligente é um sistema microcontrolado que, juntamente com um meio de entrada de informação, pode gerenciar a abertura de uma porta (CARNIEL et al., 2015). Esta entrada de dados por parte do usuário pode ser realizada através de um teclado alfanumérico, identificação por rádio frequência (RFID), NFC (*Near Field Communication*), *bluetooth*, internet e outros métodos de comunicação entre dispositivos.

Realizando uma pesquisa na internet com as palavras-chave "fechadura inteligente"é possível encontrar diversos modelos de fechaduras eletrônicas no mercado atual. A grande maioria destes modelos disponibilizam um teclado alfanumérico para o controle de acesso via senhas. Alguns modelos sofisticados já trazem leitura biométrica de impressão digital e RFID. Já fechaduras com conexão Wi-Fi não se encontra facilmente, existindo apenas um modelo com conexão via cabo de rede (CARNIEL et al., 2015). O que chama atenção porém, são os preços destes dispositivos fabricados por marcas famosas como a *Samsung*, dificultando a implantação desta tecnologia para o controle de acesso de todas as salas e laboratórios de uma universidade, por exemplo.

Neste trabalho, apresenta-se um protótipo de sistema microcontrolado para controle de acesso utilizando RFID e com conexão sem fio à rede *Wi-Fi*, possibilitando a atualização dos dados através de um dispositivo central na rede. O sistema é voltado para a implantação na Universidade Federal de Santa Catarina (UFSC), campus Araranguá, para a solução dos problemas de controle de acesso dos professores, alunos e funcionários às salas, laboratórios e demais dependências do campus.

Apesar da existência de métodos de validação de usuário mais complexos e seguros, como a biometria que engloba técnicas de leitura de impressões digitais e reconhecimento facial, a tecnologia RFID foi escolhida pois ela já está presente nos cartões de identificação da universidade. Cada aluno e professor recebe o cartão com a tecnologia de identificação por radio frequência. Porém, segundo informações cole-

tadas, ainda não existe um banco de dados com a associação de cada usuário da universidade com o ID gravado no cartão, dificultando assim a aplicação da tecnologia em sistemas de automação.

1.1 JUSTIFICATIVA E MOTIVAÇÃO

O método de controle de acesso aos laboratórios e às salas utilizado na UFSC atualmente ainda é totalmente mecânico. Existe um porta chaves (claviculário) em uma sala que todos os professores têm acesso. Quando um professor deseja abrir uma sala ele deve se deslocar até o claviculário, apanhar a chave em questão, abrir a porta da sala que deseja e ao final, retornar a chave ao claviculário. Um dos problemas dessa abordagem é a necessidade do professor se deslocar a cada intervalo de aula até o claviculário para apanhar a chave da próxima aula, o que consome tempo em seguidos deslocamentos. Além disso, caso o professor esqueça de retornar a chave, os demais professores ficarão impossibilitados de acessar a sala/laboratório até a situação ser solucionada. Através do claviculário um professor também seria capaz de acessar qualquer sala/laboratório.

Outro fato que motiva o desenvolvimento do projeto é que na UFSC, os professores e alunos já possuem um cartão de identificação que possui em seu interior um RFID. Com o RFID a leitura é realizada sem a necessidade de contato do usuário com a fechadura, realizando a abertura da porta de forma rápida e fácil. Utilizando um microcontrolador que consiga acessar a rede *wireless* da universidade, a tarefa de configuração do sistema fica facilitada, pois bastaria que o administrador configurasse em um *software* quais salas o determinado professor pode ter acesso e assim a informação seria propagada pela rede até cada fechadura.

Por fim, existem as motivações relacionadas à segurança. Uma é o aumento da mesma com o controle específico de qual sala cada usuário tem acesso. O sistema pode ser utilizado para construir um arquivo de histórico de acesso (arquivo de log) às salas/laboratórios e assim controlar o bom uso do patrimônio da universidade. Além disso, o sistema foi projetado levando em consideração melhorias que venham a ser adicionadas. Um exemplo disso é o aproveitamento da capacidade do microcontrolador para a utilização de sensores nas janelas, possibilitando saber se a janela foi esquecida aberta. Esses sensores poderiam se comunicar com a fechadura (que por sua vez estaria conectada à rede *wireless* da universidade) e assim a informação de quais salas possuem

janelas abertas estaria disponível através de um computador. Com a aplicação de sensores, várias informações de segurança poderiam ser obtidas sem a necessidade da verificação de cada sala por parte de uma pessoa responsável. O sistema pode automaticamente em determinados horários fazer uma varredura nas salas para descobrir se algo necessita ser relatada (luz acessa/janela aberta, sensor de fumaça, etc.) e assim alertar a equipe de segurança do campus para a situação.

1.2 OBJETIVOS

Os objetivos deste trabalho estão divididos entre geral e específicos.

1.2.1 Geral

Desenvolver um sistema eletrônico inteligente voltado à melhoria do controle de acesso às salas e laboratórios da Universidade Federal de Santa Catarina.

1.2.2 Específicos

1. Levantar o estado da arte das tecnologias envolvidas no projeto.

2. Estudar e definir o microcontrolador a ser utilizado no sistema proposto.

3. Estudar o métodos de troca de mensagens entre dispositivos via rede sem fio.

4. Definir os requisitos funcionais e não funcionais para o sistema de controle de acesso.

5. Desenvolver o protótipo do sistema.

6. Realizar testes com o protótipo base.

7. Avaliar os resultados obtidos com o foco na melhoria do controle de acesso da universidade.

1.3 METODOLOGIA

O projeto apresentado é um estudo de caso para a Universidade Federal de Santa Catarina, com revisão bibliográfica e desenvolvimento de protótipo experimental.

- Inicialmente será feita a revisão bibliográfica das tecnologias envolvidas no trabalho.
- Realizar as simulações inicias no desenvolvimento do *software* com o auxílio do programa simulador de circuitos *Proteus*.
- Para alcançar o objetivo de desenvolver o protótipo final, será realizada uma abordagem incremental, desenvolvendo a comunicação do microcontrolador com o leitor RFID, após isto, o desenvolvimento da conexão com a rede sem fio do campus, e ainda, o desenvolvimento da comunicação com uma outra fechadura.
- Executar os testes necessários para a validação do sistema.

1.4 ORGANIZAÇÃO DO TRABALHO

Além deste capítulo de introdução, este trabalho está dividido em mais 5 (cinco) capítulos.

O **Capítulo 2** apresenta a tecnologia de identificação por radio frequência, com suas principais características, tipos de etiquetas, frequências e padrões.

O **Capítulo 3** apresenta uma abordagem de sistemas embarcados, mostrando as aplicações e detalhando o principal componente deste tipo de sistema que é o microcontrolador.

O **Capítulo 4** aborda as tecnologias de redes de computadores que serão úteis no projeto.

No **Capítulo 5** é feita a descrição do sistema proposto, seus requisitos funcionais e não funcionais, a definição do escopo do projeto, testes realizados e os resultados obtidos.

O **Capítulo 6** apresenta as considerações finais sobre o desenvolvimento do projeto e sugestões para trabalhos futuros.

2 IDENTIFICAÇÃO POR RÁDIO FREQUÊNCIA

Neste capítulo será apresentada uma definição da tecnologia de Identificação por Rádio Frequência (RFID), bem como uma contextualização histórica. Após essa conceituação, o enfoque será nas etiquetas RFID, trazendo diferenciação de tipos, exemplos e aplicações.

2.1 DEFINIÇÃO

Processos de identificação automáticos (Auto-ID) têm se tornado muito populares atualmente, em vários segmentos da indústria, logística de compra e distribuição, fábricas e sistemas de fluxo de material, sendo possível citar desde os códigos de barra, presentes em todos os produtos atualmente, até *smart cards* como cartões de banco e de crédito, muito utilizados no dia-a-dia. Porém esses tipos de identificação têm limitações que, em alguns casos tornam a sua utilização inviável (FINKENZELLER, 2003).

Uma solução tecnicamente ótima requer que a etiqueta consiga armazenar mais dados que um simples código de barras. Utilizando um chip de silício resolve-se este problema, sendo o *smart card* o dispositivo eletrônico mais comum de armazenamento de dados neste sentido. Entretanto o contato mecânico necessário para realizar a leitura dos dados torna esta opção impraticável. Um sistema de comunicação sem contato entre o leitor e o dispositivo responsável por armazenar os dados seria o ideal. Um sistema de Auto-ID reunindo tais funcionalidades é o RFID, amplamente utilizado em vários seguimentos da indústria (FINKENZELLER, 2003).

RFID (*Radio Frequency Identification*) é um método sem fio de conectar dois circuitos eletrônicos. Esta tecnologia é amplamente utilizada em aplicações como cartões de viagem, controle de acesso predial, rastreamento de inventário sendo uma tecnologia bastante utilizada na ideia de internet das coisas ou IoT (*Internet of Things*) (GROUT; SILVA, 2014).

Segundo Domdouzis, Kumar e Anumba (2007), a tecnologia RFID é baseada na detecção de sinais eletromagnéticos, utilizando sensores sem fio. Tipicamente, um sistema RFID é composto de três componentes: uma antena ou bobina, um transceptor (leitor) e um transponder (*tag* RFID) programado eletronicamente com informação única.

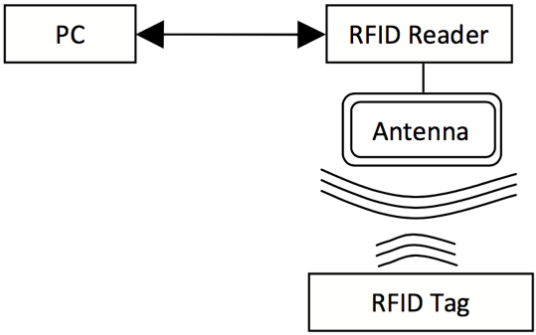

Figura 1 – Componentes de um sistema RFID.
Extraído de: (GROUT; SILVA, 2014)

2.2 BREVE HISTÓRICO

A história da identificação por rádio frequência começa em meados do século XX, devido aos grandes investimentos que a Segunda Guerra Mundial (SGM) trouxe, havendo grande desenvolvimento técnico na área de radares. Um radar envia ondas de rádio para a detecção e localização de um objeto pela reflexão da onda, sendo assim possível determinar a posição e a velocidade do objeto. Um dos primeiros trabalhos utilizando esses conceitos e explorando o RFID foi publicado por *Harry Stockman*, "*Communication by Means of Reflected Power*", em 1948.

Trinta anos se passariam até que as visões de *Stockman* alcançassem uma implementação de fato. Isso se deve aos avanços que eram necessários, mas que na época ainda não haviam sido obtidos como: transistor, circuitos integrados, microprocessadores, redes de comunicação e mudanças nos métodos de se fazer negócios. Nos anos 1970 desenvolvedores, inventores, industrias, universidades e laboratórios governamentais estavam trabalhando ativamente com RFID. Em 1975, o laboratório científico de Los Alamos (*Los Alamos Scientific Laboratory, Northwestern University*) publicou o estudo *"Short-Range Radio-Telemetry for Electronic Identification Using Modulated Backscatter*", apresentado por *Alfred Koelle, Steven Depp e Robert Freyman.* Este artigo deu origem à *tags* práticas e completamente passivas, com uma faixa operacional de dezenas de metros (LANDT, 2005).

A partir dos anos 1980 ocorreu a consolidação da tecnologia,

sendo implantada em vários seguimentos de mercado. Nos Estados Unidos, o interesse principal era na área de transporte, acesso pessoal e, em uma extensão menor, identificação de animais. Na Europa, o interesse era parecido, porém com foco maior nos sistemas para animais e indústrias, embora algumas rodovias com pedágio já eram equipadas com RFID na Itália, França, Espanha, Portugal e Noruega (LANDT, 2005). Um resumo dos fatos relevantes na história do RFID é demonstrado na Tabela 1.

Década	**Evento**
1940-1950	Uso e refinamento de Radares, devido aos esforços provocados pela SGM. RFID inventado em 1948.
1950-1960	Começo de explorações da tecnologia RFID, experimentos em laboratório.
1960-1970	Desenvolvimento da teoria do RFID. Começo dos testes em aplicações.
1970-1980	Aumento do desenvolvimento com RFID. Aceleração dos testes. Primeiras adoções de implementações com RFID.
1980-1990	Grande fluxo de aplicações comerciais com RFID.
2000-	Forte utilização do RFID continua.

Tabela 1 – Evolução histórica da tecnologia RFID conforme o passar das décadas.
Extraído e adaptado de: (LANDT, 2005)

2.3 ETIQUETAS RFID

Uma tag RFID é composta por dois componentes principais: um CI (Circuito Integrado) e uma antena, como está representado na Figura 2. O CI consiste em um microprocessador, uma memória não volátil e uma antena. O papel da antena é definir o alcance de leitura do dispositivo. As etiquetas RFID podem ser distinguidas em duas categorias, dependendo da sua capacidade de armazenamento de dados: somente leitura, do inglês *Read-Only*, e etiquetas leitura/escrita (*Read/Write*). Normalmente uma etiqueta somente leitura não possui capacidade de armazenar dados, sendo composta somente por um ID único pré-escrito no processo de fabricação. Esse ID combinado com

uma base de dados possibilita a identificação do objeto anexado à *tag* (DOMDOUZIS; KUMAR; ANUMBA, 2007).

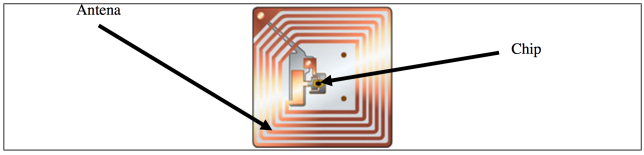

Figura 2 – Circuito interno típico de uma *tag*.
Extraído de: (TAPIA et al., 2007)

Além das características de armazenamento, as etiquetas classificam-se em passivas e ativas. As etiquetas passivas caracterizam-se por ter como fonte de alimentação o próprio leitor, ou seja, as ondas eletromagnéticas emitidas pelo dispositivo de leitura alimentam a etiqueta para que ocorra a transferência de dados, enquanto que as etiquetas denominadas ativas possuem sua própria fonte de alimentação. É claro que as diferenças vão além, fazendo com que cada tipo de etiqueta seja ideal para diferentes aplicações (MEHRJERDI, 2014). A Figura 3 apresenta exemplos de etiquetas passiva.

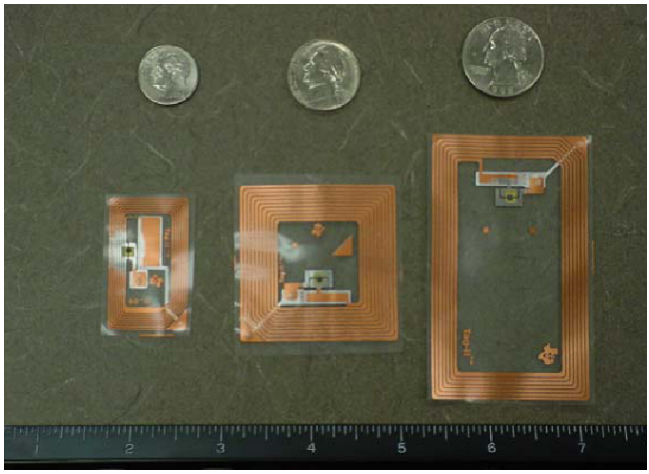

Figura 3 – Etiquetas fabricadas pela *Texas Instruments*.
Extraído de: (CUNHA, 2016)

Tags ativas tipicamente são maiores e mais caras que as passivas. O uso de bateria também limita a vida útil do dispositivo, entretanto,

com as tecnologias de baterias disponíveis atualmente, esse tempo pode durar tanto quanto 10 anos. Já as *tags* passivas tem uma vida útil ilimitada, são mais leves, menores e baratas. Por não serem alimentadas por bateria, têm um curto alcance para a realização da transferência de dados e é necessário um leitor de maior potência (ROBERTS, 2006). Um resumo das diferentes características oriundas das etiquetas é apresentado na Tabela 2.

	***tag* Ativa**	***tag* Passiva**
Fonte de alimentação	Interna	Energia é transferida do leitor
Disponibilidade	Contínua	Somente quando estiver no campo do leitor.
Potência do sinal do leitor necessário	Baixo	Alto
Potência do sinal disponibilizado pela tag	Alto	Baixo
Alcance	Longo (dezenas de metros)	Curto (centímetros)
Leituras simultâneas	Milhares de tags por um único leitor. Leitura de até 20 tags em movimento a mais de 160 km/h.	Centenas de tags por único leitor. Até 20 tags em movimento a até 18 km/h.
Armazenamento de dados	Grande (kB)	Pequeno (Alguns bytes)

Tabela 2 – *tag* ativa vs *tag* passiva
Extraído e aptado de: (DOMDOUZIS; KUMAR; ANUMBA, 2007)

2.3.1 Padrões

Existe uma variedade de padrões para assegurar a interoperabilidade de dispositivos pela especificação das camadas física e de enlace. Os padrões apresentados a seguir independem da área de aplicação, porém, devido às suas características, normalmente cada um se enqua-

dra melhor em determinado âmbito (HENRICI, 2008).

Padrões ISO (*International Organization for Standardization*) focam na comunicação entre a etiqueta e o leitor:

- ISO/IEC 14443:2000/2001:*Identification cards - Contactless integrated circuit(s) cards - Proximity cards* (Cartões de Identificação - Cartões sem contato com CI's - Cartões de proximidade)

  Parte 1: Características físicas

  Parte 2: Potência de radiofrequência e interface de sinal

  Parte 3: Inicialização e anti-colisão

  A comunicação é realizada em 13.56 MHz nesse padrão.

- ISO/IEC 15693:2000/2001: *Identification cards - Contactless integrated circuit(s) cards - Vicinity cards* (Cartões de identificação - Cartões sem contato com CI's - Cartões de proximidade)

  Neste padrão a comunicação acontece na frequência de 13.56 MHz e geralmente oferece um alcance de leitura de 1-1.5 metros.

- ISO/IEC 18000:2004: *Information technology - Radio frequency identification for item management* (Tecnologia da informação - RFID para gerenciamento de itens)

  Parte 1: Arquitetura de referência e definição de parâmetros a serem padronizados.

  Parte 2: Parâmetros para comunicações de interface aérea abaixo de 135 kHz.

  Parte 3: Parâmetros para comunicações de interface aérea em 13.56 MHz.

  Parte 4: Parâmetros para comunicações de interface aérea em 2.45 GHz.

  Parte 6: Parâmetros para comunicações de interface aérea entre 860 MHz e 960 MHz.

  Parte 7: Parâmetros para comunicações de interface aérea ativa em 433 MHz.

Estes padrões ISO são amplamente respeitados, mesmo a *EPCglobal Inc.* com uma aceitação gigantesca pela indústria, especifica seus protocolos de acordo com os padrões internacionais. Existem também outros padrões como o Zigbee que opera a 2.54 GHz, podendo ser

utilizado para propósitos de RFID. Para gerenciamento de itens existem também os padrões ISO 15961, 15962, e 15963, que definem uma aplicação específica do protocolo de dados, assim operando em uma camada mais alta (HENRICI, 2008).

2.3.2 Cartão de Identificação UFSC

Estudantes e professores da UFSC recebem um cartão de identificação, contendo informações como foto, matrícula, curso, etc. Entretanto o cartão possui em seu interior um transponder RFID passivo, que ainda não apresenta funcionalidades nas dependências da instituição, a não ser portar as informações impressas em sua superfície (Figura 4).

Figura 4 – Comparação do cartão de identificação UFSC com um cartão de crédito.

Segundo informações coletadas com a Superintendência de Governança Eletrônica e Tecnologia da Informação e Comunicação (SeTIC) da UFSC, o padrão das *tags* contidas nos cartões de identificação é o ISO 14443, que realiza a comunicação na frequência de 13.56 MHz.

2.3.3 Aplicações com RFID

Características como a capacidade de coletar, armazenar e transmitir dados fazem com que as *tags* RFID tenham uma variabilidade de aplicações. O uso comum, para a tag passiva, é no rastreamento de produção, controle de acesso predial, rastreamento de bagagens de linhas aéreas, etc. Empresas como Wal-Mart, GAP, Old Navy e P&G

usam as etiquetas no controle da sua cadeia de suprimentos. Uma aplicação muito comum é em rodovias pedagiadas, cujo sistemas do tipo "EZ-Pass" fazem a automatização da cobrança (ZHU; MUKHOPADHYAY; KURATA, 2012). Em (MEHRJERDI, 2014) o autor apresenta algumas áreas de aplicação descritas abaixo.

- Linhas aéreas - Várias companhias como *British Airways*, *United*, *Japanese* e *Southwest* têm experiência com RFID, entretanto a *Delta Airlines* é a líder no uso da tecnologia. Um programa piloto da empresa, utilizando 40000 malas, mostrou que com o RFID a leitura obteve uma resposta correta em 98% dos casos, enquanto que, com código de barras, os dados eram de 85%.

- Indústrias de manufaturas - Talvez a aplicação de maior implementação do RFID seja na área de rastreamento de inventário e recursos. Muitas empresas utilizam o EPC (*Electronic Product Code*) nas suas cadeias de suprimentos. O EPC emprega as *tags* RFID que são colocadas fisicamente em garrafas, caixas, pacotes e paletes no começo da cadeia. Com isso, os produtos podem ser rastreados conforme seus movimentos na cadeia de suprimentos.

- Indústria farmacêutica - Neste seguimento o RFID é considerado uma ferramenta importante no combate a falsificação de medicamentos. A agência americana de alimentos e medicamentos (FDA) requisitou para as empresas da indústria que começassem a investir em soluções de rastreamento utilizando a tecnologia, para melhorar a segurança da cadeia de suprimentos, visto que fatores como local de trabalho, transporte e data de validade são elementares no ramo farmacêutico.

- e-Passaporte - Aplicação básica da tecnologia para a garantia da veracidade dos passaportes, dificultando muito a falsificação de documentos.

- Identificação animal - O rastreamento e a identificação dos rebanhos são obrigatórios em muitos países (inclusive no Brasil) para a garantia da procedência dos produtos de origem animal. Isto acaba gerando um grande negócio, por exemplo, a comunidade Europeia e a Nova Zelândia se juntaram entre os anos de 2008 e 2010 para criar um mercado para a etiquetagem de ovelhas, cabras, porcos e vacas, estimando-se uma demanda de 150 milhões de *tags*.

2.3.4 Frequência

RFID é fundamentalmente baseada na comunicação sem fio, utilizando ondas de rádio, que fazem parte do espectro eletromagnético (frequências de 300kHz a 3 GHz). O RFID opera no espaço de espectro denominado ISM (*Industrial, Scientific and Medical*), entretanto as frequências exatas que constituem o ISM podem variar dependendo das regulamentações em diferentes países. Estas frequências de operação, normalmente são divididas em quatro principais bandas de frequência apresentadas na Tabela 3 (WARD; KRANENBERG et al., 2006).

Banda	**LF - Baixa Frequência**	**HF - Alta Frequência**	**UHF - Ultra Alta Frequência**	**Micro-ondas**
Frequência	125-134 kHz	13.56 MHz	433 MHz ou 865-956 MHz	2.45 GHz
Distância aproximada de leitura	Menos de 50 cm	Até 1.5 metros	433MHz= até 100m 865-956 MHz= 0.5 a 5 metros	até 10 metros
Taxa de transferência de dados típica	menos de 1 kilobit por segundo (kbps)	25 kbps	30 kbps	até 100 kbps
Características	Curta distância, baixa taxa de transferência de dados, penetra água.	Maior alcance, taxa razoável de transferência de dados, penetra água.	Longo alcance, taxa alta de dados, leitura concorrente de até 100 itens, não consegue penetrar água nem metal.	Longo alcance, alta taxa de transferência de dados, não consegue penetrar água nem metal.
Utilização típica	Identificação animal, imobilizador de carros	Etiquetas inteligentes, cartões de viagem, Acesso e segurança	Rastreamento especialista de animais, Logística	Pedágio

Tabela 3 – Frequências de operação do RFID e suas características. Extraído e adaptado de: (WARD; KRANENBERG et al., 2006)

3 SISTEMAS EMBARCADOS

Segundo White (2011), sistema embarcado é um sistema computadorizado que é construído para um propósito específico conforme sua aplicação. Geralmente referidos como computadores pervasivos ou ubíquos, sistemas embarcados representam uma classe dedicada de sistemas computacionais projetados para serem embutidos em um dispositivo (LI; YAO, 2003).

Devido às limitações da sua missão, em comparação com computadores de propósito geral, tipicamente um sistema embarcado não suporta questões que não estão relacionadas à realização da tarefa em foco, empregando um *hardware* mais restrito. Para exemplificar essas restrições, pode ser considerado uma CPU (Unidade Central de Processamento) mais lenta, projetado para consumir pouca energia para economizar bateria, ou um sistema que utilize menos memória para reduzir os custos de fabricação (WHITE, 2011).

Assim como o *hardware*, o *software* embarcado também apresenta peculiaridades em relação à computação de propósito geral, onde normalmente tudo é orquestrado por um sistema operacional. Executando várias aplicações, um computador pessoal pode atuar, ora como processador de palavras, ora como mp3 *player* ou um banco de dados. O *software* que estiver carregado no momento é que terá o controle. Em contra partida, o sistema embarcado é tipicamente dedicado, executando permanentemente uma tarefa específica, podendo ou não ter um sistema operacional. Todo o programa normalmente está contido na memória não-volátil do sistema, diferentemente do PC onde neste tipo de memória está o *boot* (que faz a inicialização do sistema) e talvez alguns *drivers* de baixo nível (CATSOULIS, 2005).

Este tipo de *software* específico para o controle de um *hardware* embarcado é denominado *firmware*, sendo este um conjunto de regras que rege o funcionamento do sistema (OLIVEIRA; ANDRADE, 2006).

3.1 MICROCONTROLADORES

Um sistema embarcado tipicamente tem como figura principal o microcontrolador. Ibrahim (2006) define microcontrolador como um computador em um único chip especialmente manufaturado para o controle de aplicações embarcadas. Estes dispositivos são de baixo custo e podem ser utilizados facilmente no controle de aplicações, visto que

a maioria dos microcontroladores têm os circuitos internos necessários para isto. Por exemplo, um microcontrolador pode ter conversores A/D (analógico para digital) de modo que sinais externos possam ser amostrados e processados digitalmente. Microcontroladores podem também serem dotados de *timer* e lógica de interrupção, com isso é possível implementar algoritmos de controle bastante precisos.

3.1.1 Evolução dos Microcontroladores

A *Intel Corporation* geralmente é reconhecida como a primeira empresa a introduzir com sucesso o primeiro microprocessador no mercado. Nomeado de 4004, foi apresentado em 1971 e evoluiu do desenvolvimento de um conjunto de *chips* para calculadoras, onde o microprocessador de 4 bits era o componente central do conjunto, chamado de MCS-4. Os outros componentes eram uma memória ROM (*Read-Only Memory*) 4001, uma memória RAM (*Randon-Access Memory*) 4002 e um registrador de deslocamento 4003. Depois do 4004, apareceram no mercado comercial três outros microprocessadores de propósito geral: o *Rockwell International* PPS-4 de 4 bits, o Intel 8008 de 8 bits e o *National Semiconductor* IMP-16 de 16 bits (RAFIQUZZAMAN, 2011).

Durante os anos 1980, quando microprocessadores de 32 bits já estavam sendo introduzidos no mercado, surgiram os microcomputadores em um único chip, como o Intel 8048. Pouco tempo depois, baseado no conceito do microcomputador em um único chip, a Intel introduziu o primeiro microcontrolador de 8 bits - o Intel 8051, que usa arquitetura Harvard e conjunto de instruções CISC (*Complex Instruction Set Computing*). O 8051 é constituído de CPU, memória, pinos de I/O, conversores A/D e D/A, *timer* e interface de comunicação serial, tudo em um único chip. Os microcontroladores de 8 bits são utilizados até hoje, pois são pequenos e adequados para aplicações embarcadas, porém são potentes o suficiente para permitirem o design de sistemas embarcados de maior complexidade e flexibilidade (RAFIQUZZAMAN, 2011).

3.1.2 Recursos Integrados

Microcontroladores, particularmente aqueles fabricados para sistemas embarcados, frequentemente disponibilizam um número de circuitos auxiliares integrados à eles. Esta integração apresenta vantagens

como a velocidade de comunicação das partes com o processador central e a economia de circuitos externos ao *chip* do microcontrolador. Cada circuito auxiliar, ou periférico, é controlado com a escrita de valores em registradores que tipicamente aparecem em uma porção fixa da área de endereçamento do microcontrolador (SIMON, 1999).

Os principais tipos destes recursos serão descritos a seguir.

3.1.2.1 *Timers*

É comum existir um ou mais *timers* em um microcontrolador. Essencialmente, este recurso é um contador incrementado através dos ciclos de *clock* do microcontrolador, causando uma interrupção no sistema quando a contagem expira. Uma característica usual dos *timers* é o *pre-scaler*, cuja função é dividir o sinal de *clock* por uma constante, ou seja, a cada x sinais de *clock* o contador incremente uma unidade (SIMON, 1999).

3.1.2.2 Pinos de Entrada e Saída

Nas aplicações embarcadas, é comum um microprocessador conter alguns ou algumas dezenas de pinos de I/O (*Input/Output*). Estes pinos podem ser configurados como saídas, onde o *software* gera nível baixo ou alto diretamente, geralmente pela escrita de um registrador, ou podem ser configurados como entradas que o programa é capaz de ler. Estes pinos podem ser utilizados para vários propósitos como: ligar e desligar diodos emissores de luz (LEDs), manipular memórias externas, *displays*, etc (SIMON, 1999).

Alguns microcontroladores apresentam uma opção extra de pinos de saída. Estes pinos são capazes de utilizar a técnica de PWM (*Pulse Width Modulation*). Esta modulação por largura de pulso é capaz de gerar uma onda quadrada e regular o "ciclo de trabalho"(*duty cycle*). Por exemplo, para um ciclo de trabalho de 50%, a onda deve estar meio período em nível alto e meio em baixo. Se a amplitude da onda for de 5V resultará em uma média de 2.5V. O PWM é uma técnica para escrever valores analógicos sem a necessidade de um conversor Digital para Analógico (CATSOULIS, 2005).

3.1.2.3 Interrupção

O fluxo de execução que um microcontrolador esteja realizando pode ser interrompido. A interrupção sinaliza para o dispositivo parar de fazer o que estava previamente fazendo e executar outro segmento de código. Esta porção de código é denominada rotina de interrupção (SIMON, 1999). Podem existir interrupções internas, como a gerada por um *timer*, e interrupções externas, sinalizadas tipicamente através de um nível lógico no pino designado para interrupção do microcontrolador. As interrupções permitem respostas imediatas do microcontrolador à eventos, liberando o mesmo para realizar sua execução normal enquanto eles não ocorrem (OLIVEIRA; ANDRADE, 2006).

3.1.2.4 Comunicação Serial

A comunicação serial envolve a transferência de dados por meio de um fio para cada direção, sendo um para a recepção e outro para a transmissão. É ideal no caso de uma conexão paralela não ser empregável, sendo por questões físicas ou em termos de custos. Em sistemas embarcados, a comunicação serial é a forma mais fácil e de baixo custo para a conexão com um computador hospedeiro, seja este parte da aplicação ou apenas para fins de depuração (CATSOULIS, 2005).

Um padrão bastante utilizado é o SPI™(*Serial Peripheral Interface*), um método de comunicação síncrono e de alta velocidade entre periféricos como um microcontrolador e uma memória externa (OLIVEIRA; ANDRADE, 2006). SPI utiliza a denominação de *master* e *slave*, sendo que o dispositivo *master* pode controlar o *clock* a até 100 MHz de velocidade. Ou seja, se o *clock* estiver sendo gerado a 8 MHz, a taxa de transferência de dados será de 1 MB/s, muito mais rápida que em outros protocolos (WHITE, 2011).

Outro protocolo de uso comum no universo dos microcontroladores é o I2C™(*Inter-Integrated Circuit*), um protocolo síncrono de apenas dois fios: uma linha de *clock* e outra de dados (OLIVEIRA; ANDRADE, 2006). Diferentemente do SPI, o I2C permite múltiplos dispositivos *masters* e *slaves*. Essa simplicidade de necessitar apenas um fio para *clock*, outro para dados e um para terra, implica em complexidade de *software* para o gerenciamento dos dispositivos interligados.

3.1.3 Aplicações com Microcontroladores

Quase tudo que envolve eletrônica atualmente emprega um microcontrolador, gerando facilidades de projeto, manutenção e diminuição das dimensões de aparelhos eletroeletrônicos. Este dispositivo é capaz de fazer o papel de vários componentes do circuito, podendo-se dizer que programando o microcontrolador para realizar um passo-a-passo de tarefas (instruções) resume-se o circuito em um único componente (MARTINS, 2005).

As áreas de atuação dos microcontroladores são as mais diversas, tipicamente quando o assunto é automação, emprega-se um ou mais microcontroladores no projeto, como em automação residencial, predial, industrial, comercial, agrícola, além de áreas como a automobilística, produtos manufaturados, etc (OLIVEIRA, 2012).

Citando um exemplo, a Microchip, empresa responsável pelos microcontroladores PIC (*Peripheral Interface Controller*), investe na produção de dispositivos que facilitem sua aplicação em automóveis. Analisando números, estima-se que sejam fabricados aproximadamente 63 milhões de veículos anualmente no mundo, gerando um mercado gigante para as empresas do ramo, visto que cada automóvel necessita em média de 30 microcontroladores para suas funcionalidades básicas, podendo dobrar este número em modelos mais completos. São aplicações básicas às mais sofisticadas, como: Injeção eletrônica de combustível, freios ABS (*Anti-lock Braking System*), controle de tração, suspensão e aceleração, acionamento de vidros e travas elétricas, *air-bag*, etc (CORTELETTI, 2006).

Oliveira (2012) define que, de uma maneira geral, os microcontroladores são componentes tecnológicos que favorecem a vida moderna, facilitando e melhorando a vida dos usuários. Aumentam a eficiência, permitem a redução de custos, mas ao mesmo tempo elevam o valor agregado dos produtos já que aumentam significativamente as funcionalidades dos mesmos.

3.2 ESTUDO DE CASO - MICROCONTROLADOR ESP8266

Produzido pela fabricante chinesa *Espressif Systems*, o ESP8266 (Figura 5) é um SoC (*System on a Chip*) *Wi-Fi* de baixo custo com a implementação da pilha TCP/IP completa. Utilizando o chip como adaptador Wi-Fi, acesso à internet sem fio pode ser adicionado a qualquer projeto microcontrolado, basta conectar o microcontrolador ao

módulo através de uma interface de comunicação serial simples como SPI ou I2C. Além de atuar como adaptador para comunicação *wireless*, ele pode também ser o microcontrolador hospedeiro da aplicação, visto que o dispositivo contêm um processador de 32 bits com baixo consumo energético e *clock* de 80 à 160 MHz (ESPRESSIF SYSTEMS, 2016b).

Figura 5 – ESP8266EX: núcleo dos módulos ESP.

3.2.1 Variações do ESP

Outra fabricante chinesa, a *AI Thinker* utiliza o ESP8266 para a fabricação de módulos largamente aceitos no mercado. Os módulos são nomeados "ESP-xx", onde "xx"representa uma numeração que até o momento vai de 01 à 14. Cada variação do ESP tem alguma característica diferente para variados tipos de projetos. Pode-se destacar o ESP-12F (Figura 6), um SoC completo, com comunicação Wi-Fi, CPU e 4 MB de memória *flash*, que para um microcontrolador é suficiente para executar aplicações volumosas, como um sistema operacional embarcado de tempo real (RTOS).

Figura 6 – ESP-12F.

É importante ressaltar que, apesar de ser um microcontrolador com diversas funcionalidade, como comunicação Wi-Fi e velocidade de processamento alta, os módulos ESP têm dimensões muito reduzidas, como é demonstrado na comparação com uma moeda da Figura 7. Outras características dos módulos são: conversor A/D com resolução de 10 bits, pinos de saída com PWM (*Pulse Width Modulation*), comunicação I2C, SPI, UART, 32 KBytes de RAM para instruções, 96 KBytes de RAM para dados e 64 KBytes de ROM para boot (CURVELLO, 2015).

Figura 7 – Comparativo de alguns módulos ESP com uma moeda.
Extraído de: (CURVELLO, 2015)

A Tabela 4 apresenta algumas características das diferentes variações do ESP.

ID da Placa	Pinos	Antena	Dimensões (mm)
ESP-01	8	Impressa na PCB	14.3 x 24.8
ESP-02	8	Nenhuma	14.2 x 14.2
ESP-03	14	Cerâmica	17.3 x 12.1
ESP-04	14	Nenhuma	14.7 x 12.1
ESP-05	5	Nenhuma	14.2 x 14.2
ESP-06	12+GND	Nenhuma	16.3 x 13.1
ESP-07	16	Cerâmica	20 x 16
ESP-08	14	Nenhuma	17 x 16
ESP-09	12+GND	Nenhuma	10 x 10
ESP-10	5	Nenhuma	14.2 x 10
ESP-11	8	Cerâmica	17.3 x 12.1
ESP-12	16	Impressa na PCB	24 x 16
ESP-12E	22	Impressa na PCB	24 x 16
ESP-13	18	Impressa na PCB	18 x 20
ESP-14	22	Impressa na PCB	24.3 x 16.2

Tabela 4 – Módulos ESP8266.
Extraído e adaptado de: (JALAMKAR; SELVAKUMAR, 2016).

3.3 ATUADORES

Atuadores são os dispositivos utilizados pelo *software* embarcado para impactar mecanicamente o ambiente no qual está inserido. O atuador de maior simplicidade é o solenoide, que pode ser idealizado como um botão reverso. Ao ser colocado em nível alto, o solenoide está em determinada posição, já em nível baixo está em outra. Esta característica é bastante usual para aplicações como ligar e desligar válvulas ou trancar e destrancar algo (WHITE, 2011).

Um solenoide é basicamente constituído de uma bobina e um núcleo de ferro macio. Quando um sinal DC ativa a bobina, o núcleo de ferro se magnetiza, podendo assim mover um elemento ferromagnético (pino ou êmbolo). Este dispositivo é considerado austero e barato, tendo aplicações como atuadores de válvulas, interruptores mecânicos,

relés e outros sistemas de posição de dois estados (SILVA, 2015). Um exemplo de solenoide em um relé é demonstrado na Figura 8.

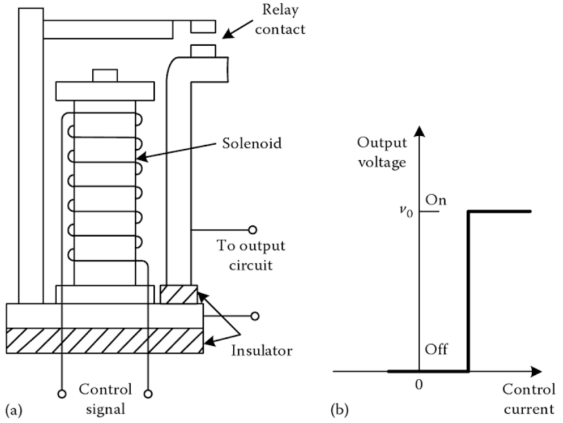

Figura 8 – (a) Componentes físicos do relé e (b) curva característica. Extraído de: (SILVA, 2015).

3.3.1 Estudo de caso - Fecho Eletromagnético Amelco FE61

O fecho eletromagnético FE61 (Figura 9) fabricado pela empresa Brasileira *Amelco* é uma solução para controle de acesso praticável para a utilização em um projeto, visto que seu custo fica abaixo dos 100 (cem) reais. O custo pode ser considerado baixo, pois seu funcionamento é bastante simples e é feito para funcionar juntamente com outro dispositivo, e.g. um porteiro eletrônico. Este outro dispositivo pode ser também qualquer solução microcontrolada que implemente um circuito acionador com 12 a 18 Volts de tensão DC. O fecho eletromagnético é instalado no batente da porta, e funciona conjuntamente com fechaduras mecânicas convencionais do tipo que movimenta a lingueta através da maçaneta pelo lado interno e somente com chave pelo externo (AMELCO S.A., 2007).

Figura 9 – Fecho eletromagnético Amelco FE61.
Extraído de: (AMELCO S.A., 2007).

4 REDES DE COMUNICAÇÃO

O assunto redes de comunicação, atualmente, remete à internet. Há pouco tempo, a definição de internet era uma rede de computadores capaz de interligar milhares de computadores. Porém, atualmente o termo "redes de computadores"soa desatualizado. Isto se deve ao fato de existirem hoje outros tipos de sistemas finais, como TVs, laptops, consoles de jogos, celulares, automóveis, etc. Estes sistemas finais são conectados entre si através de enlaces de comunicação e comutadores de pacotes. Um comutador de pacotes realiza o encaminhamento do pacote que chega em um de seus enlaces de comunicação de entrada para um de saída. Exemplos de comutadores são roteadores, que atuam no núcleo da rede, e *switches*, comumente utilizados em redes de acesso. Para exemplificar esta comutação utilizada na internet, pode-se comparar uma rodovia trafegada por caminhões carregados com seguimentos de uma carga maior. Ao chegarem no destino final, os seguimentos da carga são agrupados, formando uma grande remessa. Deste modo, os caminhões se assemelham aos pacotes, rodovias aos enlaces de comunicação e os comutadores de pacotes são relacionados aos cruzamentos existentes ao longo das rodovias e estradas (KUROSE; ROSS, 2010).

Uma rede como a internet, é definida como sendo uma rede de redes. Entretanto as redes podem ser classificadas de diversas maneiras diferentes. Uma diferenciação típica é quanto a abrangência geográfica da rede. A internet é um exemplo de WAN (*Wide Area Network*), sendo esta uma rede de longa distância, com área de abrangência maior que apenas uma cidade. Outras classificações são: MAN (*Metropolitan Area Network*), CAN (*Campus Area Network*), LAN (*Local Area Network*) e a WLAN (*Wireless Local Area Network*). As redes WLAN são bastante utilizadas atualmente devido ao número de dispositivos móveis capazes de se conectarem à internet, que fazem o uso de redes sem fio ser o mais módico para tal. A WLAN utiliza transmissões por radio frequência, padronizadas por protocolos como o IEEE 802.11, popularmente conhecido como *Wi-Fi* (TORRES, 2013).

Outra classificação das redes de computadores é quanto à topologia, sendo esta a maneira como os computadores estão conectados em uma rede local. Torres (2013) define as topologias possíveis como:

- Topologia totalmente conectada - Como o nome sugere, nesta topologia todos os computadores da rede estão conectados com todos, ou seja, existe uma conexão individual com cada computador da rede (Figura 10).

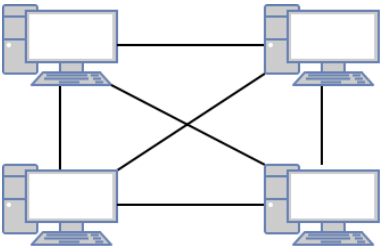

Figura 10 – Topologia totalmente conectada.
Adaptado de: (TORRES, 2013)

- Topologia em malha - Ilustrada na Figura 11, este modelo é similar ao anterior, porém nem todos os computadores estão conectados com uma conexão individual, necessitando passar por outro computador para ter acesso a determinados destinatários.

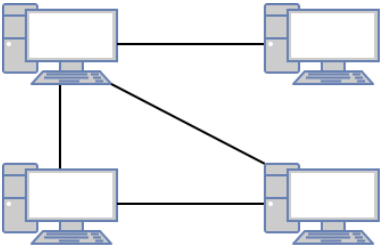

Figura 11 – Topologia em malha.
Adaptado de: (TORRES, 2013)

- Topologia em anel - Cada computador tem a conexão com o anterior e o próximo, necessitando que a comunicação de um computador com outro passe pelos dispositivos no caminho. O método utilizado para a comunicação é por passagem de ficha (Figura 12), onde somente quem detêm o quadro representativo da ficha é que pode transmitir se o canal estiver desocupado, assim é garantido que somente um dispositivo transmita dados, evitando colisões.

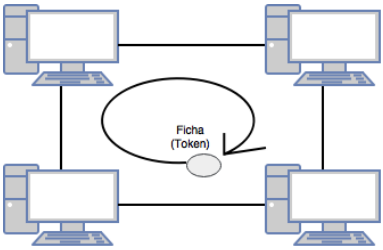

Figura 12 – Topologia em anel.
Adaptado de: (TORRES, 2013)

- Topologia linear - Topologia utilizada em redes *Ethernet* conectadas com *hub*, onde há um barramento comum a todos os computadores da rede (Figura 13).

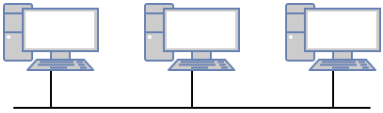

Figura 13 – Topologia em barramento.
Adaptado de: (TORRES, 2013)

- Topologia estrela - Neste tipo de ligação, os computadores são conectados à um periférico central, tipicamente um *switch* em redes *Ethernet* (Figura 14). A diferença desta para a topologia linear é que caso uma conexão falhe, as outras continuam funcionando, o que não ocorre na anterior.

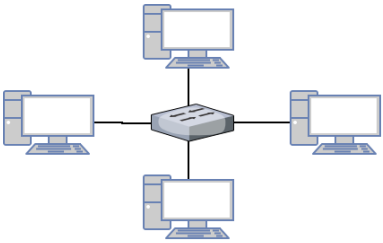

Figura 14 – Topologia em estrela.
Adaptado de: (TORRES, 2013)

- Topologia em árvore - Basicamente, é a ampliação da rede com topologia estrela, porém a conexão em árvore utiliza mais de um dispositivo concentrador (Figura 15).

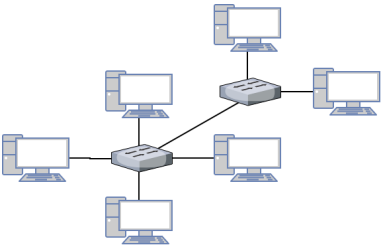

Figura 15 – Topologia em árvore.
Adaptado de: (TORRES, 2013)

- Topologia sem fio - Como o nome diz, permite conexões sem fio, sendo necessário um equipando denominado ponto de acesso (WAP, *Wireless Access Point*) para que exista a conexão dos dispositivos sem fio com a rede física (Figura 16) .

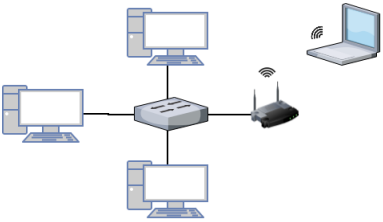

Figura 16 – Topologia sem fio.
Adaptado de: (TORRES, 2013)

- Topologia Híbrida ou mista - Utiliza mais de uma topologia ao mesmo tempo.

4.1 CLIENTE/SERVIDOR

O advento das redes de computadores possibilita a concepção de um sistema computacional distribuído. Este tipo de sistema contem aplicações e recursos dispersos entre computadores independentes interligados através de uma rede. Esta arquitetura distribuída permite que

usuários de computadores individuais conectados à rede compartilhem recursos e serviços, geralmente entre lugares geograficamente remotos (ADLER, 1995).

O modelo cliente-servidor tem sido um padrão dominante para computação distribuída desde os anos 1980. O surgimento de sistemas operacionais que pudessem suportar usuários trabalhando em seus computadores pessoais conectados por uma rede local (LAN) impulsionou a evolução e aceitação do modelo (JIA; ZHOU, 2005).

Um exemplo básico desta arquitetura é o armazenamento de dados e disponibilização de serviços de uma empresa em poderosos computadores, denominados servidores. Para se ter acesso a estes dados e serviços centralizados nestes servidores, os funcionários da empresa têm em sua mesa um computador convencional conectado à rede, podendo acessar as funções do servidor, como está ilustrado na Figura 17. Outra realização popular do modelo cliente-servidor é uma aplicação *Web*, onde o servidor é responsável por fornecer as páginas web com base em seu banco de dados em resposta às solicitações dos clientes, que normalmente são centenas ou milhares, requisitando o servidor simultaneamente (TANENBAUM, 2011).

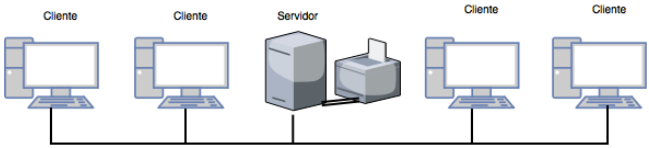

Figura 17 – Servidor para serviço de impressão.
Adaptado de: (JIA; ZHOU, 2005)

4.2 REDE DE SENSORES SEM FIO (WSN)

Redes de sensores sem fio (*Wireless Sensor Network*) são coleções de sensores sem fio altamente distribuídos, pequenos e leves, capazes de monitorar o ambiente ou sistemas (HUANG; HSIEH; SANDNES, 2008). Este tipo de rede é padronizada segundo o *IEEE 802.15.4*, protocolo este desenvolvido motivado pela aplicabilidade da tecnologia em monitoramento residencial, predial, industrial, etc. Esta motivação se deve à aplicação dos sensores sem fio em soluções de automação, capazes de aumentarem a eficiência energética, controle e a segurança dos ambientes. A redução dos custos de instalações em edifícios é outra questão que gera interesse nesta área. Estas reduções são vistas na eliminação

de custos com cabeamento e materiais relacionados, facilitando a instalação em ambientes já construídos sem a necessidade de grandes alterações (GUTIÉRREZ, 2007).

O IEEE 802.15.4 foi desenvolvido para aplicações não-críticas que não demandam alta taxa de dados na comunicação, favorecendo o baixo custo e consumo de energia dos dispositivos da rede. A eficiência energética é um ponto chave para estas aplicações, visto que a maioria dos dispositivos de uma WSN são alimentados por bateria. Em comparação com outras soluções sem fio, a primeira geração do IEEE 802.15.4 é até 50% mais eficiente que o *Bluetooth*^{TM}, por exemplo (GUTIÉRREZ, 2007).

4.3 REDES *MESH* SEM FIO

Como citado anteriormente, as redes de sensores sem fio são projetadas para comunicação simples, de baixo consumo e baixas taxas de transmissão de dados. Em contra partida, as redes *mesh* ou *Wireless Mesh Network* (WMN) são projetadas para dispositivos mais potentes, capazes de transmitir e receber dados em larguras de banda mais altas. Normalmente as WMNs são utilizadas como um *backbone* (canal principal da rede) sem fio para a interconexão de dispositivos finais. Outra funcionalidade que este tipo de rede pode oferecer é uma ligação com a internet (Figura 18), sendo ideais para a implantação em áreas que redes cabeadas não podem ser instaladas facilmente (BOUCKAERT et al., 2010).

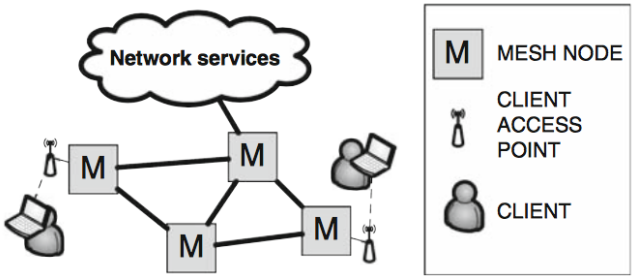

Figura 18 – Exemplo de arquitetura de rede *mesh*.
Extraído de: (BOUCKAERT et al., 2010)

4.3.1 ESP-Mesh

Em (ESPRESSIF SYSTEMS, 2016a), a internet das coisas é citada como razão do crescente número de nós conectados à rede. Entende-se nó, como qualquer dispositivo final ligado à internet. Porém, o número de nós que podem se conectar a um mesmo roteador ao mesmo tempo é limitado. Existem duas soluções para este problema: roteadores com maiores capacidades, para que os dispositivos possam se conectar diretamente ao roteador, ou uma rede *mesh* (em malha), como foi descrito na Seção 4.3 e ilustrada na Figura 19.

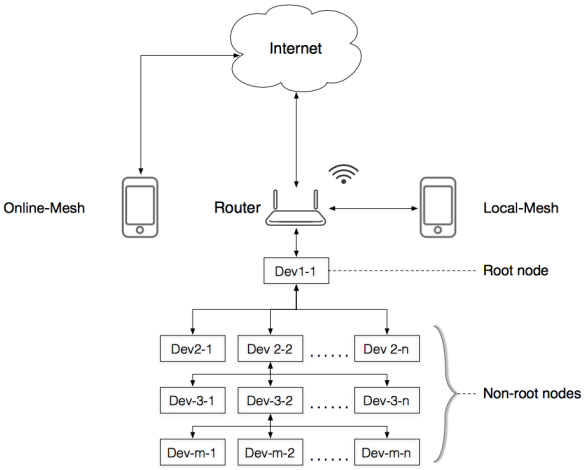

Figura 19 – Diagrama da rede *mesh*.
Extraído de: (ESPRESSIF SYSTEMS, 2016a)

A Figura 19 mostra dispositivos denominados *root node* (nó raiz) e *non-root nodes* (nós não-raiz). O nó raiz recebe e envia pacotes, bem como repassa pacotes do servidor, aplicativos móveis e de seus nós não-raiz. Já os nós não-raiz dividem-se em: nós não-folha e nós folha. Os nós intermediários (não folha) recebem e enviam pacotes e também repassam os pacotes dos seus nós pais (que estão acima dele) e filhos (nós no nível abaixo). Os nós folha somente recebem e enviam pacotes, mas não necessitam fazer o repasse de pacotes. O ESP-Mesh é uma API (*Application Programming Interface*) que auxilia no desenvolvimento dessas redes para os dispositivos descritos na Seção 3.2 (ESPRESSIF SYSTEMS, 2016a).

5 SISTEMA ELETRÔNICO INTEGRADO PARA CONTROLE DE ACESSO

Neste capítulo será apresentado o detalhamento do sistema proposto com o intuito de realizar o controle de acesso às salas e laboratórios da UFSC, Campus Araranguá.

5.1 DESCRIÇÃO

O sistema embarcado proposto engloba as tecnologias detalhadas nos capítulos anteriores. A autenticação do usuário será feita através da identificação por rádio frequência existente nos cartões de identificação da instituição. O RFID será lido por um leitor de etiquetas passivas ligado à um microcontrolador com capacidade de conectar-se à internet, sendo empregado no projeto o ESP-12, uma variação do ESP-8266, detalhados na Seção 3.2. O microcontrolador realizará a validação do usuário e o destravamento ou não de um atuador, que neste caso será um fecho eletromagnético. A ideia do microcontrolador estar conectado à rede sem fio é para a facilitação da tarefa de atualização dos dados de acesso de cada fechadura, implementando uma aplicação que irá trocar mensagens com as fechaduras em um modelo cliente-servidor. Entretanto, para se garantir que todos os dados cheguem até às fechaduras, mesmo àquelas que estão fora da cobertura da rede *wireless* do campus, as fechaduras atuam como nós em uma rede do tipo *mesh*, onde existe um nó raiz, atuando ao mesmo tempo como *Station* (ou seja, um dispositivo na rede *wireless*) e como *Access Point* que repassará as informações para os outros dispositivos de controle de acesso.

Na Figura 20 é demonstrada uma representação visual da arquitetura do sistema. O computador é o responsável por fazer a configuração das fechaduras através de uma página *web* servida localmente. O único nó conectado ao roteador é o nó raiz, com acesso simultâneo à rede *mesh* e ao *access point* mostrado, fazendo uma ponte entre os dois tipos de rede diferentes. Quando uma nova configuração é feita no computador, os dados são enviados através do *access point* para o nó raiz. Deste, os dados são enviados para a rede *mesh* até encontrar as fechaduras onde serão salvos.

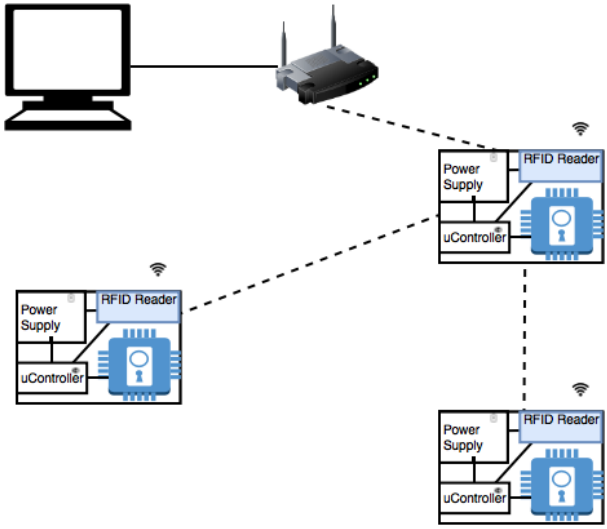

Figura 20 – Representação do sistema de controle de acesso proposto.

As características relevantes do sistema proposto são:

- componentes de baixo custo;
- capacidade de configuração remota usando rede *wireless* para evitar problemas com infraestrutura (evita passar cabos, instalar *switches*/roteadores, encontrar roteadores com portas vazias, etc);
- permitir que o sistema opere *offline*. O acesso à internet pode ser periodicamente interrompido por uma série de razões, assim não é admissível que o sistema necessite estar *online* para validar os usuários. Deve-se criar um cache de IDs válidos que fique armazenado na própria fechadura inteligente e assim quando o professor passar o seu cartão RFID, este será validado mesmo que o acesso à Internet tenha sido interrompido.

5.1.1 Requisitos do Sistema

Os requisitos definidos para o desenvolvimento do protótipo do sistema para controle de acesso, podem ser divididos em:

- **Requisitos funcionais**

1. Independente da infraestrutura de Rede Wireless da Instituição;

2. Funcionamento autônomo para validação de usuários;

3. Propagação transparente das atualizações de acesso de uma ou mais fechaduras;

4. Possibilidade de expansão através de adição de módulos sensores (sensor de luz acesa, ventilador ligado, janela aberta, etc.).

- **Requisitos não funcionais**

1. Custo Reduzido;

2. Design Compacto;

3. Interface visual de configuração.

5.2 PROJETO DE HARDWARE

Podemos dizer que o projeto de *hardware* do sistema foi simplificado graças à utilização do microcontrolador ESP-8266 que, como descrito anteriormente, detêm as capacidades de processamento e comunicação *Wi-Fi* tudo em um único *chip* de tamanho bastante reduzido. Para a construção do protótipo (Figura 21), a variação utilizada foi a placa de prototipação *nodeMCU*, que basicamente é um ESP-12 com as portas compatíveis com *protoboards* e interface USB para facilitar a comunicação com o ambiente de desenvolvimento do *firmware*. A conexão deste microcontrolador com o leitor RFID MFRC522 também não apresenta maiores problemas, visto que o *nodeMCU* disponibiliza os pinos de comunicação SPI.

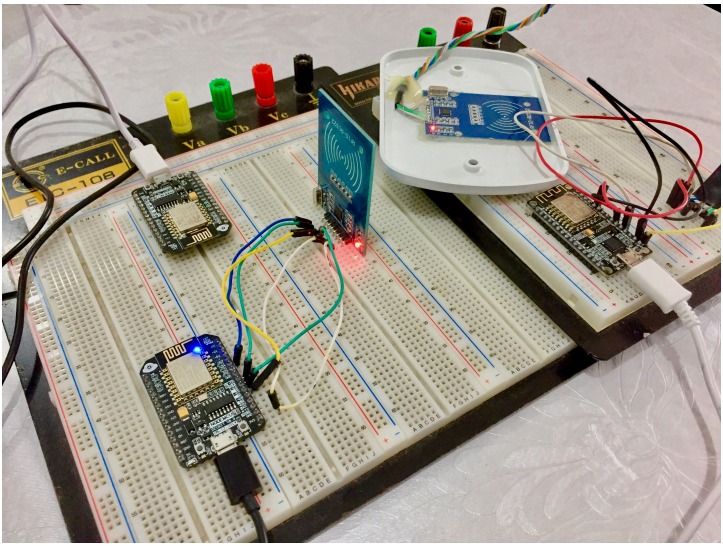

Figura 21 – Protótipo de *hardware* do sistema.

5.3 PROJETO DE SOFTWARE

O projeto de *software* é composto de duas partes principais: desenvolvimento da página *web*, sendo a interface de comunicação e visualização dos dados das fechaduras inteligentes, e desenvolvimento do *firmware* para o controle de todas as ações da fechadura. A seguir são detalhados os principais pontos destas partes citadas. Todo o código fonte desenvolvido no decorrer do projeto está disponível no repositório *GitLab* [1].

5.3.1 Interface *web* de configuração

Como mencionado anteriormente, um dos objetivos do projeto é a fácil atualização das informações de acesso à cada sala que utilize esta solução de controle de acesso. Com este intuito, foi criada uma interface de configuração amigável demonstrada na Figura 22.

[1] `https://gitlab.com/evejr/smart-locks-mesh`

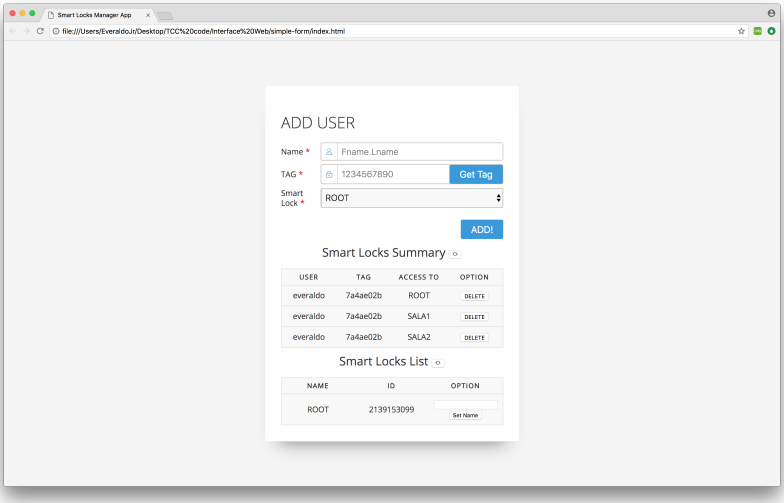

Figura 22 – Página de configuração das fechaduras.

Com o funcionamento bastante simples, a interface permite adicionar um usuário com acesso à determinada fechadura. O botão "Get Tag"pode ser utilizado para requisitar à fechadura principal a última *tag* lida por ela, para que não seja necessário um leitor RFID ligado ao computador do administrador da rede. Após definir um nome de usuário, a *tag* e a qual fechadura liberar o acesso, este usuário adicionado aparecerá na lista com todos os usuários de todas as fechaduras (*Smart Locks Summary*), com a possibilidade de ter o seu acesso removido através de um botão "*delete*".

Todos os nós (fechaduras) da rede aparecem em uma listagem na parte de baixo da página, denominada *Smart Locks List*. Nesta lista, vale destacar a opção de atribuir um nome para cada fechadura. Esta solução foi implementada devido ao fato de que cada nó da rede *mesh* é identificado por um número de identificação (ID), dificultando assim o entendimento de qual ID corresponde a qual sala do local de implementação da solução. Uma vez atribuído um nome a determinado ID, esta informação é armazenada na memória não-volátil da fechadura, podendo ser sobrescrita caso haja necessidade.

As funcionalidades da página foram implementadas utilizando a linguagem de programação *JavaScript*, que possibilita a comunicação com a fechadura através de requisições assíncronas HTTP do tipo *GET*,

utilizando AJAX (*Asynchronous JavaScript And XML*). Para padronizar o formato dos dados trocados entre a página e a fechadura é utilizado o protocolo JSON (*JavaScript Object Notation*).

5.3.2 *Firmware*

Pode-se dizer que o desenvolvimento do *firmware* de controle da fechadura é o cerne do projeto. Foram implementados dois *software* de controle: um para o nodo raiz (único na rede) e outro para todos os outros nodos não-raiz. O primeiro detêm as funcionalidades de atender as requisições da interface detalhada em 5.3.1, repassar as informações para a rede *mesh*, manipular os arquivos necessários para o armazenamento dos dados e ainda realizar a comunicação com o leitor RFID. Já o *firmware* de controle para os nodos não-raiz, implementa quase todas as funcionalidades mencionadas para o nodo raiz, com exceção da comunicação com a interface *web*.

- Módulo de comunicação com a rede *wireless* e a rede *mesh*

  Para a implementação deste módulo, foram utilizadas as bibliotecas *painlessMesh* e *ESPAsyncWebServer* disponibilizadas para utilização pela comunidade. Com as funcionalidades das bibliotecas, este nodo fica conectado com a rede sem fio local, atuando como um servidor *web* recebendo requisições de um único cliente (interface de configuração), e também conectado à rede *mesh*, repassando as informações enviadas pela interface de configuração.

  Quando o nodo raiz recebe uma requisição de adicionar ou deletar, o mesmo envia uma mensagem de texto via *broadcast* para todos os nodos da rede, montando uma instrução do tipo:

  ```
  <ADD>|<DEL> : <usuário> , <id tag>, <nome fechadura>
  ```

- Módulo de comunicação com o leitor RFID

  Para a comunicação com o leitor RFID foi utilizada a biblioteca *MRFC522* que trata da comunicação SPI entre o leitor e o ESP.

- Módulo de armazenamento das informações na memória *flash*

  Com a vantagem do microcontrolador escolhido para a aplicação disponibilizar uma boa quantidade de memória (4 MB), os nodos da rede são capazes de armazenar as informações de todos os usuários do sistema, utilizando a biblioteca FS que implementa o sistema de arquivos *SPIFFS*.

5.4 TESTES E RESULTADOS

Com o desenvolvimento deste trabalho foi atingido o resultado esperado de criar uma solução de melhoria do controle de acesso nas dependências do Campus Araranguá da Universidade Federal de Santa Catarina. A utilização de uma rede do tipo *mesh* traz os resultados esperados de que as fechaduras funcionem independentemente da rede *wireless* do campus e que a área de abrangência da rede não fique limitada ao alcance dos roteadores da universidade, uma vez que cada fechadura propaga as informações para as outras fechaduras da rede.

Para validar o sistema, foram feitos dois testes funcionais possíveis: dois nodos não-raiz (neste caso, folhas) conectados diretamente ao nodo raiz; e um nodo folha conectado à um nodo não-raiz, por sua vez conectado ao nodo raiz. Em ambos os cenários as informações foram propagadas corretamente, bem como a listagem das fechaduras da rede foram mostradas como esperado na interface *web*.

Um teste de funcionamento real, realizando o acionamento de um fecho eletromagnético para a abertura de uma porta não foi realizado pela falta deste componente. Entretanto, por se tratar de um solenoide, não deve haver nenhuma limitação de utilização desta solução, pois seria necessário apenas um sinal digital *high* ou *low* para o acionamento do fecho através de um relé.

6 CONSIDERAÇÕES FINAIS

Além do desenvolvimento de uma solução para o controle de acesso voltado à Universidade Federal de Santa Catarina, um projeto como este, potencialmente pode despertar interesses comerciais. Pensa-se que uma fechadura com as capacidades desenvolvidas pode ser uma solução não apenas para ambientes universitários, mas também para empresas e hotéis. Outro ponto relevante para uma possível comercialização do sistema, é a modularidade do mesmo. Ou seja, neste projeto ele foi projetado para utilizar o método de acesso de maior conveniência para a UFSC, sendo este o RFID. Contudo, o método de acesso pode ser alterado para moldar-se às necessidades de outros tipos de ambiente, mantendo as definições de acesso à rede e atualização dos dados da fechadura, características estas identificadas como a parte de maior inovação do projeto.

A empresa brasileira RWTECH [1] têm em seu portfólio de produtos uma fechadura inteligente que se assemelha ao projeto proposto, pois o produto pode estar configurado para comunicar-se em rede com outras fechaduras através do protocolo *ZigBee*, que é um padrão proprietário para rede de sensores sem fio com base no IEEE 802.15.4, citado na Seção 4.2. Por ser um produto inovador e ainda fazer a validação dos usuários por meio de biometria, o preço do produto é bastante elevado.

Um ponto importante do projeto é a utilização de componentes com baixo custo, tornando a tecnologia mais acessível e visando a possibilidade de implementação do sistema em um campus universitário que contem dezenas de salas. Além disso, a solução desenvolvida neste trabalho possui margem para ser ampliada visando escopos diferentes.

6.1 TRABALHOS FUTUROS

Tomando o sistema de controle de acesso desenvolvido neste trabalho como base, utilizando os métodos de comunicação definidos, é possível ampliar o projeto em trabalhos futuros. Uma ideia já citada no decorrer do trabalho é a implementação de um sistema de monitoramento de algumas variáveis de um ambiente inteligente, como janelas, luzes, ar condicionado, etc. Outra sugestão para trabalhos futuros é a utilização de protocolos de segurança para a comunicação de dados,

[1] `www.rwtech.com.br`

questão esta excluída do escopo deste trabalho.

Um ponto importante a ser explorado para um projeto deste tipo é a análise de eficiência energética, visto que tipicamente uma fechadura inteligente é alimentada por baterias. Seguindo nesta linha, testes com protocolos de comunicação sem fio de menor consumo também podem ser realizados em trabalhos futuros, bem como, realizar testes práticos de longa duração utilizando o protótipo desenvolvido neste trabalho para avaliar o funcionamento do sistema no ambiente universitário.

REFERÊNCIAS

ADLER, R. M. Distributed coordination models for client/server computing. *Computer*, IEEE, v. 28, n. 4, p. 14–22, 1995.

ALKAR, A. Z.; BUHUR, U. An internet based wireless home automation system for multifunctional devices. *IEEE Transactions on Consumer Electronics*, IEEE, v. 51, n. 4, p. 1169–1174, 2005.

AMELCO S.A. *Fecho Eletromagnético FE61*. Embu-SP, ago. 2007.

BOUCKAERT, S. et al. Strategies and challenges for interconnecting wireless mesh and wireless sensor networks. *Wireless Personal Communications*, v. 53, n. 3, p. 443–463, 2010. ISSN 1572-834X. <http://dx.doi.org/10.1007/s11277-010-9957-z>.

CARNIEL, G. et al. Projeto e desenvolvimento de fechadura eletrônica controlada pela internet. *Anais do Computer on the Beach*, p. 031–040, 2015.

CATSOULIS, J. *Designing embedded hardware*. Sebastopol, California: "O'Reilly Media, Inc.", 2005.

CORTELETTI, D. Introdução à programação de microcontroladores microchip pic. 2006.

CUNHA, A. *RFID–Etiquetas com eletrônica de ponta*. 2016. <https://www.embarcados.com.br/rfid-etiquetas-com-eletronica-de-ponta/>. Acessado em 25/11/2016.

CURVELLO, A. *Apresentando o módulo ESP8266*. 2015. <https://www.embarcados.com.br/modulo-esp8266>. Acessado em 09/11/2016.

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

ESPRESSIF SYSTEMS. *ESP8266 Mesh User Guide*. China, jan. 2016. V1.2.

ESPRESSIF SYSTEMS. *ESP8266EX Datasheet*. China, nov. 2016. V5.0.

FINKENZELLER, K. Rfid handbook: Fundamentals and applications in contactless smart cards and identification. {John Wiley\ & Sons}, 2003.

GROUT, I.; SILVA, A. C. R. da. Concept design for a rfid enabled student workbook. In: IEEE. *Remote Engineering and Virtual Instrumentation (REV), 2014 11th International Conference on*. Porto, 2014. p. 7–10.

GUTIÉRREZ, J. A. On the use of ieee std. 802.15.4 to enable wireless sensor networks in building automation. *International Journal of Wireless Information Networks*, v. 14, n. 4, p. 295–301, 2007. ISSN 1572-8129. <http://dx.doi.org/10.1007/s10776-007-0063-4>.

HENRICI, D. *RFID security and privacy: concepts, protocols, and architectures*. Berlin: Springer Science & Business Media, 2008.

HUANG, Y.-M.; HSIEH, M.-Y.; SANDNES, F. E. Wireless sensor networks and applications. In: _____. *Sensors: Advancements in Modeling, Design Issues, Fabrication and Practical Applications*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008. p. 199–219. ISBN 978-3-540-69033-7.

IBRAHIM, D. *Microcontroller based applied digital control*. Chichester: John Wiley, 2006.

JALAMKAR, D.; SELVAKUMAR, A. Use of internet of things in a humanoid robot-a review. *Advances in Robotics & Automation*, OMICS International, 2016.

JIA, W.; ZHOU, W. *Distributed network systems: from concepts to implementations*. Boston, MA: Springer US, 2005. ISBN 978-0-387-23840-1.

KASSEM, A. et al. A smart lock system using wi-fi security. In: IEEE. *Advances in Computational Tools for Engineering Applications (ACTEA), 2016 3rd International Conference on*. Zouk Mosbeh, Lebanon, 2016. p. 222–225.

KUROSE, J.; ROSS, K. *Redes de computadores e a internet: uma abordagem top-down*. São Paulo: Pearson, 2010. ISBN 9788588639973.

LANDT, J. The history of rfid. *IEEE potentials*, IEEE, v. 24, n. 4, p. 8–11, 2005.

LI, Q.; YAO, C. *Real-Time Concepts for Embedded Systems*. 1st. ed. Boca Raton, FL, USA: CRC Press, Inc., 2003. ISBN 1578201241, 9781578201242.

MARTINS, N. A. Sistemas microcontrolados. *São Paulo: Novatec*, 2005.

MEHRJERDI, Y. Z. Rfid: A bibliographical literature review with future research directions. *International Journal of Industrial Engineering*, v. 25, n. 2, p. 151–190, 2014.

OLIVEIRA, A. S. de; ANDRADE, F. S. de. *Sistemas embarcados: hardware e firmware na prática*. São Paulo: Editora Érica Ltda, 2006.

OLIVEIRA, B. B. Aplicabilidade dos microcontroladores em inovações tecnológicas. In: *VII CONNEPI-Congresso Norte Nordeste de Pesquisa e Inovação*. [S.l.: s.n.], 2012.

RAFIQUZZAMAN, M. *Microcontroller Theory and Applications with the PIC18F*. Hoboken, New Jersey: Wiley Publishing, 2011.

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

SILVA, C. W. D. *Sensors and Actuators: Engineering System Instrumentation*. Boca Raton, FL: CRC Press, 2015.

SIMON, D. E. *An Embedded Software Primer*. 1st. ed. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1999. ISBN 020161569X.

TANENBAUM, A. *Redes de computadores*. São Paulo: Pearson Prentice Hall, 2011. ISBN 9788576059240.

TAPIA, D. I. et al. Identificación por radiofrecuencia: Fundamentos y aplicaciones. *Proceedings de las primeras Jornadas Científicas sobre RFID. Ciudad Real, Spain*, p. 1–5, 2007.

TEH, P.-L.; LING, H.-C.; CHEONG, S.-N. Nfc smartphone based access control system using information hiding. In: IEEE. *Open Systems (ICOS), 2013 IEEE Conference on*. Sarawak, Malaysia, 2013. p. 13–17.

TORRES, G. *Redes de computadores*. Rio de Janeiro: Novaterra Editora, 2013. ISBN 9788561893057.

WARD, M.; KRANENBERG, R. van et al. Rifd: Frequency, standards, adoption and innovation. JISC, 2006.

WHITE, E. *Making Embedded Systems: Design Patterns for Great Software*. Sebastopol, CA: O'Reilly Media, Inc., 2011. ISBN 1449302149, 9781449302146.

ZHU, X.; MUKHOPADHYAY, S. K.; KURATA, H. A review of rfid technology and its managerial applications in different industries. *Journal of Engineering and Technology Management*, Elsevier, v. 29, n. 1, p. 152–167, 2012.