UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"
FACULDADE DE ENGENHARIA
CAMPUS DE ILHA SOLTEIRA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ROGÉRIA OLIANI

MÓDULO PARA IDENTIFICAÇÃO DE OBJETOS E TRANSMISSÃO DE DADOS SEM FIO

Ilha Solteira
2016

ROGÉRIA OLIANI

MÓDULO PARA IDENTIFICAÇÃO DE OBJETOS E TRANSMISSÃO DE DADOS SEM FIO

Dissertação apresentada à Faculdade de Engenharia - UNESP – Campus de Ilha Solteira, para obtenção do título de Mestre em Engenharia Elétrica.

Área de Conhecimento: Automação.

Prof. Dr. Alexandre Cesar R. da Silva

Orientador

Prof. Dr. Tércio A. dos Santos Filho

Coorientador

Ilha Solteira

2016

FICHA CATALOGRÁFICA
Desenvolvido pelo Serviço Técnico de Biblioteca e Documentação

O46m

Oliani, Rogéria.
Módulo para identificação de objetos e transmissão de dados sem fio / Rogéria Oliani. -- Ilha Solteira: [s.n.], 2016
87 f. : il.

Dissertação (mestrado) - Universidade Estadual Paulista. Faculdade de Engenharia de Ilha Solteira. Área de conhecimento: Automação, 2016

Orientador: Alexandre Cesar Rodrigues da Silva
Co-orientador: Tércio Alberto dos Santos Filho
Inclui bibliografia

1. Identificação por rádio frequência. 2. Bluetooth. 3. Sáude. 4. Educação.

unesp

UNIVERSIDADE ESTADUAL PAULISTA

Câmpus de Ilha Solteira

CERTIFICADO DE APROVAÇÃO

TÍTULO DA DISSERTAÇÃO: MÓDULO PARA IDENTIFICAÇÃO DE OBJETOS E TRANSMISSÃO DE DADOS SEM FIO

AUTORA: ROGÉRIA OLIANI
ORIENTADOR: ALEXANDRE CESAR RODRIGUES DA SILVA

Aprovada como parte das exigências para obtenção do Título de Mestra em ENGENHARIA ELÉTRICA, área: AUTOMAÇÃO, pela Comissão Examinadora:

PROFESSOR TÉRCIO ALBERTO DOS SANTOS FILHO
Departamento de Ciências da Computação / UNIVERSIDADE FEDERAL DE GOIÁS

Prof. Dr. JEAN MARCOS DE SOUZA RIBEIRO
Departamento de Engenharia Elétrica / Faculdade de Engenharia de Ilha Solteira

Prof. Dr. MARCELO AUGUSTO ASSUNÇÃO SANCHES
Departamento de Engenharia Elétrica / Faculdade de Engenharia de Ilha Solteira

Ilha Solteira, 26 de fevereiro de 2016

À MEMÓRIA DE MEUS PAIS,
ARDUINO E ODELITA,
DEDICO ESTE TRABALHO.

AGRADECIMENTOS

Primeiramente, gostaria de agradecer a compreensão e apoio dado pela minha irmã Ramônica e minha amiga Teresa, que me ajudaram a conciliar educação, trabalho, casa, saúde e muitos outros fatores que fizeram parte do meu dia a dia e, assim, tornaram mais brando o caminho até aqui.

Ao meu orientador Alexandre Cesar R. da Silva e coorientador Tércio A. dos Santos Filho, começo agradecendo a oportunidade que me deram de estudar nesta instituição e sob a orientação de vocês. Agradeço a confiança que depositaram em mim, os ensinamentos, os incentivos, as palavras certas e a compreensão nos meus momentos de dificuldade.

Aos amigos do LPSSD pelo apoio e bons momentos que passamos juntos.

A todos os professores que contribuíram no enriquecimento de meus conhecimentos.

A todos os funcionários da Unesp de Ilha Solteira, que através do bom desempenho de suas atividades, tornam possível a realização de sonhos, a evolução do conhecimento e contribuem, direta e indiretamente, para tornar este mundo melhor para todos.

Por fim, e acima de tudo, a Deus por me dar a Paz necessária para compreender a vida em seus momentos de fartura e escassez. Pelo tempo que me deu junto a pais maravilhosos, que souberam dosar os “sins” e “nãos”, e através de bons exemplos me educaram, fortaleceram-me e permitiram-me aprender e crescer a cada dia, mesmo após a sua partida.

“Sejam felizes, trabalhem, orem, ajudem, respeitem, vivam da melhor forma possível, eu sei que não é fácil, mas tudo terá um “porquê”, no tempo certo tudo se esclarece.” Odelita de Castro Oliani

RESUMO

Transmissão de dados sem fio tem se tornado cada vez mais presente no dia a dia, devido a comodidade da não utilização de cabos, bem como pela maior mobilidade propiciada. Este trabalho aborda duas tecnologias de comunicação sem fio atuais: Identificação por Radiofrequência (RFID) e Bluetooth, destacando suas principais características e apresenta o protótipo de um circuito que efetua a leitura de *tags* fixadas em objetos, por meio de um leitor RFID e, posteriormente, transmite a identificação dessas a um *smartphone*, por meio da tecnologia Bluetooth. Com o propósito de ilustrar aplicações do protótipo construído, foram desenvolvidos dois *softwares* para *smartphones* Android: um de controle de medicamento de idosos e outro para auxiliar deficientes visuais nas aulas práticas laboratoriais. Durante o desenvolvimento do trabalho, testes foram realizados para se verificar o alcance de leitura do leitor RFID utilizado. Também foram realizados testes com a tecnologia Bluetooth, verificando-se a distância máxima de conexão e transmissão/recepção de dados entre o protótipo desenvolvido e um *smartphone*.

Palavras-chave: Bluetooth. Etiquetas. Identificação por radiofrequência. Segurança. saúde. Educação. Idoso. Deficiente visual.

ABSTRACT

Wireless data transmission has become increasingly present in everyday life, because the convenience of not using cables, as well as the greater mobility afforded. This paper addresses two current wireless communication technologies: Radio Frequency Identification (RFID) and Bluetooth, highlighting its main characteristics and presents the prototype of a circuit that performs the reading tags attached to objects by means of an RFID reader and later transmits the identification to such a smartphone, using Bluetooth technology. In order to illustrate prototype built applications, they developed two software for Android smartphones: one for the elderly medicine control and another to assist the visually impaired in the laboratory classes. During the development work, tests were conducted to verify the read range of the RFID reader used. Also with Bluetooth technology tests were performed, checking the maximum distance connection and transmission/reception of data between the developed prototype and a smartphone.

Keywords: Bluetooth. Labels. Radio frequency identification. Security. Health. Education. Elderly. Visually impaired.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ACL	*Asynchronous Connection-Less Link*
AM_DDR	*Active Member Address*
APIs	*Application Programming Interfaces*
bps	bits por segundo
CPU	*Central Processing Unit*
CRM	*Customer Relationship Management*
DAC	*Device Address Code*
DoS	*Denial of Service*
EPC	*Electronic Product Code*
ERP	*Enterprise Resource Planning*
HF	*High Frequency*
ID	*Identification*
IFF	*Identification Friend or Foe*
ISO	*International Standards Organization*
JSON	*JavaScript Object Notation*
LF	*Low Frequency*
PIVEs	Placas de Identificação Veicular
PM_ADDR	*Parked Member Address*
RADAR	*RAdio Detection And Ranging*
RAM	*Random Access Memory*
RFID	*Radio Frequency Identification*
ROM	*Read Only Memory*
SCM	*Supply Chain Management*
SIG	*Special Interest Group*
UHF	*Ultra High Frequency*
UID	*Unique Identifier*
V	Volt(s)
XML	eXtensible Markup Language

SUMÁRIO

1 INTRODUÇÃO

A praticidade e comodidade proporcionada pelas tecnologias que possibilitam a troca de dados sem fio, vêm tornando-as cada vez mais populares e passíveis de serem encontradas nos mais diversos tipos de equipamentos, como televisores, veículos, caixas de som, *smartphones* e outros. Dentre essas tecnologias duas serão abordadas neste trabalho: Identificação por Radiofrequência (RFID - *Radio Frequency Identification*) e Bluetooth.

Identificação por Radiofrequência é um termo genérico para tecnologias que utilizam ondas de rádio para identificar automaticamente pessoas ou objetos. Um sistema RFID possui dois componentes básicos: *tag* RFID ou etiqueta RFID, e leitor RFID ou interrogador. A *tag* é utilizada para identificação de pessoas, objetos e animais e possui diferentes formatos, os quais são adequados ao tipo de identificação que se deseja efetuar. Na escolha do formato, deve-se considerar o que se deseja identificar, a distância, o ambiente onde será utilizada, o nível de segurança desejada, dentre outros fatores. O outro componente, o leitor RFID, interrogará as *tags*, recebendo os dados desta, como seu número de identificação. Da mesma forma que a *tag*, há diversos modelos de leitores RFID. Assim, a escolha destes equipamentos devem ser cuidadosamente realizada para cada tipo aplicação.

O Bluetooth é uma tecnologia projetada para propiciar a comunicação entre dispositivos a curta distância e sem a utilização de cabos. Esta tecnologia possibilita que equipamentos com diferentes funções, comuniquem-se e ampliem as suas possibilidades de utilização. Desde a sua concepção há duas décadas, a tecnologia Bluetooth vem sendo desenvolvida e ampliada a sua diversidade de aplicações, destacando-se dentre as tecnologias a serem utilizadas na “Internet das Coisas”[1] (ATMEL CORPORATION, 2014), (RIBEIRO, 2014).

As aplicações que podem ser dadas a estas tecnologias são inúmeras. Atualmente, podem ser encontradas em diversas áreas. Na agricultura, sistemas utilizando a tecnologia RFID, podem auxiliar agricultores a monitorar parâmetros do subsolo, como: temperatura e humidade (WANG; GEORGE; GREEN, 2014). As

[1] Internet das Coisas é uma rede de objetos que se comunicam entre si e seus usuários, com o propósito de ligar todas as coisas à internet e gerar informações que possam ser utilizadas em diferentes tipos de aplicações.

informações de monitoramento de solo e velocidade do vento, podem ser enviadas a computadores, através da tecnologia Bluetooth, possibilitando a analise destas (JUNCO, 2015). Na área de transporte, as pessoas com deficiência visual e os ônibus são identificadas por *tags* RFID, sendo o deficiente visual informado por voz, quanto a chegada do ônibus, e o motorista, da existência deste na estação (AL KALBANI et al., 2015). Na saúde, sistemas utilizando RFID, possibilitam que funcionários da área da saúde identifiquem pacientes através de *tags,* nas quais são gravadas informações essenciais (grupo de sangue, alergias, e outras) que são utilizadas para atender os pacientes nos hospitais em casos de emergência (CHIA et al., 2011). A tecnologia RFID também pode ser utilizada no auxílio de deficientes visuais, facilitando a localização de objetos e informando, por meio de um sinal acústico, a proximidade destes (DIONISIO; SARDINI; SERPELLONI, 2012). A diversidade de aplicações existentes, e possibilidades de novas aplicações que podem auxiliar nas diversas áreas, tornam instigante a busca por informações voltadas a estas tecnologias. E assim, este trabalhado foi desenvolvido de forma a resultar em um protótipo para identificação e transmissão de dados sem fio, denominado oIT. O oIT é um *hardware* que possibilita a identificação de *tags* fixadas em objetos, utilizando a tecnologia RFID e a transferência destes dados para um *smartphone*, utilizando a tecnologia Bluetooth. Ambas as tecnologias, foram unidas em um circuito passível de ser utilizado nos punhos de seus usuários.

O protótipo desenvolvido (oIT) possibilita sua aplicação em diversas áreas. Neste trabalho, são apresentadas duas aplicações (*softwares*) desenvolvidas para *smartphones* Android: uma na área da saúde e outra na área da educação. Na área da saúde, foi desenvolvida a aplicação denominada oMedControl, que tem por objetivo controlar o uso dos medicamentos de idosos, bem como alertar os seus cuidadores, quanto a situações de risco, como a manipulação de medicamentos dos quais os idosos sejam alérgicos. Na educação, foi desenvolvida a aplicação denominada oIS, com o objetivo de auxiliar deficientes visuais nas aulas práticas laboratoriais, por meio da identificação de objetos como ferramentas, equipamentos, dentre outros, fornecendo aos alunos informações de cunho educacional, relacionadas a estes objetos, por meio sonoro.

1.1 ESTADO DA ARTE

A proposta de soluções que atendam às necessidades dos idosos e dos portadores de deficiência visual têm sido tema de diversos trabalhos. As áreas de interesse neste trabalho são: a saúde, relacionada ao controle do uso de medicamentos por idosos e a educação, de forma a propiciar aos portadores de deficiência visual um melhor acesso a esta.

1.1.1 Controle do uso de medicamentos por idosos

O controle do uso de medicamentos pode ser realizado em ambientes com baixa ou alta rotatividade de pessoas, e atendendo desde um usuário específico até diversos simultaneamente. Hospitais são exemplos de ambientes com alta rotatividade de pessoas, visto que há sempre pacientes dando entrada e outros tendo alta, e atendem diversos pacientes simultaneamente. No caso de asilos de idosos, apesar de atender diversos usuários simultaneamente, não há uma alta rotatividade destes. Com relação as residências, o controle do uso de medicamentos atende um usuário específico ou poucos membros da família, principalmente, quando trata-se de idosos.

Nas residências, o controle do uso de medicamentos pode ser realizado mantendo estes em um local fechado e controlado, como em uma caixa (SUZUKI; JOSE; NAKAUCHI, 2011) ou armário (GOMES et al., 2013) de medicamentos, ou através de ferramentas que controlem a sua utilização independente do seu local de armazenamento (SCHREIER et al., 2013).

Suzuki, Jose e Nakauchi (2011) propõem em seu trabalho uma caixa de medicamentos inteligente para auxiliar idosos no controle de medicamentos dentro de suas residências. A caixa possui 28 divisões para armazenar os medicamentos utilizados durante os 7 dias da semana, em 4 intervalos de horário. Dentre outras características, a caixa possui um painel *touchscreen* para interface com o usuário, um computador compacto e 4 webcams para reconhecer os medicamentos em seu interior, bem com uma placa Arduino Nano que controla a abertura da tampa da caixa e os LEDs que auxiliam na formação de um fundo uniforme para as imagens capturas pelas câmeras.

Seguindo a mesma linha de controle de medicamentos em local fechado, outros dois trabalhos apresentam soluções utilizando armários de medicamentos.

No primeiro trabalho, o armário proposto por Parida et al. (2012) utiliza um sistema para o controle de medicamentos, baseado na tecnologia RFID para identificar os usuários e os medicamentos. Os dados do sistema são armazenados em um servidor web e o controle efetuado por um computador com webcam, que registra a abertura do armário realizada por um usuário sem a utilização de uma *tag* RFID autorizada. Quando isto ocorre, o sistema emite uma mensagem de voz para alertar o usuário, e na sequência, envia uma mensagem para o celular do membro responsável pela família.

No segundo trabalho, Gomes et al. (2013) apresenta um armário inteligente que utiliza a tecnologia RFID para identificar os medicamentos, as prescrições médicas e os usuários. O armário possui um mini-PC e um leitor RFID para efetuar o controle do uso de medicamentos, e instruir o usuário através de um sintetizador de voz. Uma placa microcontroladora detecta a abertura da porta utilizando um sensor de contato, e LEDs informam através da variação das cores vermelho, verde e branco, os alertas de perigo, permissão de acesso e sistema em processamento adicional, respectivamente.

Uma solução que auxilia usuários no controle de seus medicamentos, independentemente do local de armazenamento destes, é proposta por Schreier et al. (2013).

Schreier et al. (2013) apresenta em seu trabalho uma aplicação desenvolvida para *smartphone* Android com tecnologia *Near Field Communication* (NFC) que identifica o medicamento através da leitura da *tag* RFID fixada na embalagem deste. O cadastro do medicamento é realizado através do escaneamento do código de barras presente na embalagem, utilizando a câmera do *smartphone*. Os dados do medicamento são obtidos da base de dados farmacêuticos da Áustria, e o período de uso do medicamento (manhã, meio-dia, fim de tarde e noite) é definido pelo usuário, conforme a prescrição médica. A aplicação exibe uma caixa de diálogo para lembrar o usuário quanto ao uso do medicamento, caso o consumo não tenha sido registrado.

1.1.2 Portadores de deficiência visual e o acesso à educação

O acesso à educação de pessoas portadoras de deficiência visual envolve diversos fatores, como: a estrutura física da instituição de ensino, preparo dos professores, ferramentas de ensino, dentre outras. Estes fatores devem ser adequados às necessidades do estudante portador de deficiência visual.

Com relação as ferramentas de ensino, em paralelo as mais difundidas, como o Sistema Braille (criado pelo francês Louis Braille em 1825) e os *softwares* leitores de tela (DOSVOX, NVDA, Virtual Vision, JAWS e outros), outras vêm sendo propostas de forma a auxiliar os deficientes visuais, como é o caso da ferramenta P-CUBE.

P-CUBE é uma ferramenta educacional proposta por Kakehashi et al. (2013) para auxiliar deficientes visuais no aprendizado da programação. A ferramenta é constituída basicamente de blocos cúbicos, uma matriz de programação, um robô móvel e um computador. Os blocos cúbicos são divididos em blocos de ação (para frente, para trás, para a esquerda, para a direita e parar) e blocos de controle (LOOP e IF). Cada bloco é identificado por uma *tag* RFID, e cada célula da matriz de programação possui um leitor RFID. Os blocos são posicionados na matriz de programação baseado em uma estrutura de algoritmo. Os dados do algoritmo são gravados em um cartão microSD utilizando um computador conectado a matriz de programação, e este é transferido ao robô móvel, que executa os comandos ali definidos.

Com relação ao aprendizado de línguas estrangeiras, Chomchalerm et al. (2014) propõe em seu trabalho um aplicativo para *smartphone*s Android denominado Braille Dict. O Braille Dict foi desenvolvido com o objetivo de auxiliar os deficientes visuais no aprendizado da língua inglesa. O layout do aplicativo é basicamente constituído de 6 pontos, dispostos em uma estrutura matricial de duas colunas e três linhas, que são utilizados para formar um sinal do Sistema Braille. O aplicativo possibilita quatro entradas para formar o sinal Braille: toque do lado esquerdo da tela (preenche o ponto esquerdo), toque do lado direito (preenche o ponto direito), toque simultâneo do lado esquerdo e direito (preenche os dois pontos) e deslizar para baixo de ambos os lados (deixa os pontos sem preencher); sendo que cada entrada preencherá uma linha da matriz. Após efetuada as entradas, buscas são realizadas a fim de confrontar a palavra formada com aquelas existentes no dicionário

inglês/tailandês, armazenado na base de dados SQLite. Localizada a palavra, a aplicação retorna o significado desta ao usuário por meio sonoro.

Nos trabalhos de Kakehashi et al. (2013) e Chomchalerm et al. (2014) as ferramentas propostas são utilizadas diretamente pelo deficiente visual. Uma outra forma de contribuir com o acesso à educação dos deficientes visuais é através do desenvolvimento de ferramentas, que auxiliem os professores a produzir materiais adequados a este perfil de aluno.

Al-Rajhi et al. (2015) propõe em seu trabalho uma ferramenta para auxiliar professores de matemática na produção de gráficos 3D. A ferramenta consiste em um *software*, que recebe como dado de entrada uma equação matemática para criação do gráfico e a legenda deste. Como resultado, é gerado um gráfico 2D que pode ser impresso em uma impressora 3D, com a respectiva legenda em Braille. O gráfico 3D resultante pode servir como material de apoio para alunos com deficiência visual nas aulas de matemática.

1.2 ORGANIZAÇÃO DO TEXTO

Este trabalho é organizado da seguinte forma: no Capítulo 2 é apresentada uma Revisão Literária sobre as tecnologias RFID e Bluetooth, abordando a origem e características dessas tecnologias. No Capítulo 3 é demonstrada a utilização da tecnologia Bluetooth junto a um microcontrolador com a apresentação dos componentes básicos necessários à utilização do mesmo. O Capitulo 4 demonstra a utilização da tecnologia RFID e Bluetooth na construção de um protótipo para leitura e transmissão de dados sem fio, denominado oIT, bem como os testes realizados com ambas tecnologias. No Capítulo 5 é apresentada a aplicação, denominada oMedControl, para o controle de medicamento de idosos. No Capítulo 6 é apresentada a aplicação, denominada oIS, para auxiliar alunos deficientes visuais nas aulas laboratoriais. No Capítulo 7 são apresentadas as conclusões obtidas neste trabalho.

2 REVISÃO LITERÁRIA

Neste trabalho são abordadas duas tecnologias de comunicações sem fio: Identificação por Radiofrequência e Bluetooth. Ambas as tecnologias são utilizadas em diversos tipos de aplicações e diferentes áreas. A seguir, é apresentado um pouco da história dessas tecnologias, bem como suas características e exemplos de aplicações.

2.1 RFID (RADIO FREQUENCY IDENTIFICATION)

A história do RFID tem seu início na Segunda Guerra Mundial (1939–1945), na qual foi utilizado para a identificação de aeronaves. Em 1935, o físico escocês Robert Alexander Watson-Watt patenteou o sistema de Detecção e Localização por Rádio (RADAR - *RAdio Detection And Ranging*), que se consolidou como uma inestimável ferramenta de guerra na Segunda Guerra Mundial (DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO - DECEA, 2010). Através do RADAR, os países em conflito detectavam a aproximação de aviões, contudo, não era possível distinguir se o avião era de um inimigo ou não. Posteriormente, os alemães descobriram que o sinal de rádio refletido era alterado ao girar seus aviões quando retornavam a base. Este é considerado o primeiro sistema RFID passivo (ROBERTI, 2005).

O primeiro sistema de identificação ativa foi desenvolvido pelos ingleses: Identificação Amigo ou Inimigo (IFF - *Identification Friend or Foe*). Este projeto foi liderado por Watson-Watt, e tinha como base a identificação das aeronaves “amigas” através dos sinais de rádio retornados por estas. Um transmissor era colocado em cada avião britânico, e ao receber os sinais das estações de radar de solo, estas emitiam um sinal de volta identificando a aeronave como amigável (ROBERTI, 2005). Desta forma, os ingleses puderam prever os ataques inimigos definindo com precisão, a distância, a velocidade e a direção dos mesmos, o que permitiu aos seus combatentes tempo suficiente de dar o alarme para a população poder se proteger, reduzindo drasticamente as baixas civis durante a guerra, além de poder preparar e executar represálias ao inimigo (DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO - DECEA, 2010), (LANDT, 2005).

Desde então a tecnologia RFID vem se desenvolvendo, com o estabelecimento de padrões, redução de custos e ampliação do leque de aplicações. Na Figura 1 é ilustrado um resumo dos principais eventos relacionados ao RFID, de 1935 a 2003.

Figura 1 - Resumo dos principais eventos relacionados ao RFID.

1935	• Watson-Watt patenteou o sistema de RADAR (DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO - DECEA, 2010).
1939 - 1945	• Segunda Guerra Mundial - Primeiros sistemas RFID passivo e ativo (ROBERTI, 2005).
1960's	• Utilização de Sistemas de Vigilância Eletrônica de Mercadorias (EAS - *Electronic Article Surveillance*) (ROBERTI, 2005).
1970's	• Mario W. Cardullo requereu a primeira patente americana para *tag* ativa regravável; • Charles Walton - recebe a patente de um transponder passivo utilizado para destravar portas; • Laboratório Nacional de Los Alamos - utilização do RFID no rastreamento de materiais nucleares (ROBERTI, 2005).
1980's	• Utilização do RFID em pedágios (ROBERTI, 2005).
1999	• Uniform Code Council, EAN International, Procter & Gamble e Gillette se uniram para estabelecer o Auto-ID Center com o intuito de realizar pesquisas objetivando desenvolver *tags* RFID de baixo custo, que viabilizassem sua utilização na cadeia de abastecimento (ROBERTI, 2005).
2003	• EAN Internacional e a Uniform Code Council anunciam a mudança de nome de AutoID Inc. para EPCglobal Inc (VIOLINO, 2003). • A empresa Wal-Mart anuncia a seus principais fornecedores as regras para a utilização do sistema RFID (DIAS, 2012).

Fonte: Elaboração da própria autora.

2.1.1 Sistema RFID

Identificação por Radiofrequência é um termo genérico para tecnologias que utilizam ondas de rádio para identificar automaticamente pessoas ou objetos (RFID JOURNAL BRASIL, 2011). Um sistema RFID possui dois componentes básicos: *tag*,

também conhecida como *transponder* ou etiqueta, e leitor, também conhecida como interrogador.

A *tag* RFID, basicamente, possui um microchip ligado a uma antena, os quais são acondicionados em uma embalagem (encapsulamento) apropriada ao objeto ou pessoa a que se destina identificar (cartão de crédito, chave de veículo, prego para identificação de árvores ou paletes, etiquetas de vestuários, dentre outros). Na Figura 2, é apresentada diferentes formas de encapsulamentos de *tags*.

Figura 2 - Exemplos de encapsulamentos de *tags*.

Fonte: Adaptado de Cetwin Service (2013).

O leitor RFID é um dispositivo utilizado para se comunicar com as *tags* através da emissão de ondas de rádio. Este também pode ser encontrado no mercado em diferentes formatos, adaptados ao tipo de *tag* que será lida. Na Figura 3, são apresentados alguns exemplos de leitores RFID.

Figura 3 - Exemplos de leitores RFID.

Fonte: Adaptado de Motorola Solutions (2014) e Kimaldi (2014).

Os leitores RFID podem utilizar antenas externas, como é o caso do leitor RFID fixo apresentado na Figura 3. A Figura 4 ilustra um exemplo de um leitor RFID fixo utilizando uma antena externa que possibilita identificar objetos em uma esteira.

Figura 4 - Leitor fixo e antena RFID.

Antena RFID

Leitor RFID fixo

Utilização de RFID em esteira

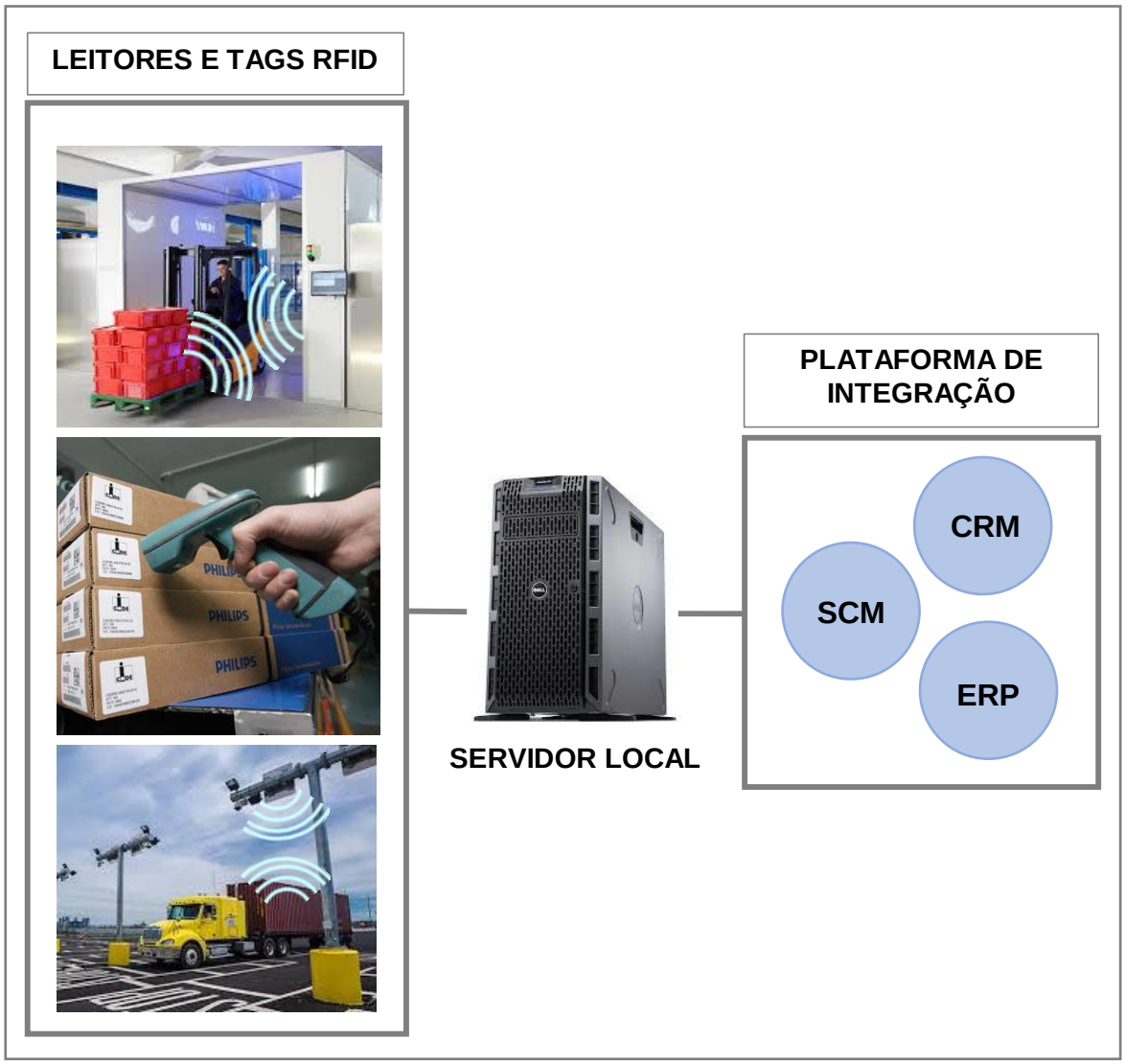
Fonte: Adaptado de Motorola Solutions (2014).

Para armazenar e fazer o controle das informações que são lidas das *tags* pelos leitores, há os servidores. Os servidores de banco de dados são computadores que armazenam o banco de dados das *tags*, e efetuam a comunicação com os leitores RFID através de uma rede (padrão IEEE 802.11, IEEE 802.15.4, dentre outros) ou, simplesmente, através de uma porta USB. As *tags* podem conter diversas informações, ou apenas um número de identificação (ID). Através do ID o servidor pode identificar a *tag* e obter as informações relacionadas a esta. Estas informações podem ser utilizadas pelas organizações para efetuarem o controle de folha de pagamento, produção, inventário, controle de processos em linha de produção, análise de perfil, tendências, dentre outros.

Na Figura 5, apresenta-se o esquema de um sistema RFID. Neste, a leitura dos dados de diversos tipos de *tags* – que identificam animais, caixas, paletes e caminhões – são realizadas por diferentes leitores, sendo o modelo de cada leitor

adequado ao tipo de *tag* que deseja efetuar a leitura. Os dados são enviados a um servidor local, no qual encontram-se armazenadas as informações referentes a cada item identificado com a *tag*. As informações localizadas no servidor local são utilizadas em uma plataforma integrada com o Sistema Integrado de Gestão Empresarial (ERP - *Enterprise Resource Planning*), Gestão de Relacionamento com o Cliente (CRM - *Customer Relationship Management*) e Gestão da Cadeia Logística (SCM - *Supply Chain Management*). Desta forma, as informações das *tags* lidas, podem ser obtidas em tempo real por toda a cadeia, podendo chegar até o cliente.

Figura 5 - Esquema de um sistema RFID.



Fonte: Elaboração da própria autora.

Os diferentes tipos de *tags* e leitores apresentados na Figura 5, possuem características distintas, como: alcance de leitura, frequência e fonte de energia das

tags. Essas características, viabilizam o uso desta tecnologia em diferente aplicações.

2.1.2 Classificação dos Sistemas RFID

Os sistemas RFID são classificados pela faixa de frequência em que operam e fonte de energia das *tags*. Com relação a faixa de frequência em que operam, FINKENZELLER (2010) e RFID JOURNAL (2013) classificam os sistemas RFID em:

1. Baixa Frequência (LF – *Low Frequency*): atuam em uma frequência de 30 a 300 kHz, e possuem uma transferência de dados lenta, bem como um pequeno alcance de leitura (até 1 metro).
2. Alta Frequência (HF – *High Frequency*): a frequência encontra-se em uma faixa de 3 a 30 MHz. Elas geralmente podem ser lidas até 1 metro de distância, e possuem transmissão de dados mais rápida que as *tags* de baixa frequência, contudo, consomem mais energia do que estas.
3. Ultra Alta Frequência (UHF – *Ultra High Frequency*): atuam em uma faixa de frequência de 300 MHz a 3 GHz, e tipicamente operam entre 866 e 960 MHz. *Tags* UHF possuem taxas de transferência mais altas e maior alcance do que as *tags* de alta e baixa frequência. No entanto, as ondas de rádio, nesta frequência, não passam por itens com alto teor de água. Em comparação às *tags* de baixa frequência, as *tags* UHF são mais caras e utilizam mais energia.
4. *Microwave*: atuam em frequência acima de 3 GHz. *Tags Microwave* têm taxas de transferência muito altas e podem ser lidas a longas distâncias, contudo, elas usam uma grande quantidade de energia e são mais caras em comparação as demais.

Em relação a sua fonte de energia, RFID JOURNAL (2013) classifica as *tags* em:

1. Passiva: Não possui fonte de energia. A energia necessária ao seu funcionamento é recebida do leitor através dos sinais emitidos por este. Em virtude desta característica, são mais baratas e têm uma maior duração em comparação as *tags* ativas. Contudo, possuem capacidade computacional e memória limitada.
2. Semi-passiva ou semi-ativa: possuem bateria interna, porém utiliza a energia fornecida pelos leitores para transmitir o sinal a estes, como ocorre com as

tags passivas. Neste caso, a bateria fornece energia ao seu microchip, permitindo que este tenha uma maior capacidade de processamento.

3. Ativas: possuem fonte de energia interna, o que possibilita o envio de sinais de transmissão de dados ao leitor, bem como alimentar circuitos mais complexos e sensores (acelerômetros para detectar movimento, temperatura, umidade e outros). Este tipo de *tag* possui um valor comercial mais alto, e um tempo de duração menor em comparação as *tags* passivas.

2.1.3 Padrões RFID

A comunicação entre *tags*, leitores e servidor RFID é realizada utilizando protocolos, os quais definem as regras de como esta comunicação ocorrerá. Estas regras definem, dentre outras questões, quais sinais são reconhecidos, como a comunicação é realizada, qual o significado dos dados recebidos das *tags* e quais dispositivos podem transmitir a cada tempo (resolvendo problemas de colisão).

A tecnologia RFID, quando desenvolvida de forma proprietária, faz com que essas regras sejam distintas a cada fabricante, inibindo a sua expansão, já que os produtos de diferentes fabricantes não poderiam se comunicar efetivamente. Por isso, é importante a padronização da tecnologia RFID, para que sistemas e equipamentos diversos sejam compatíveis, diminuindo o custo destes e facilitando sua implantação e disseminação. Neste âmbito, duas organizações se destacam: *International Standards Organization* (ISO) e a *Electronic Product Code global* (EPCglobal).

A ISO é uma união mundial de instituições nacionais de normalização, tais como DIN (Alemanha) e ANSI (EUA) e contribui com inúmeros comitês e grupos de trabalho para o desenvolvimento de padrões de RFID (FINKENZELLER, 2010). Dentre os padrões ISO pode-se citar os de baixa frequência, utilizado no rastreamento de animais (ISO 11784, ISO 11785, ISO 14223), os de alta frequência utilizados em cartões inteligentes (ISO 10536, ISO 14443, ISO 15693) e os da série ISO 18000, utilizados no gerenciamento de itens, os quais atuam em diferentes frequências (FINKENZELLER, 2010).

A EPC Global é uma organização sem fins lucrativos que visa a padronização do RFID através do Código Eletrônico de Produto (EPC - *Electronic Product Code*) e da EPC Network. O EPC é um meio para identificar de forma única paletes, caixas

ou itens. Uma *tag* EPC não carrega informações pessoais. Todas as informações sobre o objeto com a *tag* EPC é administrada exclusivamente no EPCglobal Network. O EPCglobal Network é uma tecnologia, a qual permite a parceiros comerciais documentar e determinar a localização de bens individuais na cadeia de abastecimento em tempo real (FINKENZELLER, 2010). Dentre os padrões EPC podem-se citar o Class 0, Class 1 e o Class 1 Gen 2; sendo este último reconhecido pela ISO como padrão internacional ISO 18000-6C.

2.1.4 Aplicações da Tecnologia RFID

Existe um grande número de sistemas que são implementados utilizando RFID. A diversidade de aplicações se estende pela cadeia de suprimento, agricultura, identificação de animais, controle de acesso, transporte público, pedágios, dentre outros.

A Identificação por Radiofrequência nas cadeias de suprimentos permite rastrear todo o processo produtivo, materiais utilizados na fabricação, inspeção, faturamento, distribuição, até chegar ao revendedor ou mesmo consumidor final. Na fábrica de automóveis da Volkswagen na Eslováquia, seus veículos montados nas estações de serviços finais e processos de inspeção na unidade de Bratislava, são rastreados utilizando um sistema de localização em tempo real. A solução que emprega tecnologia RFID com o uso de *tags* ativas, permite que a empresa localize os veículos estacionados e identifique quando um carro entra ou sai de cada um dos vários processos, o que torna possível melhorar a eficiência dos estágios de produção final (SWEDBERG, 2012).

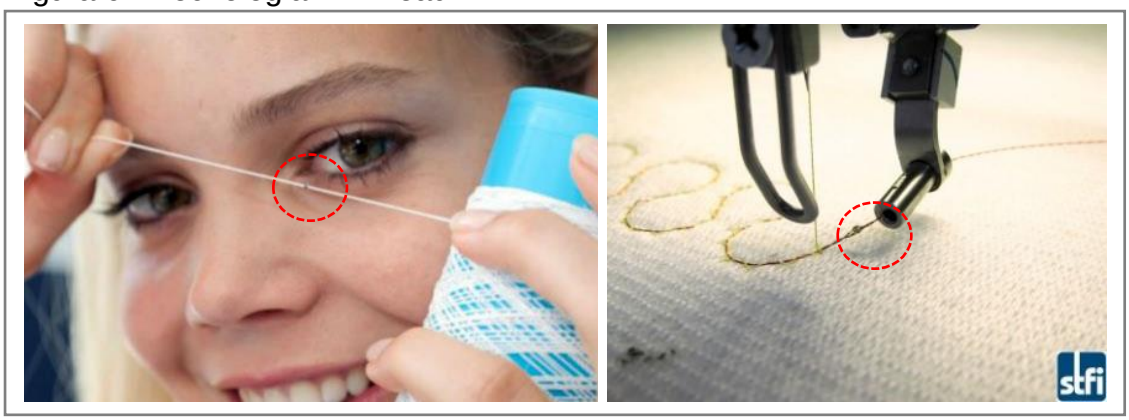
No esporte, a Liga Nacional de Futebol Americano (NFL - *National Football League*) tem utilizado a tecnologia RFID para capturar dados de desempenho de seus jogadores em tempo real. Cada jogador utiliza duas *tags* RFID ativas, uma em cada ombro, e estas emitem seus IDs para os leitores RFID mais de 12 vezes por segundo. Cada estádio participante possui uma média de 20 leitores RFID instalados nos andares superior e inferior. Os dados colhidos pelo sistema possibilita identificar a posição de cada jogador, acompanhar sua velocidade, aceleração e distância percorrido. A análise dos dados através do *software* MotionWorks, desenvolvido pela empresa Zebra, auxilia os atletas e os treinadores a melhorarem seus desempenhos nos jogos, bem como servem de base para criar gráficos que

podem ser exibidos aos telespectadores em televisores, *smartphones*, *tablets* e outros (ZAINO, 2015).

Na empresa Rolls-Royce Canadá que realiza manutenção e reparos em motores de avião de uso civil e militar, durante a execução dos serviços, seus mecânicos utilizam diversas ferramentas dentro dos motores dos aviões. O esquecimento de uma ferramenta dentro de um motor pode causar um grande dano (GREENGARD, 2014). Uma solução encontrada foi colocar *tags* passivas (UHF) nas ferramentas, e guardá-las dentro de um armário com quatro antenas RFID, localizadas em seu interior, e conectadas a um leitor RFID (UHF). O leitor RFID está conectado a um computador e a um controlador. Uma luz ligada ao controlador, apresenta o status do armário, acendendo a luz vermelha quando se esquece de guardar alguma ferramenta, possibilitando que os funcionários a localizem e evitem possíveis danos causados pelo esquecimento destas dentro de motores.

Na Industria Têxtil, *tags* RFID são agregadas aos produtos de forma a permitir o seus rastreamento, tanto dentro da fábrica, quanto no restante da cadeia, chegando até o consumidor final. Normalmente, os produtos, tais como peças de vestuário, são rotulados com etiquetas externas, contudo, atualmente, é possível incorporá-las aos produtos. Na tecnologia E-Thread (Figura 6), desenvolvida pela Primo1D**,** fios são equipados com "*tags*" UHF EPC Gen2 RFID, permitindo que estes sejam utilizados em equipamentos têxteis, como máquinas de bordar**.** Os Threads podem medir 445 microns por 490 mícrons (0,018 polegadas por 0,019 polegadas) ou menos, e ser interrogados com qualquer leitor RFID padrão UHF a uma distância de até 7 metros (SWEDBERG, 2014), (PRIMO1D, 2013).

Figura 6 - Tecnologia E-Thread.



Fonte: Adaptado de PRIMO1D (2013).

No Brasil, o Departamento Nacional de Trânsito (Denatran) está em processo de implantação do SINIAV (Sistema Nacional de Identificação Automática de Veículos), que tem por objetivo aperfeiçoar a fiscalização e gestão do trânsito e da frota de veículos, através do rastreamento destes utilizando tecnologia RFID. A resolução n° 212 do Conselho Nacional de Trânsito – CONTRAN de 13 de novembro de 2006 determina a adoção obrigatória da tecnologia de Identificação por Radiofrequência em toda a frota brasileira de veículos. O SINIAV utiliza o padrão especificado na norma ISO 18000-6 e a faixa de frequência de 915 MHz a 928 MHz para realizar a comunicação entre o leitor e as *tags* RFID (BRASIL, 2011). É previsto que a partir de 01 de janeiro de 2016 seja iniciado o processo de emplacamento eletrônico de veículos em todo território nacional (BRASIL, 2015).

A diversidade de aplicações do RFID, e a importância destas para as organizações que as implantam, tornam necessário que se dê atenção a segurança destes sistemas.

2.1.5 Segurança e Privacidade

A segurança dos sistemas que utilizam RFID engloba questões relacionadas a proteção dos dados contidos nas *tags* e disponibilidade dos serviços ao qual se destina a identificação fornecida por estas. Além do número de identificação, as *tags* podem armazenar outros dados relacionados a “quem” ou a “o que” ela se destina identificar. Estes dados podem comprometer a segurança dos processos envolvidos, bem como comprometer a privacidade das pessoas que a utilizam.

A questão da privacidade em sistemas RFID incluem o vazamento de informações contidas nas *tags*, bem como o rastreamentos destas. As *tags* podem responder aos interrogadores sem que estes tenham o conhecimento de quem as esta portando ou de seus proprietários. Quando o número de identificação da *tag* é relacionada a dados pessoais, o problema se torna maior; pois permite, por exemplo, que um comerciante trace o perfil do consumidor utilizando rede de leitores tanto dentro, quanto fora do estabelecimento comercial. No Brasil, a privacidade tem sido discutida com relação a implantação do Sistema Nacional de Identificação Automática de Veículos (SINIAV). A Ordem dos Advogados do Brasil questiona o fato do sistema permitir conhecer a exata localização do veículo de uma pessoa,

ferindo, assim, o direito constitucional à garantia de privacidade dos cidadãos (LEITÃO, 2012).

Como visto, a privacidade para ser ferida não precisa necessariamente que o sistema de RFID sofra um ataque, pois a própria entidade que disponibilizou a *tag* para o usuário, pode utilizar-se do conhecimento das informações contidas nesta, para interesses próprio.

2.1.5.1 Ataques

Os sistemas RFID são suscetíveis a ataques como todos os sistemas que envolvem transmissão e armazenamento de dados. Os objetivos de cada ataque podem ser muito diferentes, sendo assim, é importante identificar os potenciais alvos para compreender os possíveis ataques. A seguir são apresentados alguns tipos de ataque que sistemas RFID podem sofrer:

1. *Eavesdropping* (espionagem): é um ataque passivo no qual um atacante escuta a comunicação entre a *tag* e o leitor. Em virtude do RFID operar através de rádio, a comunicação entre a *tag* e o leitor pode ser realizada em diferentes distâncias. Estas variam de acordo com os equipamentos utilizados (*tags* e leitores), sendo possível, em um ataque, aumentar significativamente a distância padrão especificada nestes equipamentos. Em Kfir e Wool (2005), são descritos ataques a um sistema que utiliza cartões sem contato. Nos ataques foram utilizados dois dispositivos, fantasma e o sanguessuga. O fantasma simula um cartão para o leitor, e o sanguessuga simula um leitor do cartão. Criou-se então um canal de comunicação bidirecional entre o leitor real e o cartão da vítima com alcance muito maior do que a faixa nominal do sistema. Um exemplo deste tipo de ataque é a obtenção de dados de um cartão de crédito, como: nome do proprietário, número do cartão, data de expiração, tipo de cartão; através da captura das transmissões realizadas entre um leitor de cartão de crédito e um cartão de crédito RFID. Os dados obtidos neste tipo de ataque podem ser utilizados em ataques mais complexos, como: *Replay* e *Tracking*.
2. *Man in the middle*: O atacante se posiciona em um local intermediário entre o leitor e a *tag* que se encontra fora do alcance de leitura do mesmo. Assim,

interrompe o caminho de comunicação, e manipula as informações que serão transmitidas tanto para o leitor, como para a *tag*, enganando os dois componentes.

3. *Tracking*: O rastreador utiliza dados contidos nas *tags* para identificar a presença destas em um determinado ambiente físico, sem a autorização de quem a porta ou de seu proprietário. Desta forma é possível identificar a trajetória do objeto ou da pessoa a ela associada. Mesmo que em uma *tag* esteja armazenado apenas seu número de identificação, seria possível em uma compra, por exemplo, a loja estabelecer em seu banco de dados um vínculo entre o número de identificação da *tag* e o cliente que adquiriu o produto no qual a *tag* se encontra. Desta forma, seria possível identificar a presença do cliente na loja, quando ele voltasse portando o objeto anteriormente adquirido.
4. *Replay*: neste tipo de ataque os dados transmitidos entre a *tag* e o leitor são capturados e, posteriormente, reutilizados de forma a forjar uma nova comunicação.
5. *Cloning*: Os dados de uma *tag* válida são capturados pelo leitor do atacante e, posteriormente, escritos em uma outra *tag* (clone). Desta forma a *tag* clonada se comportará como a original perante o leitor.
6. *Spoofing*: o invasor simula uma identidade diferente da que ele tem, no caso, ele simula uma *tag* válida, e assim, pode fazer uso de todos os privilégios que aquela *tag* proporciona. A diferença entre este tipo de ataque e o *Cloning* é que neste último há uma reprodução física de uma *tag* original, enquanto no ataque *Spoofing* é utilizado um equipamento eletrônico para emular ou imitar a *tag* original (TEHRANIPOOR e WANG, 2012).
7. *Denial of Service* (DoS): Os ataques de negação de serviço têm o objetivo de impedir que usuários legítimos consigam utilizar o sistema. Ataques DoS podem ser realizados, por exemplo, utilizando dispositivos que emitam sinais de ruído na faixa de frequência utilizada pela rede RFID, reduzindo a taxa de transferência e, consequentemente, emperrando o sistema (XIAO, GIBBONS e LEBRUN, 2009). Um outro exemplo seria a utilização não autorizada do comando *KILL*, para que as *tags* deixem de responder aos leitores (TEHRANIPOOR; WANG, 2012).

Alguns ataques, em um primeiro momento, podem parecer não trazer prejuízos, como é o caso do *Eavesdropping*, contudo, servem como base para outros mais complexos (*Replay*, *Tracking*). As consequências geradas pelos diversos tipos de ataques podem atingir diferentes níveis de prejuízo financeiro, ou até mesmo relativos a privacidade de indivíduos, como podem ocorrer com o *Tracking*. Ataques como *Cloning* e *Spoofing* podem permitir acesso a áreas não autorizadas de empresas e residências, no caso destas utilizarem fechaduras com tecnologia RFID, bem como qualquer outro tipo de privilégio que se poderia ter com uma *tag* original.

A seguir, apresenta-se algumas contramedidas que podem ser utilizadas de forma a inibir diferentes tipos de ataques.

2.1.5.2 Contramedidas

Ataques ao sistema RFID podem causar grandes prejuízos financeiros às empresas que o utilizam, bem como aos usuários finais, neste último caso, podendo atingir também a privacidade destes. Assim, faz-se necessário que contramedidas sejam tomadas para evitar ataques RFID. Dentre as várias contramedidas, pode-se citar:

1. RSA *Blocker Tags*: é um produto desenvolvido pelos cientistas do laboratório RSA, em conjunto com o Professor Ronald Rivest, para a proteção da privacidade de consumidores. O RSA *Blocker Tag* cria uma região física a sua volta, a qual impede que os leitores de RFID singularizem as *tags* que se encontram nesta região (JUELS; RIVEST; SZYDLO, 2003). Desta forma, é possível que consumidores se locomovam portando *tags,* sem que estas sejam lidas por leitores RFID, preservando, assim, sua privacidade.
2. *Kill Command*: é uma forma de proteger a privacidade dos consumidores enviando um comando para matar a *tag*, não sendo mais possível que esta seja lida por qualquer leitor RFID (XIAO; GIBBONS; LEBRUN, 2008), (LÓPEZ, 2008). Desta forma, pode ser dada ao consumidor, por exemplo, a oportunidade de matar a *tag* antes de sair de uma loja, evitando o seu rastreamento.

3. Gaiola de Faraday: baseado na Gaiola de Faraday, é uma forma de bloquear as frequências de rádio utilizando um isolamento, o qual impede que os sinais do interior do objeto que possui esse isolamento alcance o seu exterior e vice-versa. Este isolamento pode ser simplesmente feito com folhas de metal, ou até mesmo, ser adquirido no mercado objetos como carteiras, bolsas, porta cartão, dentre outros, confeccionados com material próprio para esta função. Desta forma, é possível que um *e-passport* ou cartão de crédito com tecnologia RFID fique dentro de uma carteira protegido de leituras maliciosas. Contudo, este mesmo tipo de isolamento, poderia ser utilizado, por exemplo, para efetuar furtos de produtos em lojas, inibindo a leitura das *tags* dos produtos.
4. Criptografia: pesquisadores têm propostos várias versões de criptografias para serem utilizadas em sistemas RFID (DONG; ZHAN; WEI, 2013; LÓPEZ, 2008; NOMAN; RAHMAN; ADAMS, 2011; SHARAF, 2012; SUN; ZHONG, 2012). Criptografias podem ajudar a proteger o sistema contra diversos tipos de ataque, como: *Man in the middle* (XIAO; GIBBON; LEBRUN, 2008), *Cloning* (LÓPEZ, 2008), *DoS* (DONG; ZHAN; WEI, 2013), dentre outros. O grande desafio têm sido a criação de criptografias leves o bastante para serem utilizadas em *tags* de baixo custo, dado que estas possuem capacidade computacional limitada (armazenamento, circuitos e consumo de energia) (LÓPEZ, 2008).
5. *RFID Guardian*: é um dispositivo portátil alimentado por bateria que atua como um mediador das interações entre os leitores e *tags* RFID. Dentre suas funções incluem auditoria, gerenciamento de chaves, controle de acesso e autenticação. O *RFID Guardian* contém recursos de um leitor de RFID e de emulação de *tag*, os quais lhe permitem auditar e controlar as atividades de RFIDNCIL, 2010).

As contramedidas voltadas ao sistema RFID são aplicadas de acordo com o objeto ou pessoa que se deseja identificar. O nível de segurança e quanto se deseja investir financeiramente nesta, vai depender do valor do objeto a que se destina, e das informações que são armazenadas na *tag* ou aquelas a que esta permite o acesso no sistema. Assim, há contramedidas que podem ser utilizadas tanto por organizações, quanto por usuários finais, como é o caso das carteiras baseada na Gaiola de Faraday.

2.2 BLUETOOTH

Bluetooth é uma tecnologia de comunicação sem fio destinada a conexões de curto alcance entre dispositivos. Esta tecnologia foi concebida em 1994 pela equipe da companhia Ericsson, que começou a estudar a viabilidade de uma interface de rádio de baixa potência e baixo custo, que possibilitasse a comunicação entre telefones celulares e seus acessórios sem a utilização de cabos (CHAOUCHI; LAURENT-MAKNAVICIUS, 2009).

A especificação do Bluetooth foi desenvolvido pelo Bluetooth SIG (*Special Interest Group*), que em 1998 foi fundado pela Ericsson, IBM, Intel, Nokia e Toshiba; juntando-se a estas, em 1999, a 3Com Corporation, Lucent Technologies, Microsoft e Motorola. Em julho de 1999, o grupo de trabalho IEEE 802.15 (WPAN - *Wireless Personal Area Network*) propôs a especificação Bluetooth versão 1.0 (CHAOUCHI; LAURENT-MAKNAVICIUS, 2009).

Atualmente, a tecnologia Bluetooth pode ser encontrada em diversos tipos de equipamentos, como televisores, *smartphones*, óculos 3D, caixas de som e outros, permitindo que estes se comuniquem entre si, sendo possível a transferência de dados de texto, áudio, imagem, dentre outros.

2.2.1 Classificação

O Bluetooth foi concebido de forma a possibilitar o seu uso em dispositivos portáteis, possuindo assim uma antena de rádio transmissão de pequena potência, com baixo consumo de energia (BLUETOOTH SIG, 2014). Na Tabela 1 é apresentada a classificação do Bluetooth de acordo com o nível de potência de sua antena. Conforme é mostrado, o alcance do sinal aumenta à medida que se aumenta a potência da antena.

Tabela 1 - Classificação do Bluetooth.

Classe	**Potência Máxima (miliwatts)**	**Alcance Esperado (metros)**
Classe 1	100	100
Classe 2	2,5	10
Classe 3	1	1

Fonte: Adaptado de Chaouchi e Laurent-Maknavicius (2009).

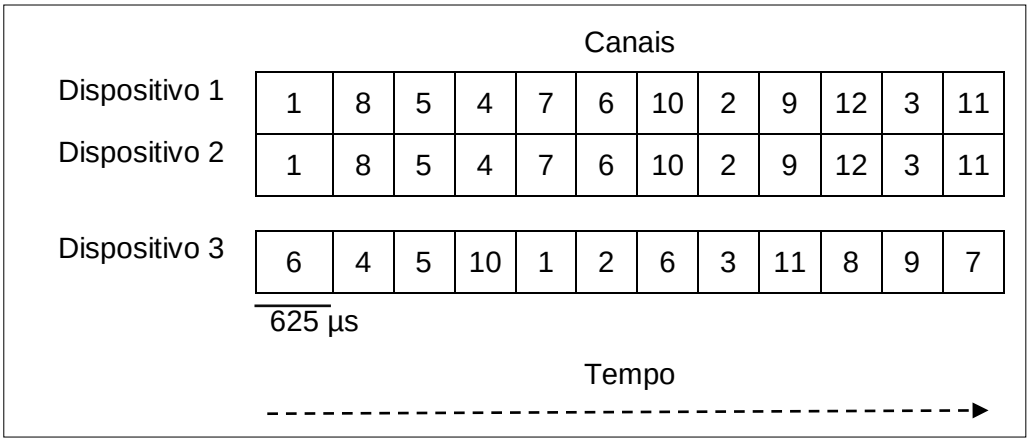
A Classe 2 é a mais utilizada em dispositivos portáteis. Já a Classe 3 é destinada, principalmente, à área industrial.

2.2.2 Frequência de Operação e Comunicação

A tecnologia Bluetooth opera em uma faixa de frequência ISM (*Industrial, Scientific and Medical*) de 2,400 GHz a 2,4835 GHz; que é dividida em 79 canais com uma largura de banda de 1 MHz por canal. A escolha desta faixa deu-se em virtude da mesma não requerer licença na maioria dos países (CHAOUCHI; LAURENT-MAKNAVICIUS, 2009), (BLUETOOTH SIG, 2014).

De forma a evitar interferências, a tecnologia Bluetooth utiliza o método de Espalhamento Espectral por Salto de Frequência (FHSS - *Frequency-Hopping Spread Spectrum).* Neste método, a mudança de canal é realizada 1600 vezes por segundo (a cada 625 microssegundos), e para que os dispositivos se comuniquem é necessário que estejam no mesmo canal, ao mesmo tempo. O período de tempo entre dois saltos (mudança de canal) é denominado *Slot.* (CHAOUCHI; LAURENT-MAKNAVICIUS, 2009), (CACHE; WRIGHT; LIU, 2010). Conforme é apresentado na Figura 7, os Dispositivos 1 e 2 utilizam o mesmo canal, no mesmo instante de tempo, sendo possível, assim, a comunicação entre estes. Com relação ao Dispositivo 3, este utiliza uma sequência de canais diferente da utilizada pelos Dispositivos 1 e 2, não sendo possível, desta forma, a comunicação entre estes e aquele.

Figura 7 - Método de Transmissão de sinais FHSS.



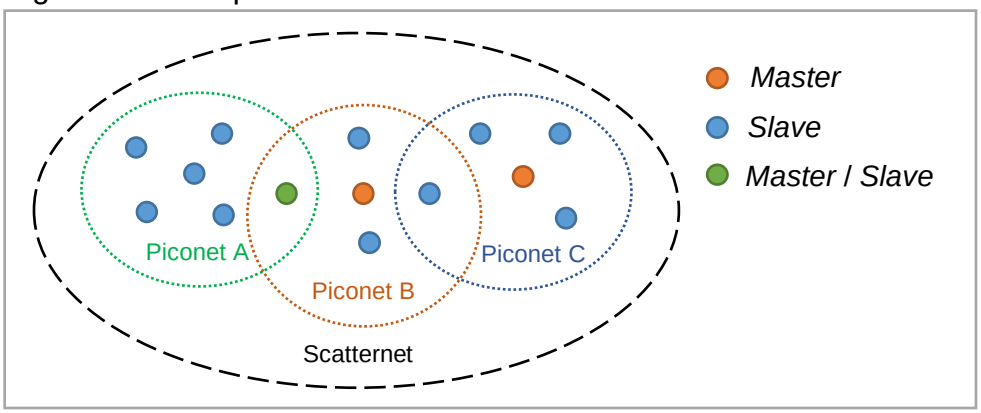
Fonte: Adaptado de Cache, Wright e Liu (2010).

2.2.2.1 Redes Bluetooth

Dispositivos Bluetooth podem se comunicar uns com os outros através de uma Rede de Área Pessoal sem Fio (WPAN - *Wireless Personal Area Network*) denominada “Piconet”, que permite a comunicação de até 8 dispositivos. O dispositivo que iniciou a comunicação opera como *Master* (mestre) e os demais dispositivos como *Slave* (escravo). A sequência de canais mostrada na Figura 7 é gerada através do endereço (BD_ADDR – *Bluetooth Device Address*) e o *clock* do dispositivo *Master*. Desta forma, o dispositivo *Master* dita as regras, sequência de canais, que devem ser seguidas pelos dispositivos *Slaves*, possibilitando a comunicação entre eles (CACHE; WRIGHT; LIU, 2010).

Uma forma de estender a rede é interconectando piconets, formando uma rede denominada “Scatternet”. Na Figura 8 é apresentada uma Scatternet com três Piconets (A, B e C). Os Piconets são interligados por um nó em comum. Pode ocorrer de um nó ser *Master* em um Piconet e *Slave* em outro, como o nó que interliga o Piconet A ao B, que ora é *Master* no Piconet A, ora *Slave* em B (CHAOUCHI; LAURENT-MAKNAVICIUS, 2009).

Figura 8 - Exemplo de uma rede Bluetooth.



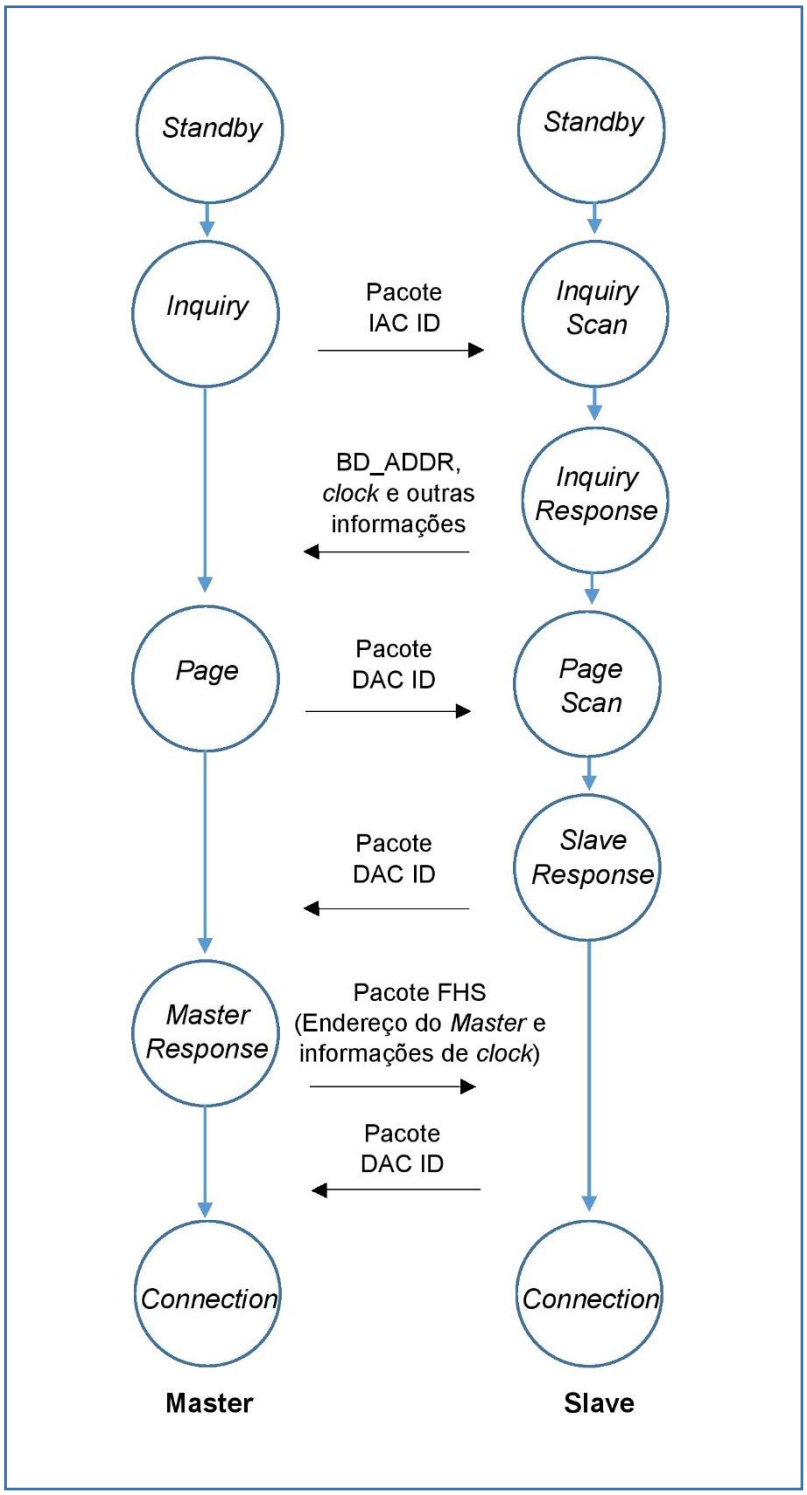
Fonte: Elaboração da própria autora.

Para que seja possível a comunicação entre os diversos dispositivos Bluetooth, vários estados são definidos (*Standby, Inquiry, Scan, Page*), permitindo que seja possível definir como os piconets são criados e os dispositivos adicionados à rede.

Na Figura 9 é apresentado um exemplo de uma conexão Bluetooth. Por padrão, os dispositivos encontram-se no estado *Standby* (Espera). O potencial

dispositivo *Master* entra no estado *Inquiry* (Interrogação) e envia pacotes do tipo *Identity* (ID) contendo o Código de Acesso de Interrogação (IAC - *Inquiry Access Code*) com o objetivo de verificar quais dispositivos Bluetooth estão em sua área de alcance (LAU; KWOK, 2007).

Figura 9 - Exemplo de uma conexão Bluetooth.



Fonte: Elaboração da própria autora.

Na outra ponta, o potencial *Slave* entra no estado *Inquiry Scan*, periodicamente, com o intuito de verificar se algum dispositivo está tentando localizá-lo (descobri-lo). Esta verificação é realizada através da busca por pacotes IAC ID. Recebido o pacote IAC ID, o potencial *Slave* entra no subestado *Inquiry Response*, e gera como resposta um pacote de Sincronização dos saltos de frequência (FHS - *Frequency Hopping Synchronization*) contendo o seu *Bluetooth Device Address* (BD_ADDR), o *clock* e outras informações. Após enviar a resposta, o potencial *Slave* entra no modo *Page Scan* e aguarda por pacotes de *page* do potencial *Master* (LAU; KWOK, 2007).

Recebido o pacote FHS, o potencial *Master* entra no estado *Page* e tenta estabelecer uma conexão com o potencial *Slave*, enviando um pacote ID com o Código de Endereço do Dispositivo (DAC - *Device Address Code*) do potencial *Slave*. O potencial *Slave* identifica seu próprio DAC e responde ao potencial *Master* com o mesmo pacote, confirmando o recebimento deste com sucesso. Em seguida, o *Master* responde informando seu próprio endereço e informações de *clock*. Recebido o pacote, o potencial *Slave* responde com o pacote DAC ID, confirmando o recebimento com sucesso. Neste momento, o potencial *Slave* passa para o estado *Connection* e utiliza a sequência de saltos da conexão derivada do *clock* e endereço do *Master*, para se comunicar posteriormente. Neste momento está formado um Piconet com um dispositivo *Master* e um *Slave* (LAU; KWOK, 2007).

Conforme LAU e KWOK (2007) e Chaouchi e Laurent-Maknavicius (2009), o dispositivo *Slave* pode participar de um Piconet de diversos modos:

1. *Active* – o dispositivo *Master* e *Slave* encontram-se sincronizados, possibilitando a transferência e recebimento de dados. O *Slave* participa ativamente da piconet e recebe um código Endereço de Membro Ativo (AM_DDR - *Active Member Address*) formado por de 3 bits.
2. *Sniff* – como no modo *Active*, o dispositivo *Slave* permanece com o código AM_DDR, contudo, o *Slave* somente tem interesse em mensagens transmitidas em *slots* específicos, determinados pelo *Master*.
3. *Hold* – o dispositivo *Slave* permanece fazendo parte da Piconet, mantendo assim seu AM_DDR; mas somente lhe é possível trocar pacotes de Enlace Síncrono Orientado a Conexão (SCO - *Synchronous Connection-Oriented Link*), interrompendo a transmissão de pacotes de Enlace sem Conexão

Assíncrono (ACL - *Asynchronous Connection-Less Link*). Neste modo, o *Slave* pode tanto reduzir o consumo de energia, quanto participar em outra Piconet, visto que não é possível que participe ativamente em mais de uma Piconet.

4. *Park* – diferente do que ocorre nos demais modos, o *Slave* disponibiliza o seu AM_DDR e recebe o código de Endereço de Membro Estacionado (PM_ADDR - *Parked Member Address*) de 8 bits. Neste caso, o *Slave* não pode participar ativamente da Piconet, mas continua fazendo parte desta.

Os modos *Sniff*, *Hold* e, principalmente, *Park* possibilitam aos dispositivos uma maior economia de energia, em comparação ao modo *Active*. O código AM_DDR de 3 bits recebido pelos *Slave*s, e que permanecem nos modos *Active*, *Sniff* e *Hold* limitam o número de dispositivos que podem atuar ativamente em uma piconet a um *Master* e sete *Slave*s (2^3). Já o número de dispositivos em modo Park em uma piconet é limitado a 256 (2^8), em virtude do seu código PM_ADDR de 8 bits.

A forma como é realizada a comunicação entre os dispositivos Bluetooth, permitindo que diversos dispositivos possam transmitir e receber dados utilizando um baixo consumo de energia, e um *hardware* compacto, possibilita que esta tecnologia seja utilizada em diversos tipos de aplicações.

2.2.3 Aplicações da Tecnologia Bluetooth

A tecnologia Bluetooth pode ser aplicada em diversas áreas, como na saúde, lazer, esporte, transporte e outros.

Na área da saúde, aparelhos de monitoramento cardíaco utilizam a tecnologia Bluetooth para transmitir os dados referentes aos batimentos cardíacos de pacientes, a um *smartphone*. Os dados são coletados através de um sensor localizado no pulso do paciente. No aplicativo instalado no *smartphone* os dados são verificados, e caso necessário, e-mails e torpedos podem ser enviados a um médico cadastrado informando as leituras cardíacas (EVERIST HEALTH, 2011).

Na área dos esportes, Azcueta (2014) apresenta em seu trabalho o sistema denominado ASSESSOR, que mensura e analisa a performance de atletas. A Unidade de Medição de Inércia, presa ao corpo do atleta, é composta basicamente de um acelerômetro, um magnetômetro e um giroscópio. Os dados colhidos por esta

unidade são transmitidos, via Bluetooth, para a aplicação ASSESSOR, instalada em um *tablet* Android, que os analisa.

Nas residências, esta pode ser encontrada sendo utilizada em teclados e mouse de computadores, lâmpadas controladas através de *smartphone*s, óculos 3D, controle remotos de *Smart Tvs* e outros.

2.3 CONSIDERAÇÕES FINAIS DO CAPÍTULO 2

As tecnologias RFID e Bluetooth apresentam características que possibilitam o uso destas de forma independente ou em conjunto. A tecnologia RFID demanda uma maior análise para sua aplicação, em comparação a tecnologia Bluetooth, tendo em vista a sua diversidade de *tags*, leitores e protocolos que devem ser escolhidos de forma a atender as necessidades da aplicação.

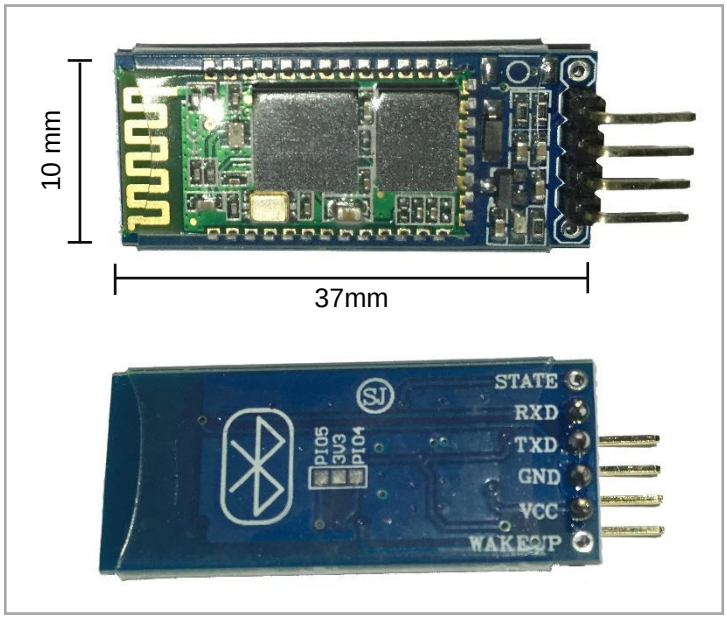
Nos Capítulos 3 e 4 serão apresentadas a utilização das tecnologias RIFD e Bluetooth, e os testes realizados neste trabalho.

3 UTILIZAÇÃO DA TECNOLOGIA BLUETOOTH E MICROCONTROLADOR

A tecnologia Bluetooth foi escolhida para a transmissão de dados sem fio, em virtude do seu baixo consumo de energia, tamanho compacto dos módulos existentes no mercado, bem como o baixo custo, em comparação a tecnologias como XBee.

O módulo Bluetooth utilizado neste trabalho foi o HC-06, apresentado na Figura 10. Este módulo possui antena embutida e atua somente em modo *Slave*.

Figura 10 - Módulo Bluetooth HC-06.



Fonte: Elaboração da própria autora.

Para a realização dos testes, foram enviadas mensagens de um microcontrolador ao módulo Bluetooth através de uma porta serial, para que este as retransmitisse a um *smartphone* com tecnologia Bluetooth.

3.1 MICROCONTROLADOR

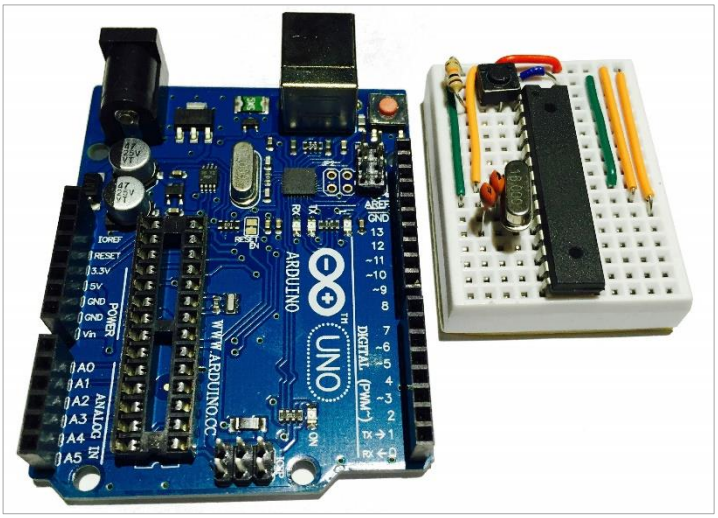
Um microcontrolador é um computador encapsulado em um único chip, projetado especificamente para aplicações de controle, em vez de aplicações gerais. Este componente apresenta Unidade Central de Processamento (CPU - *Central Processing Unit*), Memória de Acesso Aleatório (RAM - *Random Access Memory*) e Memória Apenas de Leitura (ROM - *Read Only Memory*), bem como interfaces para

entrada e saída de periféricos paralelos ou seriais, todos integrados em uma única pastilha (TOOLEY, 2007).

O microcontrolador utilizado neste trabalho foi o ATMEGA328P-PU. Desenvolvido pela Atmel e pertencente à família de microcontroladores megaAVR, este componente opera em uma frequência máxima de 20 MHz, possuí 32 Kbytes de memória Flash, 2 Kbytes de memória RAM, e pode ser alimentada entre 1,8 e 5,5 volts.

Para a realização dos testes e a gravação dos códigos de envio de mensagem do microcontrolador para o módulo Bluetooth, foram utilizados uma placa Arduino UNO e o *software* Arduino IDE. Realizada a gravação do microcontrolador, este foi transferido para uma *protoboard*, e com a adição de um oscilador a cristal de 16 MHz, dois capacitores cerâmicos de 22pF, uma chave táctil e um resistor de 10k; foi possível eliminar a necessidade do uso da placa Arduino. Na Figura 11 é apresentada a placa Arduino UNO e o protótipo do circuito construído.

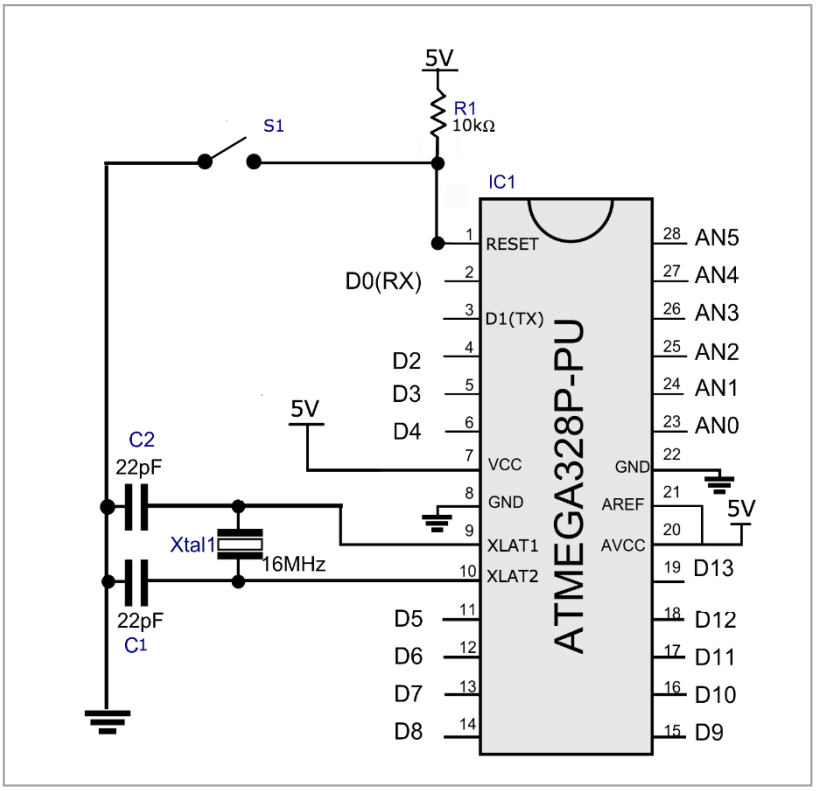
Figura 11 - Placa Arduino UNO e *protoboard*.



Fonte: Elaboração da própria autora.

O esquemático do circuito construído é apresentado na Figura 12. O oscilador a cristal conectado aos pinos XTAL1 e XTAL2 e os capacitores cerâmicos de 22 pF foram utilizados para fornecer uma frequência de clock de 16 MHz ao microcontrolador. A escolha dos capacitores utilizados e a forma de conexão destes com o cristal, seguem as especificações do fabricante do microcontrolador (ATMEL CORPORATION, 2013). O resistor e a chave táctil foram utilizados em um *Reset* Externo (sinal utilizado para inicializar o microcontrolador).

Figura 12 - Esquemático do circuito do microcontrolador.



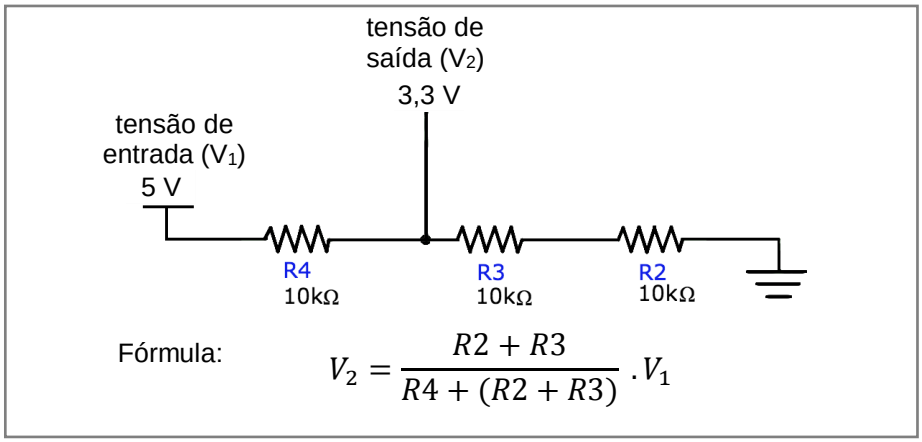
Fonte: Elaboração da própria autora.

Após a construção do circuito, o módulo Bluetooth foi adicionado ao mesmo, conectando-se a este através do pino D1(TX).

3.2 MÓDULO BLUETOOTH

O módulo Bluetooth HC-06 (Bluetooth versão 2.0) pode transmitir e receber dados através das portas seriais de Transmissão de Dados (TXD) e de Recepção de Dados (RDX) utilizando as seguintes taxas: 1200, 2400, 4800, 9600, 19200 e 38400 bps. A taxa escolhida para ser utilizada neste trabalho foi a taxa padrão: 9600 bps. Em relação a alimentação do módulo, este pode utilizar tensões entre 3,6 e 6 volts; contudo, suas portas serias operam em 3,3 volts. A tensão utilizada para a alimentação do módulo foi de 5 volts, que é a mesma utilizada para a alimentação do microcontrolador. Desta forma, na porta RDX utilizada para recepção dos dados oriundos do microcontrolador, foi necessário o uso de um Divisor de Tensão para diminuir a tensão de 5 V para 3,3 V. Na Figura 13 é apresentada o circuito utilizado como divisor de tensão neste trabalho, bem como a fórmula utilizada para definição dos valor dos resistores utilizados.

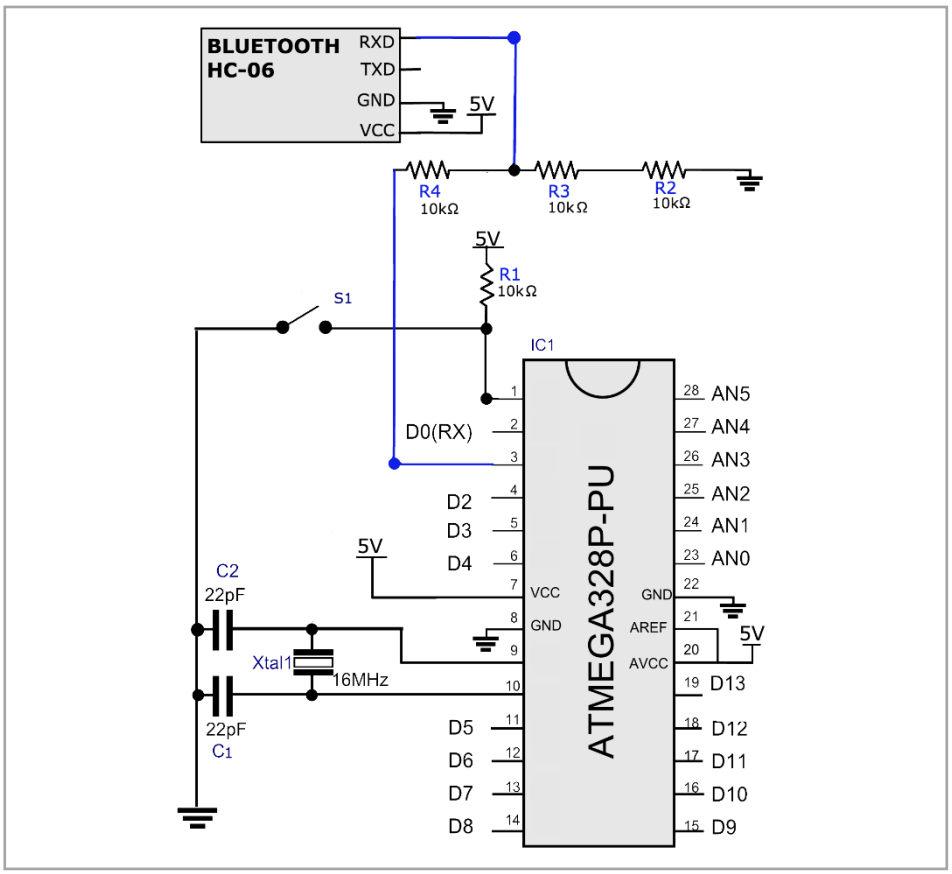
Figura 13 - Esquemático do divisor de tensão utilizado.



Fonte: Elaboração da própria autora.

Na Figura 14 é apresentado o esquemático completo do circuito incluindo o microcontrolador e o módulo Bluetooth. Os dados gravados no microcontrolador são enviados através da porta serial D1(TX), e recebidos no módulo Bluetooth pela porta serial RXD. Recebidos os dados, estes são transmitidos para o *smartphone* utilizando a tecnologia Bluetooth.

Figura 14 - Esquemático do circuito Bluetooth e Microcontrolador.

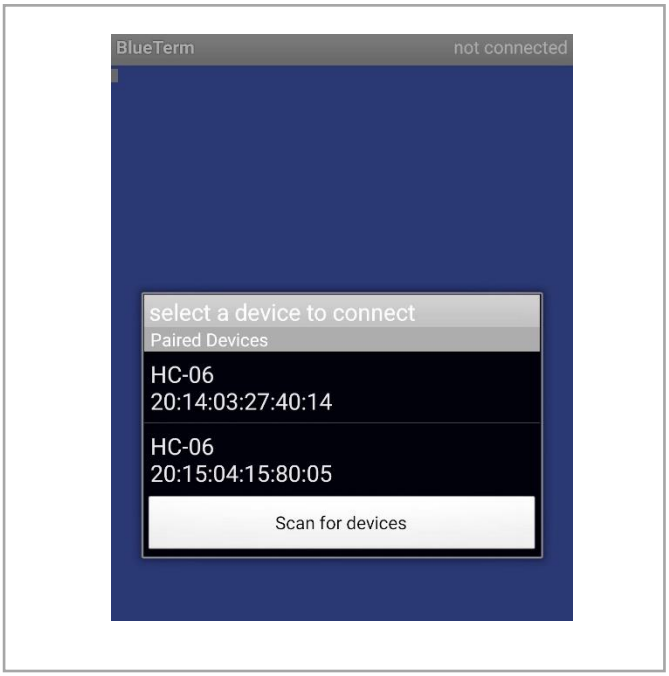


Fonte: Elaboração da própria autora.

3.3 RECEPÇÃO DO DADOS VIA SMARTPHONE

Para a realização dos testes foi utilizado um *smartphone* Samsung S4 (Bluetooth versão 4.0) com Sistema Operacional Android. Os dados enviados pelo módulo Bluetooth são recebidos no *smartphone* utilizando aplicativo BlueTerm instalado neste. O aplicativo BlueTerm, que é disponibilizado gratuitamente no Google Play (loja online da Google), possibilita a conexão com o módulo Bluetooth e exibe os dados enviados por este em um terminal. Na primeira conexão com o módulo Bluetooth, é solicitada a senha. Já nas demais, os módulo Bluetooth é apresentado na lista de dispositivos pareados com seu nome de identificação (HC-06) e seu endereço (20:15:04:15:80:05), conforme apresentado na Figura 15.

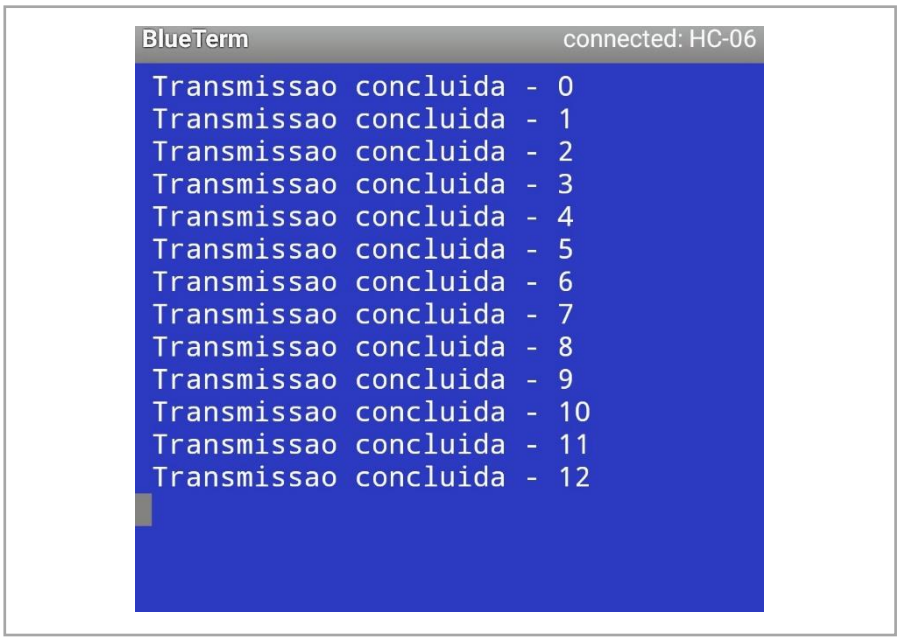
Figura 15 - Aplicativo BlueTerm. – Conexão.



Fonte: Elaboração da própria autora.

Após a conexão, o aplicativo exibe a interface do terminal com as mensagens que estão sendo enviadas pelo módulo Bluetooth, conforme é apresentado na Figura 16.

Figura 16 - Aplicativo BlueTerm – Recepção das Mensagens.



Fonte: Elaboração da própria autora.

3.4 CONSIDERAÇÕES FINAIS DO CAPÍTULO 3

O circuito construído utilizando o microcontrolador ATMEGA328P-PU e o módulo Bluetooth HC-06, resultou em um protótipo pequeno, utilizando uma tecnologia com baixo consumo de energia.

Realizados os primeiros testes com a tecnologia Bluetooth, foram iniciados os testes com a tecnologia RFID.

4 OIT (*HARDWARE*)

Para o desenvolvimento de um módulo para identificação de objetos e transmissão de dados sem fio, que resulte em um equipamento de pequeno porte, passível de ser utilizado no pulso de seus usuários, foram realizados testes com o leitor RFID ID-20LA, que resultaram no protótipo denominado oIT. O oIT é um módulo que utiliza a tecnologia RFID para identificação de objetos através das *tags* fixadas a estes e a tecnologia Bluetooth para transmissão dos IDs obtidos das *tags.* A recepção desses dados (IDs) pode ser realizada por um *smartphone* com tecnologia Bluetooth, através de uma aplicação instalada neste, com um fim específico. Na Seção 4.1, serão apresentados os materiais e métodos utilizados no desenvolvimento do módulo oIT. A Seção 4.2 apresenta os testes realizados com a tecnologia RFID, em relação ao alcance de leitura do módulo RFID ID-20LA. Na Seção 4.3, é apresentado os testes de alcance de conexão e transmissão de dados do módulo Bluetooth.

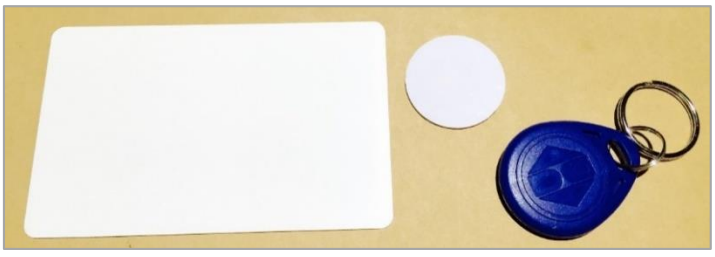
4.1 MATERIAIS E MÉTODOS

Na realização dos testes foram utilizados um leitor RFID ID-20LA, um módulo Bluetooth HC-06 e 3 *tags* RFID compatíveis com o leitor e em encapsulamentos distintos: cartão, moeda e chaveiro. Na Figura 17 é apresentado o leitor RFID ID-20LA e na Figura 18, as *tags* utilizadas.

Figura 17 - Leitor RFID ID-20LA.

Fonte: Adaptado de (SPARKFUN ELECTRONICS, 2014).

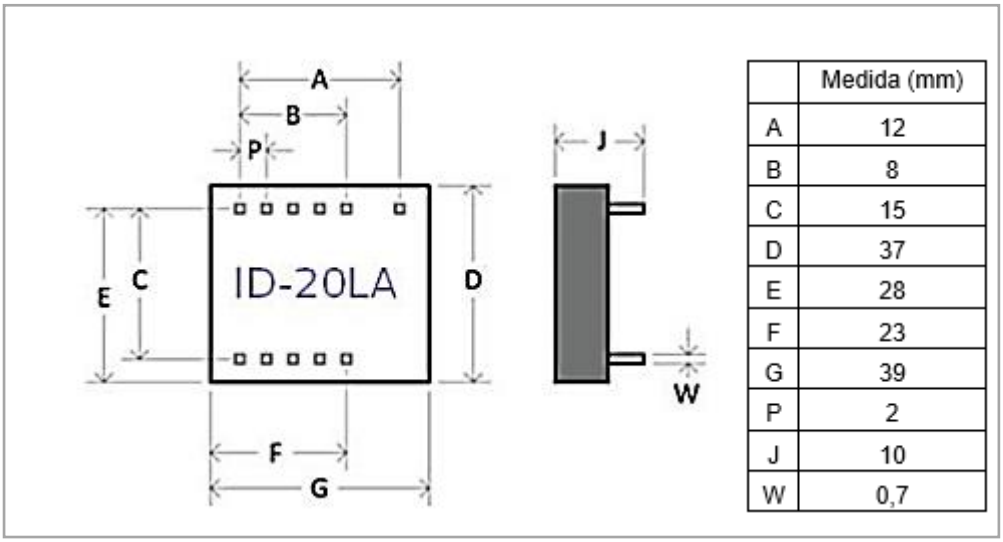
Figura 18 - *Tags* RFID.



Fonte: Elaboração da própria autora.

O RFID ID-20LA é um leitor de curto alcance (até 18 cm), com frequência de operação de 125 kHz, compatível com os padrões EM4001 e 4100, e possui dimensões que viabilizam seu uso para os propósitos deste trabalho, conforme é apresentado na Figura 19.

Figura 19 - Medidas do leitor ID-20LA.

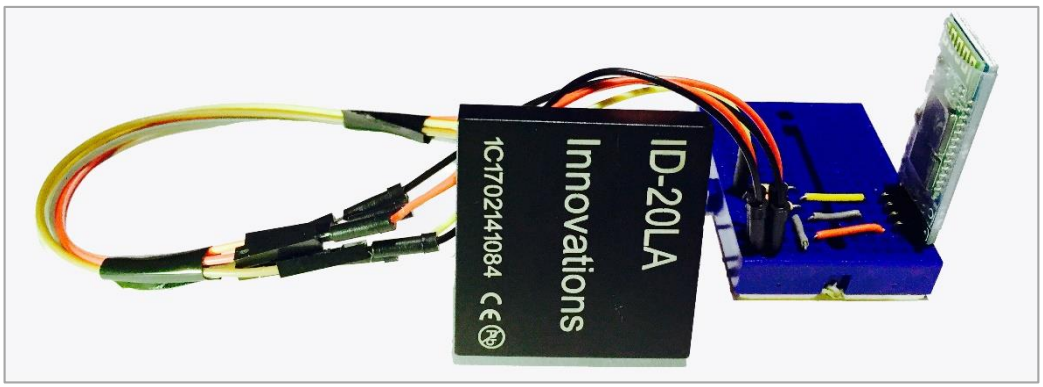


	Medida (mm)
A	12
B	8
C	15
D	37
E	28
F	23
G	39
P	2
J	10
W	0,7

Fonte: Adaptado de ID INNOVATIONS (2013).

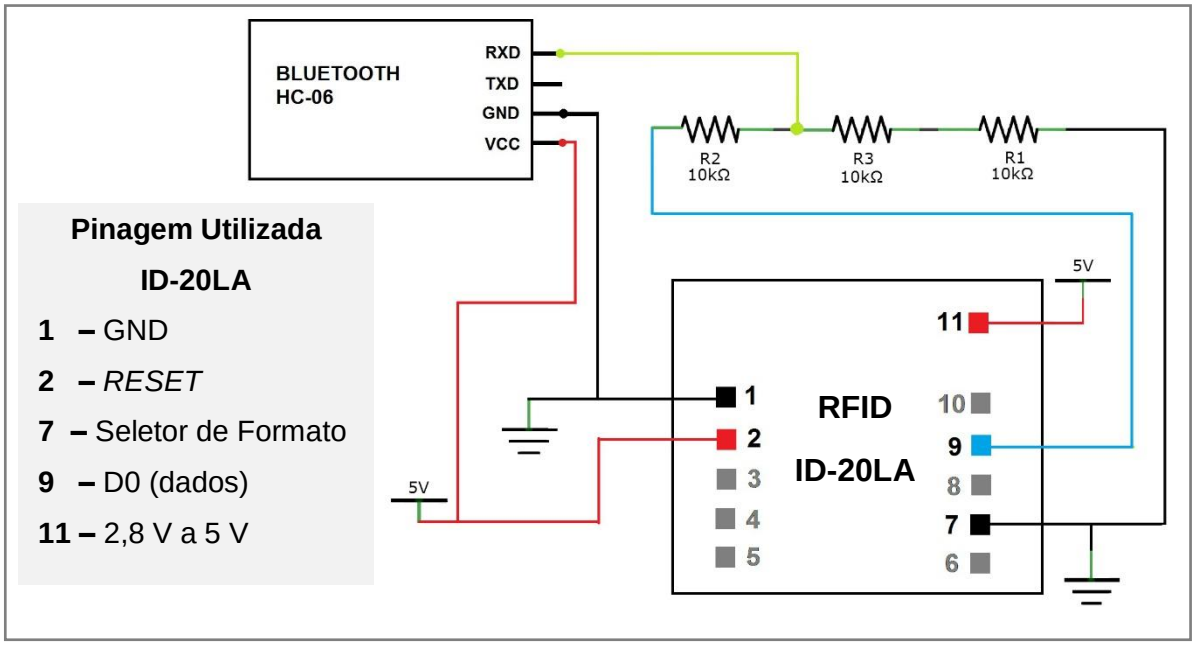
Na Figura 20 é apresentado o circuito construído para utilização do leitor RFID ID-20LA e do módulo Bluetooth HC-06, e na Figura 21, o esquemático deste.

Figura 20 - Circuito ID-20LA e Bluetooth HC-06.



Fonte: Elaboração da própria autora.

Figura 21 - Esquemático do RFID ID-20LA e Bluetooth HC-06.



Fonte: Elaboração da própria autora.

O leitor RFID ID-20LA pode transmitir os dados (IDs das *tags*) em três formatos: ASCII, *Magnet Emulation* e Wiegand26. Neste trabalho, foi selecionado o formato de Código Padrão Americano para o Intercâmbio de Informação (ASCII - *American Standard Code for Information Interchange*). A seleção foi realizada conectando o pino 7 (seletor de formato) ao GND.

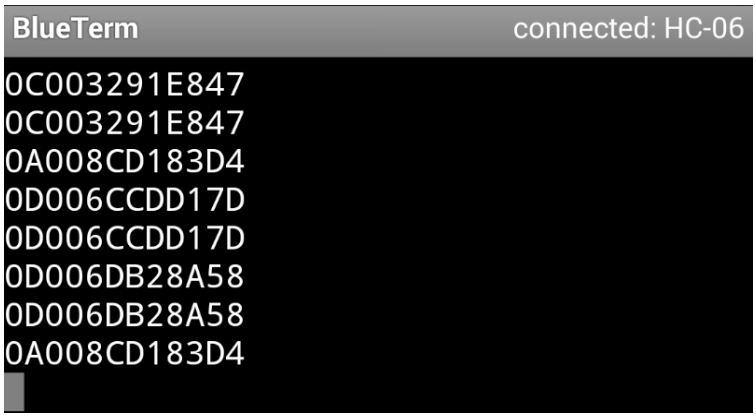
A taxa de transferência de dados no formato ASCII é de 9600 bps (a mesma utilizada no módulo Bluetooth) e a saída é dada no formato de 16 bytes. Dentre os dados enviados, 10 bytes são referentes a dados (*data*), 2 bytes são utilizados para checar os 10 bytes anteriores (*checksum*), e os demais STX (*Start of TeXt*), CR (*Carriage Return*), LF (*Line feed*) e ETX (*End of TeXt*) são utilizados para controlar a comunicação entre os dispositivos Bluetooth. Na Figura 22 é apresentado o formato dos dados de saída do leitor RFID. Na Figura 23 é demonstrada a interface do aplicativo BlueTerm com alguns exemplos de leituras de *tags* RFID, transmitidas a esse utilizando o protótipo desenvolvido.

Figura 22 - Formato dos dados de saída do leitor RFID.

STX	DATA (10 ASCII)	CHECKSUM (2 ASCII)	CR	LF	ETX

Fonte: Elaboração da própria autora.

Figura 23 - Aplicativo BlueTerm com leituras de *tags*.

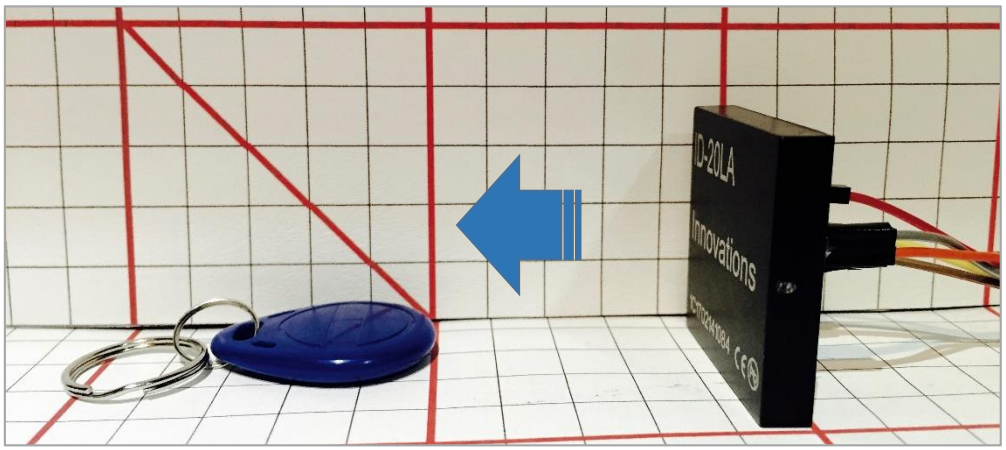


Fonte: Elaboração da própria autora.

4.2 ALCANCE DE LEITURA DO RFID ID-20LA

Ao finalizar o desenvolvimento do protótipo, foram realizados testes para verificar o alcance de leitura do RFID ID-20LA. Os testes foram realizados colocando as *tags* em diferentes posições, e movimentado o leitor RFID (na posição vertical) em direção as *tags*, conforme apresentado na Figura 24.

Figura 24 - Movimento realizado com o leitor RFID nos testes.



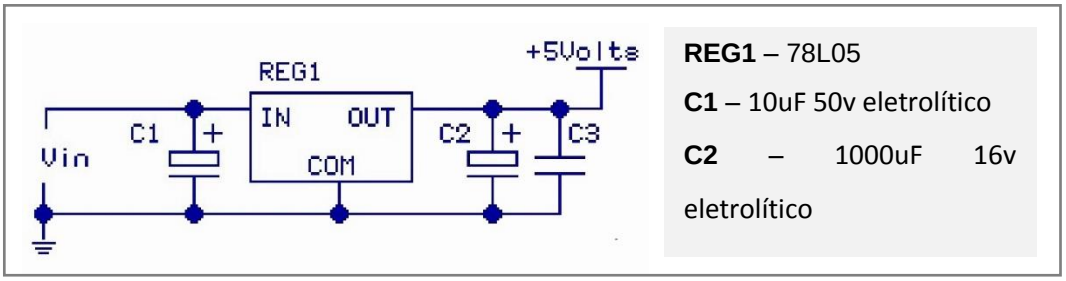
Fonte: Elaboração da própria autora.

Para a realização dos testes foi utilizada a fonte de alimentação apresentada na Figura 25, que fornece 5V de tensão para a alimentação do módulo oIT. Na Figura 26 é apresentado o esquemático da fonte.

Figura 25 - Fonte de Alimentação.

Fonte: Elaboração da própria autora.

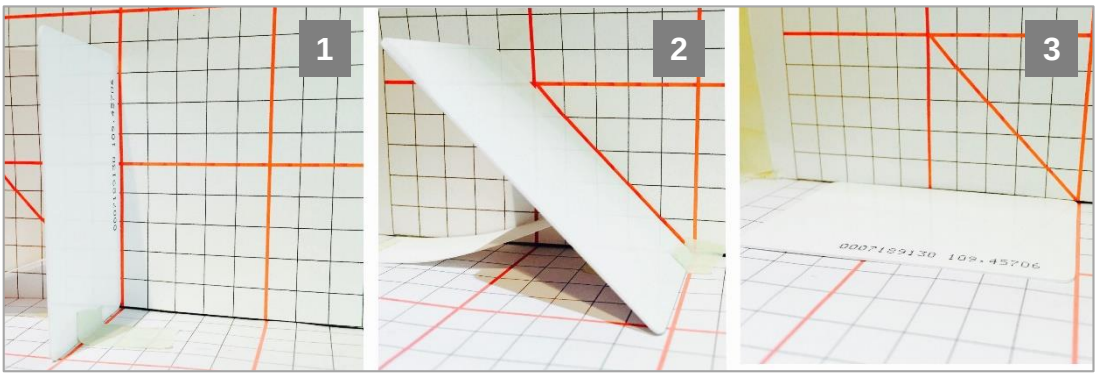
Figura 26 – Esquemático da Fonte de Alimentação.



Fonte: Adaptado de ID INNOVATIONS (2013).

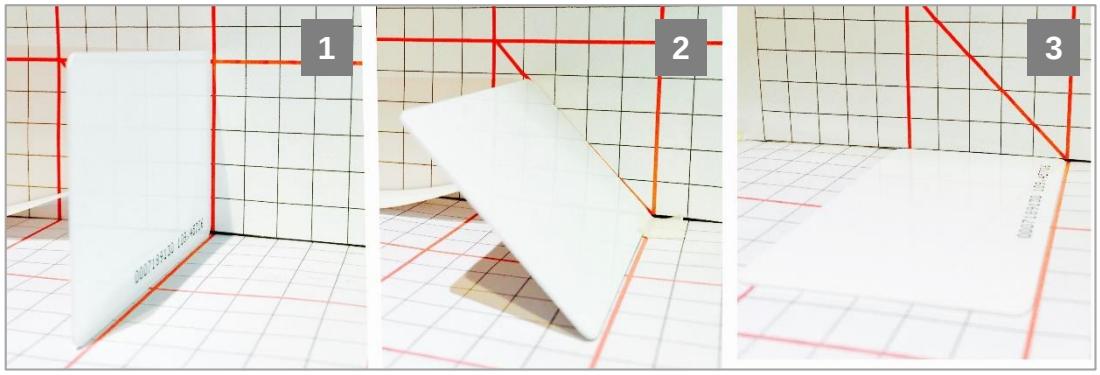
As *tags* foram colocadas em três diferentes posições: vertical (1), aproximadamente 45 graus (2) e horizontal (3), conforme apresentado nas Figuras de 27 a 30. Em virtude do seu formato retangular, as *tags* encapsuladas em cartão foram testadas ora com o lado maior virado para base, ora com o lado menor.

Figura 27 - Posição da *tag* cartão nos testes (lado menor voltado para base).



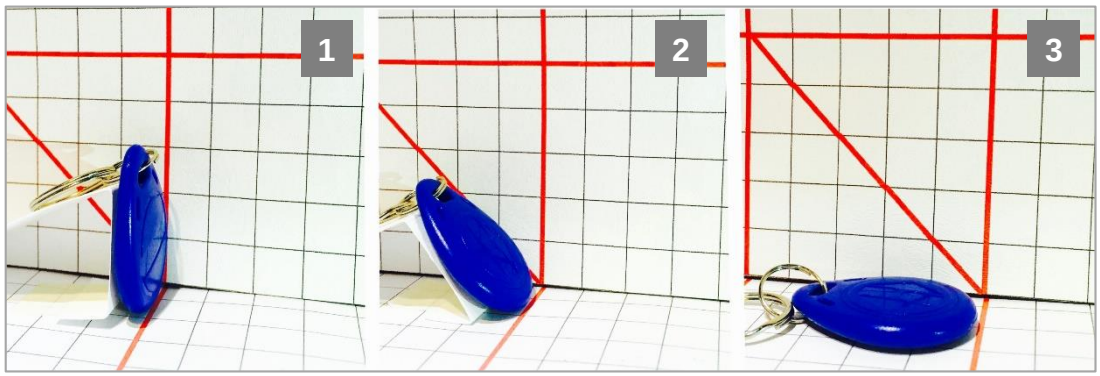
Fonte: Elaboração da própria autora.

Figura 28 - Posição da *tag* cartão nos testes (lado maior voltado para base).



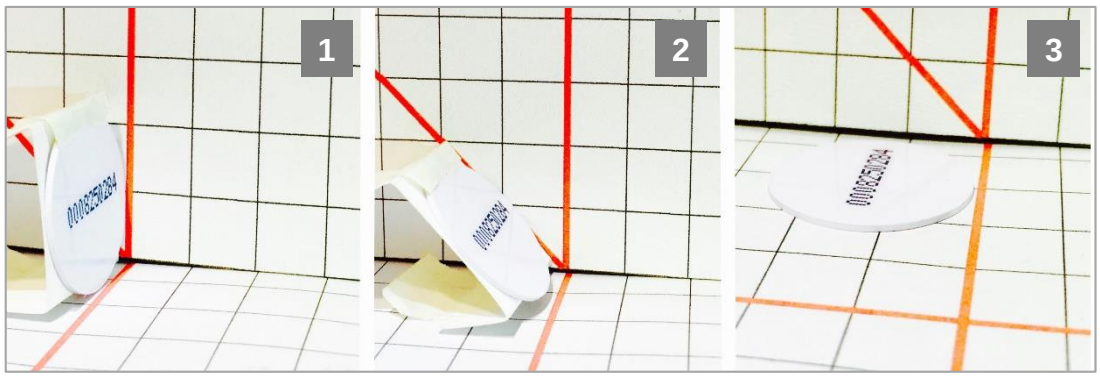
Fonte: Elaboração da própria autora.

Figura 29 - Posição da *tag* chaveiro nos testes.



Fonte: Elaboração da própria autora.

Figura 30 - Posição da *tag* moeda nos testes.



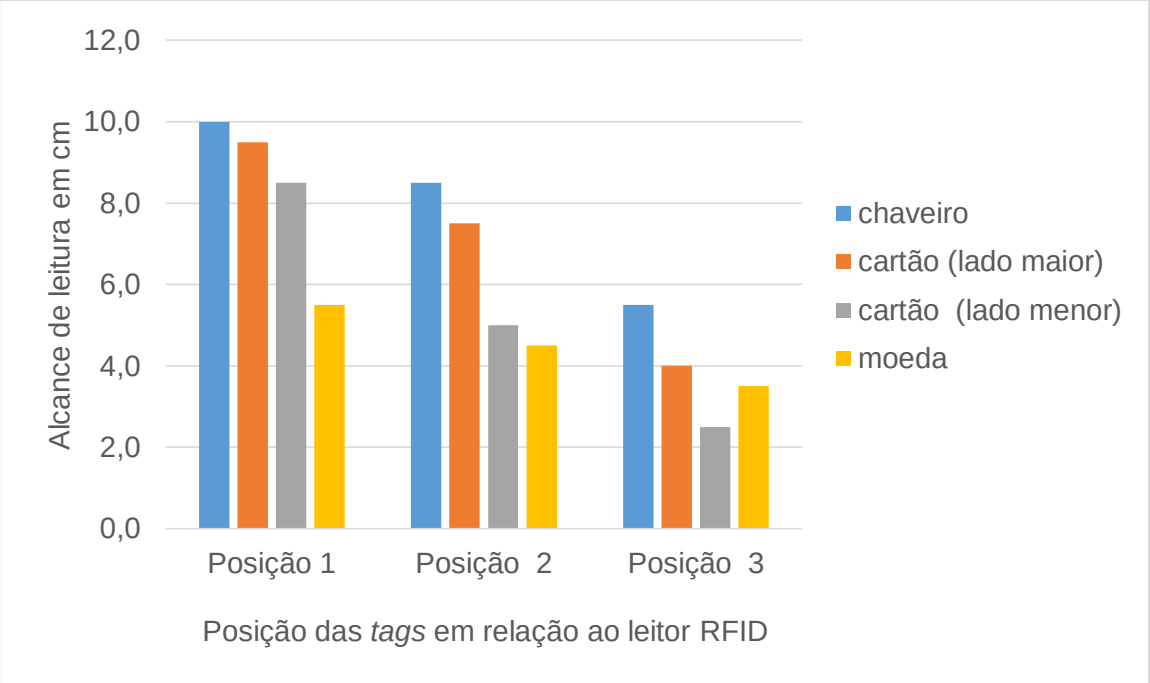
Fonte: Elaboração da própria autora.

4.2.1 Resultados

Durante os testes, foram realizadas dez leituras para cada posição das *tags*. Foram observados os valores máximos da distâncias de leitura obtidas em cada

posição. O Gráfico 1 apresenta um comparativo entre o alcance de leitura obtido para cada *tag* nas posições vertical, aproximadamente 45 graus e horizontal.

Gráfico 1 – Comparativo entre o alcance de leitura obtido em cada posição.



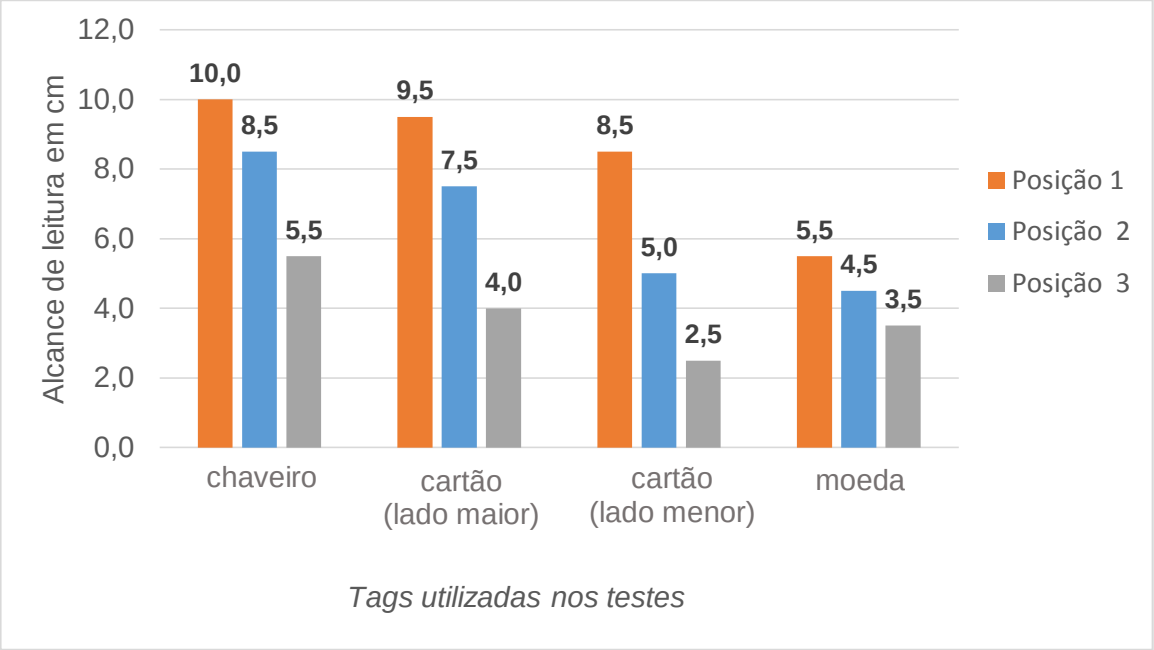
Fonte: Elaboração da própria autora.

Os resultados obtidos demonstram que o alcance de leitura diminui ao passo que se aumenta o ângulo de inclinação da *tag* em relação ao leitor, sendo o maior alcance, 10 cm, obtido pela *tag* chaveiro na posição1.

Agrupando-se os dados por *tags* (Gráfico 2), observa-se que os testes com as *tags* moeda e chaveiro resultaram em dados mais homogêneos, com um coeficiente de variação de 18% e 23% (Tabela 2), respectivamente.

Em relação a *tag* Cartão, observa-se ainda que esta diminui a distância de sua leitura quando com o lado menor voltado para base.

Gráfico 2 - Comparativo entre o alcance de leitura obtido com cada *tag.*



Fonte: Elaboração da própria autora.

Tabela 2 – Coeficientes de Variação do alcance de leitura.

Tags	**Coeficiente de Variação**
Chaveiro	23%
Cartão (lado maior)	32%
Cartão (lado menor)	46%
Moeda	18%

Fonte: Elaboração da própria autora.

4.3 ALCANCE DE CONEXÃO E TRANSMISSÃO DE DADOS DO MÓDULO BLUETOOTH

Para verificar a distância e a transmissão dos dados do módulo oIT, foram realizados testes utilizando o *smartphone*, marca Samsung, modelo GT-I9505 e o aplicativo BlueTerm.

Foram realizadas 5 conexões, e na sequência de cada uma, foram recebidos os dados até que houvesse a perda da conexão. As tentativas de conexão se iniciaram a aproximadamente 65 metros do módulo oIT, e a cada tentativa sem êxito, era realizada a aproximação do módulo oIT cerca de 1 metro, até que a conexão fosse realizada. Realizada a conexão, era afastado do módulo oIT cerca de

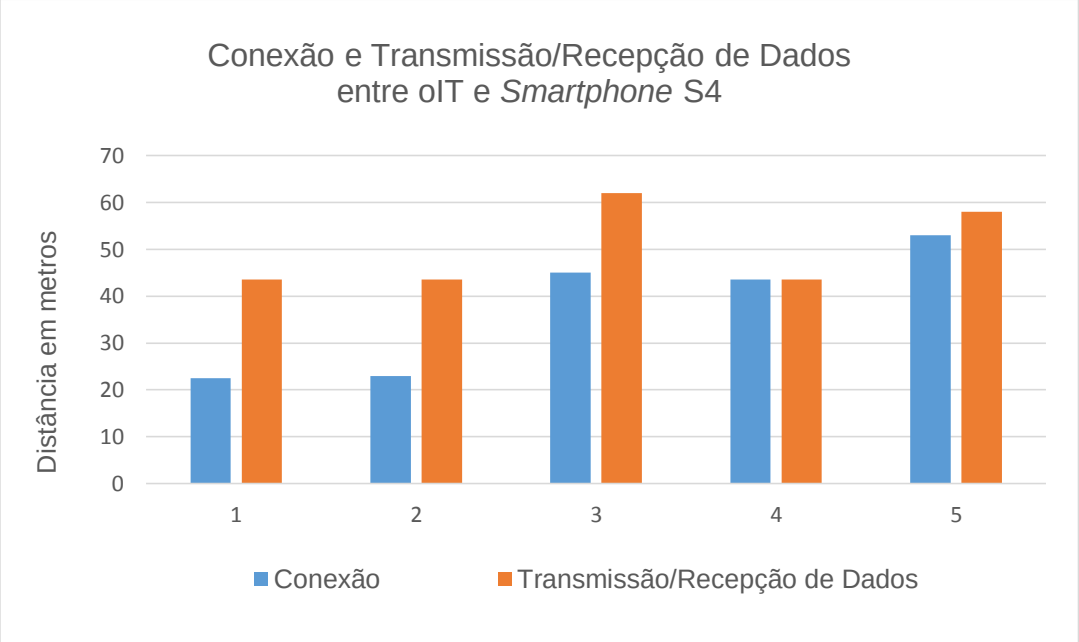
1 metro e uma tentativa de recebimento dos dados era realizada, repetindo este processo até que se perdesse a conexão.

4.3.1 Resultados

Nos testes realizados, foi possível efetuar a conexão entre o módulo oIT e o *smartphone* até uma distância de 53 metros, contudo, a primeira e segunda conexões somente foram realizadas a aproximadamente 23 metros de distância. Com relação a transmissão dos dados enviados pelo módulo oIT e sua recepção pelo *smartphone*, foi possível realizá-la a até 62 metros de distância, sendo que em 60% dos testes, somente foi possível a até 43 metros, aproximadamente.

No Gráfico 3 são apresentados os dados obtidos nos testes, e neste é possível observar que a transmissão/recepção dos dados podem ser realizadas a uma distância maior do que a necessária para a conexão.

Gráfico 3 - Comparativo de distâncias de conexão e transmissão/recepção.



Fonte: Elaboração da própria autora.

4.4 APLICAÇÕES

As características do módulo oIT, como tamanho, que possibilita sua fixação no punho de seus usuários, leitura e transmissão de dados sem fio, com a

identificação de objetos através de *tags* RFID e transmissão desta através da tecnologia Bluetooth, possibilita que este módulo seja utilizado em diversos tipos de aplicação. O tipo de aplicação é especificado no *software* desenvolvido para se conectar com o módulo oIT, e podem pertencer a diversas áreas, como segurança, educação, saúde, dentre outras. A seguir, são apresentados alguns exemplos de aplicações que podem ser dadas ao módulo oIT, nas área da segurança, educação e saúde:

- Segurança: o módulo oIT pode ser utilizado dentro das residências de deficientes visuais, auxiliando este a identificar produtos de limpeza, medicamentos, venenos, e outros que possam causar riscos à saúde deste. O módulo oIT também pode ser utilizado na segurança de idosos, fornecendo a identificação de objetos utilizados por este, bem como cômodos acessados na casa (fixação de *tags* próximas as maçanetas das portas), à um módulo que identifica a posição do idoso utilizando um acelerômetro. Auxiliando, desta forma, na identificações de ações, como: ler (idoso sentado + identificação do objeto livro), queda no banheiro (idoso caído + identificação da porta do banheiro) e outras. Identificada uma ação que possa causar riscos a integridade física do idoso, um alerta pode ser enviado a um familiar, através de um *software* desenvolvido para receber estes dados e efetuar a análise das rotinas diárias do idoso.
- Educação: o oIT pode ser utilizado para auxiliar deficientes visuais no aprendizado em aulas laboratoriais, através da identificação de laboratórios, bancadas, equipamentos e diferentes objetos, utilizando *tags* RFID fixadas a estes. Com a utilização de um *software* desenvolvido para *smartphones*, informações quanto a localização dos objetos, bem como suas características e demais informações de importância educacional, podem ser recebidas pelo aluno de modo sonoro.
- Saúde: a identificação de medicamentos através do módulo oIT pode auxiliar idosos no controle destes, com o auxílio de um *software* para *smartphone*, que alerte o idoso e seu cuidador, quanto aos horários de utilização dos medicamentos, manipulação de medicamentos do qual seja alérgico e outros alertas que auxiliem no uso correto dos medicamentos e contribuam, desta forma, para manutenção da saúde do idoso.

4.5 CONSIDERAÇÕES FINAIS DO CAPÍTULO 4

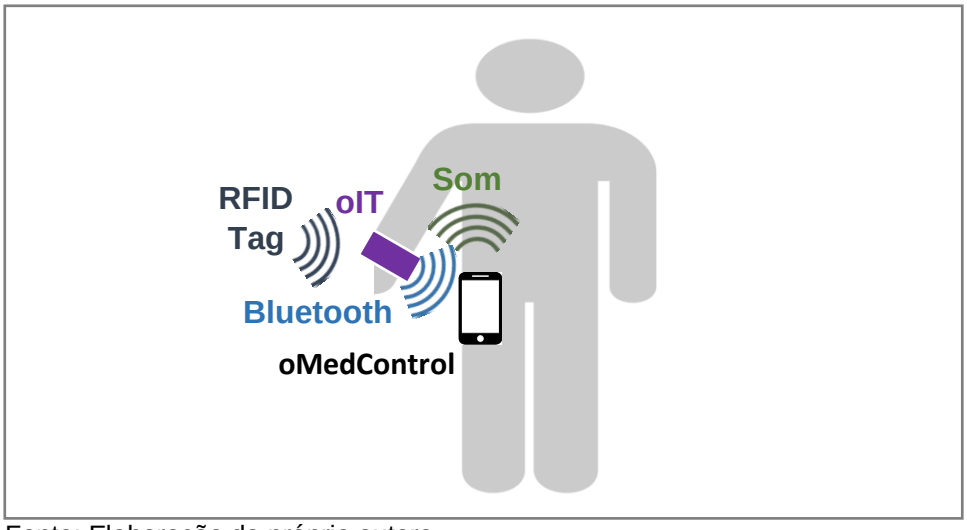
De forma a apresentar aplicações práticas do módulo oIT, foi devolvido neste trabalho, duas aplicações: oMedControl e oIS, destinadas a auxiliar idosos no controle de medicamentos e deficientes visuais nas aulas práticas laboratoriais, respectivamente.

5 OMEDCONTROL (*SOFTWARE*)

Segundo a Organização Mundial da Saúde - OMS (2015), a população idosa mundial (acima de 60 anos) vem aumentando, e a expectativa é que será duas vezes maior, de 900 milhões em 2015 para aproximadamente 2 bilhões em 2050. De acordo com Gomes e Caldas (2008), 70% dos idosos necessitam de tratamento farmacológico e uso regular de medicamentos. O aumento do uso de medicamentos, problemas de visão e memória na terceira idade, a falta de uma pessoa que esteja presente no dia a dia para auxiliar o paciente, podem levar o idoso a fazer um uso inadequado dos medicamentos. De forma a auxiliar o idoso e seu cuidador no controle de medicamentos, foi devolvido neste trabalho o aplicativo oMedControl.

O aplicativo oMedControl foi devolvido para *smartphones* Android e tem por objetivo efetuar o controle do uso de medicamentos do paciente (idoso), verificando e o alertando quanto aos horários de uso e alergia a substâncias presentes nos medicamentos manipulados por este. Outra função do aplicativo é emitir alertas ao cuidador do paciente, através de mensagens de texto enviadas ao celular deste. Sempre que não for identificado o uso do medicamento de uso contínuo no horário definido no cadastro, bem como houver a manipulação, pelo paciente, de medicamentos que não são de uso deste, e aqueles dos quais este é alérgico, o cuidador será avisado. Na Figura 31 é apresentado o funcionamento do sistema, com a comunicação entre *tag* RFID e o módulo oIT, e este com o aplicativo oMedControl, instalado no *smartphone*, que possibilita o envio de avisos sonoros ao paciente.

Figura 31 - Esquema de funcionamento do sistema oMedControl.



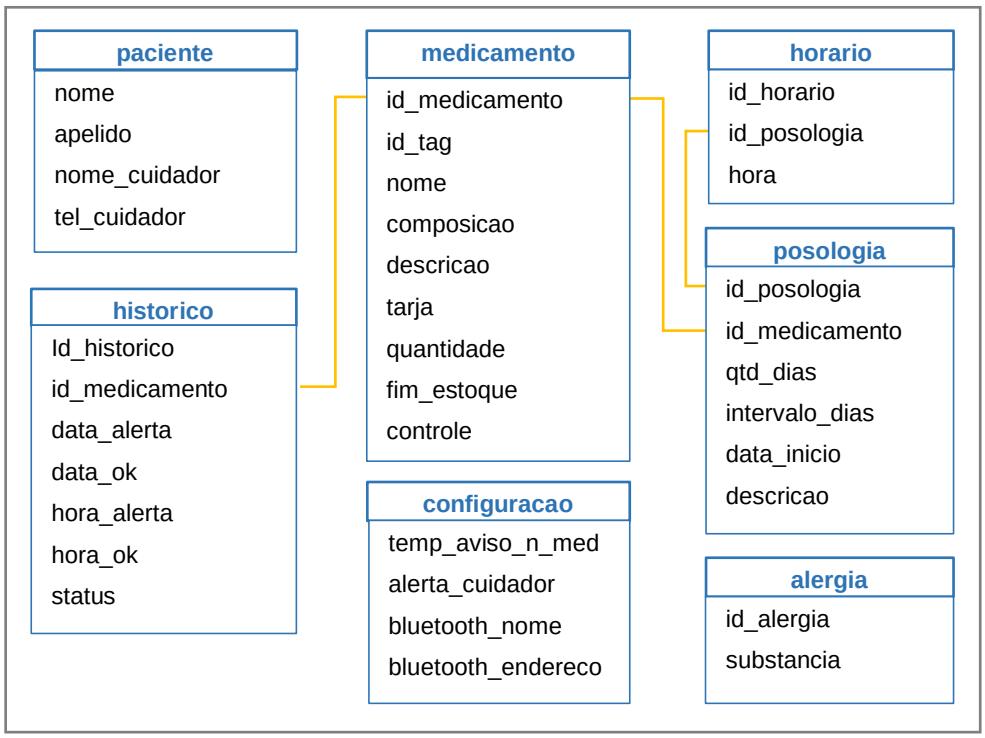
Fonte: Elaboração da própria autora.

5.1 FERRAMENTAS DESENVOLVIMENTO DO OMEDCONTROL

Para o desenvolvimento do aplicativo oMedControl, foi utilizada a linguagem de programação Java em conjunto com Kit de Desenvolvimento de *Software* (SDK) Android. Java é a linguagem padrão para o desenvolvimento de aplicativos para plataforma Android, e possui uma vasta referência bibliográfica que auxilia na utilização da linguagem e das Interfaces de Programação de Aplicativos (APIs - *Application Programming Interfaces*). A plataforma de desenvolvimento utilizada foi o Android Studio, desenvolvida pela empresa Google, e distribuído gratuitamente.

Os dados do aplicativo oMedControl são armazenados no próprio *smartphone* Android, utilizando o banco de dados SQLite, que possui suporte nativo no Android. Na Figura 32 é apresentada a estrutura do banco de dados, com suas tabelas e relacionamentos.

Figura 32 - Estrutura do banco de dados do oMedControl.



Fonte: Elaboração da própria autora.

5.2 PROCEDIMENTOS E RESULTADOS

A primeira interface apresentada na aplicação é a “Inicialização do Sistema”. Se o paciente não foi cadastrado é apresentado uma interface para que realize o mesmo de acordo com a Figura 33A. Caso contrário, será exibido o nome deste, da forma como deseja ser tratado no sistema (apelido), conforme apresentado na Figura 33B, e ao tocar no centro da tela, será apresentada a interface de controle “Medicamentos – Hoje”. Na parte inferior da interface (Figura 33C), pode ser acessado através do botão “Menu” do *smartphone*, as opções: “Usuário”, “Configurações” e “Histórico”. Na parte superior da interface (barra de título), localiza-se os botões de “Cadastro de Medicamentos”, “Cadastro de Alergias” e “Lista de Medicamentos”, apresentados nesta ordem.

Figura 33 – Interface de Inicialização do Sistema.

Fonte: Elaboração da própria autora.

No Cadastro de Usuário são registrados os dados do paciente e de seu cuidador. Em virtude da característica do *smartphone* ser de uso individual, o sistema permitirá apenas o registro de um usuário. Na Figura 34A é apresentada a interface para cadastro de usuário e na Figura 34B um castrado já efetuado. A

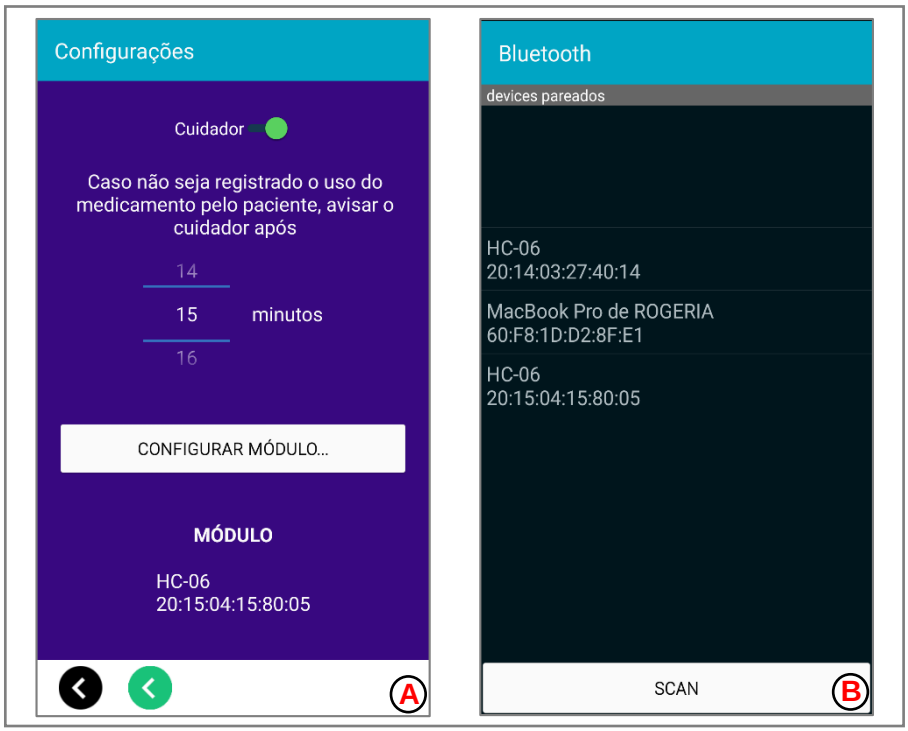
interface apresenta dois botões: o primeiro, permite voltar a interface anterior e, o segundo, salvar/alterar os dados do usuário no banco e retornar a interface anterior. Estes dois botões são padronizados nas demais interfaces do aplicativo.

Figura 34 – Interface de Cadastro de Usuário.

Fonte: Elaboração da própria autora.

Nas Configurações é possível definir se a opção para comunicar o cuidador, através de mensagem de texto, está ativa ou não. Caso ativa, é possível definir o número de minutos, após decorrido o horário do medicamento, para o envio da mensagem. Na Figura 35A é apresentada a interface de Configurações com o modo cuidador ativo e o módulo Bluetooth do oIT já configurado. O botão “Configurar Módulo” possibilita da seleção do módulo Bluetooth do oIT, conforme apresentado na Figura 35B.

Figura 35 – Interface de Configurações.



Fonte: Elaboração da própria autora.

No Cadastro de Medicamentos são registrados os dados dos medicamentos encontrados na residência do paciente. Na Figura 36A é apresentada a interface para cadastro do medicamento e na Figura 36B um castrado já efetuado.

A interface de Cadastro de Medicamentos apresenta 6 botões (Figura 36B): 5 na barra de menu inferior e 1 na barra de título. No botão da barra de título é definido pelo usuário se o medicamento é de uso ou não do paciente. Na barra de menu inferior, o terceiro botão acessa a interface de cadastro da *tag* do medicamento e o quarto botão permite o cadastro da posologia. Após o cadastro do medicamento, será apresentado o botão que permite a exclusão deste.

Os botões para cadastro da *tag* e da posologia apresentam-se, inicialmente, na cor vermelha, e após efetuados os cadastros, na cor verde.

O oMedControl possibilita o controle do estoque do medicamento e a emissão de alertas ao cuidador, através de mensagem de texto, informando quanto ao fim do estoque. O número de dias que antecede o fim do estoque pode ser configurado na opção “Alerta – Fim de Estoque”. A configuração deve ser realizada de acordo com o tempo necessário para repor cada medicamento (medicamentos que necessitam de receita médica para aquisição nas farmácias, podem necessitar de uma maior antecedência, do que aqueles adquiridos sem qualquer tipo de restrição).

Figura 36 – Interface de Cadastro de Medicamentos.

Fonte: Elaboração da própria autora.

Na Figura 37 é apresentada a interface de “Leitura da *Tag”* para cadastro desta. O oMedControl conecta-se ao oIT através da tecnologia Bluetooth e solicita ao usuário que aproxime o leitor da *tag* fixada no medicamento. Após a leitura, a aplicação retorna ao Cadastro de Medicamento.

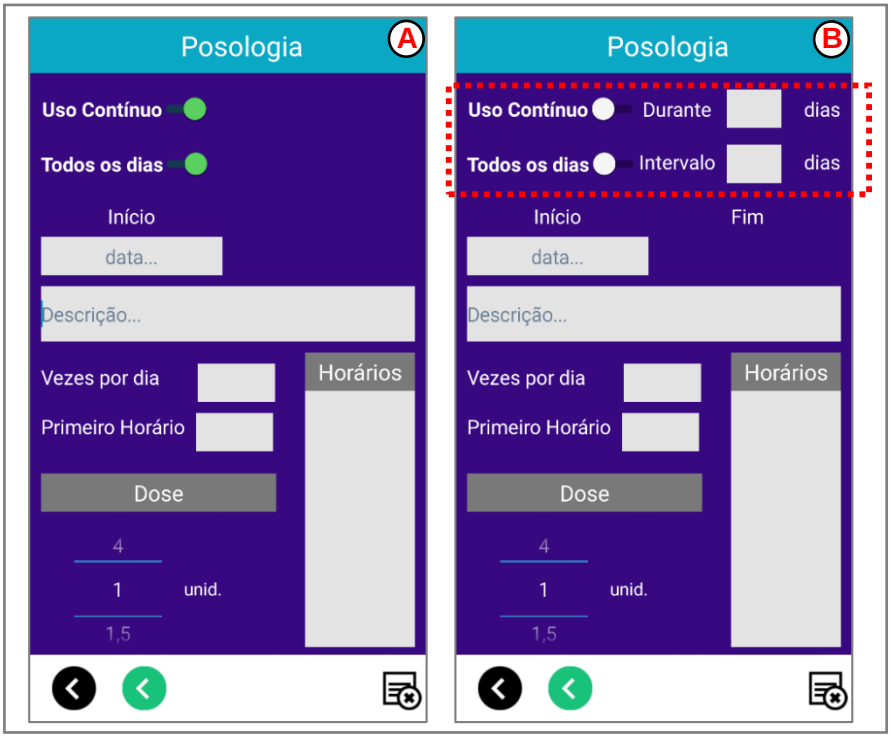
Figura 37 – Interface de Leitura da *Tag*.

Fonte: Elaboração da própria autora.

Na Figura 38 é apresentada a interface do Cadastro de Posologia. A interface possibilita ativar/desativar a opção de uso do medicamento: todos os dias e de modo contínuo (Figura 38A). Quando desativadas as opções, são exibidos os campos para definir o intervalo de dias para o uso do medicamento (alguns medicamentos são utilizados 1 vez na semana, ou outro intervalo de tempo), e para especificar o número de dias que o paciente fará uso da medicação (normalmente receitado pelo médico para um tratamento temporário) (Figura 38B).

Na barra de menu da interface de cadastro de posologia são apresentados 3 botões. Os dois primeiros de uso comum do aplicativo e o terceiro permite limpar o conteúdo de todos os campos da interface.

Figura 38 – Interface do Cadastro de Posologia.



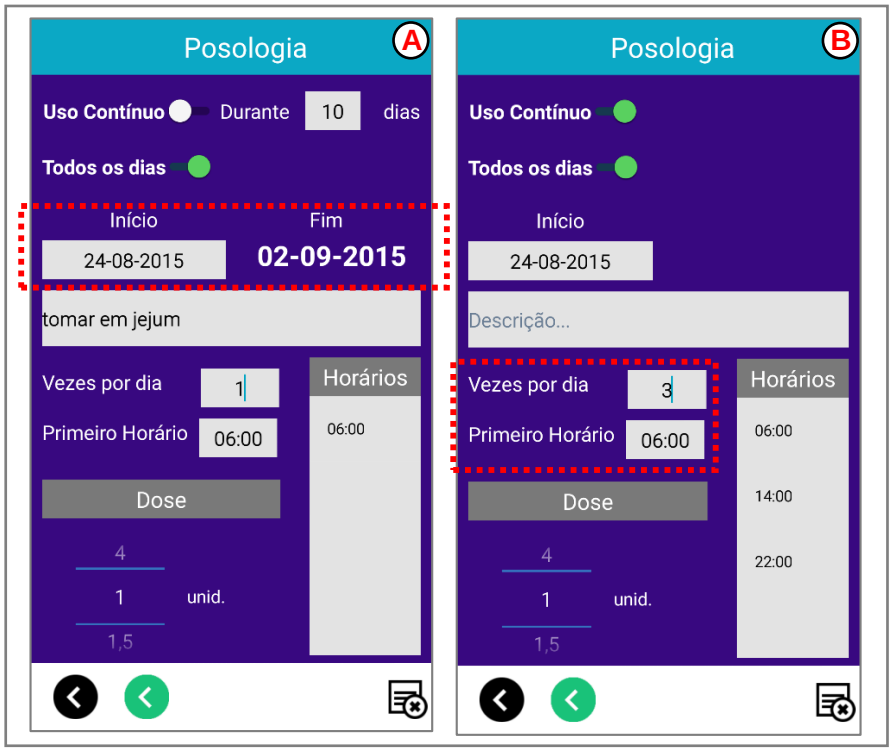
Fonte: Elaboração da própria autora.

Exemplos de cadastro de posologias são apresentados na Figura 39. Quando especificado o número de dias de uso do medicamento e a da de início, a data final de uso será preenchida automaticamente pelo sistema (Figura 39A). A interface de configuração da data de início é apresentada na Figura 40A.

Com relação aos horários para uso do medicamento, o usuário definirá o número de vezes que este será utilizado durante o dia e o primeiro horário (Figura 39B). Com base nestes dados, o aplicativo preencherá automaticamente os horários, mantendo intervalos de horas iguais entre estes. Caso o usuário deseje

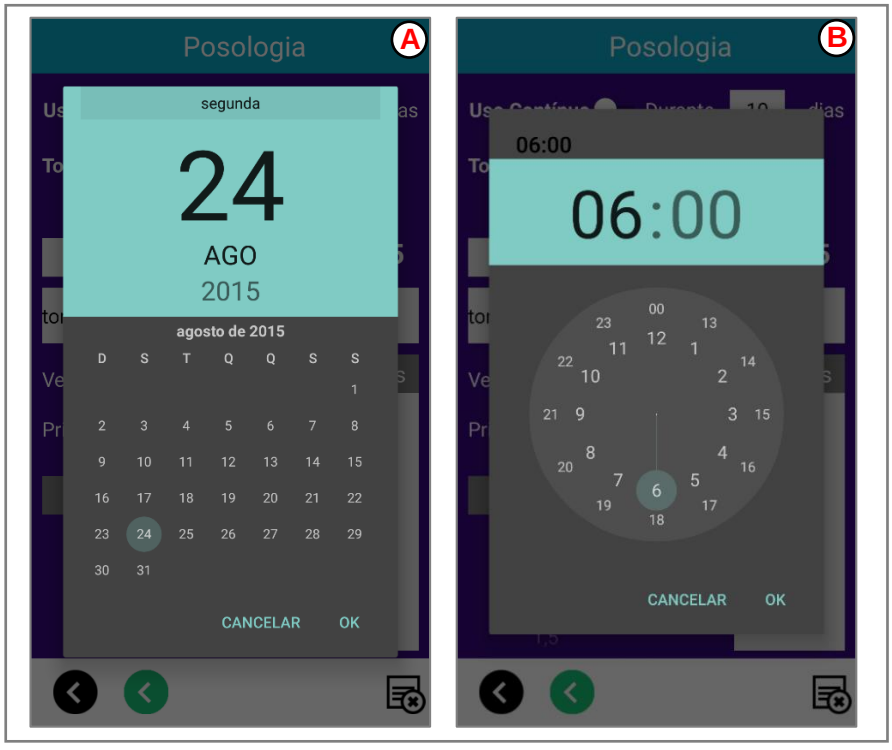
personalizar um ou mais horários, este deve tocar sobre o horário que deseja alterar e a interface para configuração do horário será apresentada, conforme exemplificado na Figura 40B.

Figura 39 – Exemplos de cadastro de posologias.



Fonte: Elaboração da própria autora.

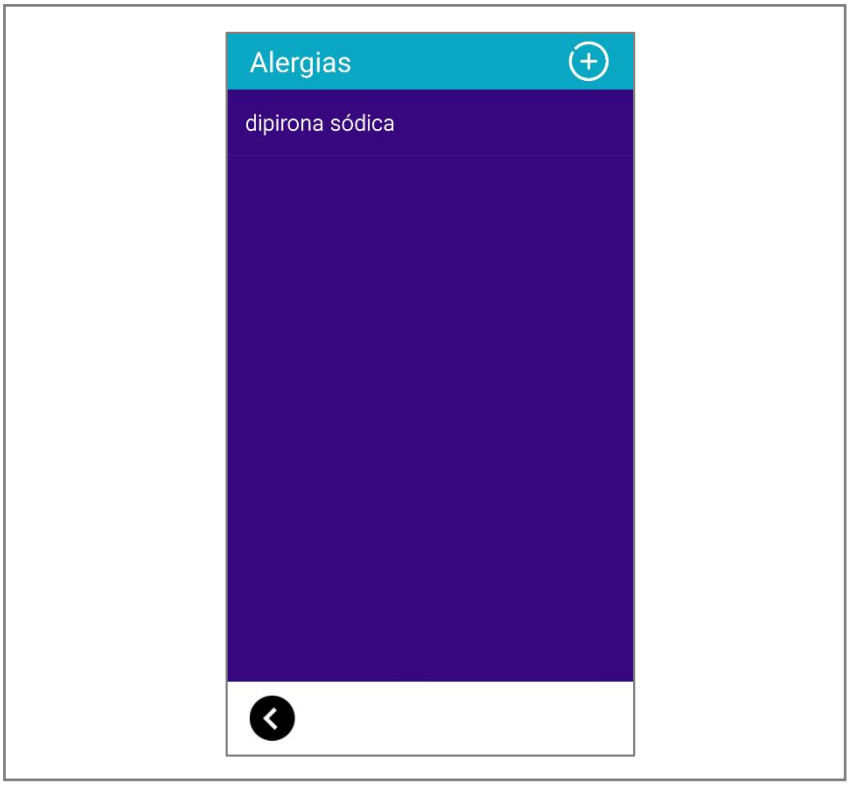
Figura 40 – Interfaces para configuração de data e hora.



Fonte: Elaboração da própria autora.

De forma a possibilitar que o paciente e o seu cuidador sejam alertados, quanto a manipulação de medicamentos, que possam possuir em sua fórmula substâncias das quais o paciente seja alérgico, o oMedControl possui uma interface para cadastro destas. Na Figura 41 é apresentada a interface com a lista das substâncias já cadastradas. Na barra de título desta, é localizado o botão para efetuar o cadastro de novas substâncias.

Figura 41 – Interface com a lista de substâncias alérgicas.



Fonte: Elaboração da própria autora.

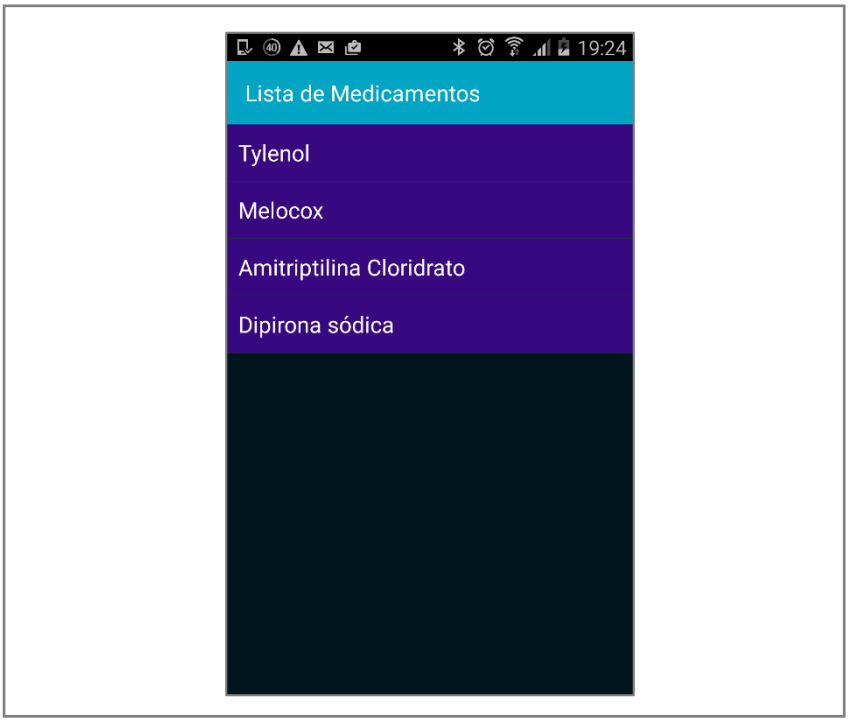
Na Figura 42A, é apresentada a interface para cadastrado de substâncias alérgicas. Para alterar ou excluir uma substância é necessário tocar sobre a mesma, na lista de substâncias (Figura 41). A interface para edição e exclusão será apresentada (Figura 42B).

Figura 42 – Interfaces para cadastro de substâncias

Fonte: Elaboração da própria autora.

A consulta aos medicamentos já cadastrados é realizada através da interface “Lista de Medicamentos”, conforme apresentada na Figura 43. Os dados são acessados tocando sobre o medicamento desejado.

Figura 43 – Interface da Lista de Medicamentos.

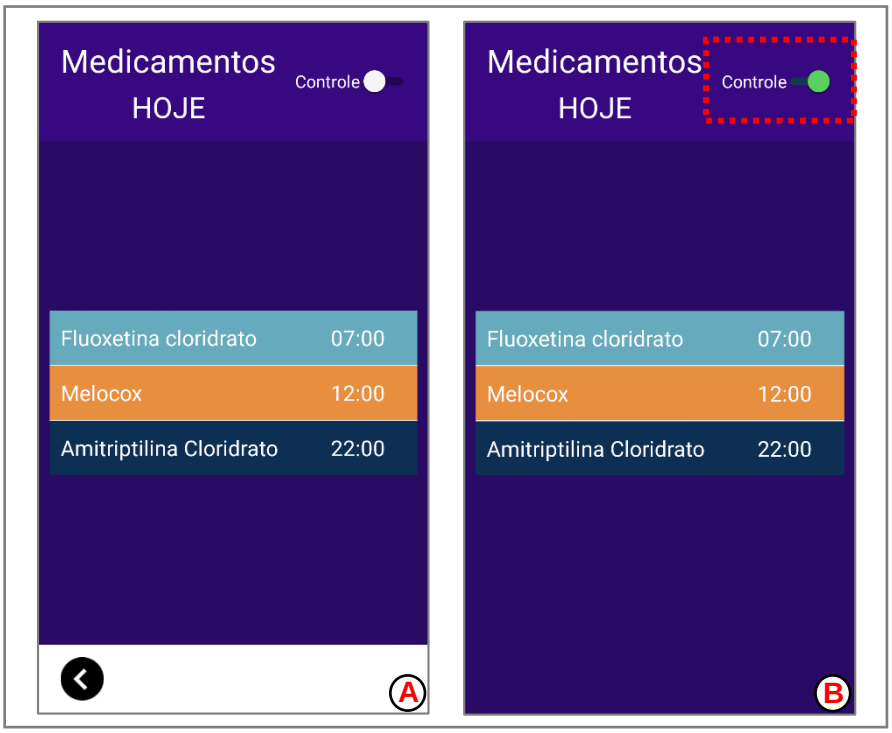


Fonte: Elaboração da própria autora.

Após efetuado o cadastro dos medicamentos, o controle destes é realizado através da interface “Medicamentos – Hoje”, apresentada na Figura 44A. Todos os medicamentos que devem ser utilizados no dia, a partir do horário que a interface foi acessada, serão listados e formatados de acordo com o horário que devem ser utilizados. Os horários da manhã, tarde e noite são formatados nas cores azul-claro, laranja e azul-escuro, respectivamente.

O controle dos medicamentos é realizado somente quando ativado o botão “Controle” (Figura 44B). Durante a execução do controle de medicamentos pelo oMedControl, a interface “Medicamentos – Hoje” deixa de exibir o botão “Voltar”. O acesso as demais interfaces do oMedControl, somente é realizado quando desativado o botão “Controle”.

Figura 44 – Interface Medicamento - Hoje.



Fonte: Elaboração da própria autora.

Durante a execução do controle dos medicamentos, a aplicação verifica a cada 1 minuto se há medicamentos a serem utilizados naquele horário. Caso haja, será emitido um alerta visual ao usuário, conforme apresentado na Figura 45A. Em paralelo, é disparado um alerta sonoro, no volume máximo do *smartphone*, para que chame a atenção do usuário, caso este não esteja ao lado do aparelho. Os alertas visual e sonoro cessam ao tocar sobre o botão “Fechar”, e a interface

“Medicamentos – Hoje” volta a ser exibida. Conforme apresentado na Figura 45B, os medicamentos que devem ser utilizados, passam a ser exibidos com fonte na cor vermelha e estilo negrito.

Figura 45 – Interface Hora do Medicamento.

Fonte: Elaboração da própria autora.

A informação quanto ao uso do medicamento pode ser recebida pela aplicação de duas formas: baixado pelo sistema ou pelo usuário.

Quando o botão “Controle” é ativado, a aplicação conecta automaticamente com o módulo oIT, e este passa a efetuar a leitura das *tags* fixadas aos medicamentos, no momento em que o módulo é aproximado destes. Se o medicamento, cuja *tag* foi lida, consta como não utilizado (fonte na cor vermelha), o sistema baixa o medicamento e o exclui da lista, conforme apresentado na Figura 46.

Caso o sistema não detecte a manipulação do medicamento, através da leitura da *tag* deste, o usuário pode baixá-lo tocando sobre este na lista de medicamentos, e confirmando seu uso, através da interface apresentada na Figura 47.

Figura 46 – Interface Medicamento - Hoje.

Fonte: Elaboração da própria autora.

Figura 47 – Interface de baixa de medicamento pelo usuário.

Fonte: Elaboração da própria autora.

A interface “Histórico”, apresentada na Figura 48, lista todos os medicamentos que foram controlados pelo sistema, incluindo a data do controle, a hora

determinada para o uso deste na posologia e a hora em que foi baixado, caso o tenha sido. O registro do histórico dos medicamentos têm suas fontes formatadas nas cores vermelho, amarelo e branco, que identificam o medicamento como: “sem tomar”, “baixado pelo usuário” e “baixado pelo sistema”, respectivamente.

Figura 48 – Interface Histórico.

Fonte: Elaboração da própria autora.

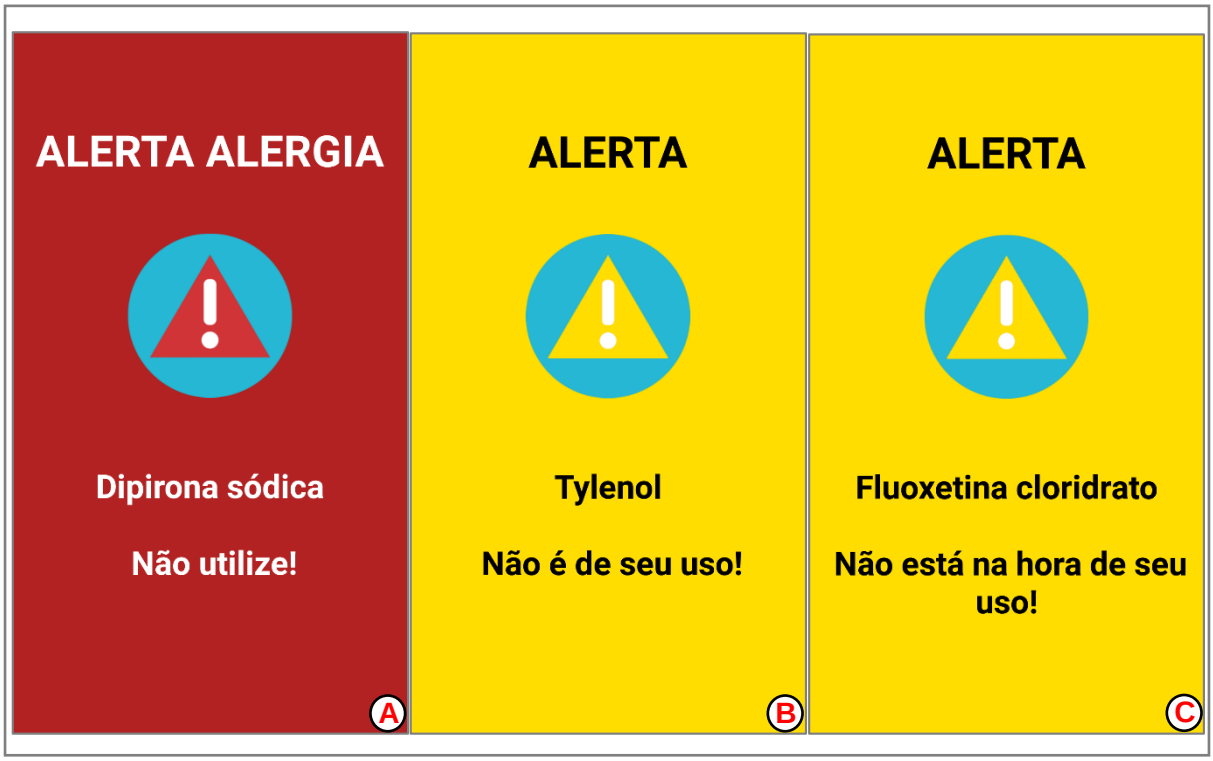
O histórico possibilita, ao cuidador do idoso, um maior controle quanto ao uso dos medicamentos, verificando o uso ou não destes, a demora no uso (através da hora da baixa) e se a baixa foi realizada pelo usuário, o que não confirma a manipulação do medicamento por este.

Outra forma de controle pode ser realizado através do estoque de medicamentos. Cada medicamento, baixado pelo sistema ou pelo usuário, é subtraído do estoque. O cuidador pode confrontar, periodicamente, o estoque registrado no sistema, com o físico. Um estoque físico maior que o registrado, sugere que o paciente não fez real uso do medicamento, nos horários devidos. Já um estoque físico menor, pode ser indício de que o paciente utilizou medicamentos a mais ou os tenha perdido, durante a manipulação destes.

Durante a leitura das *tags* fixadas nos medicamentos, além de verificar os medicamentos que devem ser utilizados naquele horário, a aplicação também consulta se estes possuem substâncias das quais o paciente seja alérgico, se o

medicamento não é de uso do paciente, e se, esse é de uso do paciente, mas não está no horário de seu uso. Identificada a manipulação indevida do medicamento, a aplicação emite um alerta visual ao usuário, conforme apresentado na Figura 49, e mensagem de voz, personalizada para cada tipo de alerta: “Alerta! Alergia ao medicamento!” (Figura 49A), “Alerta! Medicamento não é de seu uso!” (Figura 49B), “Alerta! Não está na hora do medicamento” (Figura 49C). Uma mensagem de voz com o apelido do paciente, antecede cada mensagem de alerta, de forma a chamar a atenção do paciente para o alerta que está por vir.

Figura 49 – Interface de Inicialização do Sistema.



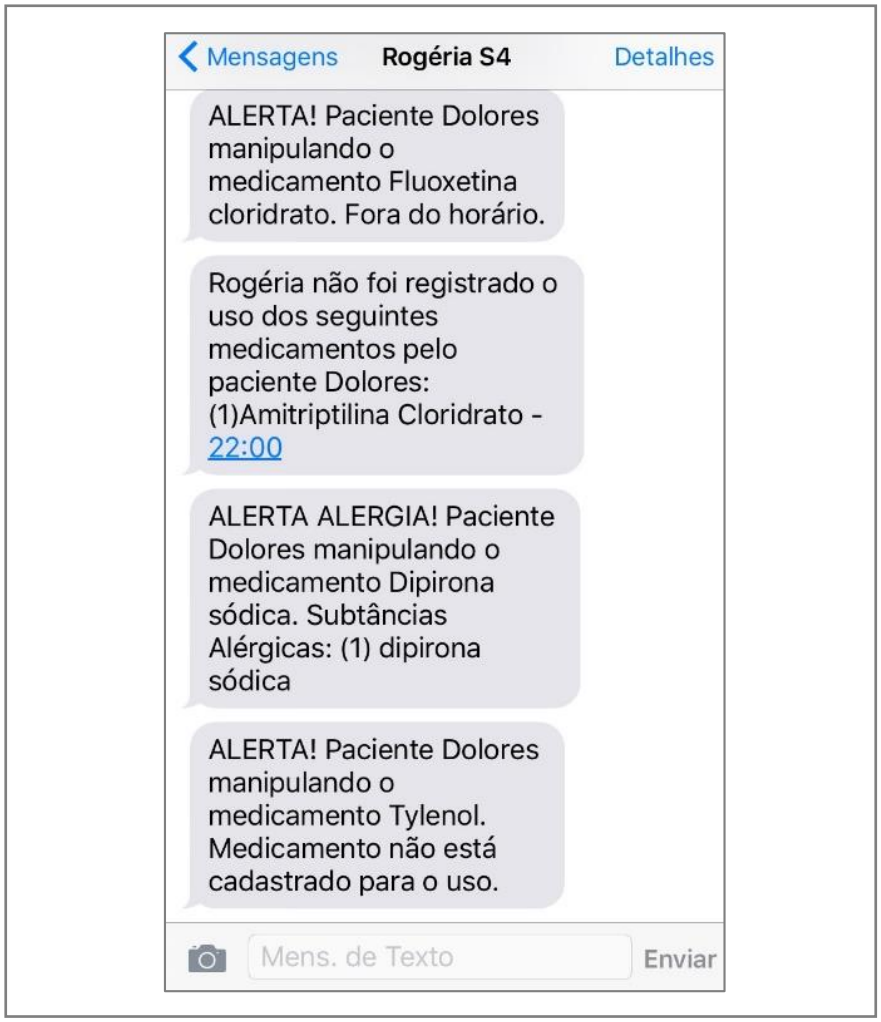
Fonte: Elaboração da própria autora.

Paralelo ao alerta emitido ao paciente, uma mensagem de texto é enviada ao celular do cuidador, alertando-o quanto a manipulação indevida de medicamentos, por parte do paciente, conforme exemplos de mensagens apresentadas na Figura 50. O envio de mensagens ao cuidador, possibilita que este tome as providências, que julgar necessária, para cada tipo de alerta, no momento que o a manipulação ocorre (o tempo de recebimento das mensagens enviadas ao cuidador, dependerá do serviço de telefônica móvel utilizado por este e pelo paciente).

O atraso no uso dos medicamentos também é informada ao cuidador, de acordo com o tempo estipulado na interface “Configurações”.

.

Figura 50 – Exemplos de mensagens enviadas ao cuidador.



Fonte: Elaboração da própria autora.

5.3 CONSIDERAÇÕES FINAIS DO CAPÍTULO 5

As características da aplicação oMedControl como: alertas visuais, sonoros e por mensagem de texto enviada ao celular do cuidador, propicia uma maior segurança ao idoso no uso de seus medicamentos, diminuindo o risco da utilização inadequado destes.

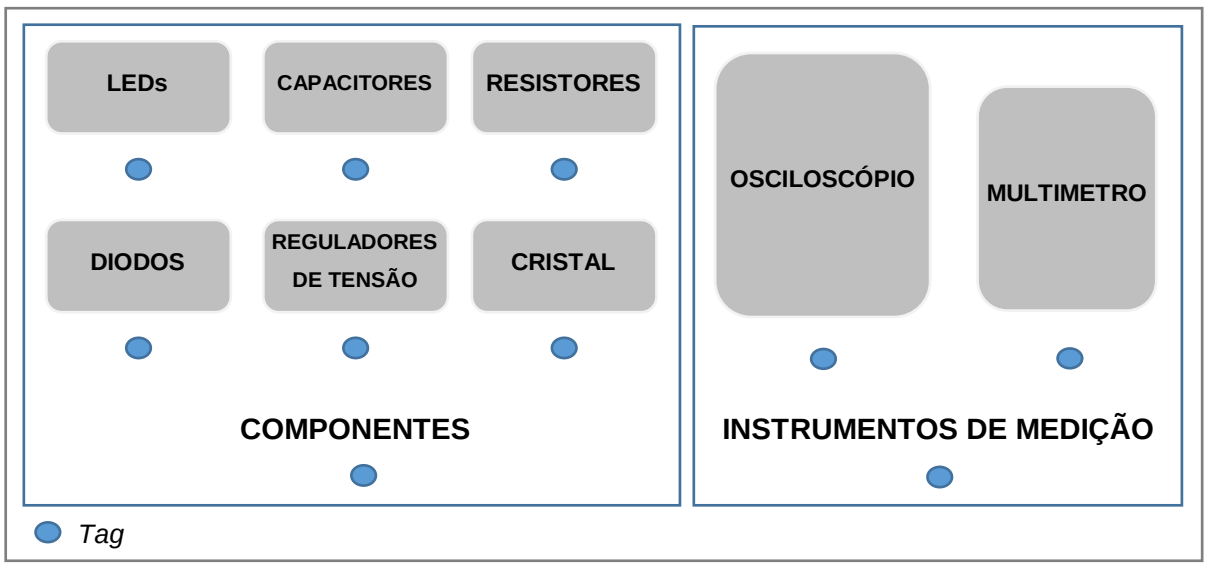
Após o desenvolvimento da aplicação oMedControl, uma nova aplicação foi desenvolvida para o módulo oIT, denominada oIS.

6 OIS (*SOFTWARE*)

Segundo a Organização Mundial da Saúde - OMS (2014), há no mundo, aproximadamente, 285 milhões de pessoas com deficiência visual: 39 milhões são cegas e 246 têm baixa visão. Dentre as diversas dificuldades enfrentas por estas milhões de pessoas, em virtude da limitação visual, encontra-se o acesso à educação. De forma a auxiliar o deficiente visual no acesso a informações de cunho educacional, foi desenvolvido neste trabalho o aplicativo oIS.

O aplicativo oIS foi devolvido para *smartphones* Android, e este tem por objetivo facilitar o acesso de alunos com deficiência visual, a informações de objetos que estes tenham acesso, em laboratórios, salas de aula, e outros. Os objetos devem estar dispostos de modo matricial, em locais como: mesas e bancadas. As informações referentes a estes, são cadastradas pelo professor no banco de dados, desta forma, é possível aplicar a ferramenta em diferentes tipos de laboratórios ou salas de aula. Na Figura 51 é apresentado um exemplo de disposição de objetos em um laboratório de eletrônica. As *tags RFID* são utilizadas para identificar os objetos e grupo de objetos, de forma a facilitar a localização desses, visto que cada objeto do grupo, como no caso do grupo “componentes”, os capacitores, têm a sua posição definida por linha e coluna: linha 2, coluna 2.

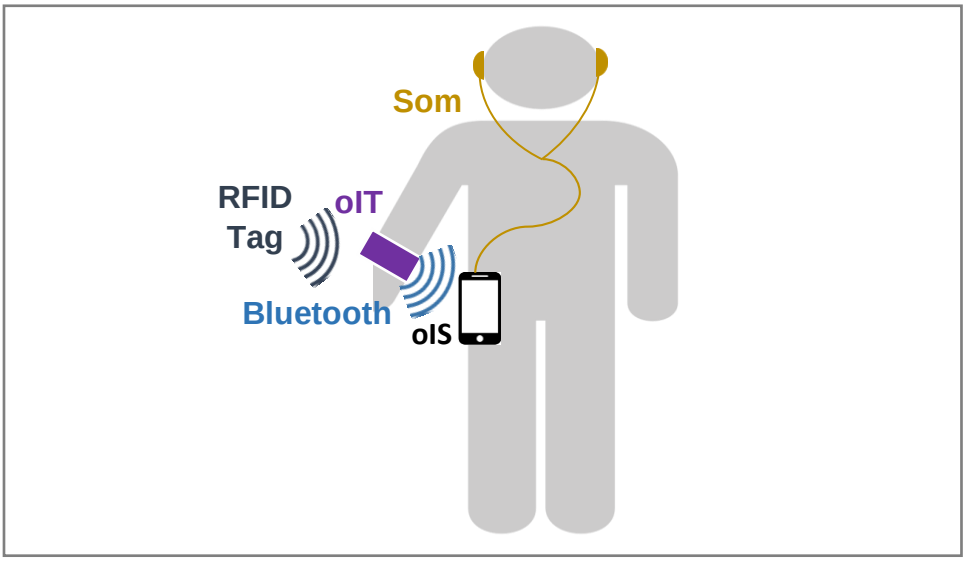
Figura 51 - Esquema de funcionamento do sistema oMedControl.



Fonte: Elaboração da própria autora.

Na Figura 52 é apresentado o funcionamento do sistema, com a comunicação entre *tag* RFID e o módulo oIT, e este com o aplicativo oIS, instalado no *smartphone*, que possibilita o envio das informações referente ao objeto ou grupo identificado, de modo sonoro ao aluno.

Figura 52 - Esquema de funcionamento do sistema oIS.



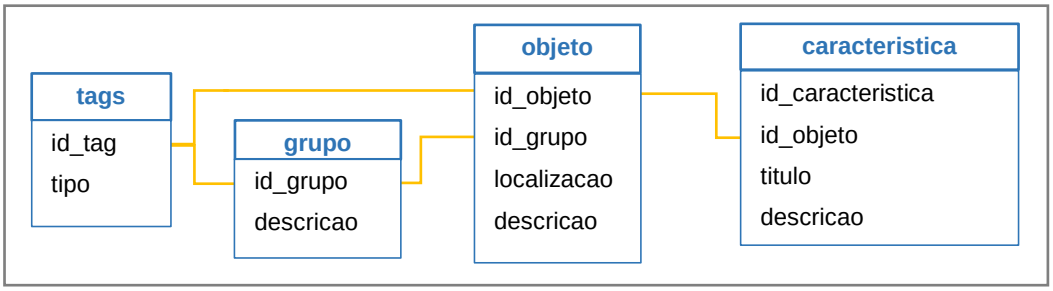
Fonte: Elaboração da própria autora.

6.1 FERRAMENTAS DESENVOLVIMENTO DO OIS

No desenvolvimento do aplicativo oIS, foi utilizada a linguagem de programação Java em conjunto com Kit de Desenvolvimento de *Software* (SDK) Android. A plataforma de desenvolvimento utilizada foi o Android Studio.

Para manipular e permitir o acesso aos dados do aplicativo oIS, foi utilizado o *software* WampServer, instalado em um computador com sistema Operacional Windows 8.1. O WampServer é distribuído gratuitamente, e agrega em seu pacote o Apache, o MySQL e o PHP. Os dados do oIS são recibos/enviados para o banco de dados MySQL, utilizando arquivos escritos com a linguagem PHP, que são acessados utilizando o servidor web Apache. Os dados recebidos pelo oIS devem vir em um formato de dados passível de ser interpretado por este, sendo assim, necessário realizar o intercâmbio das informações. Para tanto, foi utilizado o formato de dados JSON (*JavaScript Object Notation*), que é uma estrutura de dados simples e compacta, quando comparado ao XML (*eXtensible Markup Language*). Na Figura 53 é apresentada a estrutura do banco de dados, com suas tabelas e relacionamentos.

Figura 53 - Estrutura do banco de dados do oIS.

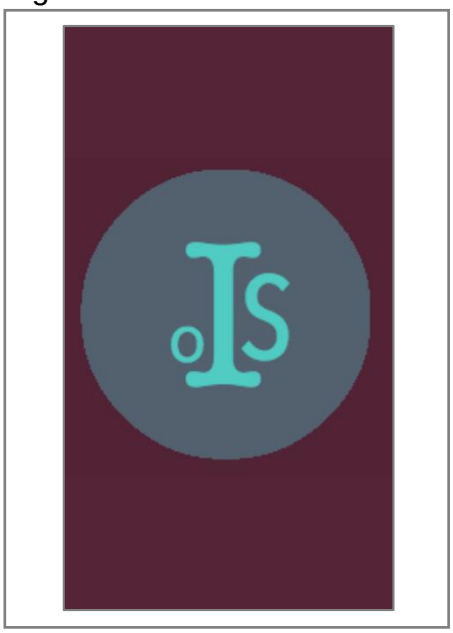


Fonte: Elaboração da própria autora.

6.2 PROCEDIMENTOS E RESULTADOS

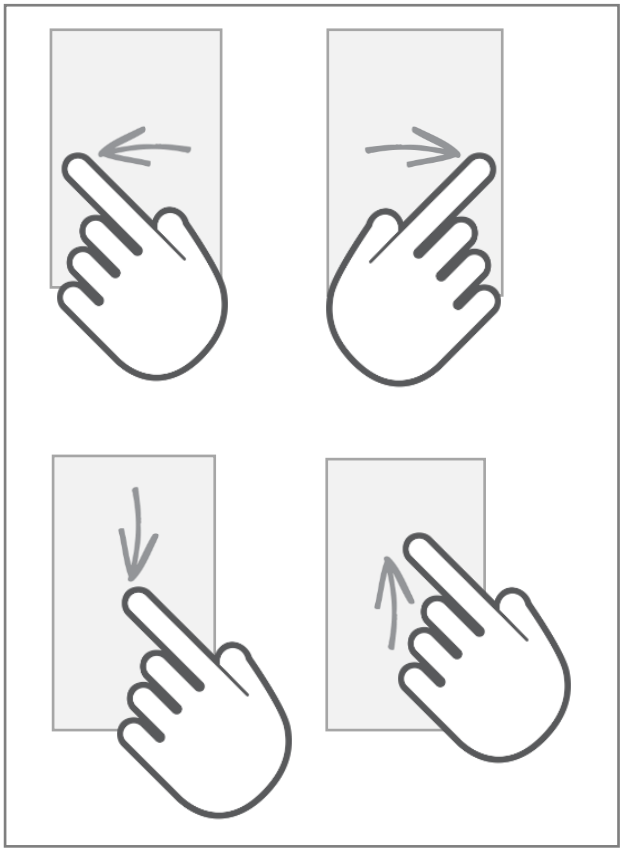
Na Figura 54 é apresentada a interface “Inicial” da aplicação oIS, que demonstra apenas o logotipo da aplicação. Em virtude da deficiência visual do usuário, as interfaces não possuem botões e a navegação é realizada por gestos, arrastando o dedo para a esquerda, para a direita, para cima e para baixo, conforme apresentado na Figura 55. O *smartphone* vibra, a cada gesto realizado pelo usuário, durante a navegação, e todas as informações direcionadas a este, são realizadas por voz. Quando a aplicação é iniciada, esta conecta-se, automaticamente, ao módulo oIT e informa o usuário, através da mensagem: “oIS iniciado!”. Na interface “Inicial”, não há navegações a serem realizadas, pois a aplicação aguarda a leitura de uma *tag*. Após efetuar a leitura de uma *tag*, a aplicação irá verificar se esta identifica um objeto ou um grupo de objetos.

Figura 54 – Interface Inicial.



Fonte: Elaboração da própria autora.

Figura 55 – Gesto de navegação.



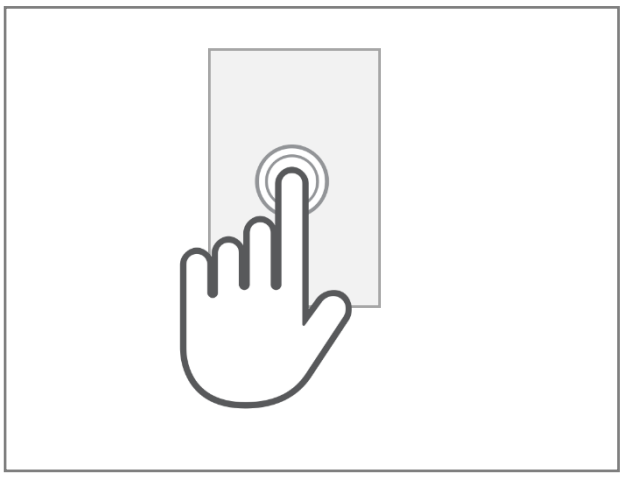
Fonte: Elaboração da própria autora.

No caso de ser identificada uma *tag* de grupo de objetos, conforme apresentado na Figura 56A, a aplicação informará ao usuário o nome do grupo, e este terá acesso a lista de objetos pertencentes àquele grupo e a localização destes, através do gesto: arrastar para a direita. Na Figura 56B é apresentada a interface “Lista de Objetos”, nesta, é possível navegar para cima e para baixo, e o usuário será informado de cada item da lista, durante a navegação. Identificado o final ou início da lista, o usuário é informado: “fim”, “início”. Todas as informações referente às *tags* consultadas, podem ser repetidas, através do gesto, toque longo (Figura 57). Durante a navegação, a aplicação orienta o usuário, direcionando-o a opções possíveis, como quando o usuário efetua o gesto, arrastar para a esquerda, na interface “Grupo de Objetos”. Neste caso, o usuário é orientado através da mensagem: “Deslize para a direita para consultar os objetos deste grupo”.

Figura 56 – Interface Grupo e Lista de Objetos.

Fonte: Elaboração da própria autora.

Figura 57 – Gesto - Toque Longo.

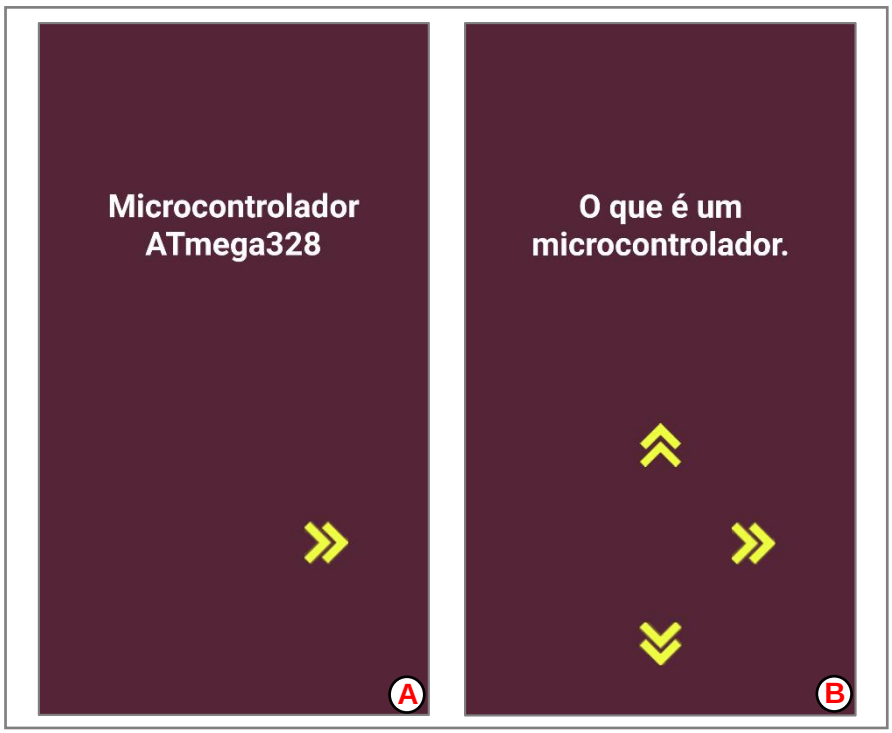


Fonte: Elaboração da própria autora.

Identificada uma *tag* de objeto, o usuário é informado quanto ao nome do objeto e sua localização. Através da navegação para a direita, o usuário terá acesso a lista de características daquele objeto, e navegando, novamente, a direita, é informado quanto a descrição da característica selecionada. Para alternar entre a características cadastradas, é utilizada a navegação para cima e para baixo. Na

Figura 58A é apresentada a interface “Objeto” e na Figura 58B, a “Lista de Características”.

Figura 58 – Interface Objeto e Lista de Características.



Fonte: Elaboração da própria autora.

6.3 CONSIDERAÇÕES FINAIS DO CAPÍTULO 6

A aplicação oIS foi desenvolvida como uma ferramenta para auxiliar deficientes visuais, contudo, suas interfaces possibilitam também que esta seja utilizada por alunos sem deficiência visual, sendo uma alternativa a ser utilizada nas aulas práticas laboratoriais na obtenção de informações relacionadas aos objetos identificados por esta.

Na Figura 59 é apresentado a interface do Android com os ícones das aplicações oMedControl e oIS instaladas. No *smartphone* Samsung S4 (utilizado nos testes), o aplicativo S Voice, disponibilizado pela Samsung, possibilita que o usuário deficiente visual abra a aplicação oIS, utilizando comando voz. O S Voice pode ser acessado apertando duas vezes o botão de início do aparelho.

A voz e velocidade da fala, utilizada para informar o usuário na aplicação oIS, pode ser alterada nas configurações do *smartphone*, na opção: Acessibilidade\Visão\Opções de texto para fala.

Figura 59 – Interface do Android.

Fonte: Elaboração da própria autora.

7 CONCLUSÃO

As Tecnologias RFID e Bluetooth vêm se desenvolvendo ao longo dos anos, e a diversidade de aplicações que são implementadas utilizando estas tecnologias têm aumentado em todo o mundo. A evolução destas tecnologias, a minimização do tamanho dos componentes, como o E-Thread, ampliam as possibilidades de aplicação, e junto com as padronizações, auxiliam na diminuição do custo das *tags* e leitores RFID, bem como dos módulos Bluetooth. As aplicações destas tecnologias, neste trabalho, resultou no módulo oIT.

A escolha dos *hardwares* utilizados no módulo oIT, levou em consideração fatores como: alcance de leitura (leitor RFID) e transmissão/recepção de dados (módulo Bluetooth), e que estes resultassem em um protótipo que possibilitasse a utilização deste circuito em um equipamento de pequeno porte, passível de ser utilizado no punho de seus usuários, para a identificação de objetos que estes venham a utilizar no dia a dia.

Desta forma, a distância de leitura efetuada pelo RFID tornou-se um fator importante que motivou a realização de testes com *tags* de diferentes tipos (cartão, chaveiro e moeda), e em diferentes posições. Os testes demonstraram que os tipos de *tags e* a posição destas em relação ao leitor, afetam de maneira expressiva o alcance de leitura. Dentre as *tags* testadas, as que apresentaram dados mais homogêneos foram as encapsuladas em moeda e chaveiro, com um coeficiente de variação de 18% e 23%, respectivamente.

Os testes relacionados à tecnologia Bluetooth, demonstraram que é necessário uma maior proximidade para se efetuar a conexão entre o módulo oIT e sua aplicação, em comparação à distância necessária para a transmissão/recepção de dados, que foi possível realizar a até uma distância de 43 metros, em 60% dos testes.

As características do módulo oIT, como tamanho, que possibilita sua fixação no punho de seus usuários, identificação de objetos, através de *tags* RFID fixadas nestes, bem como a transmissão de dados sem fio, permitem que sejam dadas ao módulo oIT diversos tipos de aplicações. Estas aplicações podem ser em diversas áreas, como educação, segurança e saúde, auxiliando pessoas como deficientes visuais e idosos. A utilização da tecnologia Bluetooth, que é encontrada em diversos tipos de equipamentos, como *smartphones*, *notebooks*, televisores, dentre outros,

amplia as possibilidades de aplicação, pois possibilita que o módulo oIT se comunique com uma diversidade de equipamentos.

Neste trabalho, foram desenvolvidas duas aplicações para *smartphone*s Android, uma na área da saúde, oMedControl, e outra na área da educação, oIS.

A aplicação oMedControl objetiva auxiliar idosos, bem como seus cuidadores, no controle dos medicamentos daqueles. Características como controle dos horários dos medicamentos, alertas emitidos por voz ao paciente e, através de SMS, ao cuidador, têm como propósito zelar pela saúde do paciente idoso e, permitir que o cuidador, mesmo à distância, auxilie para esta manutenção. Com relação as *tags* utilizadas na identificação dos medicamentos, optou-se pelo uso das encapsuladas em chaveiro, pois apresentaram nos testes, leituras com maior alcance, até 10 cm, e um coeficiente de variação pequeno, nas diferentes posições de leitura.

A aplicação oIS foi desenvolvida com características como: controle por gestos e informação por voz, de forma a auxiliar deficientes visuais na identificação de objetos utilizados em sala de aula e laboratórios, e na obtenção de informações de cunho educacional, referente a estes. A utilização de um servidor para armazenar o banco de dados, ao invés de armazenar as informações no próprio *smartphone*, traz flexibilidade aos professores para cadastrar e alterar as informações que julgarem necessárias, referentes aos objetos, e compartilha-las a todos que tiverem a aplicação instalada em seus *smartphone*s. Apesar da aplicação objetivar auxiliar deficientes visuais, esta pode ser utilizada, por aqueles que não o sejam, como uma ferramenta auxiliar nos estudos. Para a identificação dos objetos e grupos de objetos, optou pelas *tags* encapsuladas em moeda, visto que estas devem permanecer fixadas nas mesas e bancadas, próximas aos objetos, com um curto alcance de leitura, de forma a facilitar a localização dos objetos pelo aluno deficiente visual.

Como trabalhos futuros, pode-se apontar:

- Transferir o protótipo da *protoboard* para uma placa de circuito impresso, e acondicioná-la de forma a permitir sua fixação do punho de seus usuários.
- Realização de testes com usuários idosos (oMedControl) e deficientes visuais (oIS).
- Desenvolvimento de um interface Web para efetuar o cadastro dos dados relacionados ao aplicativo oIS.

REFERÊNCIAS

AL KALBANI, J.; SUWAILAM, R. B.; AL YAFAI, A.; AL ABRI, D.; AWADALLA, M. Bus detection system for blind people using RFID. In: IEEE GCC CONFERENCE AND EXHIBITION (GCCCE), 8., 2015, Muscat. **Proceedings...** Muscat: IEEE, 2015. p. 1-6.

AL-RAJHI, N.; AL-ABDULKARIM, A.; AL-KHALIFA, H. S.; AL-OTAIBI, H. M. Making Linear Equations Acessible for Visually Impaired Students Using 3D Printing. In: IEEE INTERNACIONAL CONFERENCE ON ADVANCED LEARNING TECHNOLOGIES (ICALT), 15., 2015, Hualien. **Proceedings...** Hualien: IEEE, 2015. p.432-433.

ATMEL CORPORATION. **Atmel 8-bit microcontroller with4/8/16/32KBytes In-system programmable flash - DATASHEET**. [S.l.], 2013.

ATMEL CORPORATION. **Atmel completes newport media acquisition - acquisition expands atmel's wireless portfolio to include Wi-Fi 802.11n and bluetooth. Atmel.** [S. l.], 2014. Disponivel em: <http://ir.atmel.com/releasedetail.cfm?ReleaseID=863564>. Acesso em: 23 ago. 2014.

AZCUETA, J.P.V.; LIBATIQUE, N.C; TANGONAN, G.L. In situ sports performance analysis system using inertial measurement units, high-FPS video camera, and the Android platform. In: INTERNATIONAL CONFERENCE ON HUMANOID, NANOTECHNOLOGY, INFORMATION TECHNOLOGY, COMMUNICATION AND CONTROL, ENVIRONMENT AND MANAGEMENT (HNICEM), 2014, Palawan. **Proceedings...** Palawan: IEEE, 2014. p. 1-6. ISBN 978-1-4799-4021-9.

BLUETOOTH SIG. **A look at the basics of bluetooth technology.** [S. l.], 2014. Disponivel em: <https://www.bluetooth.com/pages/basics.aspx />. Acesso em: 14 ago. 2014.

BRASIL. Conselho Nacional de Trânsito. **Resolução N° 537, de 17 de junho de 2015.** Dispõe sobre a implantação do Sistema Nacional de Identificação Automática de Veículos - SINIAV em todo território nacional. Brasília, DF, 2015. Disponível em: <http://www.denatran.gov.br/download/resolucoes/resolucao5372015.pdf>. Acesso em: 25 jan. 2016.

BRASIL. Departamento Nacional de Trânsito. **Portaria N° 570, de 27 de junho de 2011.** Estabelece regras e define os requisitos mínimos para a certificação e homologação de produtos do Sistema Nacional de Identificação Automática de Veículos - SINIAV. Brasília, DF, 2011. Disponível em: <http://www.denatran.gov.br/download/portarias/2011/portaria_denatran_570_11.pdf >. Acesso em: 25 jan. 2016.

CACHE, J.; WRIGHT, J.; LIU, V. **Hacking exposed wireless:** Wireless Security Secrets & Solutions. 2. ed. New York: McGraw-Hill, 2010.

CETWIN SERVICE. RFID-taggar. **Cetwin service**. [S. l.], 2013. Disponível em: <http://www.cetwinservice.se/products/rfid-tags.aspx>. Acesso em: 22 maio 2014.

CHAOUCHI, H.; LAURENT-MAKNAVICIUS, M. **Wireless and mobile network security**. Hoboken-London: Wiley-ISTE, 2009.

CHIA, S.; ZALZALA, A.; ZALZALA, L.; KARIMI, A. RFID and Mobile Communications for Rural e-Health: A Community Healthcare System Infrastructure Using RFID for Individual Identity. In: IEEE GLOBAL HUMANITARIAN TECHNOLOGY CONFERENCE, 2011. **Proceedings...** Seattle: IEEE, 2011. p. 371 - 376. ISBN 978-0-7695-4595-0.

CHOMCHALERM, G.; RATTANAKAJORNSAK, J.; SAMSRISOOK, U.; WONGSAWANG, D.; KUSAKUNNIRAN, W. Braille dict: Dictionary application for the blind on android smartphone. In: THIRD ICT INTERNACIONAL STUDENT PROJECT CONFERENCE (ICT-ISPC), 2014, Nakhon Pathom. **Proceedings...** Nakhon Pathom: IEEE, 2014. p. 143-146. ISBN 978-1-4799-5572-5.

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO - DECEA. Tecnologia da guerra para o mundo. **Aero Espaço**, n. 40, p. 20-21, jan. 2010.

DIAS, R. R. D. F. **RFID Journal Live! Brasil**. [S. l.: s. n.], 2012. Disponivel em: <http://www.rfidjournal.net/masterPresentations/rfid_latam2012_brasil/np/rampim_900_nov29.pdf>. Acesso em: 14 ago. 2014.

DIONISI, A.; SARDINI, E.; SERPELLONI, M. Wearable object detection system for the Blind. In: INSTRUMENTATION AND MEASUREMENT TECHNOLOGY CONFERENCE (I2MTC), 2012 IEEE INTERNATIONAL, 2012, Graz. **Proceedings...** Graz: IEEE, 2012. p. 1255 - 1258. ISBN 978-1-4577-1773-4.

DONG, Q.; ZHAN, J; WEI, L. A SHA-3 Based RFID Mutual Authentication Protocol and Its Implementation. In: IEEE INTERNATIONAL CONFERENCE ON SIGNAL PROCESSING, COMMUNICATION AND COMPUTING (ICSPCC), 2013, KunMing. **Proceedings...** KunMing: IEEE, 2013. p. 1-5.

EC-COUNCIL. RFID Hacking. In: ____. **Ethical hacking and countermeasures:** Linux, Macintosh and Mobile Systems. New York: Cengage Learning, 2010.

EVERIST HEALTH. **Everist genomics to launch cardiodefender:** world's only mobile ecg system that delivers real-time, beat-by-beat, quantitative heart monitoring data to physicians. Ann Arbor: [s. n.], 2011. Disponivel em: <http://everisthealth.com/blog/ wordpress/everist-genomics-launch-cardiodefender-worlds-mobile-ecg-system-delivers-real-time-beat-by-beat-quantitative-heart-monitoring-data-physicians/>. Acesso em: 19 ago. 2014.

FINKENZELLER, K. **RFID handbook**. United Kingdom: Wiley, 2010.

GOMES, C.E.M.; LUCENA, V. F.; YAZDI, F.; GOHNER, P. An inteligente medicine cabinet proposed to increase medication adherence. In: IEEE 15TH INTERNACIONAL CONFERENCE ON E-HEALTH NETWORKING, APPLICATIONS & SERVICES (HEALTHCOM), 2013, Lisbon. **Proceedings...** Lisbon: IEEE, 2013. p. 737-739. ISBN 978-1-4673-5800-2.

GOMES, H. O.; CALDAS, C. P. Uso inapropriado de medicamentos elo idoso: polifarmácia e seus efeitos. **Revista Hospital Universitário Pedro Ernesto**, Rio de Janeiro, v. 7, n. 1, p. 88-99, 2008. Disponivel em: <http://revista.hupe.uerj.br/detalhe_artigo.asp?id=195>. Acesso em: 24 janeiro 2015.

GREENGARD, S. **Manutenção de turbinas da Rolls-Royce avança em qualidade.** [S. l.]: RFID Journal Brasil, 2014. Disponivel em: <http://brasil.rfidjournal.com/estudos-de-caso/vision?11380/3>. Acesso em: 27 maio 2014.

ID INNOVATIONS. **Datasheet low voltage series reader modules (ID-3LA, ID-12LA, ID-20LA)**. [S.l.: s.n.], 2013. v. 1.

JUELS, A.; RIVEST, L.; SZYDLO, M. The blocker tag: selective blocking of RFID tags for consumer privacy. In: ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 10., 2003, New York. **Proceedings…** New York: [s.n.]. 2003.

JUNCO, D. F. G.; CRUZ FORERO, M. S.; DÍAZ CARO, D. F.; RUGE RUGE, I. A. Agrometeorological monitoring station based microcontroller and bluetooth communication. In: COLOMBIAN CONFERENCE ON AUTOMATIC CONTROL (CCAC), 2015, Manizales. **Proceedings...** Manizales: IEEE, 2015. p. 1-5.

KAKEHASHI, S.; MOTOYOSHI, T.; KOYANAGI, K.; OHSHIMA, T.; KAWAKAMI, H. P-CUBE: Block Type Programming Tool for Visual Impairments. In: CONFERENCE ON TECHNOLOGIES AND APPLICATIONS OF ARTIFICIAL INTELLIGENCE (TAAI), 2013, Taipei. **Proceedings...** Taipei: IEEE, 2013. p. 294-299. ISBN 978-1-4799-2528-5.

KFIR, Z.; WOOL, A. Picking virtual pockets using relay attacks on contactless smartcard. In: FIRST INTERNATIONAL CONFERENCE ON SECURITY AND PRIVACY FOR EMERGING AREAS IN COMMUNICATIONS NETWORKS (SECURECOMM), 1., 2005, Athens. **Proceedings...** Athens: IEEE, 2005. p. 47-58.ISBN 0-7695-2369-2.

KIMALDI. **Site.** [S. l.], 2014. Disponivel em: <http://www.kimaldi.com/>. Acesso em: 24 maio 2014.

LANDT, J. The history of RFID. **IEEE**, New York, v. 24, n. 4, p. 8-11, nov. 2005. ISSN: 0278-6648.

LAU, V. K. N.; KWOK, Y.-K. R. **Wireless internet and mobile computing:** interoperability and performance. New York: Wiley-IEEE , 2007. p. 285-307.

LEITÃO, T. **Sistema de identificação de veículos divide opiniões de especialistas.** Brasilia, DF: Agência Brasil, 2012. Disponivel em: <http://agenciabrasil.ebc.com.br/noticia/2012-10-03/sistema-de-identificacao-de-veiculos-divide-opinioes-de-especialistas>.Acesso em: 10 mar 2014.

LÓPEZ, P. P. **Lightweight cryptography in radio frequency identification (RFID) systems**. Leganés: Universidad Carlos III de Madrid, 2008. Disponivel em: <http://e-archivo.uc3m.es/handle/10016/5093>. Acesso em: 23 nov. 2013

MOTOROLA SOLUTIONS. **Motorola solutions**. [S. l.]: RFID, 2014. Disponivel em: <http://www.motorolasolutions.com/>. Acesso em: 24 maio 2014.

NOMAN, A. N. M.; RAHMAN, S. M.; ADAMS,. Improving Security and Usability of Low Cost RFID Tags. In: NINTH ANNUAL INTERNATIONAL CONFERENCE ON PRIVACY SECURITY AND TRUST (PST), 2011, Montreal. **Proceedings...** Montreal: IEEE, 2011. p. 134-141. ISBN 978-1-4577-0582-3.

ORGANIZAÇÃO MUNDIAL DE SAÚDE. **Elder abuse.** [S. l.], 2015. Disponível em: <http:who.int/mediacentre/factsheest/fs357/en/>. Acesso em: 08 fev. 2016.

ORGANIZAÇÃO MUNDIAL DE SAÚDE. **Visual impairment and blindness.** [S. l.], 2014. Disponível em: <http:who.int/mediacentre/factsheest/fs282/en/>. Acesso em: 08 fev. 2016.

PARIDA, M.; YANG, H. C.; JHENG, S. W.; KUO, C. J. Application of RFID Technology for In-House Drug Management System. In: 15TH INTERNACIONAL CONFERENCE ON NETWORK-BASED INFORMATION SYSTEMS (NBIS), 2012, Melbourne. **Proceedings...** Melbourne: IEEE, 2012. p. 577-581. ISBN 978-1-4673-2331-4.

PRIMO1D. **Primo1D**. [S. l.], 2013. Disponivel em: <http://primo1d.com/>. Acesso em: 27 maio 2014.

RFID JOURNAL BRASIL. **Perguntas Frequentes.** [S. l.], 2011. Disponivel em: <http://brasil.rfidjournal.com/perguntas-frequentes>. Acesso em: 19 nov. 2013.

RFID JOURNAL. **Glossary of RFID Terms.** [S. l.], 2013. Disponivel em: <https://www.rfidjournal.com/glossary/>. Acesso em: 20 nov. 2013.

RIBEIRO, G. **Intel, Dell e Samsung se unem para padronizar a 'Internet das coisas'.** [S. l.: s. n.], 2014**.** Disponivel em: <http://www.techtudo.com.br/noticias/noticia/2014/07/intel-dell-e-samsung-se-unem-para-padronizar-internet-das-coisas-entenda.html>. Acesso em: 23 ago. 2014.

ROBERTI, M. **The History of RFID Technology.** [S. l.], 2005. Disponivel em: <http://www.rfidjournal.com/articles/view?1338>. Acesso em: 27 maio 2014.

SHARAF, M. RFID Mutual Authentication and Secret Update Protocol for Low-cost Tags. In: IEEE INTERNATIONAL CONFERENCE ON TRUST, SECURITY AND PRIVACY IN COMPUTING AND COMMUNICATIONS (TRUSTCOM), 11., 2012, Liverpool . **Proceedings…** New York: IEEE, 2012. p. 25-27

SCHREIER, G.; SCHWARZ, M.; MODRE-OSPRIAN, R.; KASTNER, P.; SCHERR, D.; FRUHWALD, F. Design and evaluation of a multimodal mHealth based medication management system for patient self administration. In: ANNUAL INTERNATIONAL CONFERENCE OF THE IEEE ENGINEERING IN MEDICINE AND BIOLOGY SOCIETY (EMBC), 2013, Osaka. **Proceedings...** Osaka: IEEE, 2013. p. 7270-7273. ISSN 1557-170X.

SPARKFUN ELECTRONICS. **Sparkfun**. [S. l], 2014. Disponivel em: <https://www.sparkfun.com/products/11828>. Acesso em: 19 ago. 2014.

SUN, D.-Z.; ZHONG, J.-D. A Hash-Based RFID Security Protocolfor Strong Privacy Protection. **IEEE Transactions on Consumer Electronics**, New York, v. 58, n. 4, p. 1246-1252, 2012.

SUZUKI, T; JOSE, Y; NAKAUCHI, Y. A touchscreen-equipped medicine case as a medical interface for assisting na elderly person in medication management. In: ANNUAL INTERNACIONAL CONFERENCE OF THE IEEE ENGINEERING IN MEDICINE AND BIOLOGY SOCIETY (EMBC), 2011, Boston. **Proceedings...** Boston: IEEE, 2011. p. 5335-5338. ISBN 978-1-4244-4121-1.

SWEDBERG, C. **E-Thread provides discrete anti-counterfeiting or tracking solutions.** [S. l.]: RFID Journal, 2014. Disponivel em: <http://www.rfidjournal.com/articles/view?11587/>. Acesso em: 27 maio 2014.

SWEDBERG, C. **Volkswagen ganha eficiência no processo de acabamento de carros.** [S. l.]: RFID Journal Brasil, 2012. Disponivel em: <http://brasil.rfidjournal.com/estudos-de-caso/vision?9626>. Acesso em: 25 fev. 2014.

TEHRANIPOOR, M.; WANG, C. **Security for RFID Tags.** In: ____. Introduction to Hardware Security and Trust. New York: Springer, 2012. p. 283-302.

TOOLEY, M. **Circuitos eletronicos fundamentos e aplicaçoes**. Rio de Janeiro: Campus, 2007.

VIOLINO, B. **EAN and UCC Form EPCglobal,Inc**, [S. l.: s. n.], 2003. Disponivel em: <http://www.rfidjournal.com/articles/view?573>. Acesso em: 18 maio 2014.

WANG, CHUAN; GEORGE, D; GREEN, P.R. Development of plough-able RFID sensor network systems for precision agriculture. In: IEEE TOPICAL CONFERENCE ON WIRELESS SENSORS AND SENSOR NETWORKS (WISNET), 2014, Newport Beach. **Proceedings...** Newport Beach: IEEE, 2014. p. 64-66. ISBN 978-1-4799-2298-7.

XIAO, Q.; GIBBONS, T.; LEBRUN, H. RFID **Technology, security vulnerabilities, and countermeasures.** Viena**:** Intech, 2008. p. 357-382. ISBN 978-953-7619-35-0.

ZAINO, J. RFID's sporting life: capturing performance data in real time helps athetes improve their game and coaches and federation determine wich players to back. **RFID Journal**, New York, v. 12, n. 4, p. 20-29. Jul. 2015.