Prototipagem de sistema de segurança com localização em tempo real via Smartphone

Tecnologia como ferramenta de segurança pessoal

YURI DA COSTA GOUVEIA

CENTRO DE INFORMÁTICA
UNIVERSIDADE FEDERAL DA PARAÍBA

João Pessoa, 2019

YURI DA COSTA GOUVEIA

Prototipagem de sistema de segurança com localização em tempo real via Smartphone

Monografia apresentada ao curso Engenharia de Computação
do Centro de Informática, da Universidade Federal da Paraíba,
como requisito para a obtenção do grau de Bacharel em
Engenharia de Computação

Orientador: Alisson Vasconcelos de Brito

Maio de 2019

Ficha catalográfica: elaborada pela biblioteca do CI.

Será impressa no verso da folha de rosto e não deverá ser contada.
Se não houver biblioteca, deixar em branco.

CENTRO DE INFORMÁTICA
UNIVERSIDADE FEDERAL DA PARAÍBA

Trabalho de Conclusão de Curso de Engenharia de Computação intitulado ***Prototipagem de sistema de segurança com localização em tempo real via Smartphone*** de autoria de YURI DA COSTA GOUVEIA, aprovada pela banca examinadora constituída pelos seguintes professores:

Prof. Dr. Alisson Vasconcelos de Brito
Universidade Federal da Paraíba

Prof. Dr. Ewerton Monteiro Salvador
Universidade Federal da Paraíba

Prof. Dr. Bruno Petrato Bruck
Universidade Federal da Paraíba

Coordenador(a) do Departamento centro de informática
Fernando Menezes Matos
CI/UFPB

João Pessoa, 28 de maio de 2019

Centro de Informática, Universidade Federal da Paraíba
Rua dos Escoteiros, Mangabeira VII, João Pessoa, Paraíba, Brasil CEP: 58058-600
Fone: +55 (83) 3216 7093 / Fax: +55 (83) 3216 7117

**** Do not go gentle into that good night. ****

(Dylan Thomas)

AGRADECIMENTOS

Agradeço primeiramente à Deus por me dar forças, oportunidades e sabedoria para superar diversos desafios.

O desenvolvimento deste trabalho de conclusão de curso contou com o suporte de várias pessoas, dentre as quais agradeço:

À minha família, em especial aos meus pais, por todo o apoio e incentivo a buscar e aperfeiçoar meus conhecimentos por meio dos estudos.

À minha namorada, Maria Carolina, por me auxiliar e incentivar a crescer pessoalmente e profissionalmente.

Aos meus amigos que compartilharam comigo muitos momentos no curso e na vida, em especial a: Wellton Thyago, Abraão Allysson, Felipe Cunha, Lucas Eduardo, Kened Wanderson, Savio Fonseca, Stefano Tomei, Altair Pinto, Emmanuel Viana, Cinthya Ponce, Lucas Paiva, Arthur Cicero, Andrea Brito, Antonio Brito, Higor Anjos, Renê Alves, Yuri Oliveira, Leandro Mendes, Renno Diniz, Jefferson Lacerda, Viviano Medeiros, Carlos Eduardo Novinho, Filipe Lúcio, Eduardo Sérgio, Lucas Yan e a todos os outros que fizeram parte dessa etapa junto a mim.

Agradeço ao professor Alisson Brito, que me guiou durante minha graduação em diversos projetos, disciplinas e também me orientou neste trabalho.

E por fim, agradeço a todos os professores e profissionais que se empenharam para que eu e meus colegas pudéssemos ter uma graduação de qualidade.

RESUMO

Com o crescimento da violência no Brasil, as pessoas se sentem cada vez mais inseguras ao realizar atividades cotidianas. Com isso, este trabalho tem como objetivo o desenvolvimento de um sistema que realize a transmissão da localização do *smartphone* do usuário que informa estar em risco, por meio de um protótipo de *hardware*. Esse dispositivo, desenvolvido com o auxílio de um microcontrolador ESP8266 modelo ESP-01, se conecta ao servidor do Firebase (provedor de diversos serviços relacionados ao armazenamento e gerenciamento de dados) e muda o estado do usuário, com isso, o aplicativo Android reconhece essa alteração e informa aos contatos adicionados que o usuário em questão está em risco e permite o acesso da sua localização em tempo real no mapa, podendo facilitar ações policiais para combater a situação. O aplicativo também permite que o usuário gerencie seu estado atual, podendo definir se está seguro ou em risco e além disso, com o auxílio do Firebase, pode-se criar uma nova conta, realizar *login* de um usuário cadastrado e recuperar a senha. Para que essas funcionalidades pudessem ser realizadas corretamente, foi necessário rotear a rede do *smatphone* para o microcontrolador, pois o mesmo não possui rede própria. Por fim, foram realizados testes do protótipo desenvolvido, os quais se mostraram funcionais e eficazes para os propósitos definidos.

Palavras-chave: violência, localização, servidor, Android, ESP8266.

ABSTRACT

With the growth of violence in Brazil, people feel increasingly insecure when carrying out daily activities. Therefore, this work has the objective of developing a system that performs the transmission of the smartphone's location of the user that reported being at risk, through a hardware prototype. This device, developed with ESP8266 microcontroller model ESP-01, connects to the Firebase server and changes the user's state. After that, the Android application recognizes this change and informs the added contacts that the user is in danger, and they can access the real-time location on the map, and can facilitate police action to counteract the situation. The application also allows the user to manage their current state, being able to define whether it is safe or at risk and also, with the help of Firebase, can create a new account, log in into the app and recover the password. To these functionalities to work correctly, it was necessary to route the smatphone network to the microcontroller, since it does not have its own network. Finally, tests of the developed prototype were performed, which proved to be functional and effective for the defined purposes.

Palavras-chave: violence, location, server, Android, ESP8266.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

IoT - *Internet of Things*

Hz - Hertz

LAN - *Local Area Network*

1G - Primeira Geração

2G - Segunda Geração

3G - Terceira Geração

4G - Quarta Geração

AMPS - *Advanced Mobile Phone System*

D-AMPS - *Digital Advanced Mobile Phone System*

PDC - *Personal Digital Cellular*

GSM - *Global System for Mobile Communications*

SMS - *Short Message Service*

RDSI - Rede Digital de Serviços Integrados

FDMA - *Frequency Division Multiple Access*

TDMA - *Time Division Multiple Access*

CDMA - *Code Division Multiple Access*

GPS - *Global Positioning System*

SOC - *System on Chip*

GPIO - *General Purpose Input/Output*

IDE - *Integrated Development Enviroment*

JDK - *Java Development Kit*

SDK - *Software Development Kit*

FCM - *Firebase Cloud Messaging*

JSON - *JavaScript Object Notation*

XML - *Extensible Markup Language*

Sumário

1 INTRODUÇÃO

Com o avanço da tecnologia, torna-se cada vez mais fácil a realização de atividades cotidianas e serviços prestados a sociedade. Atividades e serviços estes, que antes só podiam ser realizados de maneira presencial, atualmente podem ser encontrados na Internet, facilitando a vida das pessoas (ABÍLIO, 2007). Hoje podemos realizar operações bancárias, como transferências e pagamento de contas, assistir cursos online, comunicar-se com pessoas em qualquer parte do mundo e diversas atividades, tudo graças a esses avanços tenológicos.

Também não é nenhuma novidade que no Brasil a segurança está em um estado crítico, chegando a ser pior do que em países que estão em situação de guerra (SOUZA; LIMA, 2006). Dessa forma, a inclusão da tecnologia da informação vem sendo continuamente empregada na vida das pessoas e também nas empresas como um meio de garantir a segurança ou prevenir situações de risco. Para isso, são utilizados dispositivos de *softwares*, como aplicativos de *smartphones* de geolocalização e aplicativos que informem áreas de risco da região a exemplo do aplicativo *CityCop*, assim como dispositivos de *hardware*, como sensores de movimento.

A criminalidade no Brasil está presente em todos os setores da sociedade, seja político, privado, público, etc. Dependendo da região do país as infrações são manifestadas de maneiras e intensidades diferentes. Há um grande investimento, por parte dos criminosos, em roubos e furtos tanto de veículos e cargas, quanto de objetos pessoais de cidadãos. Esses tipos de práticas vêm se tornando cada vez mais frequentes no cotidiano.

O medo vem tomando conta das ruas, pois os crimes mencionados não vêm ameaçando apenas o patrimônio das pessoas, visto que o acesso às armas de fogo também tem posto em risco as suas vidas, tomando como exemplo o latrocínio, isto é, roubo seguido de morte (SOARES, 2006). Devido a isso, esses problemas já não são mais tratados apenas no campo jurídico, pois ao provocar medo e insegurança na sociedade, diversas de suas áreas estudam tanto as causas e efeitos da violência, quanto maneiras de combatê-la.

A tabela 1 apresenta valores que mostram o aumento da violência, em específico o latrocínio. As informações apresentadas são em relação ao Brasil como um todo e também a cada estado do país.

Tabela 1: Ocorrências de latrocínio no Brasil

UF	2013		2014		2015		2016	
	Números absolutos	Taxa / 100 mil habitantes	Números absolutos	Taxa / 100 mil habitantes	Números absolutos	Taxa / 100 mil habitantes	Números absolutos	Taxa / 100 mil habitantes
Brasil	1.928	1	2.182	1	2.366	1	2.661	1
AC	13	2	7	1	10	1	8	1
AL	79	2	61	2	55	2	61	2
AM	36	1	45	1	73	2	93	2
AP	9	1	15	2	23	3	19	2
BA	151	1	199	1	207	1	211	1
CE	107	1	75	1	65	1	88	1
DF	29	1	50	2	46	2	42	1
ES	35	1	50	1	37	1	53	1
GO	124	2	167	3	156	2	186	3
MA	63	1	72	1	117	2	113	2
MG	84	0	63	0	122	1	116	1
MS	26	1	42	2	36	1	41	2
MT	45	1	52	2	59	2	64	2
PA	156	2	180	2	191	2	224	3
PB	28	1	19	0	48	1	33	1
PE	73	1	81	1	116	1	169	2
PI	29	1	35	1	47	1	49	2
PR	46	0	105	1	117	1	111	1
RJ	148	1	152	1	133	1	239	1
RN	16	0	62	2	58	2	48	1
RO	10	1	17	1	15	1	35	2
RR	2	0	3	1	9	2	5	1
RS	129	1	141	1	143	1	167	1
SC	55	1	57	1	71	1	62	1
SE	35	2	33	1	47	2	49	2
SP	380	1	385	1	356	1	361	1
TO	20	1	14	1	9	1	14	1

Fonte: IPEA, 2018.

Assim como os que seguem a lei à risca, os criminosos também têm acesso a esses progressos tecnológicos, e devido a isso, vêm mudando e expandindo a sua forma de atuação ao cometer delitos. Essa assenção beneficia diversas esferas do crime, desde simples assaltos urbanos até crimes organizados.

Com a crescente evolução no campo de IoT, diversos sensores e outros dispositivos vêm sendo empregados juntamente com programas para compor sistemas robustos e completos, com finalidade de promover uma maior segurança para seus usuários finais. Com essa união de sensores e de *softwares* embarcados, é possível processar os dados obtidos por meio da conexão com a rede mundial de computadores.

1.1 Objetivo geral

O objetivo geral deste trabalho é propor um sistema de segurança pessoal com localização em tempo real via *smartphone*. O usuário acionaria um pequeno dispositivo

de *hardware*, ao ser vítima de um crime e através do aplicativo de *software*, os contatos adicionados como amigos receberiam uma notificação, informando que o primeiro usuário mencionado estaria em risco e também a localização em tempo real do seu *smartphone*.

1.2 Justificativa

A segurança das pessoas está comprometida devido a violência que abrange todo o território nacional. Isso acontece de várias maneiras como assaltos, furtos, sequestros e outros tipos de ameaças à segurança pessoal.

A frequência e proporção com que esses problemas acontecem vêm aumentando progressivamente e em virtude disso, o trabalho da polícia se torna cada vez mais difícil, tanto para encontrar os criminosos como para reparar os danos e perdas sofridos pelas vítimas.

Dessa forma, o presente trabalho tem como justificativa facilitar a atuação da polícia, de prevenção e combate ao crime, assim como manter informado os parentes e amigos a situação em que o usuário se encontra. Com o auxílio de um *smartphone* e do um pequeno dispositivo de hardware, será possível rastrear o telefone móvel e conseguir identificar a localização do dono do aparelho ou do possível criminoso.

1.3 Estrutura do Trabalho

No capítulo 2 foi realizado uma revisão da literatura, abordando teorias, tecnologias e ferramentas que foram utilizados para a realização do presente trabalho. A fundamentação teórica será abordada de maneira sucinta e esclarecedora para que o leitor possa ter um embasamento para realizar a replicação do trabalho.

No capítulo 3 buscou-se apresentar o método de desenvolvimento do trabalho, expondo como foi realizado a aplicação dos conceitos da literatura abordados no capítulo 2. Foi descrito o desenvolvimento do banco de dados, do *software* e do *hardware* utilizados para construir o sistema de segurança pessoal.

No capítulo 4 foi demonstrado os resultados da construção da aplicação teorica e prática. Além do funcionamento, também são apresentados as qualidades e os problemas encontrados no projeto desenvolvido.

No capítulo 5 foi exposta uma discussão sobre os resultados alcançados com o desenvolvimento do sistema de segurança pessoal, abordando os pontos positivos e negativos do estudo e também foram propostas outras funcionalidades e aprimoramentos como trabalhos futuros.

1.4 Trabalhos Relacionados

Com a finalidade de entender e analisar sistemas que utilizam a tecnologia como meio de informar possíveis situações de risco por meio de monitoramento via *Internet*, estes trabalhos foram utilizados como base para o desenvolvimento do sistema elaborado na presente dissertação.

1.4.1 Uber

Um exemplo bastante utilizado do uso da tecnologia como meio de segurança pessoal é o sistema de acompanhamento e compartilhamento de viagens no aplicativo Uber. Esse aplicativo tem como uma das principais responsabilidades, garantir a segurança dos passageiros e dos motoristas. O Uber utiliza da tecnologia de *machine learning* para bloquear viagens para motoristas que são consideradas como inseguras. Para os passageiros, mais medidas de segurança são tomadas, como um botão para ligar diretamente para a polícia, compartilhamento em tempo real de viagem com amigos e familiares, registro do percurso de viagens, entre outros (UBER, 2018).

1.4.2 Sistema de alarme conectado via redes móveis para monitoramento e segurança de veículos automotivos através de aplicativo de telefone celular

Este trabalho propõe um método de monitoramento com intuito de verificar o estado de segurança de veículos automotivos. Através de um Arduino e sensores acoplados ao veículo, é possível saber informações sobre os faróis, ignição, travas, vidros, entre outros. Um aplicativo na plataforma Android é utilizado como interface para leitura das informações gerais do veículo. O usuário pode obter dados em tempo real do veículo ao pressionar um botão localizado no aplicativo, e também pode acionar o alarme do mesmo, caso necessite (BOFF, 2017).

1.4.3 Cerberus

O Cerberus Segurança Pessoal é um aplicativo que permite compartilhar a localização do deslocamento em tempo real para contatos selecionados através de mensagem por e-mail, SMS e publicação nas redes sociais. É possível determinar o tempo de duração que o compartilhamento permanecerá ativo, acionar um botão de emergência para pedido de ajuda e trocar mensagens com os contatos que estão acompanhando o trajeto (G1, 2018).

1.5 Fluxo do sistema

Essa seção visa explicar resumidamente o fluxo de funcionamento da aplicação desenvolvida para o trabalho em questão.

1.5.1 Dando início à aplicação

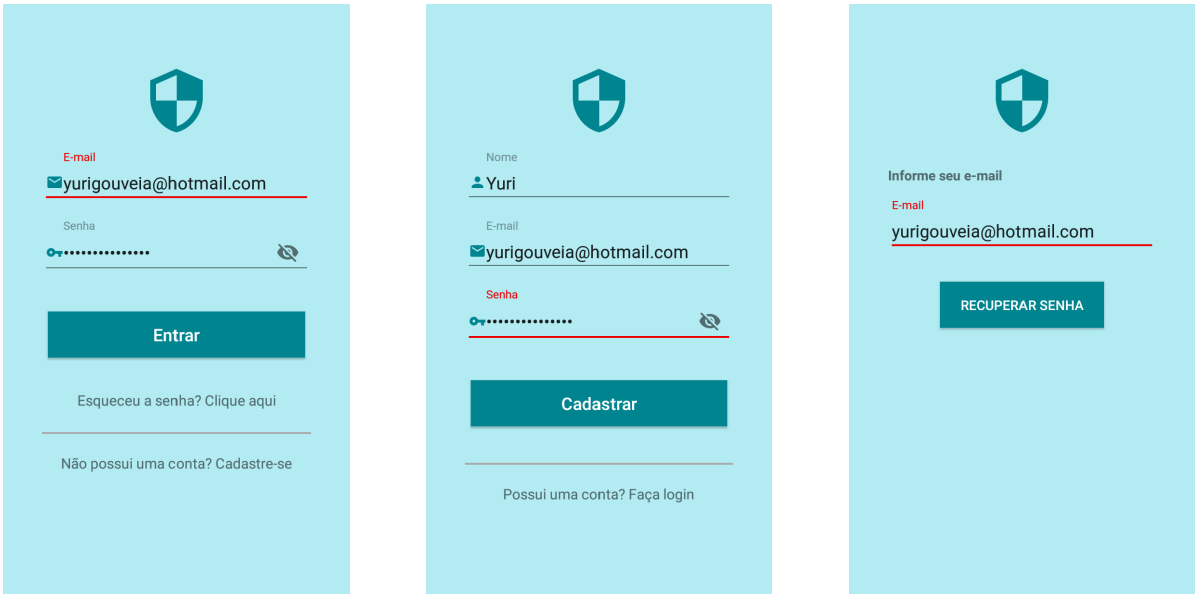
O funcionamento da aplicação se inicia quando o usuário aciona o dispositivo físico ao estar em perigo. Isso fará com que o aplicativo Android desenvolvido envie a localização do usuário para os contatos adicionados como amigos.

1.5.2 O aplicativo

Ao iniciar o aplicativo existem três funcionalidades, relativas a autenticação do usuário, as quais podem ser acessadas. As funcionalidades são:

- *Login*, caso o usuário possua uma conta.
- Cadastro, caso o usuário não possua uma conta.
- Recuperar senha, caso o usuário esqueça a senha da conta.

A primeira tela apresentada é a de entrar (Figura 1a) no aplicativo através do *e-mail* e senha; a segunda é a de fazer o cadastro (Figura 1b), podendo ser acessada ao clicar na frase "Não possui conta? Cadastre-se"; a terceira é a de recuperar a senha (Figura 1c), caso o usuário tenha esquecido a atual, clicando no texto "Esqueceu sua senha? Clique aqui".



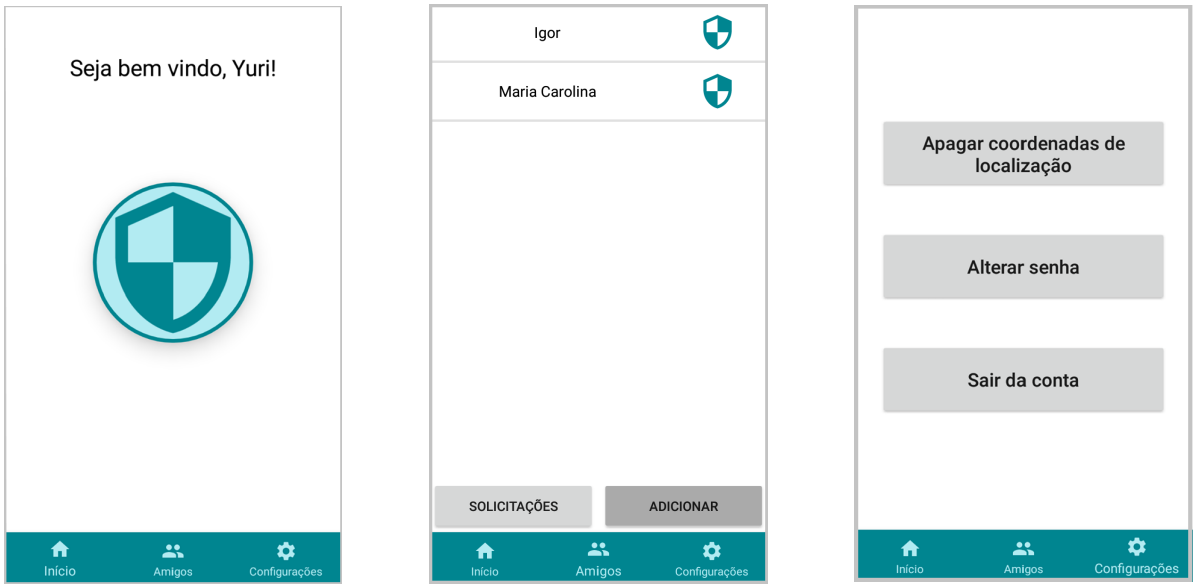
(a) *Login*. **(b) Cadastro.** **(c) Recuperar senha.**

Fonte: Autoria própria.

Figura 1: Telas de autenticação.

Após entrar na aplicação com uma conta de usuário, é apresentado a página inicial a qual apresenta na sua parte inferior três opções para se navegar:

- Início.
- Amigos.
- Configurações.



(a) Início. **(b) Amigos.** **(c) Configurações.**

Fonte: Autoria própria.

Figura 2: Telas de funcionalidades da aplicação.

Na figura 2a é possível notar a opção relativa à aba Início. Essa tela apresenta uma mensagem receptiva para o usuário logado e apresenta um botão no centro da tela, o qual informa a situação de quem utiliza o aplicativo, mudando a cor por trás do isotipo é alterada para vermelho caso esteja em risco. Ao clicar nele, o usuário pode determinar se está em segurança ou não.

Na figura 2b pode-se observar aa lista de amigos adicionados, o botão para adicionar novos amigos e outro relativo a solicitações de amizades recebidas. A imagem ao lado do nome dos amigos determina a situação em que o mesmo se encontra. Caso algum dos contatos esteja em perigo, pode-se clicar em seu nome e será possível ter acesso à sua localização em tempo real.

Por fim, na figura 2c nota-se botões de configuração e gerenciamento da conta. O primeiro botão serve para apagar as coordenadas de localização do usuário logado e só pode ser acionada caso o mesmo não esteja em alguma condição de ameaça. O segundo serve para alterar a senha da conta do aplicativo. O terceiro é o botão que serve para sair da conta acessada.

2 CONCEITOS GERAIS E REVISÃO DA LITERATURA

Este capítulo descreve os conceitos básicos para o entendimento do trabalho desenvolvido.

2.1 Tecnologia da Informação e Comunicação

A tecnologia da informação e comunicação são aquelas que buscam facilitar a comunicação entre os seres e a transmissão da informação, para isso utiliza-se ferramentas tecnológicas.

A tecnologia da informação e comunicação também busca promover o crescimento do processo comunicativo, assim como inovar outros processos de interesse geral, como segurança pública, pesquisa científica, dentre outros (OLIVEIRA, 2015).

2.2 Redes de Computadores e Internet

As redes de computadores são meios aos quais dois ou mais computadores autônomos estão interconectados por um tipo de tecnologia. Isso permite com que esses computadores possam realizar uma conexão entre si, e assim, trocar informações. Essa conexão pode ser feita de diversas maneiras, como por exemplo fio de cobre, fibras ópticas, microondas, satélites de comunicação, entre outros.

2.2.1 Redes sem fio

A comunicação realizada por meio de redes sem fio é baseada no estabelecimento de transmissão de dados através de ondas eletromagnéticas, as quais são propagadas no espaço por meio da movimentação de elétrons. O número de oscilações em um determinado período (geralmente medido em segundos) de uma onda eletromagnética é chamada de frequência e é medida em Hertz (*Hz)*.

Essas ondas podem ser transmitidas por meio de antenas ligadas a um devido circuito elétrico e podem ser recebidas através de receptores localizados a uma determinada distância, onde seu sinal depende de fatores como frequência, potência do transmissor, etc. Assim ocorre o método de funcionamento de toda rede sem fio.

Devido ao fato de existirem diversos fabricantes e fornecedores de redes, foi necessária a criação de uma padronização para que os usuários conseguissem usufruí-las de forma eficaz (TANENBAUM, 2002). Na Tabela 2 são apresentados alguns dos padrões que foram adotados mundialmente.

Tabela 2: Padrões IEEE de redes sem fio

Padrão IEEE	Frequência	Alcance	Taxa
802.11a	5 GHz	<50 m	6 – 54 Mbps
802.11b	2.4 GHz	<100 m	2 – 11 Mbps
802.11g	2.4 GHz	<100 m	20 – 54 Mbps
802.11i	2.4 GHz	<100 m	20 – 54 Mbps
802.16 (WIMAX)	10 – 66 GHz	= 10 km	60 – 100 Mbps
Celular (FDMA, TDMA, CDMA, GSM e suas Evoluções)	900, 1700, 1800 MHz	= depende da rede	4,8 Mbps

Fonte: SCHWEITZER (2006, apud BOFF, 2017, p. 21).

2.2.1.1 WiFi

Com a criação dos computadores portáteis surgiu a necessidade de se conectar a Internet através de uma rede sem fio, de modo que simplificasse o processo de acesso a *web*. Devido a dificuldade de encontrar equipamentos de transmissão e recepção de dados com frequências compatíveis, vários problemas surgiram durante a tentativa de formular esse novo tipo de acesso a rede. Em virtude dessas dificuldades, foi criado um padrão para comunicação de rede sem fio, o 802.11, popularmente conhecido como WiFi (TANENBAUM, 2002, p. 67).

De acordo com a definição do 802.11, as redes sem fio possuem dois modos de operação, um para a presença de estação base e outro para sua ausência. Em relação a esses modelos Tanembaum (2002, p. 67) diz:

> No primeiro caso, toda a comunicação deveria passar pela estação base, chamada ponto de acesso na terminologia do 802.11. No outro caso, os computadores simplesmente transmitiriam diretamente uns para os outros. Agora, esse modo costuma ser chamado interligação de redes ad hoc. Um exemplo típico é de duas ou mais pessoas juntas em uma sala não equipada com uma LAN sem fio, fazendo seus computadores se comunicarem diretamente.

Fonte: Tech Tudo, 2014.

Figura 3: Padrão de redes sem fio 802.11. Rede com comunicação a estação base, à esquerda, e rede ad hoc, à direita.

2.2.2 Sistema de telefonia móvel

Atualmente os sistemas de telefonia móvel tem como perspectiva aplicações direcionadas para a transmissão de dados. Com a finalidade de se obter a melhor velocidade de transmissão de dados, foram desenvolvidas tecnologias que permitem difusão de informações através da comutação de circuitos e pacotes (PEREIRA; GUEDES, 2004).

A respeito de telefonia móvel Tanembaum (2002, p. 128) diz:

> O sistema telefônico tradicional (ainda que ele algum dia chegue a vários gigabits entre uma extremidade e outra da fibra) não será capaz de satisfazer a um grupo crescente de usuários: as pessoas em trânsito. Agora, as pessoas esperam efetuar chamadas telefônicas de aviões, carros, piscinas e enquanto fazem jogging no parque. Dentro de alguns anos, elas também irão querer enviar correio eletrônico e navegar na Web enquanto estiverem em todos esses lugares e em muitos outros. Conseqüentemente, há um enorme interesse na telefonia sem fios.

Existem quatro gerações, com diferentes tecnologias, as quais os telefones móveis passaram e que apresentaram as seguintes características:

1. Voz analógica.
2. Voz digital.
3. Transmissão de dados.

Nas próximas seções serão brevemente apresentadas as características e informações a respeito das gerações da telefonia móvel.

2.2.2.1 Primeira Geração (1G)

Essa geração teve início no final dos anos 1970 e durou até os anos de 1980. Inicialmente chamados telefones de rádio móvel celular, utilizavam de sinais analógicos para transportar a voz (COMER, 2016, p. 244).

Antes do advento da primeira geração utilizava-se um único transmissor, posicionado no topo de um prédio ou de uma montanha e apresentava um ou dois canais de comunicação. Para manter o diálogo, os que possuíam canal único precisavam apertar um botão para ativar o transmissor e desativar o receptor, sistema conhecido como *push-to-talk*. Já os de canal duplo possuíam duas frequências, uma para enviar o sinal de voz e outro para receber, eliminando a necessidade de um botão para conversar (TANENBAUM, 2002, p. 129).

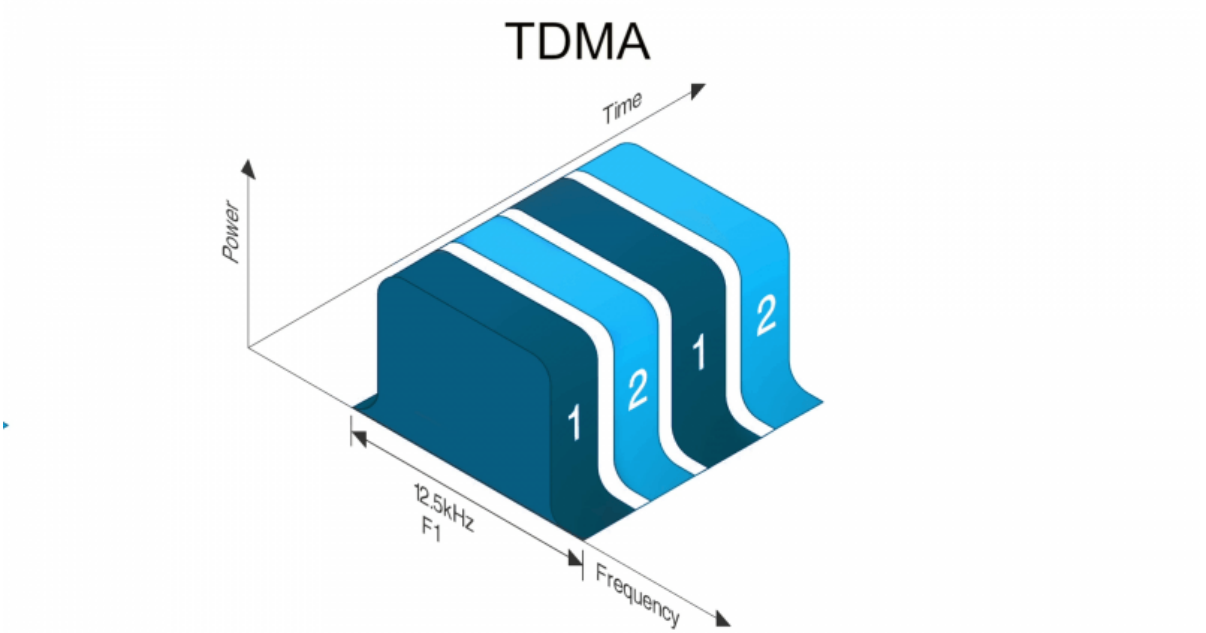
A tecnologia referente a 1G se deu com a criação do AMPS. Esse sistema é baseado na multiplexação por divisão de frequência (FDMA), que realiza a transmissão de vários sinais eletromagnéticos sem que haja interferência. Isso se deve ao fato de que existem vários canais com frequências diferentes para o envio e recepção dos sinais (COMER, 2016, p. 157–158).

2.2.2.2 Segunda Geração (2G)

A respeito da segunda geração Tanembaum (2004, p. 138) infere:

> A primeira geração de telefones celulares era analógica; a segunda geração era digital. Da mesma maneira que não havia nenhuma padronização mundial durante a primeira geração, também não havia nenhuma padronização durante a segunda. Quatro sistemas são usados agora: D-AMPS, GSM, CDMA e PDC. O PDC só é usado no Japão e é basicamente o D-AMPS modificado para compatibilidade retroativa com o sistema analógico japonês de primeira geração.

Com a chegada da segunda geração o sistema AMPS sofreu uma evolução e passou a ser conhecido como D-AMPS. Esse sistema utiliza divisão de tempo por múltiplo acesso, também conhecido por TDMA, onde cada canal de 30KHz é compartilhado por três usuários em faixas de tempos distintas. A finalidade dessa evolução se deu devido a possibilidade de uma leve transição entre a tecnologia analógica e a digital, ocupando as mesmas faixas de frequências (DIAS; SADOK, 2001).



Fonte: *Tait Radio Academy*, 2014.

Figura 4: Múltiplo Acesso Por Divisão de Tempo

No início da década de 90 surgiu o GSM, com o intuito de fornecer diversas funcionalidades através de uma Rede de Digital de Serviços Integrados (RDSI), além disso, o GSM buscou resolver o problema de fragmentação que ocorria nos primeiros sistemas celulares na Europa. Todo seu funcionamento ocorre na faixa de frequência de 900MHz e com o auxilio do TDMA (GUIMARÃES, 1998).

Segundo Guimarães (1998, p. 17), dentre as principais características do GSM pode-se destacar:

- Serviços de telefonia, incluindo fax, videotexto e telex.
- Serviços de dados com possibilidade de comunicação de dados por pacotes a taxas de até 9600bps.
- Serviços de RDSI suplementares tais como desvio de chamada, identificação de assinante chamador e serviço de mensagem. Esse último, chamado SMS (Short Message Service) permite a recepção de mensagens alfanuméricas mesmo durante uma conversação e ainda permite transmitir repetitivamente mensagens ASCII para todos os assinantes, serviço esse muitas vezes utilizado para fins de segurança e de aviso.

Para completar, um dos principais avanços da tecnologia 2G foi a criação do múltiplo acesso por divisão de código, ou CDMA. Seu desenvolvimento também foi realizado com a finalidade de transitar de um sistema de comunicação analógico para um

digital. Ele trouxe consigo a possibilidade dos usuários utilizarem a mesma faixa de frequência (GUIMARÃES, 1998). Para separar as transmissões nos canais específicos de certa frequência, é utilizada a teoria da codificação, onde cada sinal transmitido possui um código para identificar o canal ao qual ele pertence (DIAS; SADOK, 2001).

2.2.2.3 Terceira Geração (3G)

A respeito da terceira geração, Dias e Sadok (2001, p. 22) dizem:

> Os sistemas de terceira geração representam uma mudança de paradigma, proporcionando um sistema avançado de telecomunicações que viabilizará a convergência entre a telefonia celular, Internet e multimídia. A terceira geração tornará serviços de informação disponíveis instantaneamente, por exemplo, um terminal de 3G pode ser utilizado como uma câmera de vídeo da qual o usuário pode enviar cartões eletrônicos e clips de vídeo em tempo real.

Para chegar de fato a 3G, foram realizados alguns avanços que fizeram uma transição entre a segunda e a terceira geração. Esses avanços foram considerados por muitos como 2,5G (TANENBAUM, 2002, p. 140). Os principais sistemas dessa geração de transição foram o GPRS e o EDGE.

- **GPRS** - esse sistema utiliza funcionalidades presentes na rede GSM, acrescentando equipamentos na infra-estrutura da rede para suportar novos serviços de dados (PIROTTI; ZUCCOLOTTO, 2009, p. 86).
- **EDGE** - se trata de uma evolução do GSM, baseada em TDMA, o qual traz um aumento na capacidade de transmissão em relação ao seu predecessor.

Com a chegada de fato da terceira geração, houveram mudanças como melhorias na qualidade de voz, Internet de alta velocidade, serviços de mensagens e serviços de multimídia (TANENBAUM, 2002, p. 139). Essas melhorias foram feitas graças as tecnologias desenvolvidas para essa geração, o WCDMA e o CDMA2000/3X, que são evoluções do GSM e do CDMA (DIAS; SADOK, 2001).

2.2.2.4 Quarta Geração (4G)

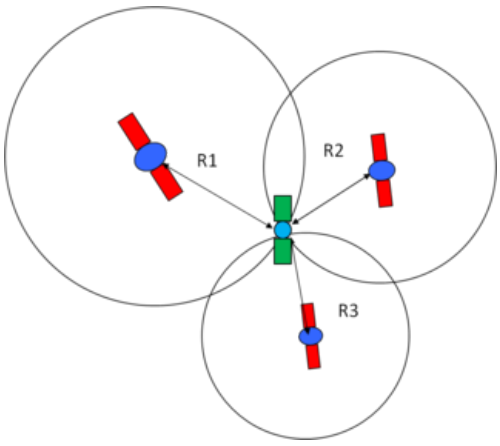
As redes 4G não possuem uma tecnologia ou padrão definido, mas apresentam um conjunto de tecnologias e protocolos, criados com o objetivo de alcançar o máximo desempenho de processamento com uma rede sem fio de baixo custo.

Alguns dos sistemas que usam tecnologia 4G são WiMAX, WiBro e LTE. Para que esta geração se tornasse uma realidade, foi necessário integrar as tecnologias existentes (2G, 3G) (PEREZ, 2010).

2.3 Sistema de Posicionamento Global

O Sistema de Posicionamento Global, conhecido por GPS, inicialmente desenvolvido com propósitos de uso militar, demonstrou grande utilidade para aplicações de uso civil. Devido a sua grande precisão ao se determinar uma localização e pelo fato de estar disponível em qualquer parte do mundo (ar, terra e mar), o GPS é considerado um excelente sistema de navegação. (DRIRA, 2006).

O GPS é um sistema baseado em radionavegação por satélite, possuindo uma constelação de no mínimo 24 satélites, localizados em 6 planos orbitais espaçados por 60 graus (DRIRA, 2006). Para seu funcionamento GPS, é necessário que a distância de um ponto na terra esteja visível a pelo menos três satélites, assim como a localização desses satélites (EL-RABBANY, 2002, p. 8).

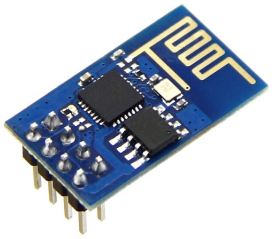


Fonte: NASA, 2012.

Figura 5: Sistema de geolocalização por satélite.

2.4 Microcontrolador ESP8266 ESP-01

O microcontrolador ESP8266, modelo ESP-01, é um dispositivo que foi desenvolvido pela Espressif Systems e que apresenta uma grande performance para SOCs sem fio. Esse microcontrolador foi desenvolvido com o intuito de oferecer uma opção de baixo custo para desenvolvimento de plataformas móveis oferecendo uma ótima capacidade para se embarcar recursos *Wifi* (PLATFORM, 2013).



Fonte: FilipeFlop, 2019.

Figura 6: ESP8266 ESP-01.

O modelo de comunicação utilizado por esse dispositivo é realizada através do modelo cliente-servidor. O cliente aciona o servidor, que sempre está a espera de alguma requisição do cliente, para que seja realizada a comunicação.

Conceituando o sistema de comunicação cliente-servidor, de Oliveira (2017, p. 20–21) diz:

> O **servidor** é um *software* que mantém uma porta de comunicação aberta à espera do cliente. Sua localização, seja pelo seu endereço ou nome, deve ser conhecida por todos os cliente que querem acessá-lo. Um servidor pode receber um grande número de solicitações simultâneas de clientes, por isso, normalmente, executa em um computador de alto desempenho. [...]. Isso não impede que um dispositivo IoT execute a função de servidor, apesar do *hardware* limitado, recebendo solicitações de clientes.
>
> O **cliente** é também um *software*, normalmente acionado por um usuário, razão pela qual é comum que tenha uma interface gráfica amigável. Um navegador web como Google Chrome, Mozilla Firefox ou Internet Explorer é um exemplo de cliente. Cabe ao cliente iniciar a comunicação com o servidor, seja acionada diretamente pelo usuário ou de forma automática, em resposta a um evento ou uma ação externa. Um dispositivo IoT também pode atuar como cliente, acessando servidores para buscar ou atualizar informações sobre seu funcionamento.

2.4.1 Especificações Técnicas

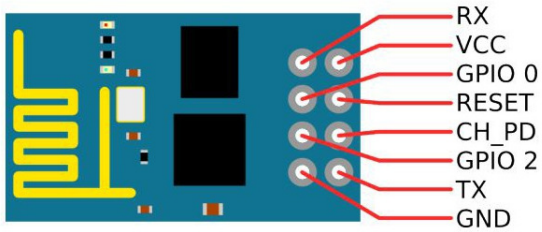
Assim como qualquer microcontrolador, o ESP possui características de funcionamento as quais permitem sua utilização de maneira correta e segura. Na tabela 3 é apresentado essas características e medidas de operação.

Tabela 3: Especificações técnicas do Microcontrolador ESP8266 ESP-01

	Descrição
Chip	ESP8266
Modelo	ESP-01
Tensão de operação	3,3V
Suporte à redes	802.11 b/g/n
Alcance	90m aprox.
Comunicação	Serial (TX/RX)
Protocolos de comunicação	TCP e UDP
Conectores	GPIO, I2C, SPI, UART, Entrada ADC, Saída PWM e Sensor de Temperatura interno
Modo de segurança	OPEN, WEP, WPA_PSK, WPA2_PSK e WPA_WPA2_PSK
Dimensões	25 x 14 x 1mm
Peso	7g

Fonte: FilipeFlop, 2019.

Já na figura 7 é apresentado a pinagem do dispositivo, o qual apresenta um total de oito pinos: RX, TX, GPIO0, GPIO2, GND, VCC, RESET e CH_PD.



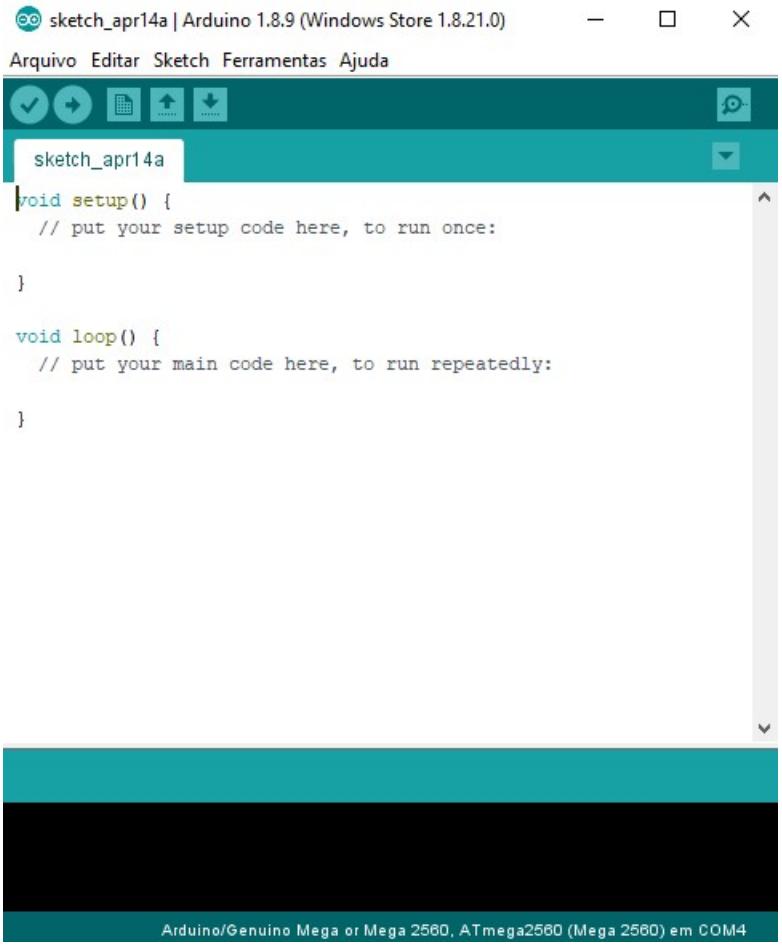
Fonte: *Open Circuit*, 2019.

Figura 7: Pinagem do ESP8266 ESP-01

2.4.2 Arduino IDE

Arduino é uma empresa de *hardware* e *software* de código aberto, ou seja, existe uma comunidade de usuários que projetam e utilizam sistemas baseados em microcon-

troladores e bibliotecas de desenvolvimento. A maneira mais comum para se desenvolver sistemas com microcontroladores é usando o Arduino IDE, que utiliza a linguagem de programação C. É através dessa IDE que é possível ter acesso a grande biblioteca do Arduino, a qual continua a crescer graças a comunidade de código aberto (ARDUINO, 2015).



Fonte: Autoria própria.

Figura 8: Ambiente de desenvolvimento integrado Arduino

2.5 Android

Android é uma plataforma de tecnologia móvel, criada pela Google, que contém um conjunto de aplicações para celulares, possuindo um sistema operacional, *middleware*, aplicativos e interface de usuário (PEREIRA; GUEDES, 2004).

Com o intuito de tirar total proveito do que um dispositivo móvel possa oferecer, o Android foi desenvolvido para ser um sistema de código aberto, havendo uma facilidade de aderir novas tecnologias a esse sistema. O sistema em questão foi desenvolvido com base no sistema operacional Linux, e possui recursos que agem nas diversas fases da criação do projeto, a partir da execução até a criação de programas específicos. Apesar de ter

sido baseado em um sitema Linux, o Android não possui algumas funcionalidades desse sitema operacional, caracterizando-o como um sistema diferente do Linux (PEREIRA; GUEDES, 2004).

Além das características citadas no parágrafo acima, outra justificativa para o uso dessa plataforma é a familiaridade com a plataforma em questão.

2.5.1 Android Studio

Android Studio é uma IDE que foi criada para o desenvolvimento de aplicações Android. Essa IDE apresenta um conjunto de ferramentas as quais permitem com que os desenvolvedores tenham uma maior facilidade para editar, depurar, realizar testes e gerar perfis de código (ANDROID, 2019).

Para utilizar o Android Studio é necessário instalar duas ferramentas no ambiente de desenvolvimento, o JDK e o Android SDK. A primeira ferramenta se trata de um conjunto de utilitários que permitem o uso do Java. Já a segunda é relativa a um conjunto de pacotes com recursos que permitem o desenvolvimento na plataforma em questão (CRAIG; GERBER, 2015, p. 1).

2.6 Firebase

Em termos práticos, Firebase é um provedor de serviços em nuvem que gerencia e armazena dados para aplicações Android, iOS e *web* (STONEHEM, 2016), o qual facilita o trabalho dos desenvolvedores fornecendo um serviço de alta qualidade para seus aplicativos (GOOGLE, 2019).

Alguns serviços disponibilizados pelo Firebase são descritos nas seguintes subseções.

2.6.1 Firebase *Analytics*

O Firebase *Analytics* fornece uma avaliação do uso do aplicativo, permitindo com que o desenvolvedor saiba como o usuário utiliza o programa (KHAWAS; SHAH, 2018). Essa análise é feita através de relatórios gerados a partir de eventos-chave e propriedades do usuário capturados automaticamente (GOOGLE, 2019).

2.6.2 Firebase *Auth*

O *Firebase Auth* permite com que o desenvolvedor implemente de maneira simples um sistema de autenticação extremamente segura. É possível realizar autenticação através

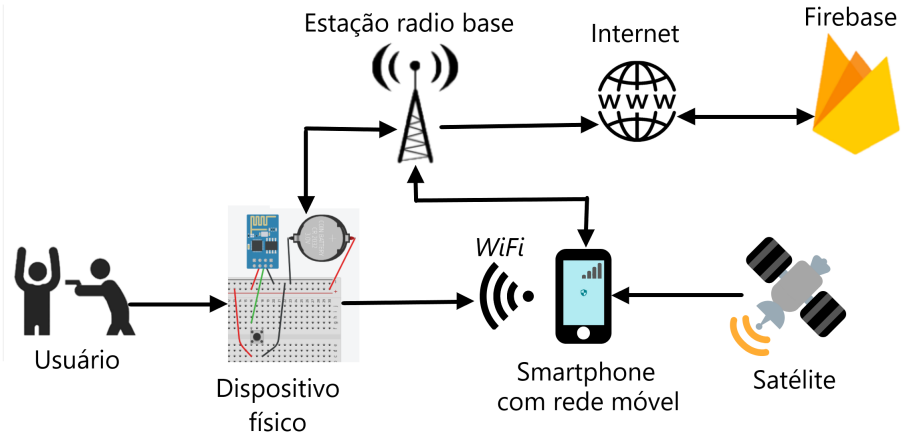
de *e-mail* e senha, autenticação por telefone, login do Google, Twitter, Facebook e outros (GOOGLE, 2019).

2.6.3 *Real-time Database*

Funcionando como um banco de dados NoSQL, esta ferramenta armazena e sincroniza dados JSON em tempo real. Essa sincronização permite com que diversos usuários possam ter acesso as mesmas informações em um curto intervalo de tempo (GOOGLE, 2019).

3 PROTOTIPAGEM DO SISTEMA DE SEGURANÇA

O fluxo vital de toda a aplicação desenvolvida é apresentado na figura 9, onde, de modo simplificado, existem quatro atores: o usuário, o dispositivo de *hardware*, o Firebase e o aplicativo de *software*. As setas indicam o sentido em que as informações são transmitidas para os atores em questão.



Fonte: Autoria própria.

Figura 9: Fluxo de funcionamento do sistema.

Nas seguintes seções serão apresentadas o método de conexão dos dispositivos, o gerenciamento feito pelo Firebase e o modo de como o protótipo físico e o aplicativo foram desenvolvidos.

3.1 Comunicação dos Dispositivos com a Rede

A comunicação dos dispositivos com o servidor do Firebase ocorre através da rede móvel do *smartphone*. Para a aplicação realizada utilizou-se uma rede de quarta geração (4G) para que tanto o celular quanto o dispositivo físico conseguissem acessar a Internet. Apesar da rede 4G ter sido utilizada, o sistema funcionaria corretamente caso fosse utilizado a de outras gerações, como a 2G e 3G.

Ao conseguir acesso à rede, o *smartphone* podem enviar ou receber dados da estação radio base que por sua vez conecta-se com a internet e , por fim, ao servidor.

O protótipo do dispositivo de *hardware* proposto não possui um método próprio de acesso a rede. Devido a isso, o telefone móvel foi utilizado como um roteador WiFi, pertmitindo com que o dispositivo físico se comunique com a estação rádio base.

3.2 Gerenciamento do Firebase

Para o desenvolvimento do presente trabalho o Firebase foi utilizado como servidor da aplicação, ferramenta de armazenamento e gerenciamento de dados.

Para que haja a comunicação entre o aplicativo e dispositivo físico (clientes) com o Firebase (servidor) foi necessário adicionar um arquivo de configuração, no formato JSON, do Firebase ao projeto Android. Esse arquivo contempla informações básicas de acesso e segurança do servidor Firebase e do aplicativo android, conforme pode-se observar na figura 10.


```
{
  "project_info": {
    "project_number": "691015331362",
    "firebase_url": "https://safeband-tcc-2019.firebaseio.com",
    "project_id": "safeband-tcc-2019",
    "storage_bucket": "safeband-tcc-2019.appspot.com"
  },
  "client": [
    {
      "client_info": {
        "mobilesdk_app_id": "1:691015331362:android:ed8408995e2b8b0b",
        "android_client_info": {
          "package_name": "com.example.tcc.activities"
        }
      },
      "oauth_client": [
        {
          "client_id": "691015331362-5fppi7g52i65njm95s1ilmga1ink19a3.apps.googleusercontent.com",
          "client_type": 3
        }
      ],
      "api_key": [
        {
          "current_key": "AIzaSyBr5qVZjF2I4yAxoZhcvz5K8tJ3MlGehak"
        }
      ],
      "services": {
        "appinvite_service": {
          "other_platform_oauth_client": [
            {
              "client_id": "691015331362-5fppi7g52i65njm95s1ilmga1ink19a3.apps.googleusercontent.com",
              "client_type": 3
            }
          ]
        }
      }
    }
  ],
  "configuration_version": "1"
}
```


Fonte: Autoria própria.

Figura 10: Arquivo JSON de configuração da conexão entre cliente e servidor.

Para que a o protótipo pudesse se comunicar corretamente com o servidor corretamente os campos de nome “firebase_url” e “package_name” foram dois dos mais importantes, pois, o primeiro se refere ao endereço ao qual será transmitido e recebido dados, já o segundo se trata de um identificador único do aplicativo que está sendo desenvolvido.

Ao conseguir estabelecer a comunicação entre o sistema desenvolvido e o Firebase, foi possível criar registros referentes a usuários e também ler essas informações. A figura 11 é a forma em que os dados são organizados na ferramenta *Realtime Database*.

(a) Estrutura JSON. **(b) Estrutura no Firebase.**

Fonte: Autoria própria.

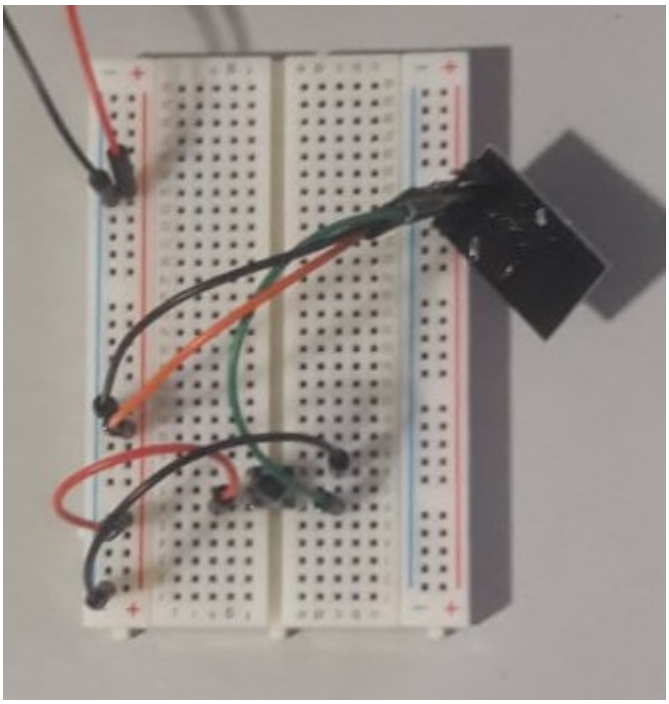
Figura 11: Estrutura de disposição de dados do Firebase.

Cada usuário irá possuir um identificador único, o qual será a chave para se ter acesso às suas informações. Quem possuir uma conta cadastrada no aplicativo possuirá obrigatoriamente três campos: o campo *SAFE*, que define se o usuário está em perigo, possuindo valor *false*, ou seguro, apresentando valor *true*; o campo *nome* contendo o nome definido pelo usuário; o campo *email*, contendo o endereço de *e-mail* utilizado no cadastro.

Os outros campos não estarão, obrigatoriamente, presentes em todas as ocasiões devido aos seus comportamentos particulares. Esses campos são: o campo de *amigos* que conterá uma lista com os identificadores de cada usuário adicionado como amigo e o valor *booleano true* associados às chaves de identificação, pois o formato JSON exige que cada chave possua um valor associado. Esse campo só estará presente caso existam usuários adicionados como amigos; o campo *solicitacoes*, contendo o identificador de cada conta e o valor *true* associado a cada um deles. Esse último estará presente caso haja alguma solicitação de amizade pendente; por fim as *coordenadas*, com as quais será possível ter acesso à localização do usuário que está em perigo, através da latitude, em *lat*, e longitude, em *lon*. Esse campo estará presente se o usuário já definiu estar em perigo alguma vez e não apagou as informações de sua localização.

3.3 Prototipagem do dispositivo de *hardware*

O protótipo de *hardware* foi desenvolvido com o auxílio de um microcontrolador ESP8266 modelo ESP-01, um botão e *jumpers*. O microcontrolador em questão foi escolhido devido ao baixo custo e desempenho satisfatório para o desenvolvimento do projeto.



Fonte: Autoria própria.

Figura 12: Protótipo físico montado na *protoboard*.

Na figura 12 pode-se observar o circuito funcional montado em uma *protoboard*. Os fios pretos estão conectados no terra, os fios vermelhos e laranja estão conectados em tensão de 3,3 V, suficiente para alimentar o dispositivo. O fio verde serve para transmitir dados de entrada, reconhecendo o acionamento do botão.

Ao informar que está em uma situação de risco, ou seja, ao pressionar o botão, é feita a conexão do circuito, transmitindo o sinal que vem do fio vermelho conectado a tecla para o fio verde, que por sua vez, transmite o sinal para o ESP8266. O tratamento dessa ação é feita por meio do código implementado por meio da IDE Arduino.

3.3.1 Leitura e tratamento das informações

Para realizar a comunicação do ESP-01 com a internet e com o servidor do Firebase, foi necessário a utilização de duas bibliotecas na plataforma Arduino. São elas:

- ESP8266WiFi.h

- FirebaseArduino.h

A primeira biblioteca serve para que o código feito pela IDE seja compilado e executado corretamente no microcontrolador utilizado. Já a segunda, serve para realizar a conexão com o servidor. Na figura 13 é possível observar as variáveis de configuração do microcontrolador.

```
#define FIREBASE_HOST "safeband-tcc-2019.firebaseio.com"
#define WIFI_SSID "Yuri"
#define WIFI_PASSWORD "yuri1234"
```

Fonte: Autoria própria.

Figura 13: Variáveis de configuração do ESP8266 e do servidor Firebase.

A variável *FIREBASE_HOST* contém o endereço para o dispositivo se conectar ao servidor, podendo, com isso, obter e escrever informações na base. O microcontrolador ESP8266 modelo ESP-01 não possui rede própria, necessitando de um dispositivo para que consiga acesso a internet. Com o fato de que o *smartphone* foi utilziado como roteador WiFi, as variáveis *WIFI_SSID* e *WIFI_PASSWORD* são referentes, respectivamente, ao nome da rede roteada pelo celular e a sua senha acesso.

A leitura do acionamento do botão é feita de acordo com a figura 14, de modo que essa funcionalidade é disposta no método *loop*. Dessa forma, sempre que o botão for pressionado, a condição presente nesse método será verificado, podendo alterar, ou não, o valor da variável *SAFE* na base de dados do usuário responsável pelo *hardware*.

```
void loop() {
  val = digitalRead(botton);

  if (val == LOW) {
    Firebase.set("PbEdXJYf4LPOVJLWaH39E1lhrti2/SAFE", !flagVal);
  }
}
```

Fonte: Autoria própria.

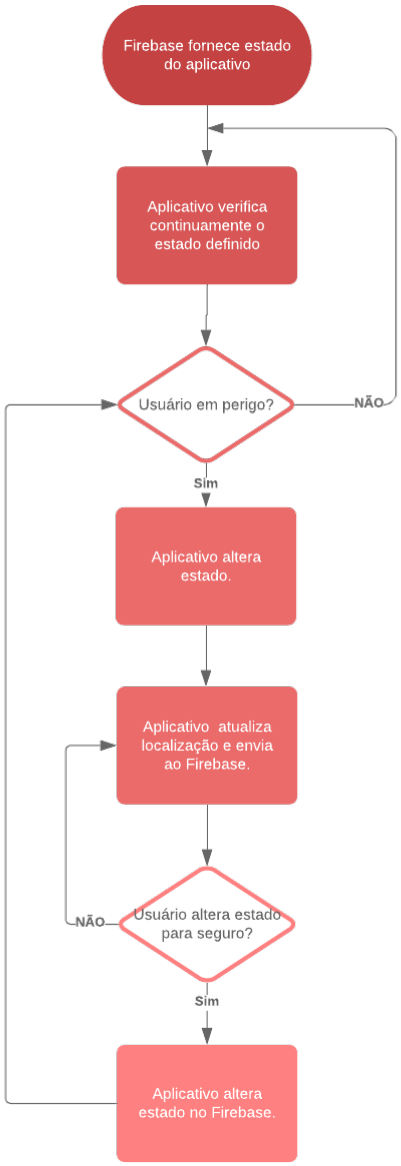
Figura 14: Método de verificação de acionamento do botão.

3.4 Prototipagem do sistema de *software*

Nesta seção será descrito o desenvolvimento do aplicativo levando em consideração o acionamento do dispositivo físico.

O elemento principal do sistema está presente no aplicativo desenvolvido, pois ele faz a manipulação dos dados, por meio da rede móvel, provenientes do servidor e graças

ao protótipo de *software* pode-se alcançar o objetivo do trabalho. A figura 15 representa o fluxograma de funcionamento do aplicativo de um usuário qualquer.



Fonte: Autoria própria.

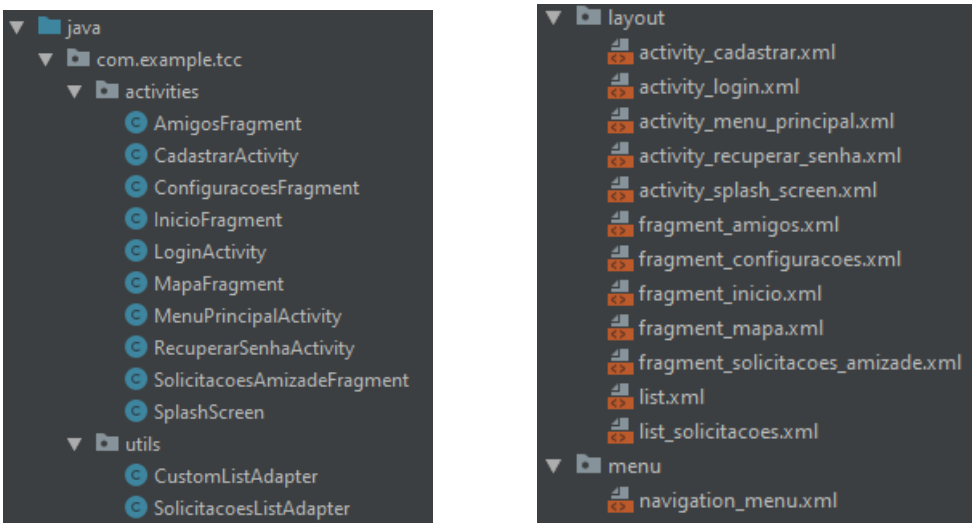
Figura 15: Fluxograma de funcionamento do aplicativo do usuário.

Ao entrar na conta cadastrada e tendo uma conexão com a internet, o aplicativo realiza a conexão com o servidor e passa a verificar continuamente o estado atual do aplicativo, fornecido pelo Firebase. Caso o usuário esteja em risco, o *software* reconhece esse estado e altera as condições no aplicativo, mudando a cor de fundo do botão central, na página de início, para vermelho. Após isso, a cada dois segundos atualiza-se as coordenadas da posição em tempo real do *smartphone* e envia essas informações para o *Realtime Database*. Esse comportamente se repete até o momento em que o usuário muda o estado para seguro, impedindo, assim, que seus amigos tenham acesso a sua localização no mapa

e volta ao passo de verificação continua da condição do usuário.

3.4.1 Estrutura das classes

O aplicativo foi desenvolvido completamente na plataforma Android, onde as classes são arquivos Java e telas de *layout* são arquivos XML, como apresentado na figura 16.



(a) Classes em java. **(b) Arquivos XML.**

Fonte: Autoria própria.

Figura 16: Estrutura de classes.

No diretório *activities*, apresenatado na figura 16a, tem-se as classes responsáveis pelo funcionamento do aplicativo, definindo como as telas deverão se comportar e como será feita a comunicação com o servidor. Ainda na mesma imagem, pode-se observar as classes no diretório *utils*, que são responsáveis pela maneira como os dados serão apresentados nas listagens das telas de lista de amigos, com a classe CustomListenAdapter, e na de solicitações, com a classe SolicitacoesListAdapter.

Na figura 16b estão representados os arquivos responsáveis pela definição da aparência das telas. Os arquivos no diretório *layout* são as definições das telas e posição dos itens em cada uma dels. O arquivo no diretório menu, contém a aparência do menu de navegação da parte inferior presente nas telas de início, amigos e configurações.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Nesta seção serão apresentados os resultados e a análise do resultados obtidos com o funcionamento do protótipo desenvolvido. Sendo assim na primeira seção, será apresentado o resultado do *hardware* (ESP8266 ESP-01 e botão). Em seguida, o aplicativo Android desenvolvido.

4.1 Comportamento do protótipo do *hadware*

O sistema físico, montado em uma *protoboard*, se mostrou funcional para os testes realizados, de modo que seu acionamento, pelos eventos identificados por meio do botão foi o gatilho para iniciar a aplicação. A alimentação desse sistema foi feita por meio de uma porta serial USB 3.0 de um computador, a qual forneceu uma tensão e corrente suficientes para funcionameto do ESP8266, cerca de 5 V e 900 mA, respectivamente.

Ao precionar o botão, o protótipo do *hardware* muda o estado de uma *flag* no Firebase, quase isntantaneamente, que é identificada pelo aplicativo, de modo acionar as funcionalidades do mesmo.

4.2 Comportamento do protótipo do *software*

O sistema de *software*, desenvolvido para a paltaforma Android, se mostrou funcional ao se acionar o sistema descrito na seção 4.1. Ao ser acionado a partir do sistema físico, o aplicativo idenfica que no banco de dados foi alterado uma *flag* que inicializa a funcionalidade principal do *app*.

Ao se iniciar a função principal do aplicativo, é enviado uma notificação para todos os usuários que estão na lista de contatos da conta em questão. A partir disso, todos esses contatos poderão ter acesso à localização em tempo real do celular do indivíduo que está em uma situação de risco, mostrando a sua localização atual até o momento em que seu funcionamento seja comprometido devido a problemas citados na seção 5.

4.2.1 Autenticação

O sistema de autenticação composto pelas telas de *login*, cadastro e recuperar senha não apresentaram problemas e cumpriram com o seus respctivos propósitos.

Na tela de *login* (Figura 1a), o usuário pode entrar no aplicativo com sua conta cadastrada, fornecendo seu endereço de *e-mail* e sua senha. Caso as informações concedidas estiverem incorretas o Firebase *Auth* retornará uma mensagem de erro ou caso alguma das informações não seja preenchida o *app* faz as devidas validações e retorna

que é necessário preencher os campos para realizar o *login*. Para as validações feitas pelo Firebase as mensagens erro são apresentadas na língua inglesa.

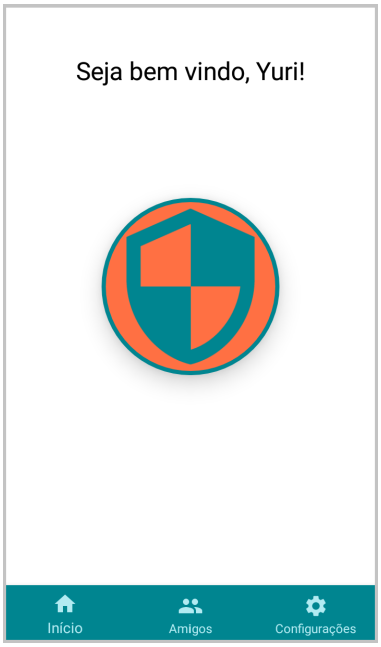
Na tela de cadastro (Figura 1b), o usuário deve fornecer o seu nome, e-mail e a senha para o aplicativo. Caso não digite algum dos campos ou digite um e-mail inválido não será possível realizar essa operação, graças à validações criadas para isso. Ao preencher corretamente todos os campos o Firebase *Auth* verifica se o e-mail fornecido já está cadastrado, de modo que o registro só é feito caso ele esteja disponível. Para as validações feitas pelo Firebase as mensagens erro são apresentadas na língua inglesa.

Na tela de recuperar senha (Figura 1c), o usuário tem a opção de recuperar a senha informando seu *e-mail* de cadastro. Com isso, ao clicar no botão de "Recuperar Senha" o Firebase *Auth* gerencia a recuperação da senha, enviando um link para o endereço de *e-email* cadastrado que possibilita o usuário inserir uma nova chave de acesso para o aplicativo.

Ao passar por vários testes, essas três funcionalidades se mostraram operantes para os seus propósitos.

4.2.2 Aplicação

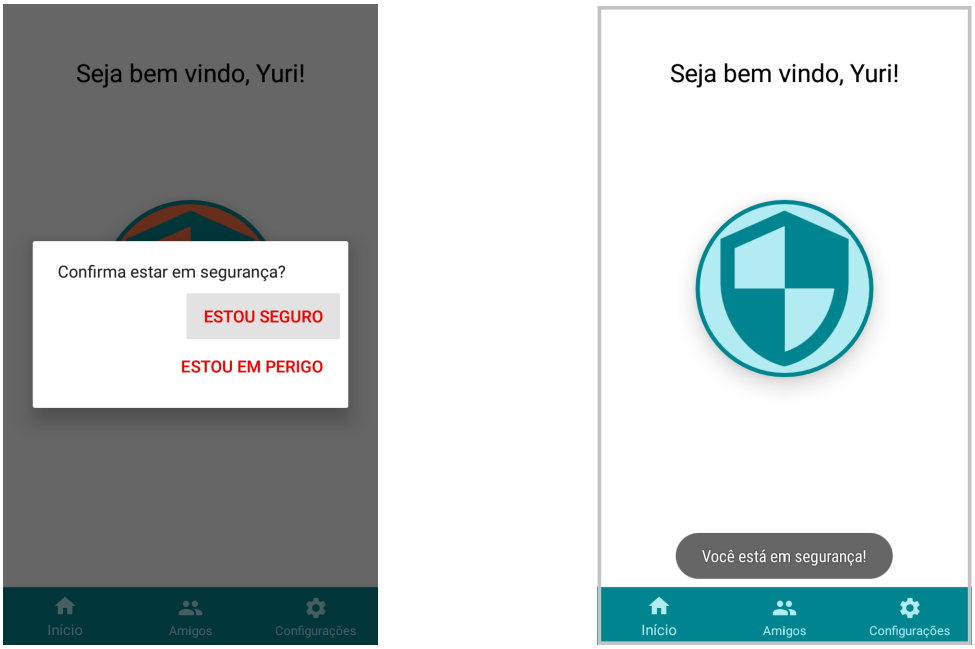
Como mencionado na seção 1.5 na tela de início do aplicativo é apresentado a situação atual do usuário por meio da cor de fundo do botão central. Ao acionar o dispostivo físico, mencionado na seção 4.1, o botão muda de cor conforme apresentado na figura 17.



Fonte: Autoria própria.

Figura 17: Tela de início informando situação de perigo do usuário.

Ao precionar o botão central, o usuário pode determinar se está seguro ou está em uma situação de risco, podendo assim, alterar o estado atual no aplicativo, conforme a figura 18.

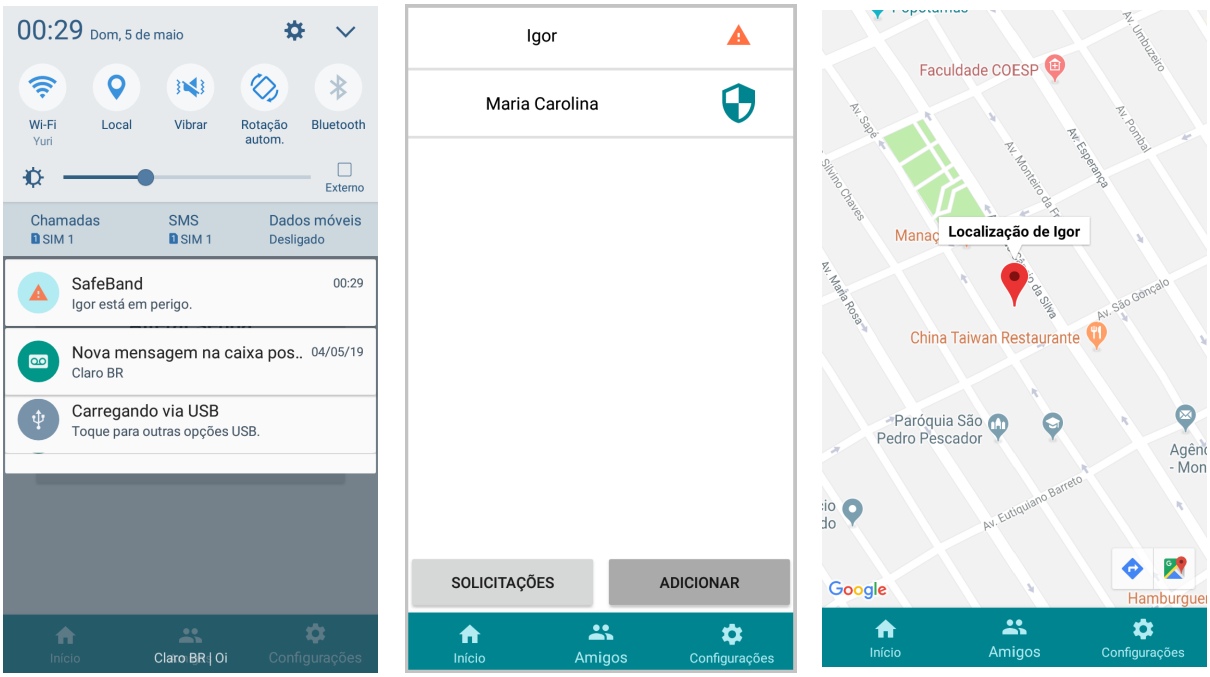


(a) Modal de definição do estado atual. **(b) Estado atual alterado.**

Fonte: Autoria própria.

Figura 18: Mudança de estado do aplicativo.

Na tela de amigos, todas as funcionalidades também funcionaram corretamente com relação aos seus objetivos. Na figura 19 podemos observar foi informado a situação de risco do contato adicionado como amigo e ao clicar em seu nome temos acesso a sua localização em tempo real, cumprindo o objetivo do trabalho. Quando um contato da lista de amigos aciona o estado de perigo no aplicativo, uma notificação é apresentada na tela de todos os seus contatos para informar essa mudança de condição, representado na figura 19a. Na tela de amigos, o ícone de um contato em risco é alterado, como mostrado na figura 19b, e dessa forma pode-se clicar no nome do mesmo e apresentando a sua localização em tempo real no mapa, como mostrado na figura 19c.



(a) Notificação de amigo em perigo. **(b) Amigos.** **(c) Marcação do amigo em perigo no mapa.**

Fonte: Autoria própria.

Figura 19: Localização de uma amigo em perigo em tempo real.

Por fim, as funcionalidades que constam na tela de configurações também apresentaram seus devidos funcionamentos de maneira correta.

5 CONCLUSÕES E TRABALHOS FUTUROS

No presente trabalho foi apresentado um protótipo de um sistema de segurança, que ao ser acionado passa a emitir a localização do *smartphone* em tempo real e exibido para os contatos do aplicativo. Esse sistema não garante a proteção do usuário, mas seu funcionamente permite com que as autoridades tenham uma ação para solucionar a eventual situação de perigo em que o usuário se encontra.

O protótipo funcionou como esperado, porém seu funcionamento pode ser prejudicado em situações em que o telefone móvel não possua conexão com a internet, ou ainda se o mesmo não esteja com a funcionalidade de localização ativada, impedido o aplicativo de capturar a posição do dispositivo por meio do GPS. Outra falha encontrada no protótipo acontece quando o celular não realiza o roteamento de internet para o dispositivo de *hardware*, fazendo com que ele não consiga realizar a comunicação com o serviço do Firebase para informar a possível situação de risco.

Uma dificuldade encontrada durante a implementação do projeto foi gerenciamento dos dados armazenados no Firebase. Por se tratar de uma ferramenta com armazenamento limitado de informações, foi utilizado uma lógica a qual administra os dados referentes as posições determinadas pelo GPS. Sem esse controle, eventualmente esse limite máximo de dados seria alcançado, o que impossibilitaria o uso do sistema desenvolvido da maneira esperada.

Apesar das falhas e dificuldades encontradas, o protótipo se mostrou funcional para o objetivo idealizado. Isso se deve pelo fato do sistema fornecer a localização em tempo real dos usuários que informaram, através do dispositivo físico, estar em uma situação de risco, mostrando para os contatos da lista de amigos o trajeto o qual o *smartphone* percorreu a partir do momento de acionamento do *hardware*.

Para trabalhos futuros, pode-se fazer o protótipo virar um produto, simplificando o dispositivo físico para ficar com um tamanho compacto e discreto. Para isso será necessário um estudo e investimento para que esse *hardware* possua uma conexão própria com a internet, por meio de um módulo 2G/3G, e também uma bateria que suprisse o consumo de energia desse dispositivo. Outra proposta para trabalhos futuros é utilizar inteligencia artificial no aplicativo com a finalidade do sistema identificar padrões de rotas percorridas pelo usuário e alertar aos contatos quando é realizada algum trajeto totalmente fora do padrão.

REFERÊNCIAS

ABÍLIO, M. I. R. Globalização: características mais importantes. ***Revista Visões***, 2007. Disponível em: ⟨http://www.fsma.edu.br/visoes/ed03/3ed_artigo1.pdf⟩.

ANDROID. *Recursos do Android Studio*. 2019. Disponível em: ⟨https://developer.android.com/studio/features⟩. Acesso em: abr. 2019.

ARDUINO, S. A. Arduino. *Arduino LLC*, 2015.

BOFF, W. M. Sistema de alarme conectado via redes móveis para monitoramento e segurança de veículos automotivos através de aplicativo de telefone celular. 2017.

COMER, D. E. *Redes de Computadores e Internet-6*. [S.l.]: Bookman Editora, 2016.

CRAIG, C.; GERBER, A. *Learn Android Studio: Build Android Apps Quickly and Effectively*. [S.l.]: Apress, 2015.

DIAS, K. L.; SADOK, D. F. H. Internet móvel: tecnologias, aplicações e qos. *XIX Simpósio Brasileiro de Redes de Computadores*, 2001.

DRIRA, A. Gps navigation for outdoor and indoor environments. *University of Tennessee, Knoxville*, Citeseer, 2006.

EL-RABBANY, A. *Introduction to GPS: the global positioning system*. [S.l.]: Artech house, 2002.

G1. *Cerberus: aplicativo de segurança pessoal permite compartilhar localização em tempo real com os amigos e pedir socorro pelo celular*. 2018. Disponível em: ⟨http://g1.globo.com/tecnologia⟩. Acesso em: mar. 2019.

GOOGLE. *Firebase*. 2019. Disponível em: ⟨https://firebase.google.com/⟩. Acesso em: abr. 2019.

GUIMARÃES, D. A. Introdução às comunicações móveis. *Revista INATEL Telecomunicações*, v. 1, n. 01, 1998.

KHAWAS, C.; SHAH, P. Application of firebase in android app development-a study. *International Journal of Computer Applications*, 2018.

OLIVEIRA, J. S. d. As tecnologias da informação e comunicação na gestão administrativa e operacional da segurança pública. 2015.

PEREIRA, M. M.; GUEDES, L. G. d. R. Perspectivas das comunicações móveis no brasil. *Revista Digital Online*, v. 2, p. 25–41, 2004.

PEREZ, F. Redes móviles terrestres 4g. *Esc. Técnica Super. Ing. Univ. Pontif. Comillas*, p. 1–12, 2010.

PIROTTI, R. P.; ZUCCOLOTTO, M. Transmissão de dados através de telefonia celular: arquitetura das redes gsm e gprs. *Revista Liberato, Novo Hamburgo*, v. 10, n. 13, p. 81–89, 2009.

PLATFORM, E. S. C. Esp8266. *Espressif Systems*, 2013.

SOARES, L. E. Segurança pública: presente e futuro. *Estudos avançados*, SciELO Brasil, v. 20, n. 56, p. 91–106, 2006.

SOUZA, E. R. d.; LIMA, M. L. C. d. Panorama da violência urbana no brasil e suas capitais. *Ciência Saúde Coletiva*, SciELO Public Health, v. 11, p. 1211–1222, 2006.

STONEHEM, B. *Google Android Firebase: Learning the Basics*. [S.l.]: First Rank Publishing, 2016. v. 1.

TANENBAUM, A. S. *Redes de computadores Quarta edição*. [S.l.: s.n.], 2002.

UBER. *Compromisso com a segurança*. 2018. Disponível em: ⟨https://www.uber.com/pt-BR/safety/⟩. Acesso em: fev. 2019.