UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ

***CAMPUS* LUIZ MENEGHEL**

GUSTAVO FONTOLAN

UMA APLICAÇÃO PARA DISPOSITIVOS MÓVEIS INTEGRADA COM UM DISPOSITIVO TOKEN PARA PROTEÇÃO EM CASO DE PERDA OU ROUBO

Bandeirantes
2016

Gustavo Fontolan

UMA APLICAÇÃO PARA DISPOSITIVOS MÓVEIS INTEGRADA COM UM DISPOSITIVO TOKEN PARA PROTEÇÃO EM CASO DE PERDA OU ROUBO

Trabalho de Conclusão de Curso submetido a Universidade Estadual do Norte do Paraná, como requisito parcial para a obtenção do grau de Bacharel/Licenciatura em Sistemas de Informação.

Orientador: Prof. Ricardo Gonçalves Coelho

Bandeirantes

2016

Gustavo Fontolan

Uma aplicação para dispositivos móveis integrada com um dispositivo token para proteção em caso de perda ou roubo

Trabalho de Conclusão de Curso submetido à Universidade Estadual do Norte do Paraná, como requisito parcial para a obtenção do grau de Bacharel/Licenciatura em Sistemas de Informação.

COMISSÃO EXAMINADORA

_____
Prof. Ricardo Gonçalves Coelho
UENP – *Campus* Luiz Meneghel

_____
Prof. Glauco Carlos Silva
UENP – *Campus* Luiz Meneghel

_____
Prof. Bruno Squizato Faiçal
UENP – *Campus* Luiz Meneghel

Bandeirantes, 11 de julho de 2016

Para Família, Amigos e
Professores...

AGRADECIMENTOS

Agradeço primeiramente a Deus por ser a base durante o período da graduação e de todos os momentos de minha vida, também agradeço a minha família e amigos, pois foram eles que nunca me deixaram desistir durante essa vida universitária cheia de desafios e batalhas.

A universidade pelos professores, a direção e a administração, pois através deles que foi possível a realização dos meus estudos, permitindo o meu avanço acadêmico e profissional, sou muito grato a todos. Gostaria de agradecer em especial, o meu orientador Prof. Ricardo Gonçalves Coelho pelo empenho e dedicação durante à elaboração deste trabalho e também a banca examinadora pelo tempo e dedicação na melhora do trabalho.

Aos meus pais, pelo amor, incentivo e apoio incondicional, ao meu pai pelo incentivo e apoio, a minha mãe, pelo amor durante os dias mais difíceis e a minha irmã que mesmo não falando muito, significa muito para mim, assim como toda a minha família.

Agradeço a todas as pessoas que de alguma forma, direta ou indiretamente, fizeram parte da minha formação, muito obrigado por tudo.

Não fui eu que lhe ordenei? Seja forte e corajoso!
Não se apavore, nem se desanime,
pois o Senhor, o seu Deus, estará com você
por onde você andar". (***Josué 1:9***)

RESUMO

Neste trabalho é apresentada uma aplicação para auxiliar na proteção de dispositivos eletrônicos contra perda e roubos desenvolvida em Android, que realizará a comunicação com o protótipo do token feito em Arduino através do Bluetooth, baseando na disponibilidade do token para a ativação da proteção do aparelho. Para auxiliar no desenvolvimento, algumas ferramentas para modelagem foram utilizadas durante o processo, como o Astah para a criação dos diagramas de classe e caso de uso, o Fritzing para a construção do sketch do Arduino, exibindo visualmente a estrutura do protótipo do token e a ferramenta Bizagi utilizada na descrição visual do processo de ativação da segurança no aplicativo. A aplicação se destaca com a forma em que é feito a ativação da segurança do aparelho de modo automático, ficando independente de ação do usuário ou de um acesso à rede, tornando assim o processo mais eficiente e se diferenciando dos aplicativos já existentes.

Palavras-chave: Android; Arduino; Bluetooth.

ABSTRACT

This paper presents an application to help protect electronic devices against loss and theft developed Android, which will make communication with the token prototype made in Arduino via Bluetooth, based on the token availability for device protection activation. To assist in the development, some modeling tools were used during the process, as Astah to create class diagrams and use case, the Fritzing for the construction of the Arduino sketch, visually displaying the token of the prototype structure and Bizagi tool used in visual description of the application security activation process. The application stands out in the way that is done the activation of security automatically set, being independent of user action or a network access, thus making the process more efficient and differentiating existing applications.

Key-words: Android; Arduino; Bluetooth.

Lista de ilustrações

Figura 1 - Estatísticas de roubo (Curitiba-PR).....6
Figura 2 - Aplicação Prey Anti-Theft.....7
Figura 3 - Aplicação Android Lost 8
Figura 4 - Arquitetura de comunicação 22
Figura 5 - Protótipo do Token.....23
Figura 6 – Fluxograma do processo de ativar segurança 24
Figura 7 - Exemplo de múltiplas conexões.....25
Figura 8 - Diagrama de classe da aplicação Android 26
Figura 9 - Diagrama de caso de uso da aplicação Android 26
Figura 10 - Tela inicial para ativar a segurança.....36
Figura 11 - Tela inicial com o menu lateral.....37
Figura 12 - Listagem dos alarmes disponíveis 38
Figura 13 - Tela para edição do tempo do alarme.....39
Figura 14 - Listagem dos tokens 40
Figura 15 - Tela para adicionar um novo token 41
Figura 16 - Listagem dos amigos 42
Figura 17 - Tela para adicionar um novo amigo 43
Figura 18 - Tela para descrição do aplicativo.....44

Lista de tabelas

Tabela 1 - Comparativo entre Wi-Fi Direct e Bluetooth 19

Lista de siglas

GPS Global Positioning System

IDE Integrated Development Environment

LED Light Emitting Diode

P2P Peer-To-Peer

Wi-Fi Wireless Fidelity

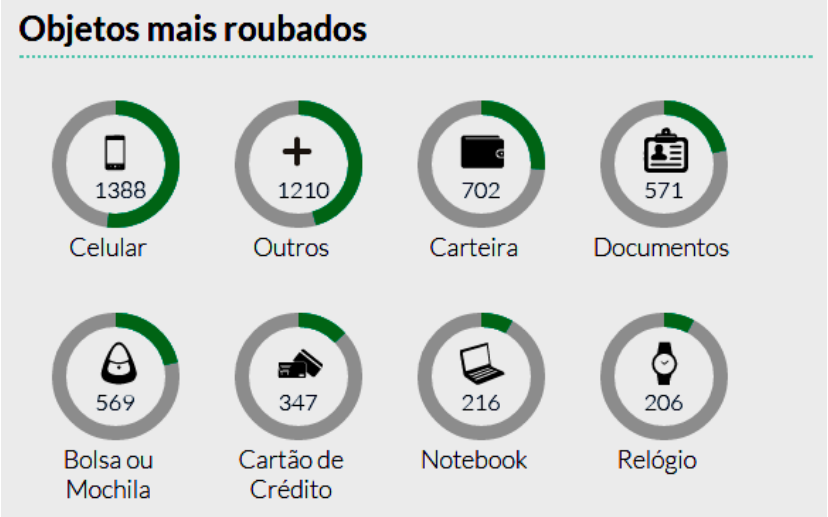
Sumário

1. Introdução 6
1.1 Problema 8
1.2 Justificativa 9
1.3 Objetivos 9
1.3.1 Objetivos específicos 10
1.4 Organização do trabalho 10
2. Fundamentação Teórica 11
2.1 Wi-Fi Direct 11
2.2 Bluetooth 15
2.3 Comparativo das tecnologias 17
3. Desenvolvimento 20
3.1 Android 20
3.2 Arduino 21
3.3 Arquitetura do sistema 21
3.3.1 Descrição dos diagramas de casos de uso 27
4. Conclusão e trabalhos futuros 45
Referências 47

1. Introdução

O número de perdas e furtos de celular tem crescido gradativamente com o passar do tempo, com isso, a quantidade de celular bloqueados também aumenta. Os celulares são os dispositivos pessoais que ganham o ranking de objetos mais roubados, ultrapassando os cartões de crédito e demais objetos de valor. Na Figura 1 é apresentado o número de celulares roubados na região de Curitiba-PR, ficando acima de relógios, com 206 itens e carteiras com um pouco mais de 700 itens.

Figura 1 - Estatísticas de roubo (Curitiba-PR)



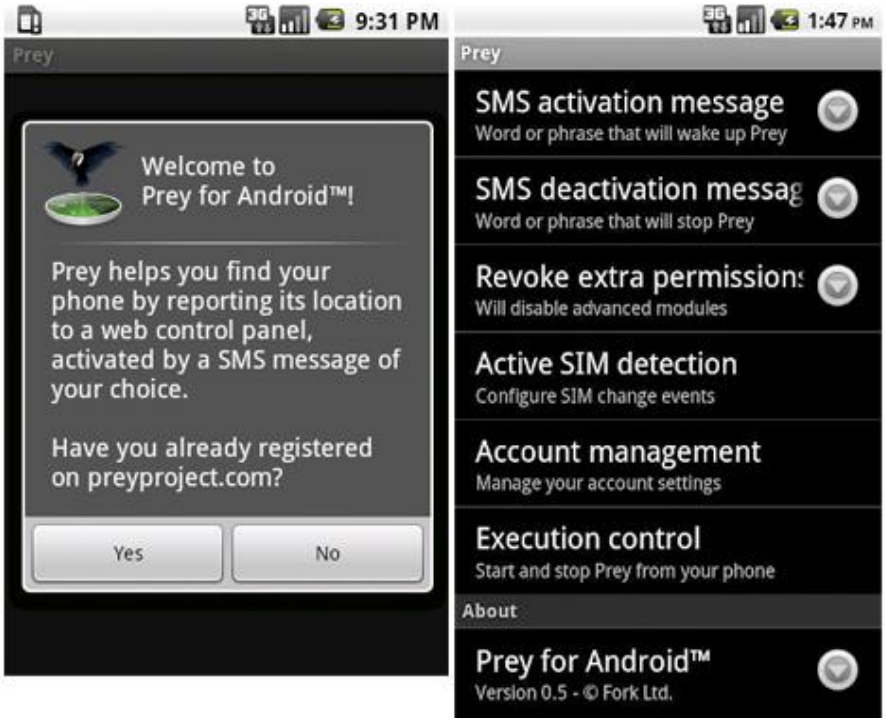
Fonte: Onde fui roubado, 2016

Aplicativos são desenvolvidos para combater esse tipo de pratica de furto com celulares, que propõe como funcionalidades o bloqueio do aparelho, alarme sonoro, apagar todos os dados do cartão de memória, nomes de contatos, mensagens, aplicativos e também a localização do smartphone via GPS por serviços online. Os aplicativos analisados e apresentados a seguir, funcionam de forma única, sem um outro agente externo do aparelho celular para auxiliar na ativação dos modos segurança, fazendo com que o usuário dependa somente do aplicativo para a proteção do seu dispositivo móvel.

Agrela (2012) apresenta em sua pesquisa sobre aplicações desenvolvidas para esta funcionalidade, que seria o Prey Anti-Theft mostrado na Figura 2, é um aplicativo muito leve, tem pouco mais de 2 MB e, depois de ser instalado, roda escondido no aparelho. Caso ele seja roubado ou perdido, o usuário pode acessar um painel de controle no site do Prey e marcar o dispositivo como perdido. Outro exemplo é Android Lost na Figura 3, que permite o usuário bloquear o celular, limpar

dados, localização pelo GPS, controlar a câmera, acessar mensagens de texto, disparar um alarme e programar o envio de mensagens de texto.

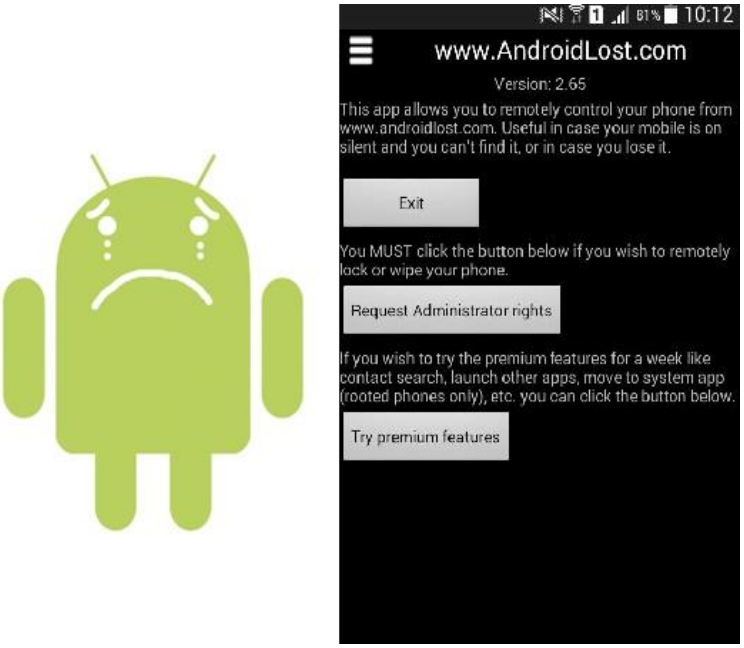
Figura 2 - Aplicação Prey Anti-Theft



Fonte: Abril, 2012

Ações como ativar ou desativar o GPS e o WiFi, fazer soar o alarme ou exibir uma mensagem na tela demoram poucos segundos para ser executadas quando celular está numa rede Wi-Fi e, mesmo no 3G, o tempo não aumenta tanto.

Figura 3 - Aplicação Android Lost



Fonte: Autor, 2016

Um ponto a ser destacado entre os aplicativos mostrados é que ambos dependem de uma rede de conexão para receber as solicitações de execução dos mecanismos de segurança.

1.1 Problema

As aplicações e mecanismos desenvolvidos com o foco para segurança de dispositivos, desde o rastreamento até as funções que formatam o celular por completo, enfrentam problemas em suas execuções e funcionalidades.

Um dos maiores problemas enfrentados pela maioria dos cidadãos quando o celular é roubado ou perdido, é o fato de eles possuem aplicativos em seus aparelhos para que estes sejam bloqueados, porém não possuem acesso à rede de internet, impossibilitando que o proprietário consiga enviar a solicitação de bloqueio do aparelho para que ele seja bloqueado.

Mesmo que o indivíduo de alguma forma consiga solicitar o bloqueio do aparelho, a conexão ao aparelho celular é um requisito imprescindível para ativar os mecanismos de segurança nele existente, pois se não for possível estabelecer uma conexão, o bloqueio do aparelho não será efetivado.

Falhas tecnológicas são os principais problemas para a concretização do bloqueio, no entanto há outro fator que pode afetar a eficiência da aplicação de

bloqueio, isso ocorre quando ele é roubado e a reação de algumas pessoas é entrar em estado de choque, ficando impossibilitadas de realizar qualquer tipo de ação.

Selye (1974-1976) explicava em suas teses sobre estímulos sensoriais e psicológicos que em certos casos, uma pessoa que se depara com uma situação de agressão, vivencia um alto nível de estresse no momento e logo após o acontecimento, mas tende a voltar seus padrões psicológicos e de ação normal com o passar do tempo. Tendo em vista que o aparelho pode não estar mais disponível para uma conexão, por ter sido desligado, impossibilitando a realização do bloqueio.

1.2 Justificativa

Requisitos tecnológicos são alguns dos problemas apresentados que impossibilitam os mecanismos de segurança serem efetivados, pois estes são dependentes do acesso ao celular para que a aplicação consiga executar as suas funcionalidades.

O uso de apenas uma aplicação para realizar a segurança do aparelho raramente será suficiente ou eficaz. Melhorias na arquitetura e na forma de ativação das funcionalidades da aplicação poderiam garantir que os mecanismos de segurança tenham uma melhora na garantia no bloqueio do aparelho.

Benefícios poderão ser alcançados com o desenvolvimento de um aplicativo que tenha interação com um dispositivo de nome de token funcionaria como uma chave, tendo maior garantia das funcionalidades, com isso o bloqueio do celular seria algo eminente após a perda ou o roubo do aparelho já que o mecanismo de segurança seria ativado assim que o celular perdesse a conexão com o dispositivo token.

1.3 Objetivos

O principal objetivo do trabalho é apresentar uma aplicação de segurança integrada com um dispositivo token, que permita o usuário ter um mecanismo de segurança com maior eficiência caso o aparelho celular venha ser perdido ou furtado.

A utilização do token em conjunto com o aplicativo permite bloquear o celular de forma automática, caso o mesmo venha ser furtado ou até mesmo perdido, através de mecanismos de segurança que poderão ser definidos na aplicação

instalada no celular, proporcionando uma zona de segurança para o aparelho, pois caso o dispositivo se distancie, o mecanismo de segurança é ativado, emitindo a localização para outro celular e até mesmo um alarme, auxiliando na localização do mesmo.

1.3.1 Objetivos específicos

- Propor um protótipo de token em Arduino
- Desenvolver uma aplicação Android para segurança
- Realizar a integração da aplicação com o dispositivo token

1.4 Organização do trabalho

Esta seção apresenta como o trabalho é organizado. A Seção 2 são descritos os fundamentos para a criação do projeto, com as tecnologias para comunicação, Wi-Fi Direct, Bluetooth e um comparativo entre elas, na Seção 3 é apresentado o desenvolvimento utilizado para a realização do projeto e por último a conclusão do projeto na Seção 4.

2. Fundamentação Teórica

Neste capitulo serão abordados conteúdos para o funcionamento da aplicação no contexto de transmissão de informações, apresentando os principais conceitos sobre Wi-Fi Direct e Bluetooth e por último é apresentado uma tabela comparativa das características entre as redes.

2.1 Wi-Fi Direct

A Wi-Fi Alliance anunciou uma nova especificação de rede sem fio Wi-Fi Direct, que permite a comunicação direta ponta-a-ponta entre dispositivos sem a necessidade de dispositivos de gerenciamento. (MORITZ; ZEEB; PRÜTER, 2010)

Em uma rede típica de Wi-Fi, os clientes procuram e associam-se a WLANs, que são criados e anunciados por um ponto de acesso, a grande novidade do Wi-Fi Direct é que esses papéis são especificados de forma dinâmica, portanto, um dispositivo Wi-Fi Direct pode implementar tanto o papel de um cliente e o papel de um ponto de acesso.

Dispositivos com o Wi-Fi Direct, eram conhecidos anteriormente como dispositivos de rede P2P, comunicavam-se através do estabelecimento da comunicação em grupos P2P, que funcionam da mesma maneira e até mesmo equivalentes as redes tradicionais de infraestrutura Wi-Fi. (CAMPS-MUR; GARCIA-SAAVEDRA; SERRANO, 2013)

A Wi-Fi Alliance desenvolveu o Wi-Fi Direct para introduzir uma nova opção de tecnologia para conectividade que não segue o modo de infraestrutura tradicional, o seu funcionamento é feito das seguintes formas, os dispositivos podem se conectar a qualquer dispositivo que aceitam os pedidos comunicação, incluindo dispositivos legados, comunicando de forma efetiva mesmo com software definidos para AP (Access Point). A segurança é feita pelo Wi-Fi Protected Setup e WPA2 ™ - Personal, que são bem adequados para garantir o tráfego de informações locais, mas não fornecem recursos de segurança de nível empresarial. (ALLIANCE, 2016)

O Wi-Fi Direct foi projetado para fornecer conectividade local entre dispositivos usando métodos de segurança de configuração WPA2-Personal e Wi-Fi Protected. Esses métodos foram desenvolvidos para proteger redes residenciais. O Wi-Fi Direct não suportar WPA2-Enterprise, que é comumente usado em empresas

com uma estrutura de autenticação centralizada a gestão do fornecimento de credenciais para autenticar dispositivos móveis para a rede. (ALLIANCE, 2015)

Os dispositivos Wi-Fi Direct, são formalmente conhecidos como dispositivos P2P, que realizam a comunicação através da formação de grupos P2P, que são funcionalmente equivalentes as redes de infraestrutura Wi-Fi tradicionais. O dispositivo que implementar a funcionalidade AP (Access Point) no Grupo P2P é referido como o Proprietário do Grupo P2P (P2P GO), e dispositivos agindo como clientes são conhecidos como Clientes P2P. Dado que esses papéis não são estáticos, quando dois dispositivos P2P descobrir o outro negociam seus papéis (Cliente P2P e Proprietário do Grupo P2P) para estabelecer um Grupo P2P. Uma vez que o Grupo P2P é estabelecida, outros clientes P2P podem se juntar ao grupo como em uma rede Wi-Fi tradicional. (CAMPS-MUR; GARCIA-SAAVEDRA; SERRANO, 2013)

Existem várias maneiras em que dois dispositivos podem estabelecer um grupo de P2P, dependendo se eles têm para negociar o papel de P2P GO, ou se há alguma informação disponível já compartilhada anteriormente sobre segurança, para a formação da comunicação entre dispositivos através do Wi-Fi Direct, existe o caso mais complexo dos casos descrito como o Standard Case e os outros casos mais simples nomeados de Autonomous e Persistent Cases. (CAMPS-MUR; GARCIA-SAAVEDRA; SERRANO, 2013)

O Standard Case os dispositivos P2P tem primeiro de descobrir um ao outro, e em seguida, negociar qual dispositivo que vai atuar como Proprietário do Grupo P2P. Os dispositivos Wi-Fi Direct geralmente começam realizando uma varredura tradicional Wi-Fi (ativa ou passiva), por meio do qual eles podem descobrir os Grupos P2P e redes Wi-Fi existentes. Após esta análise, o algoritmo Discovery é executado.

Primeiramente o dispositivo P2P seleciona um dos chamados canais de comunicação, nomeado os canais 1, 6 ou 11 na faixa de 2,4 Ghz, sendo os seus canais de escuta. Em seguida, ele alterna entre dois estados: um estado de busca, em que o dispositivo realiza varredura ativa, enviando Probe Requests em cada um dos canais de comunicação; e um estado de escuta, em que o dispositivo de escuta os Probe Requests em seu canal de escuta para responder com Probe Requests. A quantidade de tempo que um dispositivo P2P gasta em cada estado é distribuído

aleatoriamente, tipicamente entre 100 ms e 300 ms, mas cabe à cada implementação de decidir sobre o mecanismo a troca para o tempo de descoberta com a poupança de energia através dos intervalos de ciclos de dormir no processo de descoberta.

Uma vez que os dois dispositivos P2P encontraram um ao outro, eles começam a fase de Negotiation Phase Group Owner. Isto é implementado usando um aperto de três vias, nomeadamente solicitação de negociação para Proprietário do Grupo / Resposta / Confirmação, para que os dois dispositivos entre em acordo sobre qual dispositivo irá funcionar como P2P GO e em qual canal o grupo irá operar, que pode ser em a 2,4 GHz ou 5 GHz.

Após os dispositivos terem descoberto um ao outro e chegaram a um acordo sobre os respectivos papéis, a próxima fase é o estabelecimento de uma comunicação segura usando Wi-Fi Protected Setup, que é chamada como fase WPS Provisioning e finalmente, uma troca de DHCP para configurar a configuração de IP.

No caso Autonomous o dispositivo P2P pode autonomamente criar um Grupo P2P, onde ele imediatamente se torna o Proprietário do Grupo P2P, sentando-se em um canal e começar o Beacon. Outros dispositivos podem descobrir o grupo estabelecido utilizando mecanismos tradicionais de busca, em seguida, começar diretamente com a fase WPS Provisioning e as fases de configuração de endereço. Em comparação com o caso anterior a fase de descoberta é simplificada, neste caso, como é o dispositivo que cria o grupo, ele não alterna entre os estados e não é necessária a fase de Negotiation Phase GO.

Durante o processo Persistent a formação do grupo é feita pelos dispositivos P2P que podem declarar um grupo como persistente, usando uma bandeira nas Capabilities P2P que é atributo presente em Beacon frames, Probe Responses e GO Negotiation Frames. Desta forma, os dispositivos formam as credenciais para o grupo rede e o GO P2P é atribuído e os papéis de Cliente são instanciados subsequentes no grupo P2P. Especificamente, após a fase de descoberta, se um dispositivo P2P reconhece ter formado um grupo persistente correspondente a um ponto no passado, qualquer um dos dois dispositivos P2P pode usar o procedimento de convite para rapidamente recriar o grupo. O Standard Case assume-se como linha de base e a fase Negociação do Proprietário do Grupo é substituído pela troca

de convites, e a fase de WPS Provisioning é significativamente reduzida, porque as credenciais de rede armazenados podem ser reutilizadas.

A comunicação direta de dispositivos e a grande capacidade de transmissão sem a necessidade de fios são algumas das vantagens proporcionadas pela utilização da rede Wi-Fi Direct, outro ponto a ressaltar sobre a qualidade da tecnologia é o seu mecanismo de economia de energia, que emprega dois mecanismos responsáveis para gerenciar o consumo.

Wi-Fi Direct possui dois mecanismos de economia de energia: o Opportunistic Power Save e NoA (**N**otice **o**f **A**bsence).

A ideia básica do Opportunistic Power Save é aproveitar os períodos de sono dos clientes P2P (**P**eer **t**o **P**eer). O mecanismo possui um protocolo de economia de energia que funciona da seguinte maneira.

O proprietário do grupo P2P anuncia uma janela de tempo, denominada CTWindow, entre cada Beacon e Probe Response Frames. Esta janela especifica a quantidade de tempo mínimo após a recepção de um Beacon, o proprietário do grupo P2P e os clientes P2P vão permanecer acordados, para iniciar o processo economia de energia. Se após a CTWindow o proprietário do grupo P2P determina que todos os clientes conectados estão em estado de doze, ou porque anunciou uma mudança para esse estado através do envio de uma mensagem com o PM (**P**ower **M**anagement) bit definido como 1, ou porque eles já estavam no estado de cochilo durante o intervalo de Beacon anterior, o proprietário do grupo P2P pode entrar no modo soneca até a próxima Beacon programada, caso contrário, se um cliente P2P permanecer no modo de poupança de energia, o proprietário do grupo P2P é forçado a ficar acordado até que todos os clientes P2P entrem no modo de poupança de energia. (CAMPS-MUR; GARCIA-SAAVEDRA; SERRANO, 2013)

O segundo mecanismo empregado na economia de energia é o NoA (**N**otice **o**f **A**bsence) que é descrito da seguinte forma.

O protocolo permite que um proprietário do grupo P2P possa definir intervalos de tempo, referidos como períodos de ausência, onde os clientes P2P não estão autorizados a acessar o canal, independentemente de se eles estão no modo economia de energia ou no modo ativo. Desta forma, um proprietário do grupo P2P pode autonomamente decidir desligar a comunicação para economizar energia.

Como no protocolo Opportunistic Power Save, no caso de NoA o proprietário do grupo P2P define períodos de ausência com um elemento de sinalização incluídos em mensagens de Beacon e Probe Responses.

O proprietário do grupo P2P define uma programação NoA usando quatro parâmetros: (i) a duração de cada período de ausência, (ii) intervalo que especifica o tempo entre os períodos de ausência consecutivos, (iii) tempo de início que especifica o início tempo do primeiro período de ausência após o Beacon atual, e (iv) a contagem que especifica quantos períodos de ausência será agendada durante o NoA atual. (CAMPS-MUR; GARCIA-SAAVEDRA; SERRANO, 2013)

2.2 Bluetooth

Bluetooth é uma tecnologia de rede destinado a aplicações de baixa potência e de curta transmissão. Ele foi inicialmente desenvolvido pela Ericsson, mas é governada de forma aberta pelo Bluetooth SIG (**S**pecial **I**nterest **G**roup). Bluetooth é uma proposta de padrão para curto alcance, de comunicação sem fio de baixa potência.

Não há conexões de cabo entre estes dispositivos Bluetooth, permitindo a comunicação perfeita entre todos eles, substituindo o que hoje é feito através de uma combinação de cabos seriais e paralelos, e ligações de dispositivos com conexão infravermelho. (SINGH; SHARMA; AGRAWAL, 2011)

Devido à sua robustez, o custo dos dispositivos são relativamente baixo e com a comunicação de custo livre, não necessitando de autorização para ser utilizada, por conta disso o Bluetooth é muito utilizado. Muitos telefones móveis modernos usam Bluetooth como um recurso padrão para comunicar com computadores ou outros dispositivos. Em carros e caminhões, o Bluetooth é utilizado para estabelecer chamadas telefónicas sem a necessidade das mãos ou outra comunicação multimídia. Portanto, na maioria dos dispositivos portáteis os transmissores Bluetooth estão sempre ligados, podendo realizar a comunicação com outros dispositivos possíveis a qualquer momento. (MARGREITER; ZEH; SPANGLER, 2015)

A vantagem de utilização de uma rede Bluetooth é a sua economia de consumo, permitindo o uso de um dispositivo por maior tempo e também a sua

facilidade de não precisar utilizar fios em sua comunicação, que é feita por frequências de rádio.

O que torna o Bluetooth realmente atraente é que ele automaticamente controla o processo de comunicação entre dispositivos. Varrendo a área em volta na busca por outros dispositivos Bluetooth e, permitindo estabelecer uma conexão entre os dispositivos descobertos. Quando um dispositivo é encontrado, uma mensagem é criada para informar a existência da rede Bluetooth, denominada piconet, que é propagada entre os dispositivos criando uma rede de comunicação.

O Bluetooth foi feito pensando-se em segurança, oferecendo serviços como autenticação, criptografia, qualidade de serviço e outros recursos de segurança. No entanto, a tecnologia ainda está vulnerável em vários aspectos, abrindo portas para ataques. (KOVACS; MONTEIRO, 2007)

De acordo com Bluetooth (2016), o Bluetooth pode operar tanto em BR (**B**asic **R**ate) e EDR (**E**nhanced **D**ata **R**ate), através de uma camada física que opera sem a licença de banda ISM a 2.4GHz, possuindo um sistema com a finalidade de combater interferências e perca de informações, no entanto o Basic Rate suporta uma taxa de transmissão de até 1 Mbps já o Enhanced Data Rate consegue suportar 2Mb/s.

O Bluetooth define não apenas uma interface de rádio, mas uma pilha de comunicação inteira que permite que os dispositivos possam encontrar outro e anunciar os serviços que eles oferecem. O controle fornece uma interface de comando para o Link Manager e os Baseband Levels, proporcionando assim uma interface coerente para hardware desenvolvidos por diferentes fabricantes.

O L2CAP (**L**ogical **L**ink **C**ontrol **A**daptation **P**rotocol) fornece uma camada orientado a conexão e serviços sem conexão para os níveis superiores. Suas funções incluem: i) protocolo de multiplexação, que é necessário porque o protocolo Baseband não inclui um campo "tipo" para a identificação da origem do pacote a partir dos níveis superiores; ii) segmentação e remontagem das unidades de dados de protocolo provenientes dos níveis superiores; e iii) QoS (**Q**uality **o**f **S**ervice) para apoio. É possível implementar um IP diretamente no L2CAP, mas no Bluetooth 1.1 não é possível definir um perfil com esta facilidade. (FERRO; POTORTÌ, 2005)

O Link Manager pode comunicar qualquer violação dos parâmetros de QoS solicitados para os níveis superiores da pilha de Bluetooth. O conjunto de

parâmetros configuráveis fornece a base para a implementação de uma política de QoS completas usando uma pilha Bluetooth.

A segurança de uma rede Bluetooth pode ser dividida em três modos:

- Modo 1: não segura
- Modo 2: Service Level aplicadas de segurança (após o estabelecimento do canal).
- Modo 3: Link Level aplicadas de segurança (antes do estabelecimento do canal).

Autenticação e criptografia em nível de link são manipulados por meio de quatro entidades básicas: i) o endereço do dispositivo Bluetooth, que é um identificador exclusivo de 48 bits atribuído a cada dispositivo; ii) uma chave de autenticação privada (número aleatório); iii) uma chave privada de criptografia (número aleatório); iv) um número aleatório de 128 bits que é mudado frequentemente, gerado de forma dinâmica por cada dispositivo. (FERRO; POTORTÌ, 2005)

A tecnologia Bluetooth e dispositivos associados são suscetíveis a ameaças a que estão sujeitas redes sem fio em geral, tais como ataque por negação de serviço (DoS - **D**enial **o**f **S**ervice), espionagem, ataque MITM (**M**an-**I**n-**T**he-**M**iddle), modificação de mensagem e apropriação indevida de recursos. Eles também são ameaçados por formas mais específicas de ataque relacionadas à tecnologia Bluetooth como por exemplo, ataques direcionados a vulnerabilidades conhecidas em implementações e especificações Bluetooth. (PADGETTE, 2011)

2.3 Comparativo das tecnologias

Nesta seção são apresentadas as características de cada tecnologia utilizada na comunicação, no final os conceitos são organizados na Tabela 1, realizando um comparativo de cada tecnologia.

A taxa de comunicação entre dispositivos é um aspecto a ser notado, pois a necessidade de tempo de resposta para usuário é algo essencial.

Wi-Fi Direct promete velocidades de transferência de dispositivo para o dispositivo de até 250 Mbps, enquanto o Bluetooth 4.0 promete velocidades semelhantes para Bluetooth 3.0 de até 25Mbps. (PAUL; PCWORLD, 2016)

O principal ponto de uma comunicação de dispositivos sem fio a ser notado é a habilidade de comunicar com outro dispositivo com a maior distância possível e outra característica a ser considerada é a capacidade da tecnologia suportar múltiplos dispositivos se comunicando.

A Wi-Fi Alliance propõem que os dispositivos Wi-Fi Direct podem alcançar ao outro dispositivo a uma distância máxima de 200 metros de distância.

Segundo a Bluetooth SIG sugere o alcance em uma distância de pelo menos 60 metros por um dispositivo Bluetooth. (PAUL; PCWORLD, 2016)

A restrição de um dispositivo Bluetooth é que não pode conter mais do que 7 escravos, implicando a todos os nós associados com mestres deve ter um grau inferior ou igual a 7. (SINGH; SHARMA; AGRAWAL, 2011)

Uma rede Wi-Fi Direct possui dispositivos um-para-um ou um-para-muitos. O número de dispositivos numa rede Wi-Fi Direct pode variar de acordo com o dispositivo de conexão. (ALLIANCE, 2016)

Uma característica a ser observada nas tecnologias de comunicação sem fio é a maneira de como consomem a energia do dispositivo, se permitem uma duração satisfatória do dispositivo e se possuem mecanismos para que seja capaz de economizar a bateria do dispositivo visando uma maior durabilidade da utilização e consumo de forma controlada.

Wi-Fi Direct possui dois mecanismos de economia de energia: o Opportunistic Power Save e NoA (**N**otice **o**f **A**bsence). (CAMPS-MUR; GARCIA-SAAVEDRA; SERRANO, 2013)

Bluetooth possui a mais impressionante das tecnologias para economia de energia, a Bluetooth LE (**L**ow **E**nergy) que permiti uma bateria funcionar durante um ano ou mais antes de ser totalmente descarregada. (CLARK, 2015)

Em média, um dispositivo Bluetooth absorve cerca de 1 a 35 mA, enquanto que um dispositivo Wi-Fi requer entre 100 e 350 mA. (FERRO; POTORTÌ, 2005)

Após destacarmos pontos pertinentes de cada tecnologia, a Tabela 1 apresenta as informações de forma organizada, listando de forma comparativa cada aspecto principal de cada tecnologia, expondo as características nas linhas e nas colunas representando as tecnologias de comunicação.

Tabela 1 - Comparativo entre Wi-Fi Direct e Bluetooth

Tecnologia	Wi-Fi Direct	Bluetooth
Taxa de comunicação (Mbps)	250	25
Distancia (M)	200	60
Número de dispositivos	Ilimitado	7
Consumo de bateria (mA)	100 a 350	1 a 35
Mecanismo para economia de energia	Sim	Sim

Fonte: Autor, 2016

Sobre os aspectos de distância para a aplicação, a segurança é baseada na disponibilidade de conexão, o que não necessitaria uma grande distância e a taxa de comunicação não é relevante, pois não é transmitido nenhuma informação entre o dispositivo móvel e o dispositivo de segurança, apenas é verificado se o dispositivo está disponível para conexão.

Mesmo que o Wi-Fi Direct supere o Bluetooth em aspectos como a taxa de comunicação e até mesmo na distância, a necessidade da aplicação é o consumo de bateria, o que permite uma maior durabilidade do dispositivo móvel do usuário.

Após uma análise sobre as tecnologias e a necessidade para aplicação, a tecnologia escolhida foi a tecnologia Bluetooth, por conseguir enviar informações a curta distância sem a necessidade de fios e por possuir mecanismos para economia de energia, o que é necessário para aplicação para preservar a bateria do dispositivo móvel do usuário.

3. Desenvolvimento

O desenvolvimento do projeto apresentado neste capitulo é divido em seções, inicialmente é descrito as tecnologias que serão utilizadas para o desenvolvimento da aplicação no celular e o protótipo do token, que são o Android e Arduino respectivamente, descrevendo informações sobre cada tecnologia, a arquitetura do sistema, apresentando as características de funcionamento do projeto, e por último os diagramas de casos de uso e de classe da aplicação para celular.

3.1 Android

Android é o nome do sistema operacional móvel feito pela empresa americana Google. É instalado em uma variedade de smartphones e tablets de diferentes fabricantes que oferecem aos usuários acesso a serviços do próprio Google, como busca, Youtube, Maps, Gmail e muito mais.

O Android é um sistema operacional personalizável e fácil de usar que move mais de um bilhão de dispositivos ao redor do mundo, desde smartphones e tablets a relógios, TVs, carros e, em breve, ainda mais. Android é o sistema operacional que move mais de um bilhão de smartphones e tablets. Cada versão do Android recebe o nome de uma sobremesa. (ANDROID, 2016)

Isto significa que você pode facilmente procurar informações na web, assistir a vídeos, escrever e-mails em seu telefone, tal como faria no seu computador, existem muitas outras funcionalidades no Android do que estes exemplos simples. (TODD, 2016)

A plataforma Android é uma plataforma independente de dispositivo, o que significa que você pode desenvolver aplicativos para vários dispositivos. Estes dispositivos incluem, mas não estão limitados a telefones, leitores de e-book, notebooks, dispositivos GPS e TV. (MICHAEL; DONN, 2012)

As vantagens de desenvolver em Android é a facilidade de encontrar informações para o desenvolvimento na internet, além é claro do incentivo da empresa Google, fornecendo material sobre todas as funcionalidades do Android. Outra grande vantagem é a presença da plataforma em diversos tipos de dispositivos, permitindo a criação de aplicações para diferentes dispositivos e aparelhos.

3.2 Arduino

Arduino é uma plataforma de prototipagem de código aberto baseado em hardware e software fácil para uso. As placas de Arduino são capazes de ler entradas – sensores de luz, pressão em um botão, ou uma mensagem de Twitter - e transformá-lo em uma saída - a ativação de um motor, ligar um LED, publicar algo online. Você pode dizer a sua placa o que fazer através do envio de um conjunto de instruções para o micro controlador na placa. Para fazer isso você usa a linguagem de programação Arduino e o software Arduino, com base em processamento. (ARDUINO, 2016)

As grandes vantagens do Arduino em relação as outras tecnologias é o baixo custo de mercado, a possibilidade de programação em múltiplos sistemas operacionais, funcionando em Windows, Linux e até mesmo iOS. Outra grande vantagem é o código fonte tanto de hardware, quanto de software ser aberto, sendo permitido qualquer pessoa modificar de acordo com as suas necessidades de uso.

Uma grande vantagem do Arduino é a quantidade de modelos disponíveis no mercado, com diversos tamanhos e cada um com uma quantidade de funcionalidades.

3.3 Arquitetura do sistema

O projeto tem como objetivo apresentar uma aplicação em Android integrada com um dispositivo token feito em Arduino para a proteção de dispositivos móveis.

O desenvolvimento foi feito através da IDE de programação Android Studio, fornecida pela empresa idealizadora do projeto, o Google, permitindo uma melhor performance de desenvolvimento e visualização sobre o projeto, pois a ferramenta conta com emuladores de celulares para testar o funcionamento das aplicações.

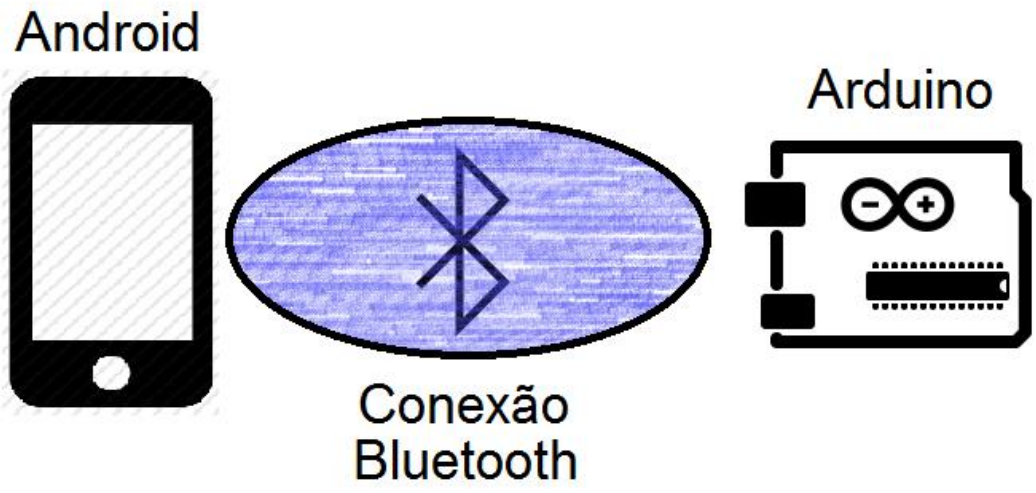
O aplicativo de segurança feito em Android tem como objetivo executar mecanismos de segurança, como emitir um alarme sonoro, caso a conexão com a aplicação do token seja perdida. Dentro do aplicativo o usuário pode definir qual função executar quando a conexão for perdida, como por exemplo, o bloqueio do celular ou apagar todos os arquivos no cartão de memória.

A aplicação do token em Arduino terá o seu desenvolvimento feito na própria IDE de desenvolvimento do Arduino, também fornecido pela empresa idealizadora do produto e além é claro de informações e descrições sobre as funções de

programação e de outros componentes utilizados para o funcionamento em conjunto com a placa em Arduino.

A aplicação token feita em Arduino tem como objetivo responder as requisições feitas pelo aplicativo via Bluetooth para certificar que o smartphone ainda está próximo do dispositivo token.

Figura 4 - Arquitetura de comunicação

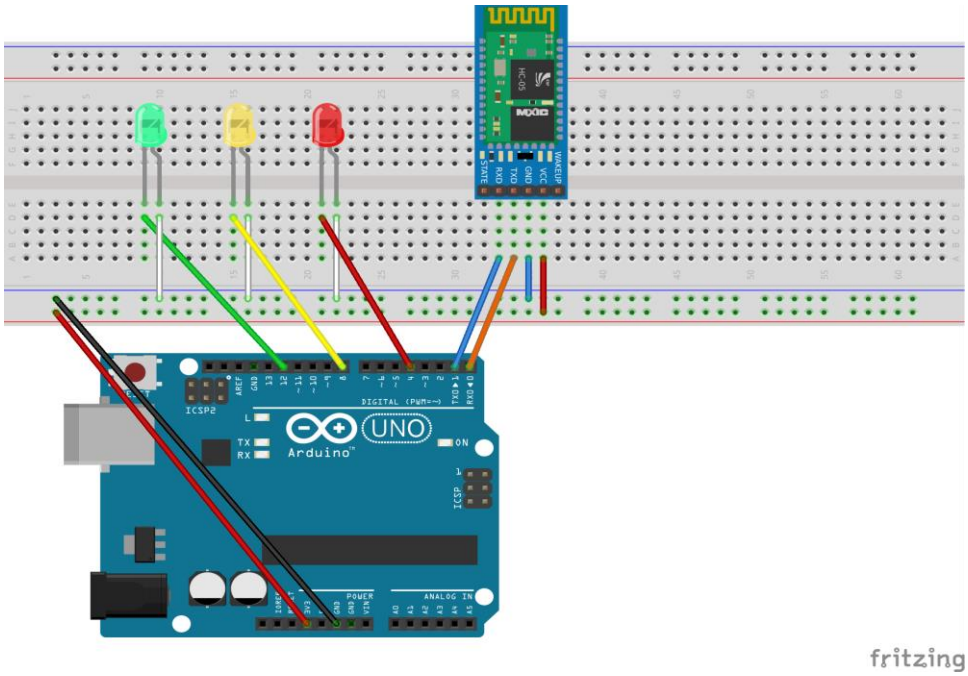


Fonte: Autor, 2016

Os componentes principais do projeto são um smartphone com o sistema operacional Android e uma placa de Arduino, a arquitetura de comunicação do projeto é ilustrada na Figura 4. O smartphone tem instalado o aplicativo desenvolvido para a segurança e através da rede Bluetooth se comunica emitindo requisições de verificação para a aplicação na placa de Arduino.

O protótipo do token, apresentado na Figura 5, foi desenvolvido em Arduino utilizando um modulo Bluetooth HC-05 para a comunicação com o aparelho celular que possui a aplicação de segurança desenvolvida em Android. Para uma melhor visualização de como é esperado o funcionamento do token, foi adicionado 3 (três) LEDs (**L**ight **E**mitting **D**iode) no protótipo, um LED na cor verde para indicar que a comunicação ainda está ativa com o celular, um LED na cor amarela para indicar que a comunicação com o celular se perdeu a mais de 7 (sete) segundos e por último um LED em vermelho indicando que o tempo da conexão com o celular passou de 20 (vinte) segundos.

Figura 5 - Protótipo do Token

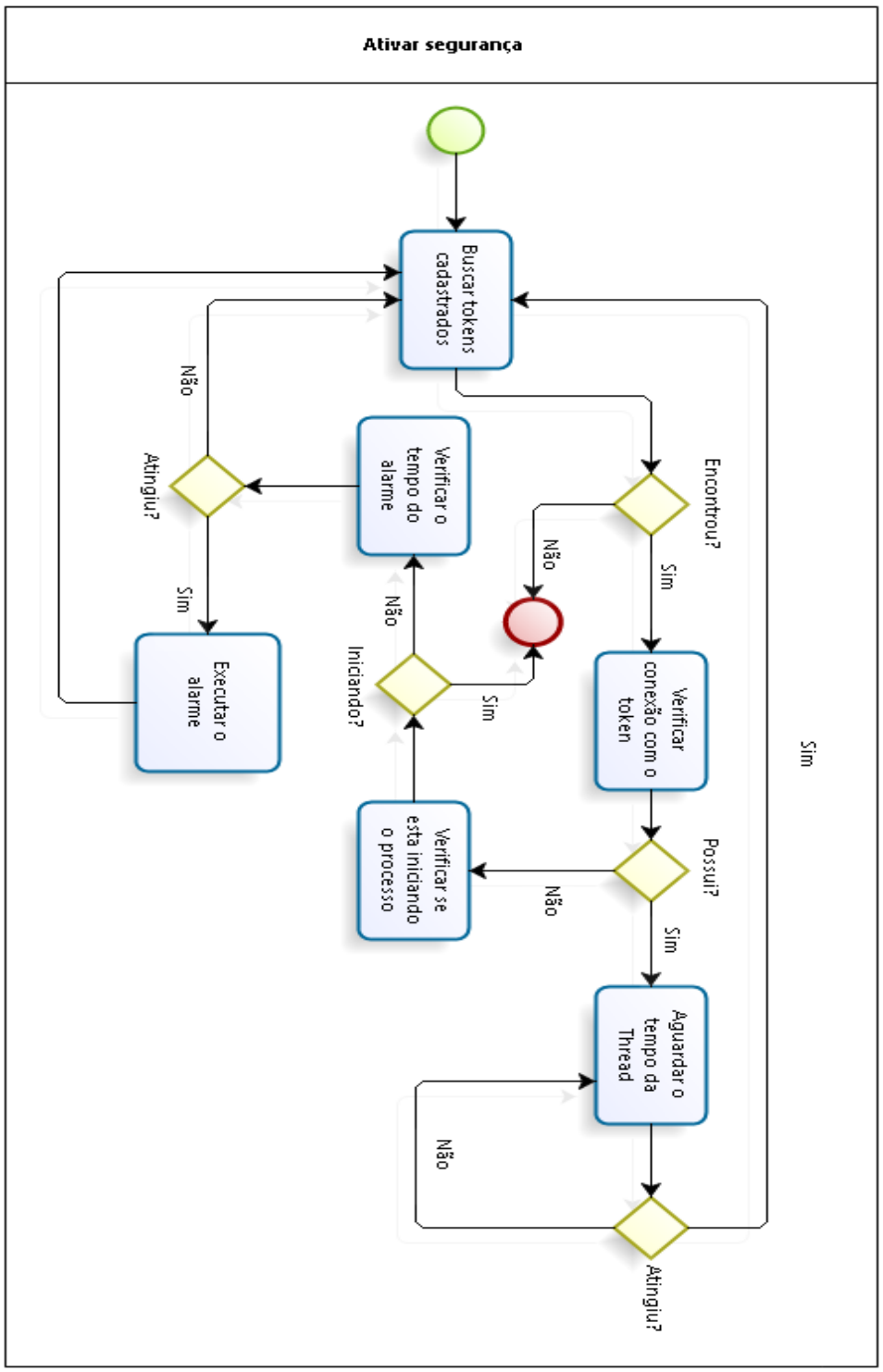


Fonte: Autor, 2016

O modulo Bluetooth HC-05 utilizado no protótipo foi escolhido por conta dos seus modos de funcionamento, em que é possível trabalhar tanto no modo escravo quanto no modo mestre. No protótipo é utilizado o modo escravo, porque quem inicia a comunicação é o celular com a aplicação de segurança, ou seja, o aparelho celular Android com a aplicação inicia a comunicação com o protótipo desenvolvido em Arduino.

A ativação do mecanismo de segurança possui um processo de execução descrito na Figura 6, em que o usuário inicia o processo, é feito uma busca dos tokens cadastrados pelo usuário, uma verificação de conexão é executada em cada token cadastrado, caso o token encontra-se conectado é aguardado um tempo para uma nova verificação, caso o mesmo não esteja conectado e é a primeira vez que o processo é executado, o mesmo é finalizado, pois é necessário encontrar pelo menos um token disponível para começar o processo, se não for a primeira vez é verificado se o tempo de conexão perdida é igual ao tempo de execução dos alarmes definidos, caso for, executa o alarme que teve o tempo atingido e o processo é finalizado.

Figura 6 – Fluxograma do processo de ativar segurança



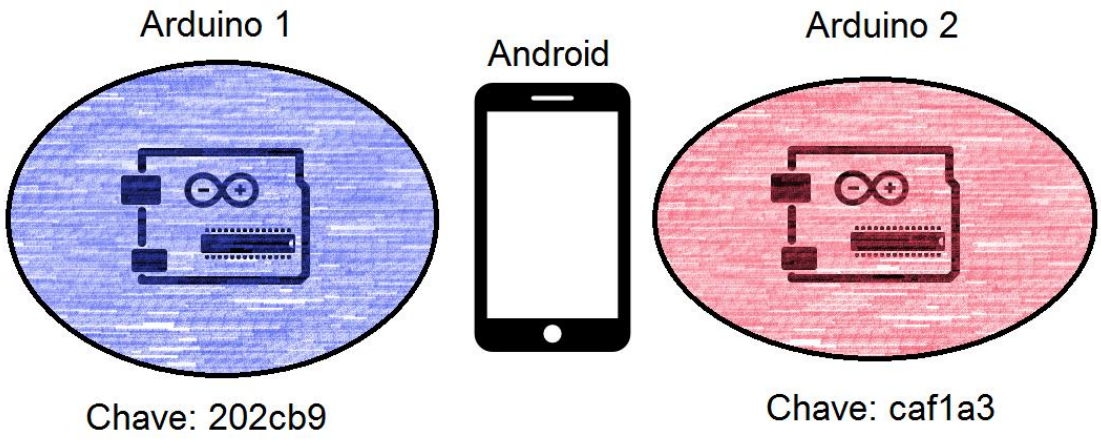
Fonte: Autor, 2016

A segurança empregada entre a comunicação do aplicativo Android e o dispositivo token para o funcionamento do projeto, é feito através de uma chave única definida no dispositivo em Arduino, em que é feito o cadastro no smartphone

do token pelo aplicativo e a partir desse cadastro, os tokens que estão na lista de cadastrados funcionam como uma chave para o aparelho celular.

A distribuição dos valores de chave para cada dispositivo token é feita de uma maneira que garanta a exclusividade de valor, podendo ser observado na Figura 7, unicamente dividido, de modo que um token não possua o mesmo valor da chave de outro token, o que permitiria a comunicação com o aplicativo no smartphone.

Figura 7 - Exemplo de múltiplas conexões



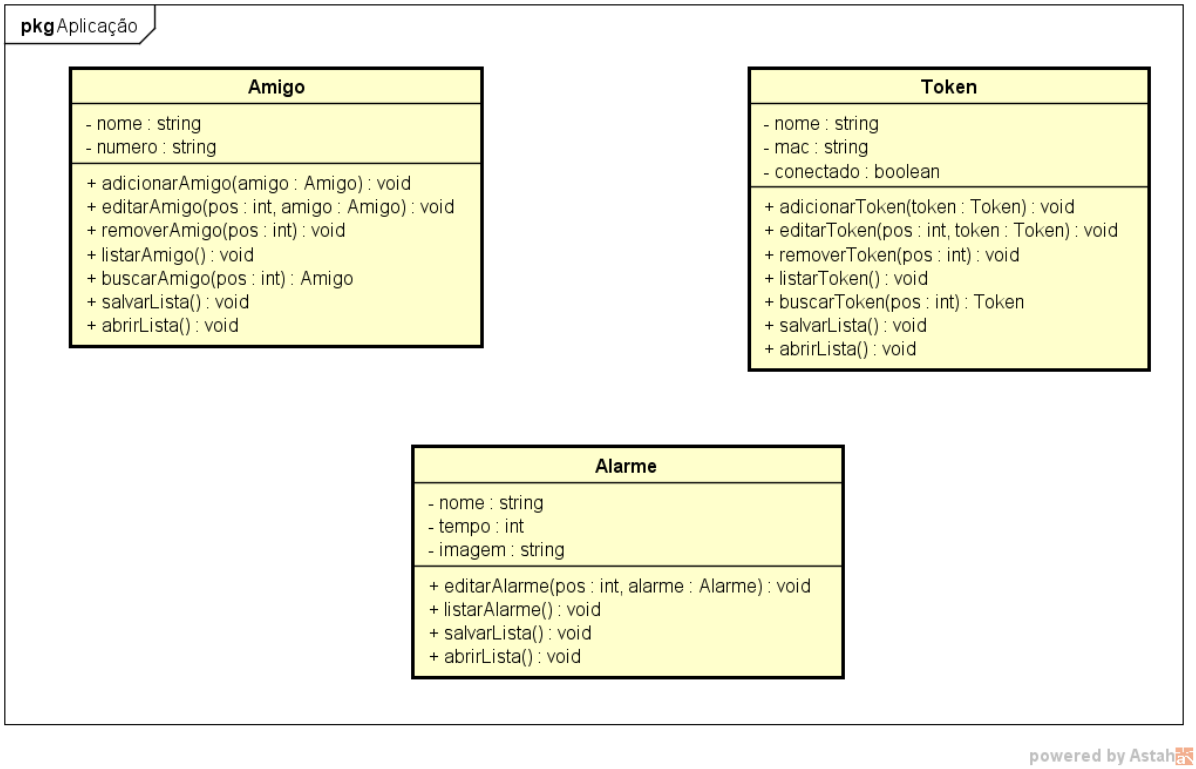
Fonte: Autor, 2016

Os mecanismos de segurança do aplicativo são ativados quando não é possível a comunicação com a placa Arduino, ou seja, quando o celular do usuário perder a comunicação com a placa, os mecanismos de segurança definidos no aplicativo são ativados de maneira automática.

A descrição das funcionalidades da aplicação é feita através do Astah, uma ferramenta utilizada na área da engenharia de software para especificação de sistemas, neste projeto foram desenvolvidos os diagramas de classe e diagramas de casos de uso, para a aplicação feita em Android estão na Figura 8 e na Figura 9, logo após as figuras, são descritos os casos de uso de cada funcionalidade apresentada no diagrama de casos de uso.

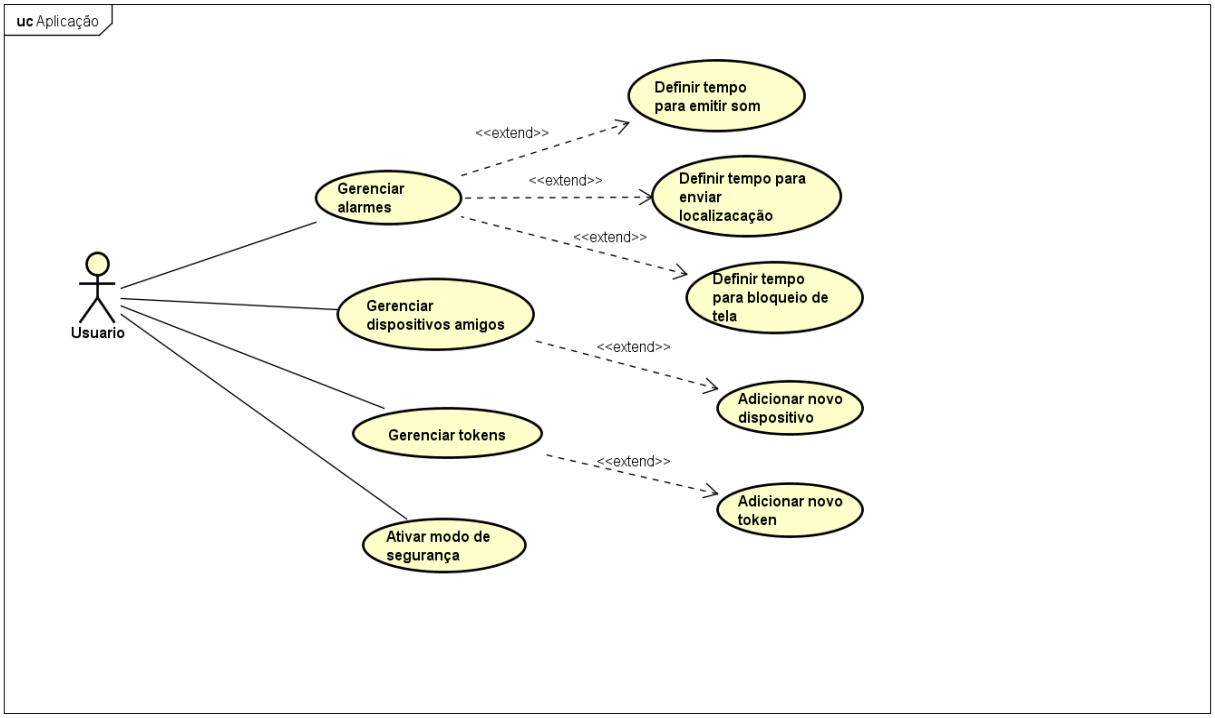
Os diagramas ajudam a entender melhor é o funcionamento do sistema, porém, no diagrama de casos de uso é feito uma descrição detalhada para cada ação no diagrama, as descrições dos diagramas são feitas após as figuras dos diagramas.

Figura 8 - Diagrama de classe da aplicação Android



Fonte: AUTOR, 2016

Figura 9 - Diagrama de caso de uso da aplicação Android



Fonte: Autor, 2016

3.3.1 Descrição dos diagramas de casos de uso

Descrição de gerenciar alarmes

Nome

Gerenciar alarmes

Atores

Usuário

Descrição sucinta

O usuário gerencia os alarmes já definidos no sistema.

Pré-condição

O usuário abriria a aba de menus para visualizar a opção “Alarmes” dentro da aplicação.

Fluxo básico

1. O usuário abre o aplicativo no celular.
2. O usuário abre o menu de opções.
3. O sistema lista os menus na tela.
4. O usuário seleciona a opção “Alarmes”.
5. O sistema lista os alarmes.

Fluxos Alternativos

Descrição de definir tempo para emitir som

Nome

Definir tempo para emitir som

Atores

Usuário

Descrição sucinta

O usuário define o tempo para o alarme de “Emitir som”.

Pré-condição

O usuário ter executado a opção “Alarmes” e escolher a opção de alarme “Emitir som”.

Fluxo básico

1. O usuário seleciona a opção “Alarmes”.
2. O sistema lista os alarmes.
3. O usuário seleciona a opção de alarme “Emitir som”.
4. O sistema abre uma nova tela com o nome do alarme e o tempo para execução do alarme.
5. O usuário define o novo tempo para a execução.
6. O usuário salva as alterações.
7. O sistema retorna a tela de “Alarmes”.

Fluxos Alternativos

Descrição de definir tempo para enviar localização

Nome

Definir tempo para enviar localização

Atores

Usuário

Descrição sucinta

O usuário define o tempo para o alarme de “Enviar localização”.

Pré-condição

O usuário ter executado a opção “Alarmes” e escolher a opção de alarme “Enviar localização”.

Fluxo básico

1. O usuário seleciona a opção “Alarmes”.
2. O sistema lista os alarmes.
3. O usuário seleciona a opção de alarme “Enviar localização”.
4. O sistema abre uma nova tela com o nome do alarme e o tempo para execução do alarme.
5. O usuário define o novo tempo para a execução.
6. O usuário salva as alterações.
7. O sistema retorna a tela de “Gerenciar Alarmes”.

Fluxos Alternativos

Descrição de definir tempo para bloqueio de tela

Nome

Definir tempo para bloqueio de tela

Atores

Usuário

Descrição sucinta

O usuário define o tempo para o alarme de “Bloquear tela”.

Pré-condição

O usuário ter executado a opção “Alarmes” e escolher a opção de alarme “Bloquear tela”.

Fluxo básico

1. O usuário seleciona a opção “Alarmes”.
2. O sistema lista os alarmes.
3. O usuário seleciona a opção de alarme “Bloquear tela”.
4. O sistema abre uma nova tela com o nome do alarme e o tempo para execução do alarme.
5. O usuário define o novo tempo para a execução.
6. O usuário salva as alterações.
7. O sistema retorna a tela de “Alarmes”.

Fluxos Alternativos

Descrição de gerenciar dispositivos amigos

Nome

Gerenciar dispositivos amigos

Atores

Usuário

Descrição sucinta

O usuário gerencia os dispositivos amigos que são enviados a localização do celular quando ativado o alarme “Enviar localização”.

Pré-condição

O usuário abriria a aba de menus para visualizar a opção “Amigos” dentro da aplicação.

Fluxo básico

1. O usuário abre o aplicativo no celular.
2. O usuário abre o menu de opções.
3. O sistema lista os menus na tela.
4. O usuário seleciona a opção “Amigos”.
5. O sistema lista os amigos já cadastrados.

Fluxos Alternativos

Descrição de adicionar novo dispositivo

Nome

Adicionar novo dispositivo

Atores

Usuário

Descrição sucinta

O usuário adiciona um novo dispositivo amigo para que possa ser enviado a localização do celular quando for ativado o alarme “Enviar localização”.

Pré-condição

O usuário abriria a aba de menus para visualizar a opção “Amigos” dentro da aplicação.

Fluxo básico

1. O usuário seleciona a opção “Amigos”.
2. O sistema lista os amigos já cadastrados.
3. O usuário seleciona a opção “Cadastrar”.
4. O sistema abre uma nova tela para cadastro.
5. O usuário define os valores do novo dispositivo amigo.
6. O usuário seleciona a opção “Salvar”.
7. O sistema armazena o novo dispositivo amigo.
8. O sistema retorna para a tela da lista dos amigos já cadastrados.

Fluxos Alternativos

Descrição de gerenciar tokens

Nome

Gerenciar tokens

Atores

Usuário

Descrição sucinta

O usuário gerencia os dispositivos tokens que são utilizados para a segurança do celular.

Pré-condição

O usuário abriria a aba de menus para visualizar a opção “Tokens” dentro da aplicação.

Fluxo básico

1. O usuário abre o aplicativo no celular.
2. O usuário abre o menu de opções.
3. O sistema lista os menus na tela.
4. O usuário seleciona a opção “Tokens”.
5. O sistema lista os tokens já cadastrados.

Fluxos Alternativos

Descrição de adicionar novo token

Nome

Adicionar novo token

Atores

Usuário

Descrição sucinta

O usuário adiciona um novo token para que possa ser utilizado na segurança do celular.

Pré-condição

O usuário abriria a aba de menus para visualizar a opção “Tokens” dentro da aplicação. Para realizar o processo de adicionar um novo token, o mesmo deve ter sido pareado anterior, por se tratar de um dispositivo Bluetooth.

Fluxo básico

1. O usuário seleciona a opção “Tokens”.
2. O sistema lista os tokens já cadastrados.
3. O usuário seleciona a opção “Cadastrar”.
4. O sistema abre uma nova tela para cadastro.
5. O usuário define os valores do novo token.
6. O usuário seleciona a opção “Salvar”.
7. O sistema armazena o novo token.
8. O sistema retorna para a tela da lista dos tokens já cadastrados.

Fluxos Alternativos

Ativar modo de segurança

Nome

Ativar modo de segurança

Atores

Usuário

Descrição sucinta

O usuário aciona o modo de segurança para a proteção do celular.

Pré-condição

O usuário abriria a aba de menus para visualizar a opção “Home” dentro da aplicação.

Fluxo básico

1. O usuário seleciona a opção “Home”.
2. O sistema apresentaria o estado atual do modo de segurança.
3. O usuário seleciona a opção “Ativar segurança”.
4. O sistema verifica se o Bluetooth do dispositivo está ativado.
5. O sistema pesquisa os dispositivos Bluetooth disponíveis na lista de “Tokens”.
6. O sistema atualiza o “Token” selecionado.
7. O sistema atualiza o “Modo de segurança” para “Ativado”.

Fluxo Alternativo: Bluetooth desativado

4.1. O sistema solicita ao usuário para ativar o Bluetooth.

4.2. O usuário concorda com a ativação do Bluetooth.

4.3. Retorna no passo 5.

Fluxo Alternativo: Token não encontrado

5.1. O sistema apresenta uma mensagem indicando que nenhum “Token” foi encontrado.

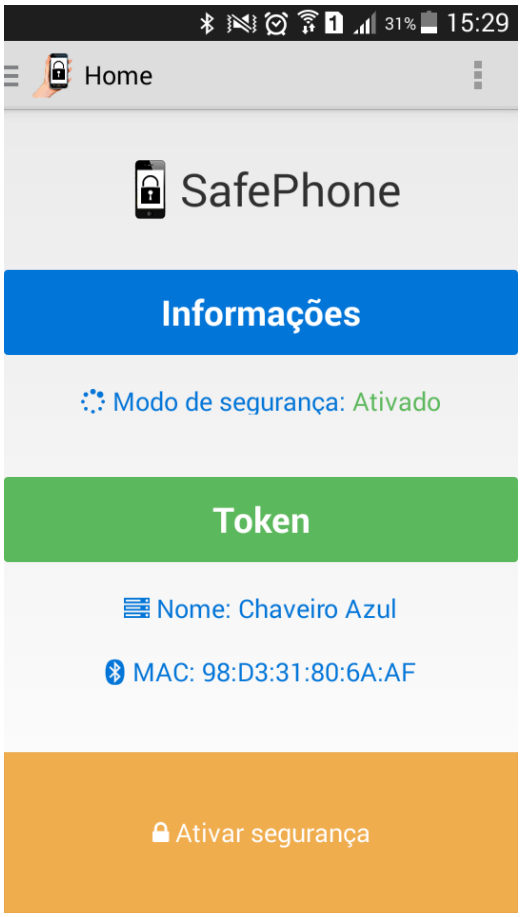
5.2. O sistema permanece com o “Modo de segurança” em “Desativado”.

5.3. Finaliza o caso.

Após a elaboração e descrição dos casos de uso e a construção do diagrama de classes, o desenvolvimento e aplicação dos casos de uso são apresentados nas telas do aplicativo desenvolvido em Android, que são apresentados nas figuras seguintes.

Na Figura 10 é apresentado a tela inicial do aplicativo, exibindo as informações sobre o estado atual do modo de segurança, o nome e o MAC do token ativo no momento e também o botão para ativar o segurança do dispositivo móvel.

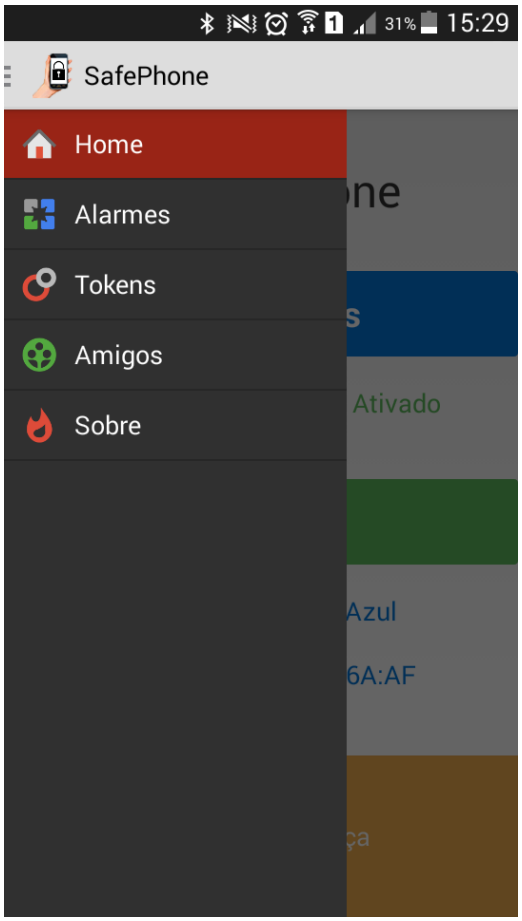
Figura 10 - Tela inicial para ativar a segurança



Fonte: Autor, 2016

Na Figura 11 é apresentado a aplicação com o menu lateral mostrando os itens para escolha.

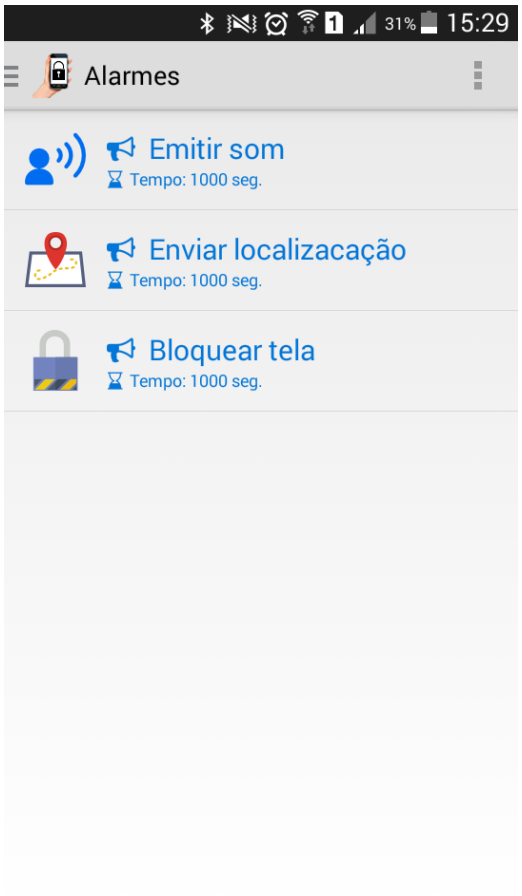
Figura 11 - Tela inicial com o menu lateral



Fonte: Autor, 2016

Na Figura 12 é apresentado a tela de listagem dos alarmes, que permite ao usuário selecionar um alarme para alterar o seu tempo de ativação.

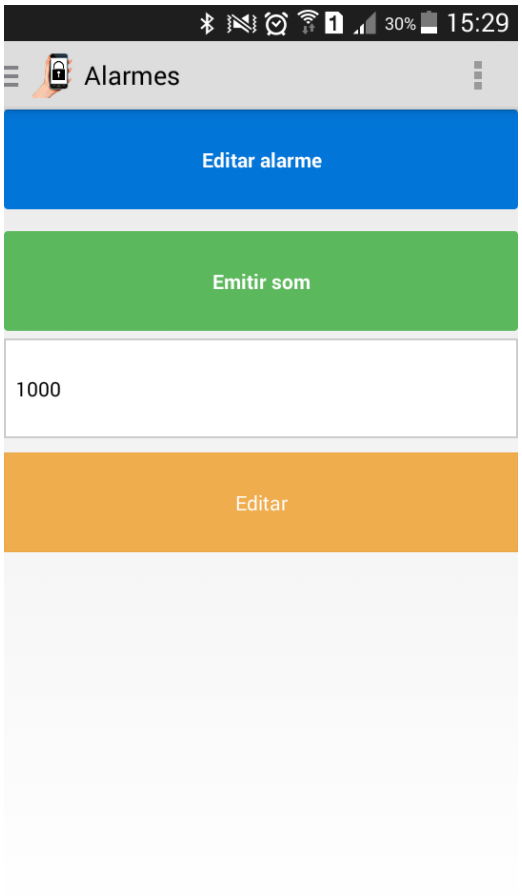
Figura 12 - Listagem dos alarmes disponíveis



Fonte: Autor, 2016

Na Figura 13 mostra a tela a edição do tempo do alarme, em que o usuário define um tempo em segundos para ativar o alarme.

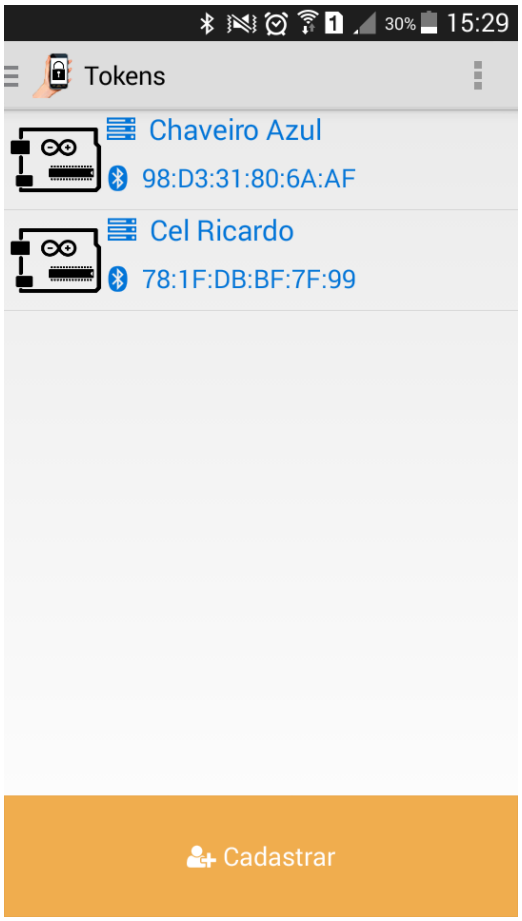
Figura 13 - Tela para edição do tempo do alarme



Fonte: Autor, 2016

Na Figura 14 é apresentado a tela da listagem dos tokens cadastrados pelo usuário que são utilizados para a segurança do aparelho.

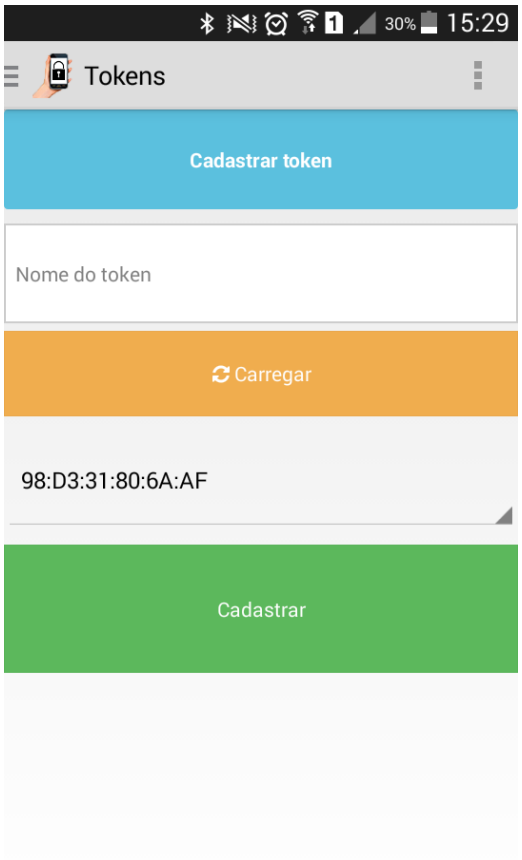
Figura 14 - Listagem dos tokens



Fonte: Autor, 2016

Na Figura 15 é apresentado a tela de cadastro de um novo token, a onde o usuário adiciona um novo token a sua lista de tokens.

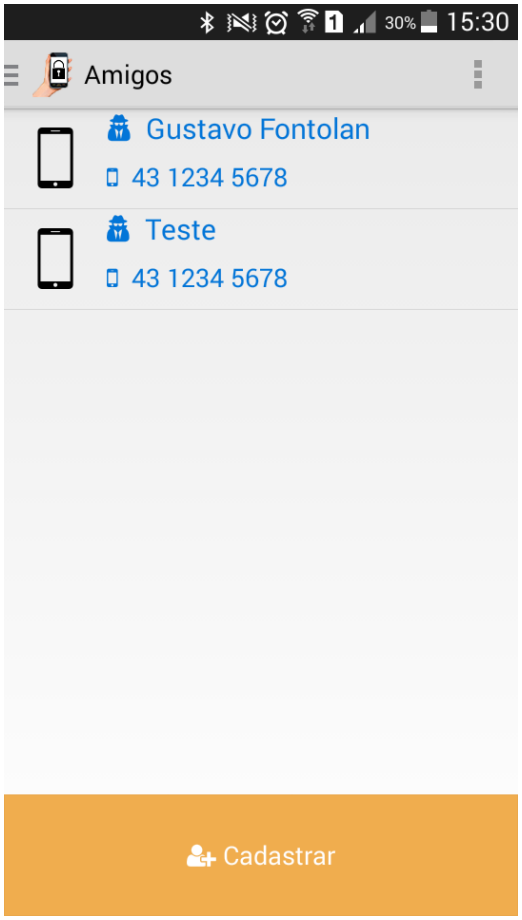
Figura 15 - Tela para adicionar um novo token



Fonte: Autor, 2016

Na Figura 16 é apresentado a listagem de celulares amigos cadastrados na aplicação pelo usuário, que serão utilizados posteriormente pelo alarme para enviar a localização do aparelho, caso o alarme venha ser ativado.

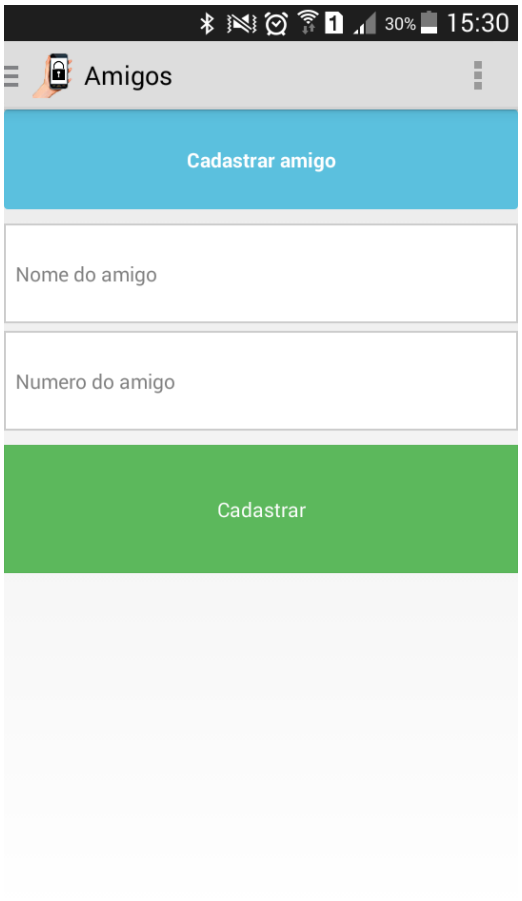
Figura 16 - Listagem dos amigos



Fonte: Autor, 2016

Na Figura 17 é apresentado a tela para o cadastro de um novo celular amigo na lista de amigos do usuário.

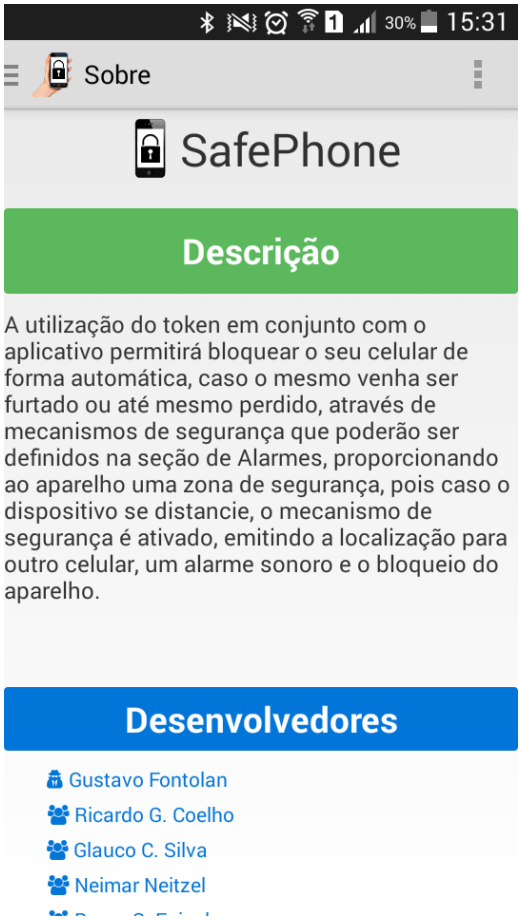
Figura 17 - Tela para adicionar um novo amigo



Fonte: Autor, 2016

Na Figura 18 é apresentado a tela de descrição do aplicativo, em que mostra uma breve descrição sobre os objetivos da aplicação e o nome dos desenvolvedores que participaram da construção da aplicação.

Figura 18 - Tela para descrição do aplicativo



Fonte: Autor, 2016

4. Conclusão e trabalhos futuros

O projeto apresentado neste trabalho demonstrou ser uma nova alternativa tecnológica para proteção de aparelho celulares, pois a aplicação se destaca na forma em que é feito a ativação da segurança do aparelho, não dependendo de ações do usuário para ativar seus mecanismos de segurança ou até mesmo uma conexão posterior para a solicitação da ativação dos mecanismos, ou seja, o aplicativo instalado no aparelho realiza o processo de segurança de forma automática.

Porém, sobre os custos iniciais do desenvolvimento utilizados durante o projeto ainda possui custos medianos por conta da utilização de hardwares não específicos, ou seja, destinado especificamente para a criação do token que comunicará com a aplicação, porém, durante o projeto foram utilizadas as tecnologias e arquiteturas do Arduino, em que se concentrou o maior gasto do projeto, podendo superar até mesmo o valor do aparelho celular do próprio usuário, o que seria para o mesmo inviável a utilização.

Durante o desenvolvimento do projeto, inicialmente a ideia era fazer com que cada token possuísse uma chave de identificação única, porém, no decorrer do projeto, a autenticação para o funcionamento da segurança do aparelho passou a ser feita através dos endereços MAC dos tokens, pois concluímos que, não seria necessário o envio de mensagens entre o token e o celular com o aplicativo inicialmente no protótipo desenvolvido, apenas saber que o token está disponível para conexão, ou seja, está a uma distância próxima ao celular possível para estabelecer uma comunicação.

A ideia do protótipo e a forma como ele é usado para a segurança de dispositivos eletrônicos, pode ser utilizado posteriormente como base para outros projetos que permita a utilização das mesmas tecnologias e ideias utilizadas ou até mesmo melhorias para um dispositivo desenvolvido especificamente na proteção de aparelhos móveis.

Como sugestão de trabalhos futuros, seria o desenvolvimento de um aparelho de hardware, especificamente para este tipo de funcionalidade, o que poderia diminuir o custo do produto, pois no projeto os componentes são genéricos, podendo ser utilizados em qualquer tipo de projeto, o que pode ter deixado o protótipo com um custo elevado, outro ponto a ser levado em conta é o tamanho do token a ser

desenvolvido para ser utilizado, pois a ideia, é que ele venha ser imperceptível, fazendo com que possa ser confundido até mesmo com um chaveiro ou apenas um item pessoal.

Referências

AGRELA, Lucas. **7 apps para encontrar seu Android roubado.** 2012. Disponível em: <http://exame.abril.com.br/blogs/aplicativos/android/7-apps-para-encontrar-seu-android-roubado/>. Acesso em: 06 mar. 2016.

ALLIANCE, Wi-Fi. **Wi-Fi Direct: Discover Wi-Fi**. Disponível em: http://www.wi-fi.org/discover-wi-fi/wi-fi-direct. Acesso em: 22 fev. 2016.

ALLIANCE, Wi-Fi. **Wi-Fi Direct® in the enterprise: Evaluating peer-to-peer Wi-Fi® connectivity**. 2013

ANDROID. **A história do Android.** 2016. Disponível em: <www.android.com>. Acesso em: 05 jul. 2016.

ARDUINO. **What is Arduino?** Disponível em: https://www.arduino.cc/en/Guide/Introduction. Acesso em: 22 fev. 2016.

BLUETOOTH. **Bluetooth.** Disponível em: http://www.bluetooth.com. Acesso em: 22 fev. 2016.

CAMPS-MUR, Daniel; GARCIA-SAAVEDRA, Andres; SERRANO, Pablo. **Device to device communications with Wi-Fi Direct: overview and experimentation.** 2013.

CLARK, Bryan. **The Differences Between Bluetooth 4.0 and Wi-Fi Direct You Need To Know.** 2015. Disponível em: <http://www.makeuseof.com/tag/the-differences-between-bluetooth-4-0-and-wi-fi-direct-you-need-to-know/>. Acesso em: 07 mar. 2016.

FERRO, Erina; POTORTÌ, Francesco. **Bluetooth and Wi-Fi wireless protocols: A survey and a comparison.** 2005.

HILDENBRAND, Jerry. **What is Android?** 2015. Disponível em: http://www.androidcentral.com/what-android. Acesso em: 22 fev. 2016.

KOVACS, Bruno Paulo Usiglio; MONTEIRO, Vanesa de Freitas. **Um estudo prático das ameças de segurança em dispositivos portáteis com Windows Mobile.** 2006.

LEE, Jin-shyan; SU, Yu-wei; SHEN, Chung-chou. **A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi.** 2007. Disponível em: https://www.researchgate.net/publication/224307357_A_comparative_study_of_wireless_protocols_Bluetooth_UWB_ZigBee_and_Wi-Fi. Acesso em: 22 fev. 2016.

LUGLI, Alexandre Baratella; GUILHERME SOBRINHO, Darlan. **Tecnologias Wireless para automação industrial: Wireless_Hard, Bluetooth, WISA, Wi-Fi, Zigbee e SP-100.** 2012

MARGREITER, Martin; ZEH, Thomas; SPANGLER, Matthias. **Bluetooth-Measured Travel**

Times for Dynamic Re-Routing.2015. Disponível em: <https://www.researchgate.net/publication/281375003_Bluetooth-Measured_Travel_Times_for_Dynamic_Re-Routing>. Acesso em: 21 mar. 2016.

MORITZ, Guido; ZEEB, Elmar; PRÜTER, Steffen. **Devices Profile for Web Services and the REST.** 2010.

ONDE FUI ROUBADO. **Aplicativo Onde Fui Roubado.** 2016. Disponível em: ondefuiroubado.com.br. Acesso em: 22 fev. 2016.

PADGETTE, John, SCARFONE, Karen. **Guide to Bluetooth Security (Draft)**. Gaithersburg: National Institute of Standards and Technology, 2011.

PAUL, Ian; PCWORLD. **Wi-Fi Direct vs. Bluetooth 4.0: A Battle for Supremacy.** Disponível em: <http://www.pcworld.com/article/208778/Wi_Fi_Direct_vs_Bluetooth_4_0_A_Battle_for_Supremacy.html>. Acesso em: 07 mar. 2016.

PEREIRA, Luiz Antonio Malta. **SISTEMA DE MONITORAMENTO E COMUNICAÇÃO AUTOMATO, COM TRANSMISSÃO DE DADOS UTILIZANDO TECNOLOGIA DE REDE SEM FIO.** 2013. Disponível em: http://retec.fatecourinhos.edu.br/index.php/retec/article/view/28. Acesso em: 22 fev. 2016.

SELYE, Hans (1974). **Stress without Distress**. Nova York, NAL

SELYE, Hans (1976/1978) **The Stress of Life**, New York, Mc Graw Hill, revised edition.

SILVA, Edna L.; MENEZES, Estera M. **Metodologia de Pesquisa e Elaboração de Dissertação**. Florianópolis: 2005. 4 ed. 138p. Disponível em: http://www.convibra.com.br/upload/paper/adm/adm_3439.pdf. Acesso em: 11 jun. 2013

SINGH, Mrs. Pratibha; SHARMA, Mr. Dipesh; AGRAWAL, Mr. Sonu. **A Modern Study of Bluetooth Wireless Technology.** 2011.

TODD, Alex. **What is Android and what is an Android phone?** 2016. Disponível em: https://recombu.com/mobile/article/what-is-android-and-what-is-an-android-phone_M12615.html. Acesso em: 22 fev. 2016.

XING, Bo; SEADA, Karim; VENKATASUBRAMANIAN, Nalini. **An Experimental Study on Wi-Fi Ad-Hoc Mode for Mobile Device-to-Device Video Delivery.** 2009.