Mobile Theft Detector

Kshitij S. Yadav[1] Dhrumil S. Shah[2]
[1,2]B.E Student
[1,2]Department of Electronics and Telecommunication Engineering
[1,2]K.J Somaiya College of Engineering, Maharashtra, India

Abstract— Mobile theft is a rising problem in metropolitan city. Everyday a large number of cell phones and other devices are stolen and complaints are filed every day. The mobile theft prevention device is a dynamic and portable device which works on the basis of short range Bluetooth technology. The device and the mobile application in the Android phone are connected via class 3 Bluetooth module which has a range of 1 to 2 meters. As soon as the connection breaks, which means the device and the phone have gone out of each other's coverage area, both the device and the phone, start ringing and vibrating which notifies the user about a possible theft. The device can be effectively used in crowded public places.

Key words: Bluetooth, Global Positioning System(GPS), Wi-Fi, Near Field Communication(NFC)

I. INTRODUCTION

A. Why This Project?:

The major fear we have about mobile while travelling in crowded public places is of them being stolen away. With the rising prices and importance of the smartphones in today's world it is essential to find a viable option to ensure security for the smartphones. The aim of this project was to design a device which can curb the possibility of mobile being stolen by reacting dynamically.

B. Existing Gadget Security System:

Current Gadget security system use Global Positioning System (GPS) for the purpose of tracking and thereby provide security. Gadget Security using Global Positioning System (GPS) is carried out using a GPS unit that is available network carrier of the user mobile phone. The precise location of the user device, and hence that of its carrier, is tracked using Global Positioning System. The location data can be stored in the GPS unit of the user or can be transmitted to a central location database using GPRS of the carrier. The tracker needs a GPS software to analyze the data received.

There are two drawbacks of this system. The victim of the mobile theft might come to know about the theft much later after the phone is stolen and the phone might not be retrieved. The victim cannot start the tracking process unless he gets an internet access.

C. Proposed Gadget Security System:

The proposed System consists of two parts, hardware and Application development. The hardware and the Application are connected to each other through air interface using Bluetooth technology. A class 3 Bluetooth module is incorporated on the hardware side and the Mobile Phone Bluetooth is used for the application side connection. As soon as the connection breaks, the device as well as the mobile phone starts buzzing and vibrating. This indicates the possibility of a potential theft.

D. Why Bluetooth Over NFC And Wi-Fi?:

The range of Wi-Fi is about 50 to 100 meters, whereas the range of NFC is only 0.2 meters. However the required range for the desired application is 1 to 2 meters. Only Class 3 Bluetooth can provide such small range of coverage area consuming low power. Also, the power consumption in Wi-Fi is very high due to such large coverage area. The device is a portable device; hence low power consumption has to be one of the major features of the device.

E. System Overview:

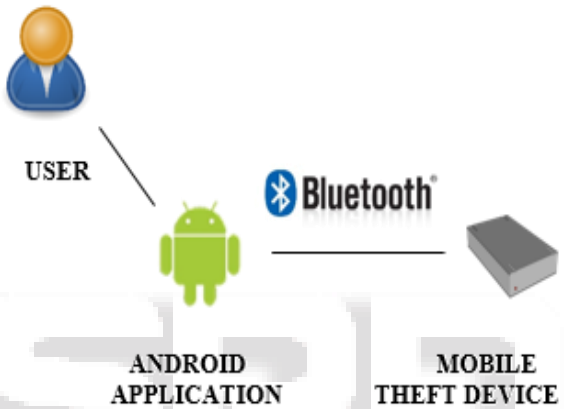

Fig. 1:

II. LITERATURE SURVEY

The Bluetooth combines different industries such as computers and cell phones using a single low power globally acceptable short range radio frequency named as Bluetooth. Bluetooth originated in 1994 when Ericsson began working on an idea to replace cables with wireless networks. It is used to connect to Bluetooth devices through Bluetooth communication. For security reasons, Bluetooth devices should be paired before using the communication network. The connected devices before connecting will share a password through RFCOMM channel to transmit data. The simple process of connecting Bluetooth is Find device, pair with the device, enter password and connect with the device. The device then gets connected and is ready for data transmission.

The development of Android did not start immediately, even though Google purchased it in 2005. In 2007, The Open Handset Alliance announced Android to be an Open Source Platform. This marks the beginning of actual development in Android. In the same 2008 the G1 phone was produced by HTC and was retailed within the T-Mobile carrier. 4 new versions of Android rolled out in the next couple of year. Android became the best spread mobile operation system platform after Blackberry, having more than 60 different models running Android in it in 2010.

III. MOBILE SECURITY DEVICE

A. Architecture:

The Circuit Diagram of the Gadget Security Device is shown below. The main component used in the circuit is ATMEGA328P chip. It is an 8-bit microcontroller which has fully static Operational functions.

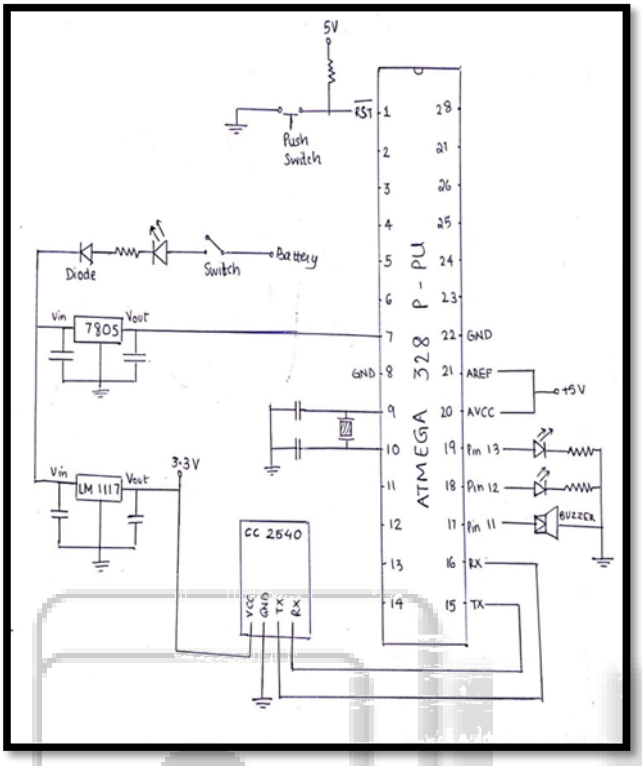

Fig. 2:

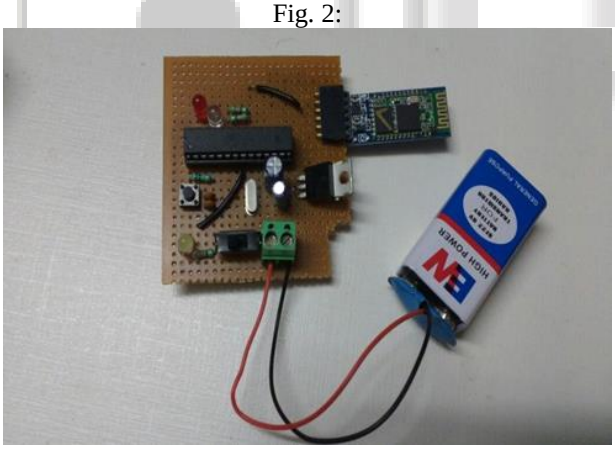

Fig. 3:

B. List Of Components:

- ATMEGA328P-PU
- BLUETOOTH MODULE CC2540
- LM1117
- IC7805

IV. MOBILE SECURITY ANDROID APPLICATION

A. Objective:

The application has been developed to act as an interface between user and the mobile security device as well as for authentication purposes.

The application consists of features like enabling protection, disabling protection, setting up password and changing the password. Password is essential in order to ensure that only the user can switch off the buzzing action. The app ensures that buzzing action is continued until the correct password is entered.

B. Background:

The terminologies and technologies used in this project are briefly described as follows.

1) An Android Operating System:

An Android Operating System is a free and open source mobile operating system for mobile devices such as mobile phones and tablets developed by Google.

2) Interactive Media:

Interactive media normally refers to products and services on digital computer-based systems which respond to the user's actions by presenting content such as text, graphics, animation, video, audio, games, etc.

C. Analysis and Design:

The following is the GUI of the Android Application. It consists of 5 Buttons, 6 Textboxes, 2PasswordBoxes and 1 Label. The text typed in Password Boxes is showed in form of "*" (astrix). When the correct Password is entered and Enter Button is pressed, the connect and disconnect button become visible. When Change Password button is pressed, the Connect and disconnect button become invisible and Password Box 2 becomes visible where the new password is to be entered after entering the old password in the Password Box1.

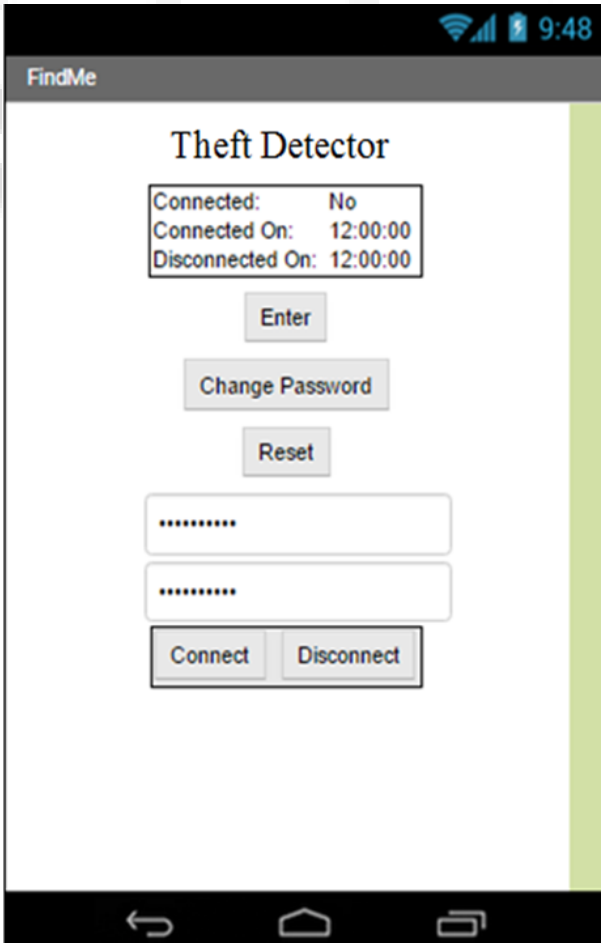

Fig. 4:

V. CONCLUSIONS

On successful creation of link between the device and the android phone, the security system enables and both, the mobile phone and the device, keep a track of each other, and check if the connection still exits. As soon as the connection breaks, the mobile phone and the device both start the buzzing action. This indicates that the connection is lost, which shows a possibility of either the device or the mobile phone been stolen.

The entire system is based on immediate response by the mobile phone and the device. The buzzing action is extremely quick due to which it is possible to know that the stolen instrument might have not gone too far from the user at that particular moment when the buzzer starts ringing. Hence it is possible to recover the stolen Phone or device.

Thus to conclude, this project in whole, might not give complete protection from theft, but it definitely increases the chances to recover the stolen phone.

REFERENCES

[1] IEEE paper on Wi-Fi (IEEE 802.11) and Bluetooth coexistence: issues and solutions
[2] IEEE paper on Implementation of Wi-Fi/Bluetooth-based Smart Narrow Field Communication
[3] The Bluetooth Special Interest Group. Bluetooth Specification Core v4.0.(2009-02). http://www.bluetooth.org.
[4] Andre N Klingsheim. J2ME Bluetooth Programming [D]. Department of Informatics University of Bergen, 2004.

