BLUETOOTH BASED ANTI-THEFT DEVICE FOR SMARTPHONES

[1]Harish Kalla, [2]Dereje Tekilu, [3]Tadesse Hailu
[1]Assistant Professor,[2]Assistant Professor, [3]Lecturer,
Department of Electronics and Communication Engineering
Adama Science & Technology University, Adama, Ethiopia.

***Abstract*—**Current smartphones are provide lots of the capabilities of traditional personal computers (PCs) and, in addition, offer a large selection of connectivity options, such as IEEE 802.11, Bluetooth, GSM, GPRS, UMTS, and HSPA. This plethora of appealing features has led to a widespread diffusion of smartphones that, as a result, are now an ideal target for attackers. Mobile phone robberies and extraction of personal data has become a growing concern. Increase in cost of mobiles has also led to increase in the number of robberies of mobile phones. Hence there is a need of a system which will in dictate immediately that the theft is taking place and produce an alarm to scare the thief and also make surrounding people note of such incidence. This can be implemented using Bluetooth module which will be kept inside the pocket. The Bluetooth module is paired with the Bluetooth of the mobile. Here the mobile contains based 'Locate Beacons' software to connect and measure the BLE beacon's distance. The other end i.e. hardware device contains a microcontroller interfaced with BLE beacon. If the connectivity between mobile and Bluetooth module is more than two meters, mobile sends the command to hardware. Then hardware receives the command and gives the alarm and vibration continuously. At the same time in mobile also toggle the light and sound to identify the mobile location. This hardware device is small and looks like a key chain to keep in pocket.

Keywords: *Smartphones, Bluetooth Module, controller, RSSI, distance.*

I. INTRODUCTION

One of the greatest threats to our personal welfare in the digital age is the theft of our mobile phones can be replaced at significant heartache and expense, a mobile phone might contain the keys to your banks accounts, employer's intranet, or your identity. Bluetooth based identify the positioning is one of the hotspots in LBS since Bluetooth 1.0 published in 1999. At present, more than 80% of mobile devices support Bluetooth, including nearly 100% of smart phones and PDAs. Besides, it is easy to establish an economic Bluetooth wireless sensor networks due to its low cost and low power consumption. BLE adopted by Bluetooth Special Interest Group in 2010 has many improvements compared with the traditional standard. The most prominent feature is its low energy consumption. Very low operation and standby power can make a button battery works continuously for several years, which makes using Bluetooth to realize identify the positioning has broad application prospect. Another advantage is the longer range than originals. It can be as long as 100 meters by adjusting the transmit power, which makes it possible to realize wide range indoor positioning by using Bluetooth 4.0. In addition, Bluetooth 4.0 is fully compatible with previous standards and retains the adaptive frequency hopping mechanism, which makes the Bluetooth positioning more feasible and reliable man other positioning technologies [1].

This paper focuses on Bluetooth indoor positioning. Bluetooth provides several major kinds of parameters related with location estimation such as received signal strength indicator (RSSI) and link quality indicators (LQI). We concern with RSSI only in this paper. RSSI based positioning methods commonly used can be divided into range-based methods and range-free methods and we will study the former in this paper. Therefore, the algorithm developed in this paper is to find the relation between RSSI and range, which would be used in real-time location. Lots of work has been done on this direction. [2], [3], [4] focus on optimizing correlation model between RSSI and distance, while [5] is interested in establishing the relational database for RSSI and distance.

II. RELATED WORK

A. Mobile Anti-theft apps

These apps provide precautions against loss of mobile phones. They offer features not only to guard but also regain it in case it is lost or stolen or accidentally taken. Hounds, Prey, adgetTrak, Motion Alarm, Snuko are few of the examples of such apps.

B. Blue Watchdog

Blue watchdog turns your mobile phone into an all-purpose anti-theft device which sets a user-defined protection radius of between one and 30 meters around the mobile phone in your pocket using Bluetooth functionality. The credit-card-sized, EUR60 Secu4 Blue Watchdog is so useful it just might generate killer app adoption levels for protecting your valuables, luggage, and perhaps even your children when you're on the go [6].

C. Personal Safety Apps

The aim of the features of this mobile app is to aid personal security. This includes sending text messages or emails that consists the location of the victim, generating alarm etc. It triggers using different mechanisms like pressing and holding the phone's switch button for a few seconds, shaking the phone vigorously [7].

D. ILA Security

ILA Security device was designed by Simon McGivern, James Phillips, and Neil Munn. It consists of three personal alarms. These are easy to carry and used to shock and disorient potential attackers thus drawing attention of public towards any dangerous situations. Extremely loud female yell is emitted when the Dusk alarm is activated. The ILA Pebble sounds a piercing 130-decibel alarm on its activation. Both can attach to a keychain or clip onto a handbag for easy access [8].

III. METHODOLOGY

Numerous theoretical derivation and empirical formula show that there is a definite relationship between the RSSI and range. In fact, there are repeatability and interchangeability in measurement of RSSI and moderate changes of RSSI have rules to follow. In this paper, we analyze the relationship between BLE RSSI and transmission distance based on the commonly used logarithmic attenuation model in [9] that is shown in (1).

$$[P_r(d)]_{dbm} = [P_r(d_0)]_{dbm} - 10nlg\left(\frac{d}{d_0}\right) + X \quad (3.1)$$

Pr(d) represents the received signal strength of receiving end when it is d away from transmitting end; Pr(d0) represents the received signal power when the it is the reference distance away from transmitting end and d0 is the reference distance; n is attenuation factor for RSSI; X is normally distributed variable whose average is 0. It can be seen from above, RSSI decreases as distance increase and each RSSI mapping for a distance value. However, we would use a simplified formula below based on (1), which we set the reference distance is 1meter.

$$P = A - 10nlgd \quad (3.2)$$

Here, we use P represents the received signal strength of receiving end when it is d away from transmitting end; A presents the received signal power when the it is lm away from transmitting end and n represent the attenuation factor.

A. Unified sampling but training alone

We design and develop four CC2540 development boards integrated with BLE function as the BLE reference nodes in positioning in our research. Although the structures and features of these nodes are of the same kind, their propagation model of RSSI has certain differences because of different location. In order to eliminate the heterogeneities between reference nodes, we develop the RSSI sampler on smart phones, which is able to sample uniformly for different reference nodes at a time. Training method takes the MAC address marked in the training data of reference node as an identifier to isolate it and performs training for these nodes respectively. The result is shown in figure-1. The results show that unified sampling but training alone can reduce the differences between reference nodes in real environment, which could improve the accuracy of positioning in real time without increasing the workload.

B. Gaussian filter for training data

The value of RSSI will fluctuate because of the randomness of RF signals when you collect the training data. Consequently, there is no one-to-one correspondence relationship exists between RSSI and distance any more, which makes it hard for sample data used directly. Therefore, the premise of improving accuracy of positioning is to reduce the randomness of training data. The method commonly used is averaging the data obtained from multiple sampling and taking the result as the valid value.

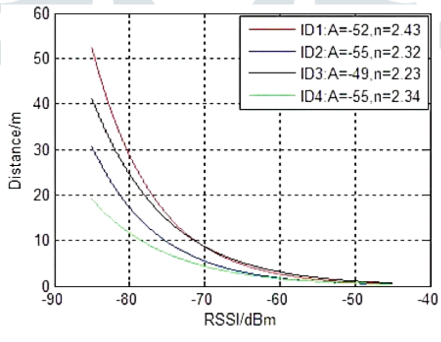

Figure-1.Reference Nodes for different propagation Models

It can be seen as shown in formula (3):

$$RSSI = \frac{1}{m}\sum_{i=1}^{m} RSSI_i \quad (3.3)$$

However, using the averaging method does not reflect the actual features of RSSI in real environment. What's the worse, the effects of reducing the randomness would be remarkable only when large amount of data is collected, especially there is a big random perturbation exists in data, which increase the workload greatly.

Another method is to take the RSSI and distance of known pairs of nodes as reference when you calculate the distance between targets and known nodes, namely, using the existing information to adjust the real-time RSSI. However, it is not always effective because of differences that exist in structures and real environment of different nodes. Besides, there is no exact proportional relationship between RSSI and distance. Lots of research has been done on RSSI propagation and they attempt to explain the fluctuations of RSSI. Reference [10] uses the Markov model to perform joint state estimation of no-line-of-sight propagation and line-of-sight propagation, which aims at judging whether the RSSI suffers reflection and diffraction effect. However, the method is of complicated calculating and multipath effect is difficult to quantify [1].

Therefore, practicality of this method is not high. It is known to all that the limit distribution of the sum of independent random variables is normal distribution. In fact, a large number of experiments show that the randomness of RSSI is relative dependent and the distribution of RSSI at a certain point can be thought as a Gaussian distribution. To be cautious, we perform extensive statistical analysis on BLE RSSI and the result is shown in figure-2.

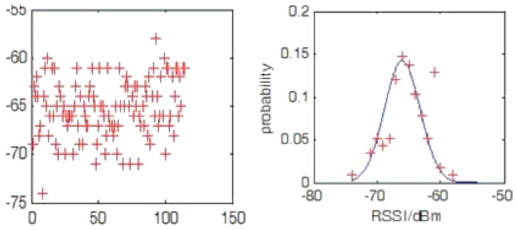

Figure-2.Distribution of BLE RSSI

As can be seen above, Gaussian distribution can reflect the randomness of RSSI in real environment better. Therefore, we will use Gaussian filter to filter out the values of RSSI of small probability to solve the problem that propagation of BLE RSSI are susceptible to interference, as well as to eliminate those short disturbance of small probability. Algorithm process as shown below:

1. Using an array to store the training data for every sampling point.
2. Calculating the mean and variance of every Gaussian filter with the formulas below.

$$\mu = \frac{1}{m}\sum_{i=1}^{m} RSSI_i \quad (3.4)$$

$$\sigma^2 = \frac{1}{(m-1)}\sum_{i=1}^{m}(RSSI_i - \mu)^2 \quad (3.5)$$

$$f(RSSI) = \frac{1}{\sigma\sqrt{(2*\pi)}} e^{-(\frac{(RSSI-\mu)^2}{2*\sigma^2}} \quad (3.6)$$

3. Determining the effective range of RSSI according to μ and σ2 and a critical value choose to be 0.6 according to analysis of large amount of training data. Formula is shown as below.

$$0.6 < \int_{MIN\_RSSI}^{MAX\_RSSI} f(RSSI)dRSSI < 1 \quad (3.7)$$

4. Averaging the values which are in the effective range and taking the results as the input of the training model.

IV. Experiment

A. Hardware

To evaluate the performance of the proposed algorithm, we conducted experiment at electronics laboratory. The BLE beacons used in the experiments are based on Texas Instruments (TI) BLE chip CC2540. This chip broadcasts channel information and RSSI value together for each advertisement channel, which can received by an android OS device when using smartphone.

A hardware connection shown in figure-3. The BLE beacon Tx and Rx pins are connected to the Arduino's pins D8 and D9 respectively. So, Arduino and BLE beacon communicate through serial communication. The buzzer and vibrator connected to Arduino's pins D6 and D7 respectively.

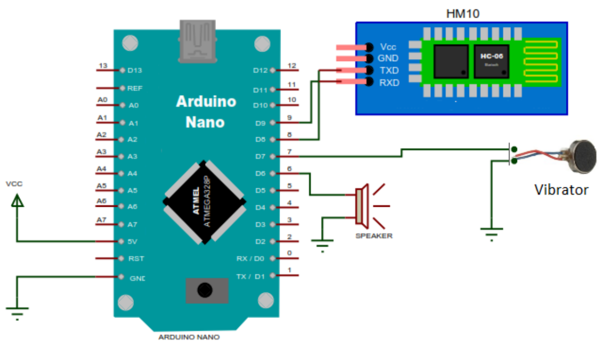

Figure-3.Hardware schematic circuit diagram.

B. Software

In this experiment developed android app using App Inventor to communicate BLE beacon and Mobile. App Inventor 2 (AI2) is a fairly easy way to get in to creating Android apps. It uses the Blocky programming system rather than text and does a lot of the heavy lifting for you. AI2 is contains latest BLE extension. Figure-4 has shown the schematic sketch of AI2 for android app. The figure-5 has shown design of android app, it contains scan the Bluetooth devices and connect the Bluetooth and status of buzzer which having a hardware receiver.

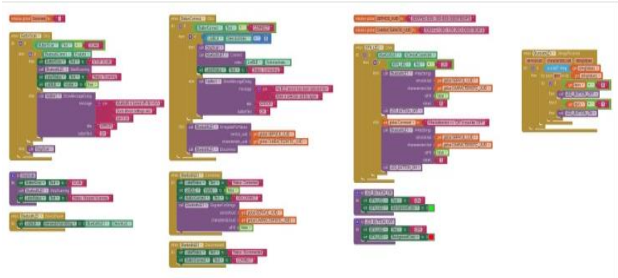

Figure-4.Schematic sketch of AI2

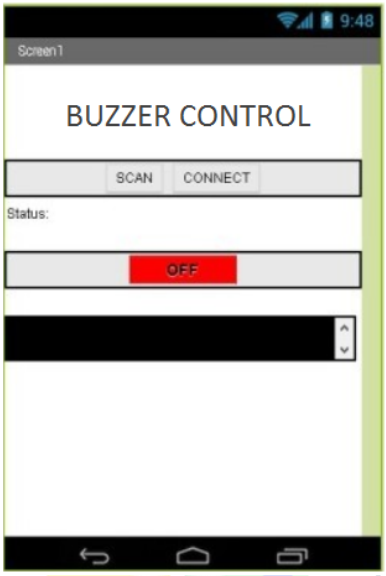

Figure-5.Mobile app for connect BLE and buzzer control indication.

V. RESULTS AND DISCUSSIONS

First we paired the smartphone and BLE, then collected the RSSI data of BLE beacon shown in figure-6. We identified RSSI value of two meters distance is -75db, so we gave the command in mobile app when the RSSI value exceeds -75db, the mobile send the command 'Buzzer ON' to Arduino microcontroller via BLE beacon. The Arduino decode the command switch on buzzer and vibrator at the same time. The android app also toggles the speaker and flash in smartphone to identify the smartphone direction. This hardware is very small and possible to make as a keychain or tag. So to protect the mobile from thieves keep the hardware is either in pocket or in bag and activate the app in mobile. Using this Bluetooth Based Anti-Theft Tag for Smartphones user can understand when mobile snatching from his pocket or hands and react immediately.

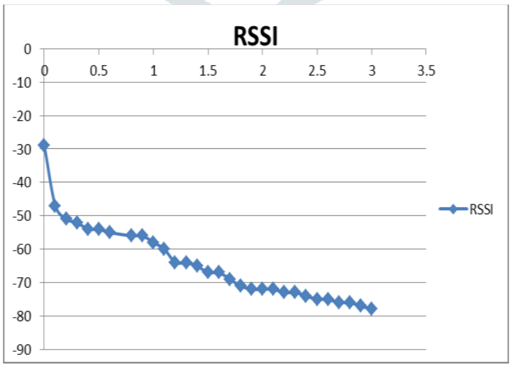

Figure-6.Graph between RSSI value and distance

We kept the RSSI value of -72db at distance of 2meters. When the distance is increased more than two meters

VI. CONCLUSION

Bluetooth based anti-theft device for smartphones system can be tested using mobile easily. This security system is suitable for a real time monitoring of the smartphone and avoid the theft. If the connectivity between mobile and Bluetooth module is more than two meters, mobile sent the command to hardware. Then hardware received the command and gave the alarm and vibration continuously. At the same time in mobile also toggled the light and sound to identify the mobile location. This hardware device is small and looks like a keychain to keep in pocket. Bluetooth Based Anti-Theft Device for Smartphones system will anonymously and securely help you to find adumbrate the smartphone snatching. This essentially expands your reach to anywhere in the world. The more number of people use it the better the capability.

REFERENCES

[1] Zhu jianyong, Luo haiyong, Chen zili, Li zhaohui, "RSSI Based Bluetooth Low Energy Indoor Positioning", 2014 International Conference on Indoor Positioning and Indoor Navigation, 27th-30th October 2014.

[2] Zhen Fang, Zhan Zhao, Daoqu Geng, Yundong Xuan, Lidong Du, Xunxue Cui, "RSSI Variability Characterization and Calibration Method in Wireless Sensor Network", International Conference on Information and Automation, June 20-23, 2010, pp.1532-1537.

[3] A . Awad, T. Frunzke, and F. Dressler, "Adaptive distance estimation and localization in wsn using rssi measures," in DSD, 2007, pp. 471–478.

[4] H. Y. Shi, "A new weighted centroid localization algorithm based on RSSI," in Proc. International Conference on Information and Automation, 2012, pp. 137-141.

[5] Pei-gang SUN, Hai ZHAO, Ding-ding LUO, "Research on RSSI-based Location in Smart Space," ACTA ELECTRONICA SINICA, 2007,vol 35(7),pp:1240- 1245.

[6] https://newatlas.com/blue-watchdog-mobile-phone-all-purpose-anti-theft-device/16471.

[7] https://en.wikipedia.org/wiki/Personal_safety_app last accessed on 19 July 2015, at 17:04.

[8] http://www.ilasecurity.com/uk/ last accessed on 19 July 2015, at 17:30.

[9] M. Hata, "Empirical Formulae for Propagation Loss in Land Mobile Radio Service, " IEEE Trans. Vehic. Tech., vol. VT-29, no. 3, pp.317-325 198.0.

[10] J. Wang , Q. Gao , Y. Yu , H. Wang and M. Jin, "Toward robust indoor localization based on Bayesian filter using chirp-spread-spectrum ranging", IEEE Trans. Ind. Electron., vol. 59, no. 3, pp.1622-1629 2012 .