Off-phone Tracker

Mihir Tayshete, Shaurya Sharma, Ranveer Shah,
Shreyash Suthar and Jalpa Pandya

Off-phone tracker

Mihir Tayshete
Department of Engineering Science & Humanities
Thakur College of Engineering & Technology (TCET), Kandivali East, Mumbai
mihirtayshete@gmail.com

Shaurya Sharma
Department of Engineering Science & Humanities
Thakur College of Engineering & Technology (TCET), Kandivali East, Mumbai
shaurya064@gmail.com

Ranveer Shah
Department of Engineering Science & Humanities
Thakur College of Engineering & Technology (TCET), Kandivali East, Mumbai
ranveer2001s@gmail.com

Shreyash Suthar
Department of Engineering Science & Humanities
Thakur College of Engineering & Technology (TCET), Kandivali East, Mumbai
shreyash.91suthar@gmail.com

Jalpa Pandya
Department of Electronics Engineering
Thakur College of Engineering & Technology (TCET), Kandivali East, Mumbai
jalpa.pandya@thakureducation.org

Abstract—**In this age of technology, one of the worst things to happen to an individual is to lose one's cellphone which contains all important data. It is found that one in every 10 smartphone users are a victim of phone theft with recovery rate being less than 10%. The aim of this study is to increase that recovery rate with the help of existing wireless technology. Current locating systems use GPS and IMEI but that becomes ineffective when the device is turned off. This paper discusses our concept of tracking a phone indirectly through existing wireless technology which requires certain tweaks to give the current system security enhancement.**

Keywords—tracking; switched off; Bluetooth; locating; stolen; finding

I.   INTRODUCTION

Local trains are the lifeline when it comes to cities like Mumbai. Millions commute through it daily and unfortunately it is the hotbed for phone theft. 56,486 phones were stolen in 2018-19 alone which amounts to ₹6.08 crores. According to GRP (general railway police), the data percentage of phones recovered was 8.65%. This is the state of just Mumbai railways which only comprises the reported data. 7 crore phones are stolen each year with only 7 % being the global recovery rate.[1] In current systems, we are using GPS through applications like find my device(google), GPS WOX, Find My (Apple), etc. This software is useful only if the device is ON. Tracking through IMEI No. relies on the SIM in the phone hence it becomes untraceable if the SIM is removed. Also, the IMEI No. can be altered easily by just rooting the phone. By using already available Bluetooth technology we can track a stolen phone. Bluetooth's low-energy radio wave technology transmits frequency between 2.400 GHz to 2.4835 GHz which has a practical range of up to 10 meters. We can transmit data which can be used to indirectly locate a phone [2].

II.   COMPARATIVE STUDY

Apps, like 'find my device' for Android, have features like erasing device memory, playing alert tones, allowing users to remotely lock their devices and sending emergency messages. These features become useless if a thief goes offline, switches off the phone or factory resets it. Similar is the case with other operating system and their software. Ideas have been proposed suggesting to use solutions like smartphone remotes wherein an alarm will be triggered at the press of a button through a remote manually even when the phone is switched off. There's a major drawback that the phone should be under the vicinity of 5-20 m of the remote [3].
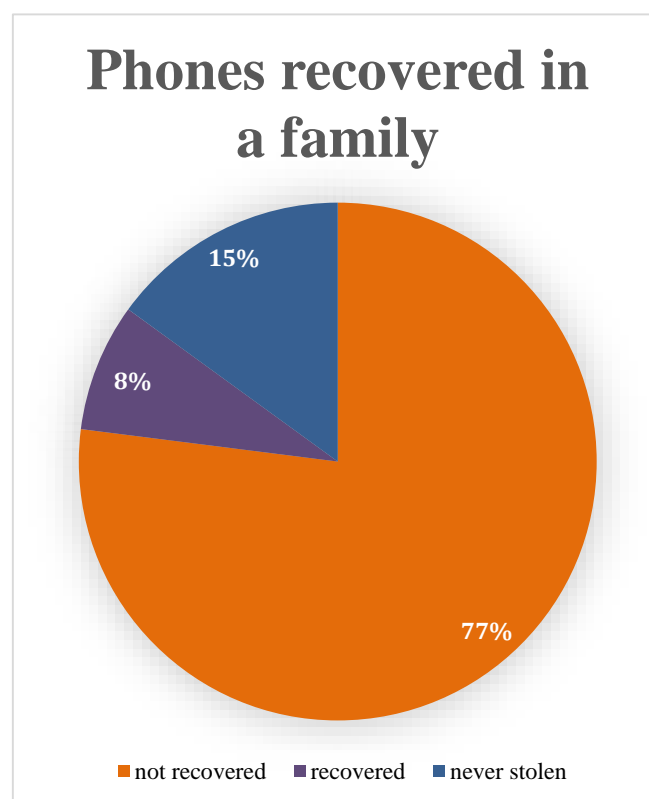

Fig. 1.   Statistics of stolen phones

The concept of the undetachable SIM has been considered where the SIM will be built into the motherboard itself. Here the SIM can be triggered impelling the phone to turn ON. But no research has been done yet regarding it and it'll be useless if the battery drains out. Besides, this must be added to new devices which is not feasible.

III. TECHNIQUES USED

The main concept revolves around using a Bluetooth module which activates when the phone is switched off. This Bluetooth module will transmit a certain unique code which will be provided by us at the time of a new registration or with the purchase of a new phone. This code will be received by the phones in the vicinity. This data can be sent to a maximum of seven phones by the Bluetooth module. Fig.2 shows how these phones can work together to accurately determine the position of the switched-off phone, similar to the current G.P.S functioning. This requires the Bluetooth of the receiver to be continuously ON. Users might worry that keeping Bluetooth always ON would drain their battery life. But that's not completely true.

If we just keep 100 mAh of supply separate for our Bluetooth module, it can work up to 6 days. Knowing these stats, simple provisions can be made by IOS & Android to keep the Bluetooth ON every time. A Separate partition will be required to be made so that the Bluetooth keeps working even while the user might have drained all its battery. For an existing device, this partition of 100 mAh shall be done virtually by the means of software tweaking, while newer phones can be provided with a separate battery. A separate battery provided should be embedded deeper into the phone making it more secure from being accessed by the thief. Coming back to how the nearby devices can help locate the phone? These surrounding devices (if G.P.S enabled) will be sending us their location with all the Bluetooth codes they can scan at the moment. The information of the sender will remain anonymous similar to Google Maps' traffic overlay. According to a short survey conducted by us [Figure 4], 55 % of users have their G.P.S ON every time while international studies have shown that this stat can be as high as 70%. After all these steps, if the crowd is unwilling to accept the required steps, we can keep them choosing to opt-in this ecosystem to have their phones founded or find other's devices, similar to how WhatsApp works with its privacy. The location that we get from the receiver's mobiles can be received onto an online server. This server can be accessed by the victim, on logging in with the secure password that will be given to the user on the purchase or creating an account.

IV. WORKING & CHARACTERISTICS

A. Battery

The Bluetooth low-energy present in all phones will consume as low as 1mW of power and can do with a maximum power of 2.5 mW of power for basic functions. For a relation, with an average battery of 2500 mAh and taking the power consumption to be 2.5 mW, it will work for a total of 3600 hours [5] that is equal to 5 months approximately.

B. Bluetooth module and receiver

To find the devices in its proximity, the Bluetooth does an inquiry scan where it sends those devices a request, asking for their MAC addresses. The Bluetooth module in the nearby active devices will send an inquiry request to the switched-off phone. The recommended inquiry scan duration given by Bluetooth is 10.24 seconds but this can be reduced to 11.25 milliseconds of short bursts repeating every 1.28 seconds without losing any efficiency [4]. This will help conserve power and lead to a lesser interference in the neighbouring Piconets. The sensitivity of the Bluetooth module is -70dBm.

The Bluetooth module can then read the MAC addresses of the phones and continue to update it on the server. This whole process is secure as there is no pairing that happens.

C. Server

All the information about the location collected needs to be gathered somewhere. For this purpose, a server is set up wherein the different devices also known as clients can send their co-ordinates. This server will provide different services. For example, the user can access this server through his account and check for the location of his phone by entering the specified code. The server is secure as the location can be accessed only by one user but the location can be constantly updated by multiple people who are already part of the network after coming within the proximity of the phone.
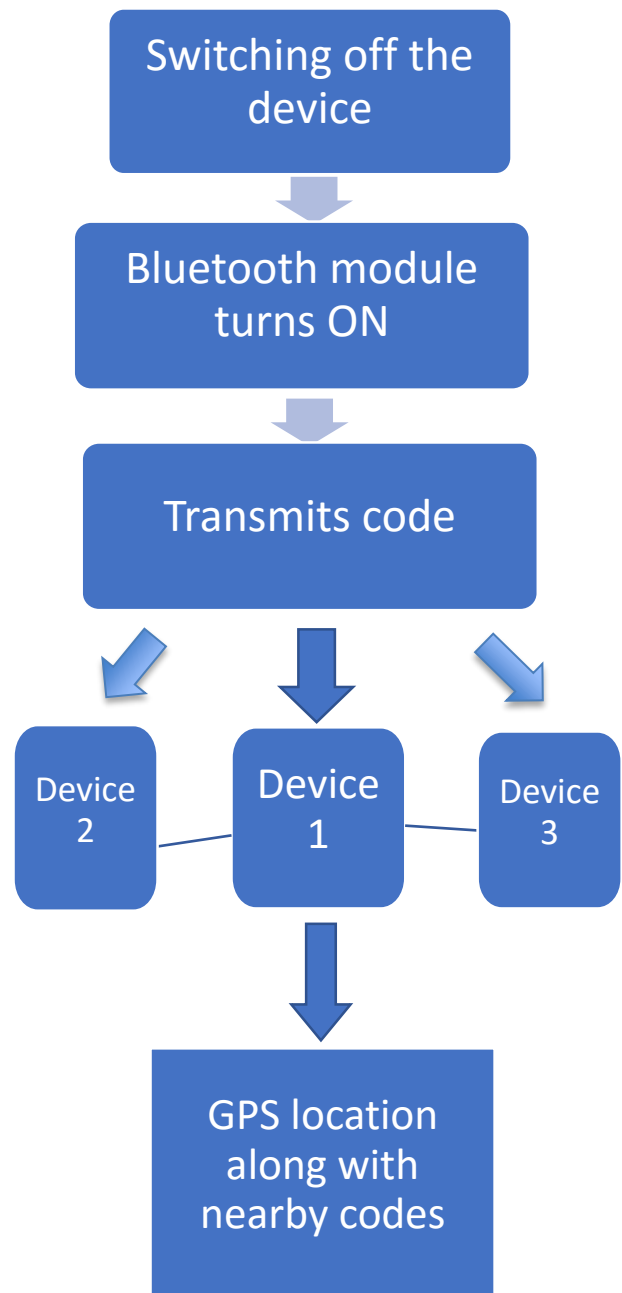

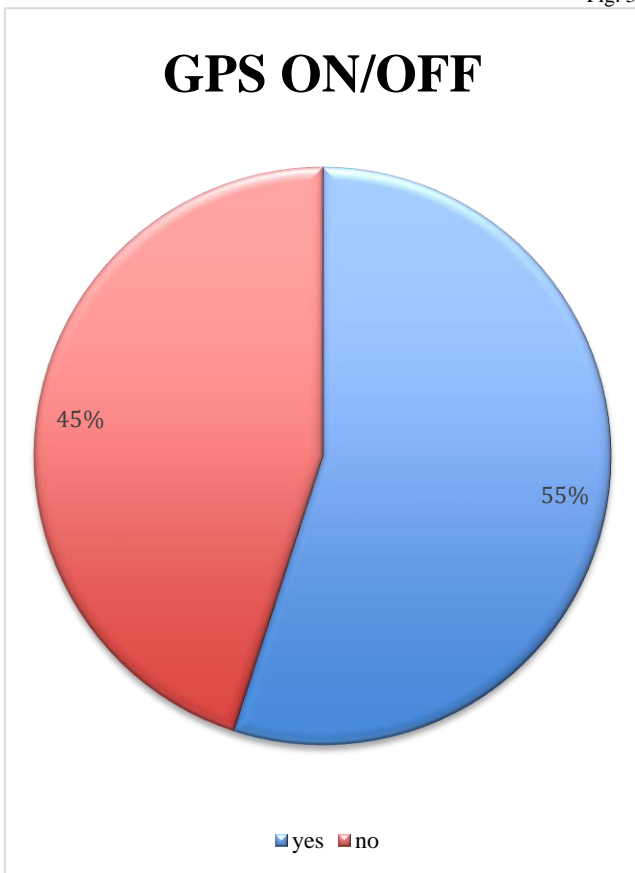Fig. 2.   Basic Protocol

Fig. 3. Stolen phone cycle

Fig. 4. G.P.S status based on the survey

VI. CONCLUSION

Bluetooth and wireless technology have never ceased to grab our attention and its applications are vast in today's technological world. Bluetooth modules can be utilized to transmit phone location data to other devices and help to track a stolen phone even while it's switched off. A global network of tens of million devices with our Bluetooth modules shall create an anonymous location tracking network in which stolen switched off phones can be tracked which shall result in propelling the recovery rate of stolen phones. This provides powerful resistance against a threat to important data which makes the world more secure and connected.

VII. FUTURE SCOPE

Later on, this can be converted into a standalone device with a dedicated battery and a Bluetooth module which will be compact. This standalone device could be used in dog collars for finding out dogs in case they go missing, on Alzheimer patients, finding out where your child is, etc. Furthermore, the advancement in wireless technology will result in an increase in the data transfer speed, range and also power efficiency. With the development in Bluetooth technology, the size of the devices is becoming smaller and smaller with the current smallest Bluetooth module SESUB-PAN-T2541 having dimensions of only 4.6 mm x 5.6 mm x 1.0 mm. [6] We look forward to carrying our research shortly.

REFERENCES

[1] 77 phones stolen daily on locals; Mumbai Mirror; January 28, 2020.

[2] Carles Gomez, Joaquim Oller Bosch, Josep Paradells, "Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology," research gate December 2012

[3] Newton Lwanga, "Integrated Phone Locator (IPL): Lost Mobile Phone Tracking and Recovery Designs," ResearchGate April 2016

[4] B.S. Peterson, R.O. Baldwin, J.P. Kharoufeh, "Bluetooth Inquiry Time Characterization and Selection," IEEE Transactions on Mobile Computing (Volume 5, Issue: 9, SEPT,2006).

[5] Lawrence Finch, Wi-fi and Bluetooth Battery Drain and other considerations," Apple Community forum Oct 24, 2017

[6] Micro modules: World's smallest Bluetooth Smart module in production; News Centre TDK global; Feb 12, 2014.