An Application of IEEE 802.21 Standard for Laptop Theft Deterrence

Nygil Alex Vadakkan; S.E.Vinodh Ewards
School of Computer Science and Technology
Karunya University
Email: nygilalexvadakkan@karunya.edu.in; ewards@karunya.edu

***Abstract*—Theft of electronic gadgets like laptops, mobile phones, etc. is a problem that has been affecting people all over the world for a long time. So, a scheme of RFID/Wi-Fi hybrid based theft deterrence that is effective and can be easily employed in laptops and similar computing devices is being proposed here for the future as the price of these hybrids come down. The main focus here is on IEEE 802.21 standard which has been developed for Media Independent Handover (MIH) Networks meaning that the particular device would be able to communicate with a multitude of networks including the telecom network, Wi-Fi networks, etc. The selection of IEEE 802.21 standard is to use it as a model for communication as it could be the next major change in the standard of communication networks, thereby paving the way for Internet of Things (IoT) based devices with a multitude of connection options.**

Keywords: IEEE 802.21, IEEE 802.11 Theft, Active RFID, IoT.

I. Introduction

In recent years, as man's dependence on electronic devices have greatly increased, so has the rate of their theft. It is estimated that smart phones are the ones that are being targeted the most, as they are usually small and quite convenient to be stolen in comparison to larger electronic gadgets. The proposed mechanism here can be installed in a variety of gadgets, once IEEE 802.21 standard supported devices are available within the market. The aim is to develop a model and setup experimentally the possibility of data retrieval between a stolen device and other RFID readers and/or 802.11 Wi-Fi Access Points, so as to create a map of left-over digital fingerprints of the stolen device.

II. Background

IEEE 802.21 standard was defined by the IEEE for the ability of a device to connect to a heterogeneous set of 802.11 networks seamlessly based on various user-defined policies.

The basic components of Media Independent Handover (MIH) architecture in IEEE 802.21 standard has been shown in Fig.1. The Mobile Node (MN) performs seamless handoffs, using Media Independent Handover (MIH) framework which are guided by the following important services, i.e., Event Service, Command Service, and Information Services. They are detailed as follows:

- Event Service is responsible for sending triggers based on the occurrence as well as change of events in an MIH service.
- Command Service on the other hand works on the basis of certain pre-determined commands that are used for making changes in the handover control procedures.
- Information services gives detailed information on the availability of networks, their types, standard of operation followed for service request, etc. MIH Function is an interim layer that controls and coordinates the information transfer among a multitude of devices for the purpose of handover decision making.

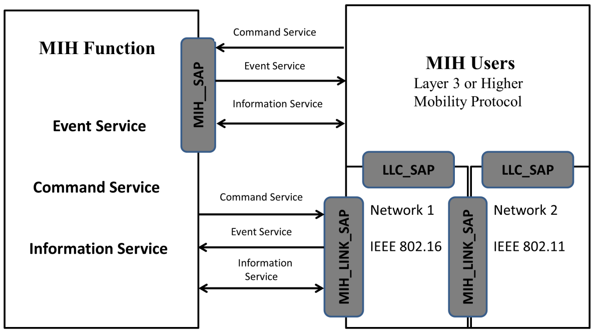

Fig. 1. IEEE 802.21 based MIH architecture

Media Independent Handoff Service Access Point (MIH-SAP) is a part of the MIH function that deals with initiation and subsequent termination of the handoff services. MIH-LINK-SAP is responsible for providing the interface between the MIHF and lower layers of the protocol stack [1].

III. Related Work

Before moving onto the proposed mechanism, an analysis of the older and current security models used are important, so as to have an idea about how various security strategies have evolved over time.

A. Software Based Systems

There are multitudes of software based anti-theft system in the market that promises quite a lot of options to choose from when it comes to anti-theft technologies. Some of the common ones are as follows:

- Remote lock down of the electronic gadget
- Sound a siren/alarm tone
- Display the actual owner's alternate telephone number in case the device was misplaced by the owner.
- Display of the mobile phone location on a map with the help of service provider's tower coupled with Global Positioning System (GPS).
- Alert to alternate mobile number with the International Mobile Equipment Identification Number (IMEI) in case a new Subscriber Identity Module (SIM) is inserted in the stolen mobile phones
- Delete confidential files
- Activation of the mobile/laptop front-facing camera to snap pictures of the person who is using the device which are silently sent to the original owner's alternate email-address or mobile number.

The working system is based on the reception of a pre-determined text message to the mobile or a remote message to the installed monitoring application in the case of laptop which triggers the default response set by the owner. There also exists software based systems that are designed to overcome total formatting of the device's internal memory. [2].

B. Service Provider Based Systems

In the case of support from the service provider [3], it mainly involves blacklisting and/or monitoring the phone with the help of unique IMEI number. The service provider can also block the usage of the phone rendering it completely useless based on a national level blacklist.

C. Hardware Based Systems

Although not much commonly used in comparison to software, various types of hardware locks are available in order to tie down laptops to a given objects. The locks could have built-in functions such as buzzers or alarms when tampered. [4]. Hybrid solutions that couple both hardware and software are also available in the market.

D. RFID Tags

There are mainly two types of RFID tags – Passive RFID and Active RFID. The passive RFID tag has two main parts which are the tag's antenna and the integrated circuit. The passive RFID works by receiving a signal to the antenna from the RFID reader and using it to power the circuit which generates a signal back to the reader known as backscatter.

The active RFID tag has an additional part compared to the passive RFID which is the additional battery. Among active RFID tags, there are mainly two types- which is the transponder type and the beacon type. The transponder type waits for a signal from reader similar to the passive tag and then sends out the relevant information. This helps to conserve the battery life of the tag by not having to transmit continuously. The beacon type transmits consistently on fixed intervals [8].

IV. Design Considerations

The proposed mechanism mainly focuses on using a hybrid kind of active RFID tags coupled with the ability to connect to IEEE 802.11 based wireless networks. This allows the active tags to push basic device information to the entire wireless network it can connect to. With the help of additional developments in the IEEE 802.21 standards, the active tags should also be able to easily connect with much more communication networks in the future. Such kinds of tags are known as 802.11 Active RFID tags [7]. Similarly, Multimode RFID tags can acts as Passive RFID tags and 802.11 Active tags depending on how they are programmed.

- GPS: There are also special reasons as to why the usage of a Global Positioning System (GPS) was not considered in the case of laptops as it consumes typically more power over a longer period of time, costs much more and could also have problems locating satellites depending on where they are. The inbuilt availability of GPS transceivers in smart-phones can also increase the option of tracking stolen mobile phones if they are powered on and has supported software installed into it by default.
- Bluetooth: Another option would be to use the Bluetooth Low Energy (BLE) module, but again the estimated coverage depending on the type of chosen module would be limited.
- RFID tags: Currently, Active RFID tags are quite expensive compared to their cheaper counterpart Passive RFID tag. The reason active tags are much more expensive is that they have an additional battery and use it to communicate to the reader or receiver [5]. The cost would vary depending on the coverage and the type of Active tags used. For example, the Ultra High Frequency Generation 2 RFID Active tags have higher range and coverage and it is on the cheaper side when compared to similar alternatives with the same range [6], [8].
- Role of IEEE 802.21: The IEEE 802.21 standard implementation is done in such a way that it can be used on a wide variety of hardware without compatibility problems. The major challenge in implementing the MIH system is to develop and test an algorithm that decides when a device has to perform the handover from one WLAN network to another or in case of WLAN unavailability, the option to switch directly to the telecom networks without human intervention. Moreover, there are also low-power Wi-Fi enabled modules that would perform way better than RFID tags, but here the focus is not just large coverage but also conservation of power where RFID tags would be way better with very low coverage and at the same time also has the option to connect to WLAN access points when required. So, here the proposition is made totally focusing on the usage of a hybrid 802.11 RFID tags.

V. Handover

The basic handover among networks is based on the determination of signal parameters like Received Signal Strength

Indicator (RSSI) or commonly known for 802.11 networks, Received Channel Power Indicator (RCPI) that would determine whether a successful handoff is possible or not from one network to another. A real life scenario would be, when we move from one WLAN coverage area to a different WLAN area, a computer typically tries to connect to the new one automatically as long as the new network has the required RCPI and has saved the access credentials first time it was entered. The value of RSSI is calculated in terms of decibels (dB) or varies from 0 to 100 in terms of simple numbers.

In our model, we can decide the required signal strength for an attempted connection to a given WLAN network as low as possible because the aim here is to track an electronic gadget by making maximum number of connection attempts (successful or failed) to any available 802.11 networks with a preset interval. Most enterprise grade access points have logs for Media Access Control (MAC) both successful and failed login attempts. So, this can help us create a rough digital map of the area the device has been moving through, although this would require combing through the logs of various access points in the vicinity where the device was stolen with the help of law enforcement officials. In short, the proposal here is to develop a system with these features acting like a 'beacon' while the perpetrator is on the run with stolen gadgets.

VI. Tamper proofing the design

When security systems are designed or proposed, a lot of effort and testing goes into it to make sure that the system is not easily vulnerable to tampering. So, the following is an analysis on such possibilities from the perspective of an Original Equipment Manufacturer (OEM) to make the proposed system here free from tampering:

- Make sure that the circuitry involving the control and communication of the active 802.11 RFID module are deeply integrated into the motherboard circuitry of laptop. This makes it really hard to tamper as the probability of damaging other components increases.
- Integrating the power circuitry for the active RFID tag into that of the laptop's battery plus a tiny backup battery. This makes sure that even if the laptop is charging or not, the tag consistently receives relatively some amount of power from the laptop battery or backup cell for 'beaconing'. A point of weakness here is that the backup cell could be cut out or the laptop battery be removed by the perpetrator. In this case, it is quite easy for the OEMs to make sure in the Basic Input / Output System (BIOS) that the laptop boots up 'only' if there is either an external power source (AC adapter) or the laptop's battery coupled with the tiny backup battery. Hence, it ensures that any tampering with the active 802.11 RFID tag would make the laptop totally useless.
- Another additional proposition which is commonly seen in the market for high end smart-phones would be to create a system by laptop manufacturers to remotely track the laptop in real time whenever the device is connected to the Internet and send the log files automatically to the actual owner once the device is marked as missing. There are free and paid versions of programs like 'Prey' that provides similar solutions. The installation of such software would really speed up the recovery process of the laptop with the help of enforcement agencies as it allows remote control of laptop camera, Internet logs, location, etc. [9].

VII. Experimental Setup

- MFRC522: The experimental setup involved the use of an electronic MFRC522 reader and writer for contact-less communication at 13.56 MHz. It was used for reading data from the RFID tag as well as writing data into it. It supports I2C, SPI and UART protocols. SPI interfacing was used for this project.

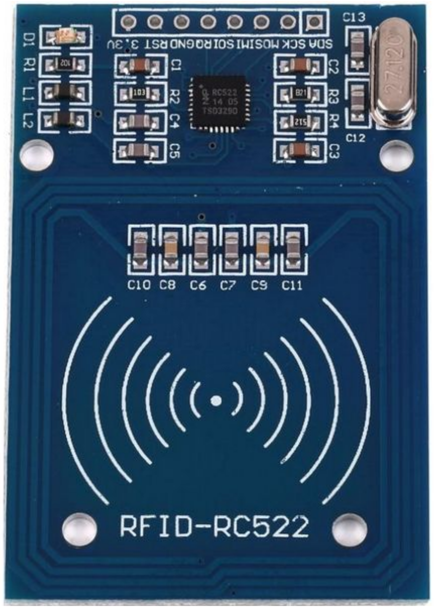

Fig. 2. MFRC522

- RFID tag: A cheaper passive tag was used as an alternative to the much more expensive active 802.11 based active tags.

Fig. 3. Passive keychain tag

- Arduino UNO R3: An Arduino UNO R3 circuit board with ATMega328P micro-controller was programmed to read the data directly from the RFID reader and was pushed to the USB serial output and saved as log files in the remotely connected machine within the same network. The logs were read out from the serial output using a Python script along with system time stamps and saved as text files which could be sent to any machine or remotely monitored. An additional possibility of pushing data out directly into a server connected to the Internet is also done using the Ethernet shield.

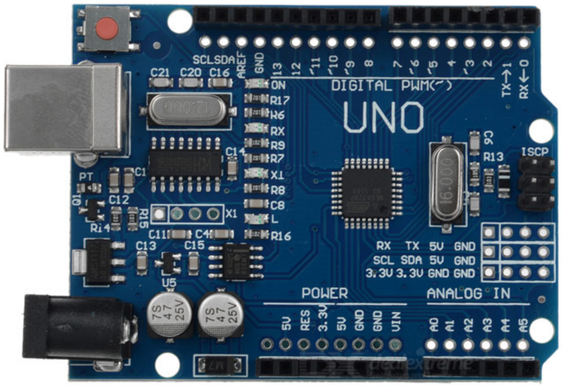

Fig. 4. UNO R3

- Ethernet Shield: The Ethernet shield allows to pass the data read from the RFID tag to an Ethernet port using RJ-45 cable and eventually into a local server within the same network configured to receive and store data allowing the possibility of accessing logs remotely from anywhere in the world.
- 20 female to male cable: The female to male cables were used for interfacing the RFID reader to the data pins and 3.3V power supply of UNO R3.

VIII. Tracking and Recovery

The retrieval of relevant data on connection attempts from Access point logs would require a formal intervention from law enforcement officials but this would give out very important information like how long it was connected to the specific access point in case of open network 'or' how many times it attempted to connect to the access point in relatively short period of time even if the connection attempt was unsuccessful. The period of time could give a hint as to whether the perpetrator was walking away or moving too fast as the device left the area of WLAN coverage.

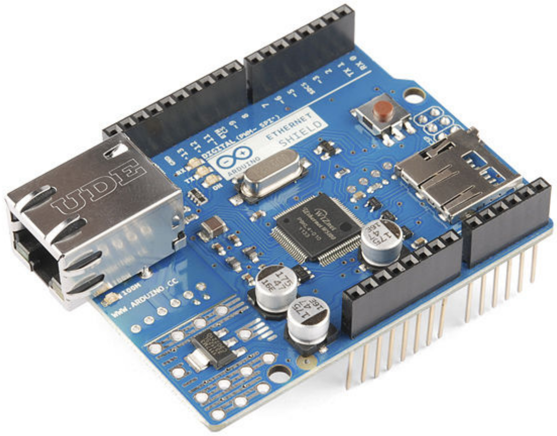

Fig. 5. Ethernet Shield

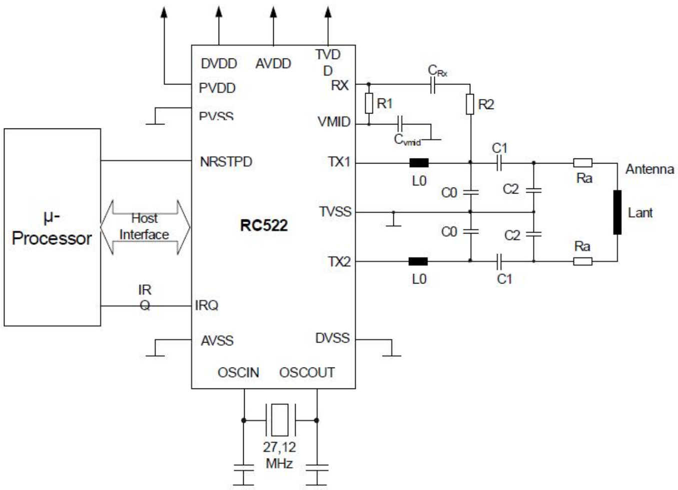

Fig. 6. Circuit diagram for reading RFID tag data

A recovery is only possible after a thorough analysis of the access point logs nearby and if remote theft prevention programs have been installed by default, then the laptop could be visible sooner or later once it appears online. So, a better strategy to keep devices from being lost or stolen would be to rely on a multitude of options to ensure that devices are safe and could be remotely controlled.

If it is found that the specific machine or laptop has attempted successful connections with many open access points or failed connections identifying them with the unique MAC ID (counting out the possibility of being spoofed), then the location of the access points can be marked on a local map which could even show the initial route the perpetrator would have taken to escape the premises. It is true that combing through connectivity logs can be delayed until the authorized law enforcement officials arrive, but here again the key is 'time' or 'time-stamp'. By knowing the rough estimate of local time when the laptop was stolen itself can help in filtering out

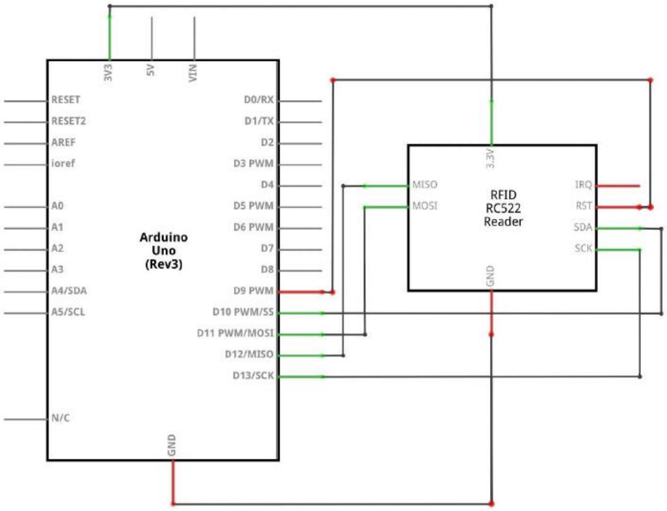

Fig. 7. Connection diagram

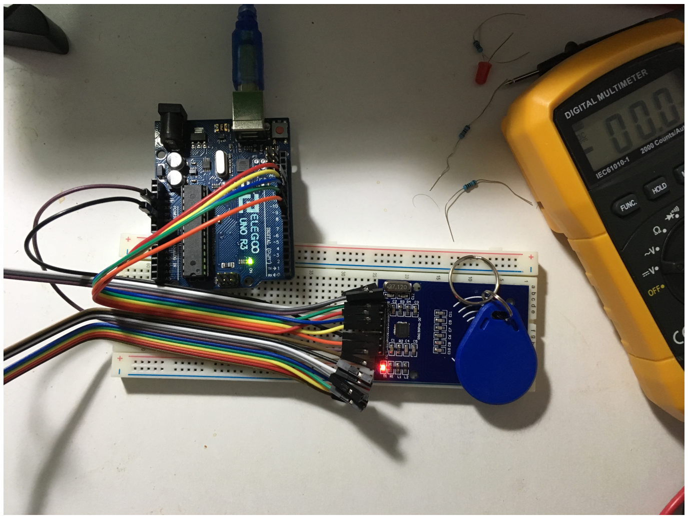

Fig. 8. Setup for USB Serial Out for local storage

large amounts of unnecessary network log data.

IX. Conclusion

The standard of IEEE 802.21 has still the future possibility of evolving much further. It could integrate the possibility of sending and transmitting data even through a wider types of channels and networks. But, due to the difference in hardware specifications of various architectures and technologies, as of now it is only possible to route them through the internal or external memory of the core device involved before sending them to a heterogeneous network.

Acknowledgment

The authors would like to thank the Institute of Electrical and Electronic Engineers (IEEE) for accepting the proposal and funding the application paper research.

References

[1] IEEE Standards Committee, “Part 21: Media Independent Handover Services”, Available at http://standards.ieee.org/getieee802/download/802.21- 2008.pdf, 2009.

[2] Absolute Lojack, [Online], Available: https://lojack.absolute.com/en/persistent

[3] Optus Australia, Lost, Stolen or Found your Mobile Device? [Online], Available: http://www.optus.com.au/shop/support/answer/lost-stolen-or-found-your-mobile-device?requestType=NormalRequestid=1501typeId=5

[4] Kensington Locks, [Online], Available:http://www.kensington.com/us/us/4480/security

[5] Comparison of Intelleflex Semi-passive BAP, Active, and Passive RFID [Online], Available: http://www.intelleflex.com/Products.Semi-Passive-vs-Active-RFID.asp

[6] RFID Frequencies, [Online]. Available: http://www.impinj.com/resources/about-rfid/the-different-types-of-rfid-systems/

[7] RFID tag considerations, [Online]. Available: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/WiFiLBS-DG/wifich6.html

[8] Active RFID vs Passive RFID, [Online], Available at http://blog.atlasrfidstore.com/active-rfid-vs-passive-rfid

[9] Prey Project, [Online], Available: https://preyproject.com/