Spy Device Forensics Using Zig Bee

Aditya Chaubey[1] Mayur Dere[2] Omkar Sonawane[3] Roydon Quadros[4]
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]F.C.R.I.T., Vashi

Abstract— The unprecedented growth of competition in the Information technology has raised the importance of maintaining security in digital field in order to secure all confidential company's information and databases. Analyzing Company's databases for any type of malicious attacks on company may lead to loss of company's assets. This study presents a new stage frame-work of identifying the malicious signals that an attacker can perform within the company's environment in order to get access of databases related to company's assets, employee details, Tender projects, high level catalyst projects. This system will provide information about attacker's scenario that can lead to loss of any data .in this system we will be focusing on all aspects of attacker and in order to intercept attackers function with respect to system's functionality. We will try to intercept the attacks that an attacker will try to get access to assets of the company using signaling frequency.

Key words: Android Application, Android Studio, Wireless communication system, Arduino, X-CTU system, zig bee 802.15.4, PAN ID, Mesh Network, Bluetooth

I. INTRODUCTION

Zig bee is a wireless communication system, there is always a possibility that the transmission could be deliberately jammed or intercepted, or that false or modified information could be passed to the piconet devices. Hence to avoid such unwanted users to get access within the enterprise or within Bluetooth network we will be creating Surveillance tool. In this Project we will be identifying the several spy devices over the wireless network that are untraceable by normal devices ,and regarding wireless network we are mainly focusing on Zig bee Spy Devices.

II. LITERATURE SURVEY

- Zig Bee is an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios .Zig Bee device will help us to trace other hardware devices in the same personal area network.
- Spy pen camera, GSM surveillance spy camera etc are used. All these devices are controlled via Bluetooth. Certain algorithms that are perform on Bluetooth protocol stack for Bluetooth security systems. Secure Simple Pairing (SSP): SSP also improves security through the addition of ECDH public key cryptography for protection against passive eavesdropping and man-in-the-middle attacks (MITM) during pairing.

III. PROPOSED SYSTEM

In today's world, there are several malicious activities are trending. Some activities contains devices such as hidden cameras, audio devices, etc to get unauthorized access in the environment. To avoid such activities, our project can be can be used.

Spy device forensics will enable you to scan the network and track the malicious devices. It will also display the information about the device hardware and will trace that textual data transfer among them.

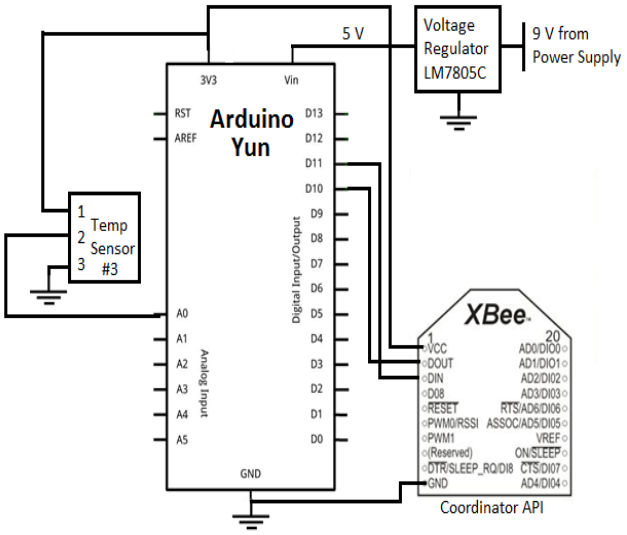
The authorized user will be authenticated using user id and password once the user got access to the system he van use our system for scanning the network which will be interacted by android user interface in which user will be scanned by normal Bluetooth scanner.

User will be able to access the information like User id, required signal strength, User data that are being broadcasted using that signal, audio devices that can be traced, videos that are being used for broadcasting purpose and data about attacker's system information's like OS, IP address, MAC address. Which will be sufficient for authorized user to track the attacker within that environment.

- XBee to Arduino connection.
- Connectivity using XCTU.
- Mesh Network
- Bluetooth to Xbee Connectivity
- Bluetooth to Android device connectivity
- Scanning device
- Data acquired from scanned devices
- PAN ID, UID to Bluetooth

1) Xbee to Arduino Connection:

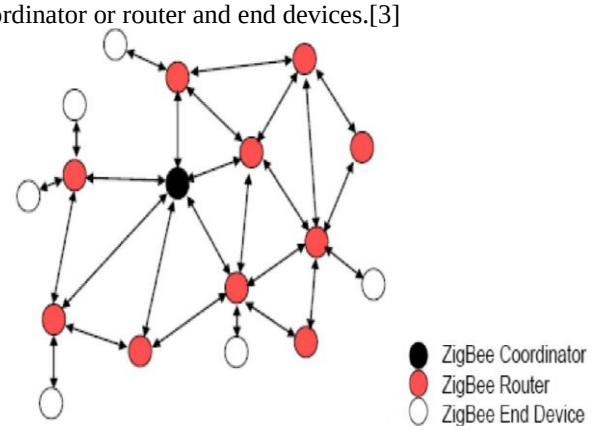
The systems that are being implanted in that working environment will be taken by zig bee chip connected to arduino microcontroller in which zig bee will be operated using arduino interface.[1]



2) Connectivity using X-CTU:

In this step we will be providing the desired input that needed for getting the zig bee chip information by setting its pan id within the mesh network of zig bee devices.[2]

3) Mesh network:
Mesh network gets created using different roles of zig bee as coordinator or router and end devices.[3]



4) Bluetooth to xbee connectivity:
We will be using xbee pin for configuring and Bluetooth modem for connecting it with mobile devices.
5) Bluetooth to android devices:
Bluetooth API's are used in order to connect Bluetooth devices in an android device.
6) Scanning Device:
We will be providing the Bluetooth scanner in order to scan the malicious devices and identify its information.
7) Data acquired from scanned devices:
We will be able to track the unwanted data that are being transmitted within the system and try to intercept those data.
8) PAN ID, UID to Bluetooth:
Using device information we will tracking its data and try to avoid its information to get broadcast.

IV. DESIGN

A. Block Diagram:

The block diagram of our system consist of two modules hardware and software which shows the user and attacker scenarios in which user will be able to track down the attackers activities within the working environment.
Hardware:
The system consist of zigbee chip connected to hardware micro controller for getting the data serially using serial input output pin of zig bee .USB connectors are used for receiving and sending the data within that mesh network and each zigbee chip is used for providing system information along with its user data.

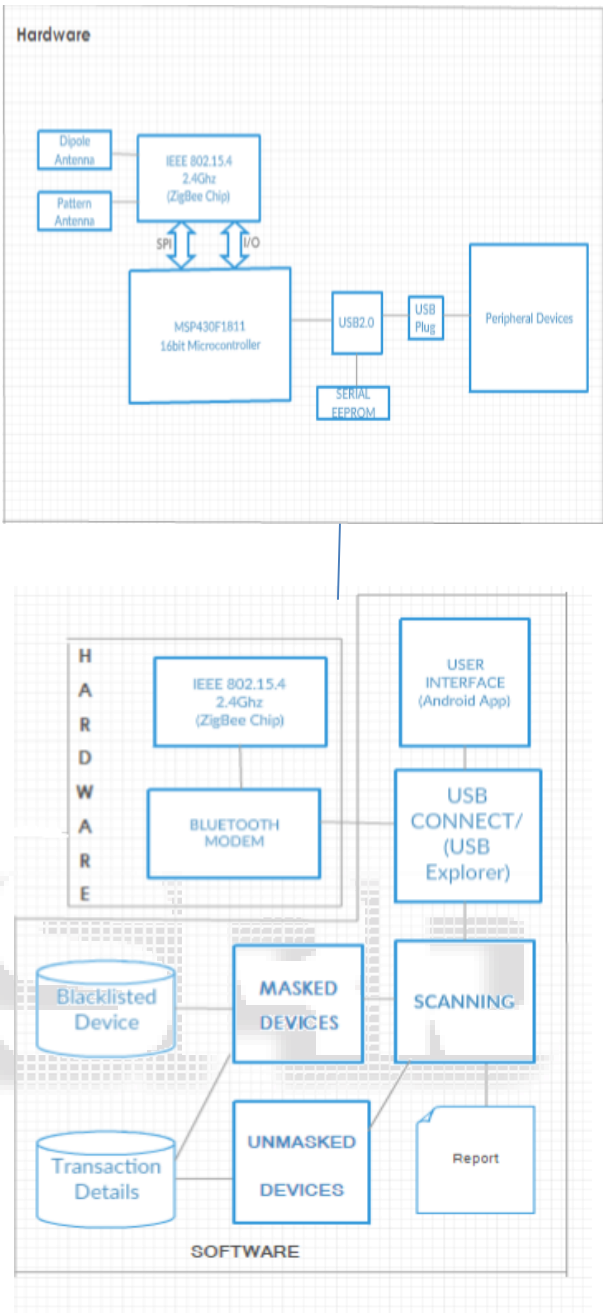


Fig.1: Block Diagram

System consist of data that can be retrieved using zig bee chip and can be transmitted to another zig bee module and each module is connected within that same pan network. Each data that are being transmitted over zig bee module can be tracked down by our software system specifying source, destination, and amount of data that are transmitted and received by particular module.
Software:
The system consist of user interface as software part in which user will be interacted with the system in order to track down the attacker's signals and its data that are being transmitted over the mesh network.

1) To perform user interface we have used the android Graphical user interface API's for user interaction purpose.
2) Bluetooth API's that are being used for providing scanning feature within the user interface.

3) USB explorer is used for connecting zig bee chip along with micro controller for tracking those zigbee modules that are connected over attacker's scenario.
4) Databases are maintained for identifying masked and unmasked user within the working environment.

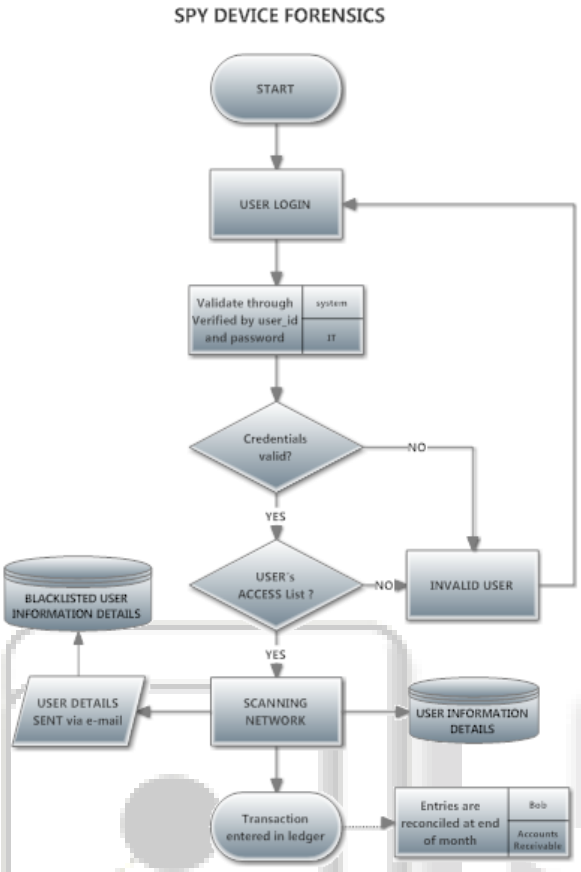


Fig.2: Flow Diagram

B. Flow Diagram:

1) The user on the home screen will be requested to select the type of user he/she is. Once the type is selected the user will be asked to enter the login credentials.
2) User credentials are validated and according to user_id and password system gives access to user access list.
3) Validation of user credentials are done by database that are maintained by enterprise database system.
4) There is separate blacklisted databases are maintained whenever any scanned unwanted signals are tracked by the system those user's data are entered in blacklisted database.
5) Once the system tracked the user's information i.e its source and destination its data are being sent over the email to authorized user of the enterprise.
6) The user data are maintained with proper security in the hashed form so that no other unauthorized user should get access to the system.
7) Scanner scans the network which are used to track the attacker's network via zig bee

V. CONCLUSION

Thus our paper represents how we can help any enterprise to track those signals those are not traceable by normal devices .those signals can consist of any form of data such as audio, video or any text data which might affect the confidentiality of the enterprise.

Our system will provide all information that can be masked by attacker for any normal devcies those data are more vulnerable for enterprise security solution.

Our system will help in identifying other signals those are part of attackers and try to provide security to the enterprise environment.

Our system consist of hashed data of the user so any external user will not be able to identify user's details or credentials to get access to the system.

REFERENCES

[1] Diagram (Zigbee to arduino) http://forcetronic.blogspot.in/2014_02_01_archive.html
[2] zigbee to arduino to xctuhttps://learn.sparkfun.com/tutorials/exploring-xbees-and-xctu
[3] Mesh network http://www.csurambox.com/documents/report/report.htm
[4] Greenhouse Monitoring and Control System Based on Zigbee Wireless Senor Network Jian Song College of Machinery, Weifang University, Weifang, 261061, China Email: sjian11@163.com

