Grenze International Journal of Engineering and Technology, June Issue

Data Collection for Frequency Domain Analysis of Bluetooth Frames

Pragati Dhage[1], H. D. Gadade[2], Ravi Marravulla[3] and Shivraj Jadhav[4]
[1]College of Engineering Pune, Artificial Intelligence and Robotics, Pune, India
Email: dhagepv20.mfg@coep.ac.in
[2]College of Engineering Pune,Department of Computer and IT, Pune, India
Email: hdg.comp@coep.ac.in
[3]Technical Head, HELLA India Automotive Private Limited, Pune, India
Email: ravi.marravula@hella.com
[4]Senior Engineer, HELLA India Automotive Private Limited, Pune, India
Email:shivraj.jadhav@hella.com

***Abstract*—In today's era many new devices are coming in the market. This devices are susceptible to attacks. This paper will prosper a brief description of data Collection for Frequency Domain Analysis of RF Frames to detect the changes in the device. In this paper we are collecting the data for different smartphone device, from this data we will detect how through different smartphones this RF data changes and also how RF data changes for similar smartphones i.e. device to device change of RF signal which can be used for device identification. RF data has been observed under various circumstances such as Line of Sight (LoS), Non-Line of Sight (NLoS), various temperature effects etc. From this data we will able to determine device to device tolerances and also how the signals changes. Based on the experiment result, we will determine how radio frequency will help to detect individual devices.**

***Index Terms*— Frequency Domain Analysis, RF Frames, RF signal, Line of Sight, Non-Line of Sight.**

I. INTRODUCTION

Different device have different radio frequency domain analysis which can be use to treat them from which transmitting end the signals has been transmitted which is then used for device identification. This radio frequency domain analysis has been carried out under various circumstances such as Line of Sight, Non line of sight and temperature. Every device have different imperfection which can be used to detect the individual device.

To protect the system from relay attack we need to protect it at physical layer. Physical layer security is also know as Frequency Domain Analysis of Bluetooth Frames. Frequency Domain Analysis of Bluetooth Frames method is use to provide identity to the specific wireless device. Imperfection in radio frequency domain analysis arises due to the hardware imperfection at the time of manufacturing. Suppose we are taking two similar phone of same model but still there will be hardware imperfection at the time of manufacturing which will reflect at the time when we send a specific signal from the phone which can be treated as a Collection of data for Frequency

Grenze ID: 01.GIJET.8.2.26

Domain Analysis of Bluetooth Frames .As no two humans have same fingerprinting likewise no two phones have same radio frequency domain analysis . It is very much difficult for the attacker to copy the RF fingerprinting which will make this technique more efficient. For RF fingerprinting extraction we required various data.

There are two main extraction approach of Data Collection for Frequency Domain Analysis of Bluetooth Frames i.e. Modulation based approach and Transient based approach. Modulation based techniques based on imperfection in the modulator of the radio transceiver. Transient based approach consist of observing the unique characteristics of the transient phase when radio is turned on. It is used to distinguish classes such as model and manufacturer and also used to distinguished individual device of same model. Generally in transient based system ,extracting the unique characteristics from off state to on state .This feature are transmitter specific and use to identify unique device. Now a days Researcher community has given more import to transient based RF fingerprinting technique. In this paper we will discuss on transient based Frequency Domain Analysis of Bluetooth Frames methodology. Transient detection is an important step to identify the transmitting devices through transient based Frequency Domain Analysis of Bluetooth Frames. Through signal characteristics such as amplitude, frequency ,phase and energy ,this can be achieved. Using energy envelope we can detect the starting and end point of transients. The paper is divided into various sections to understand each aspect of the subject technically and separately. Sections1: Gives a brief introduction to this paper consisting background, relevance of the paper. Chapter 2: Gives a brief review of the related literature and presents the proposed system's scenario. Chapter3: Describes System Schematic and Specification and block diagram with its detailed explanation. Chapter4: Describes the implementation of the project with its hardware and software requirement.

II. LITERATURE SURVEY

A. M. Ali et al. [1] proposed a RF fingerprinting method to detect the attack on the keyless entry system , which unlock the door when the key fob is in the proximity . Various attack had been detected on passive keyless entry systems through various experiment . Experiment give average positive rate of 0.27% and false negative rate of 0% for relay attack in car theft detection on keyless entry system.

Uzundurukan , E. et al. [2] proposed a Radio frequency fingerprinting for physical layer protection .This paper collected the Bluetooth signals for different smartphones with different manufacturers with several model .This data is then used in detect the transient based algorithm to sech the solidity of the Bluetooth signals Boris D. et al.[3] This paper proposed various fingerprinting method of performing attack on modulation method based and transient method based.Through this paper which method is feasible is shown so that the thieves is not able to reproduce the signal .

Li et.al [4]explain a method of Passive keyless entry system(PKES).This paper proposed attack on the smartphone type PKES system. The PKES system uses User context detection which uses the barometer of smartphone and accelerometer of the smartphone to detect the user . Different experiment has been performed Saeed U.et al [5] proposed a Radio frequency fingerprinting method also know as Physical layer security for wireless device . In this paper various low end receiver is used to detect the signal and note their changes Receiver impairment decrease the success rate of impersonating attack on RF fingerprinting. This paper suggest how signals changes with receiver.

M. Köse.et.al [6] proposed a classification algorithm for a low complexity RF fingerprinting method . In this method turn on transient signals of the energy spectrum from which unique characteristics of wireless device has been extracted . From the extracted transient signals different spectral component had been extracted .This spectral component is then used to develop the classification model to proposed a spectral fingerprinting .In this paper they demonstrated the effectiveness of spectral fingerprinting.

Y. Shi .et.al [7] proposed a deep learning based method for classification based solution in realistic wireless solution .This paper has considered some point such as signal changes over the time ,some data is unknown as there is no training data ,signal can be manipulated using smart jammer ,different signal can be superimposed The paper considered various cases such as Elastic Weight Consolidation (EWC) based loss is used for continual learning and to trained a Convolutional Neural Network (CNN) . For case 2, Minimum Covariance Determinant (MCD) and k-means clustering methods is applied to detect the output of the unknown signals through outlier detection.

S. Riyaz. Et.al[8] This paper proposed a overview of deep learning based approach .This paper describe method of identifying a radio signals among normally similar device using machine learning(ML) and software defined radio (SDR) sensing capability .The key benefit is that Machine Learning is operating in the raw I/Q data and distinguish device using transmitter hardware induced imperfection. Higher level decoding, feature engineering,

or protocol knowledge is not needed, further mitigating challenges of ID coexistence and spoofing of multiple protocols in a shared spectrum. It has achieved experimental accuracy of 90-99%.
Kyungho J . et al [9] This paper used a method of attack detection on Passive keyless entry system .This paper present RF fingerprinting method to detect attack on keyless entry system .Through different method Relay attack detection has been performed on PKES system .This paper achieved a average false rate of 0.27% and false negative rate of 0% for the detection of the attack .This paper also considered some factor such as Temperature , LoS and NLoS.

III. DATA COLLECTION

Fig 1 :Data collection processes

Large amount of data will be required for determining the individual phone which will use in future for making a machine learning model to detect the genuine user . For data collection phase we are using 12 different types of phone which is Redmi note 10 pro, Samsung S20,Samsung M32 and vivo with three model each. The reason for choosing three model of each is that we need to figure the difference in similar model which we treated them as identical but in practical there is slight difference in the making of each phone which will result in the signal imperfection which can be treated as a fingerprint. . BT signals are collected from 12 phone (4 manufacturers with different model and serial number) with different phone brands, models and serial numbers. 2400 MHz and 2483.5 MHz is the operational band of Bluetooth(BT) signals. Different data which we have collected is Central Frequency, Chip Temperature, Min Con interval, Max Con Interval ,SP Battery Temperature, SP Tx Power, Packet Encoder, CTE Mode, Sync Word, RSSI, AGC, ADC. Different phones signals has been tested in various scenarios , line of sight(LoS),Non Line of sight(NLoS) and different temperature range

A. Line of Sight (LoS)

In line of sight we fixed our phone in one end and RSL15 chip at opposite end so that no disturbance must come in between them. We have collected data in indoor and outdoor for different distance which is 1m,2m and 10 meter. The main aim of choosing this distance is that we need to check signal at different distance to note it's fluctuation . We have also collected data for different power based condition.

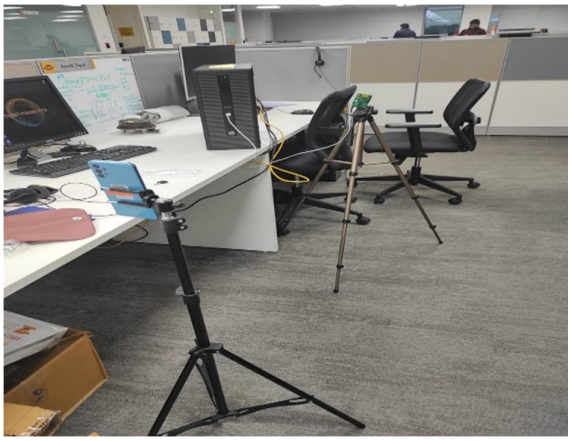

Fig 2 : Indoor environment Data collection

B. Non line of sight

In non line of sight condition we have collected data by putting the phones into our pocket. For this also we have collected data in different scenarios for different distance. In this we have also checked the Tx power level

Fig 3 : Outdoor environment data collection

condition. We collected the data for different Tx power which is -1dBm,-7dBm,-15dBm,-21dBm,by default it is -1dBm

C. Temperature

Temperature has a wide effect on the data ,so for this reason we have collected the data .In this we have used temperature chamber for achieving temperature change. We have put our Bluetooth chip and phone in the temperature chamber. We have collected the data for -10,0,10,20,45 degree Celsius.

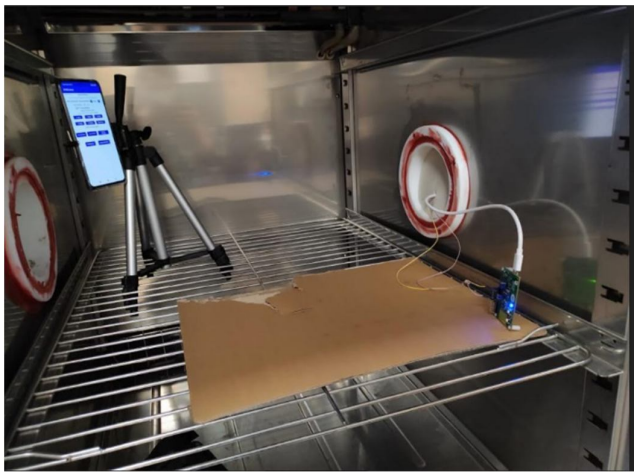

Fig 4 : Data collection from Temperature chamber

From the collected data different plots had been plot

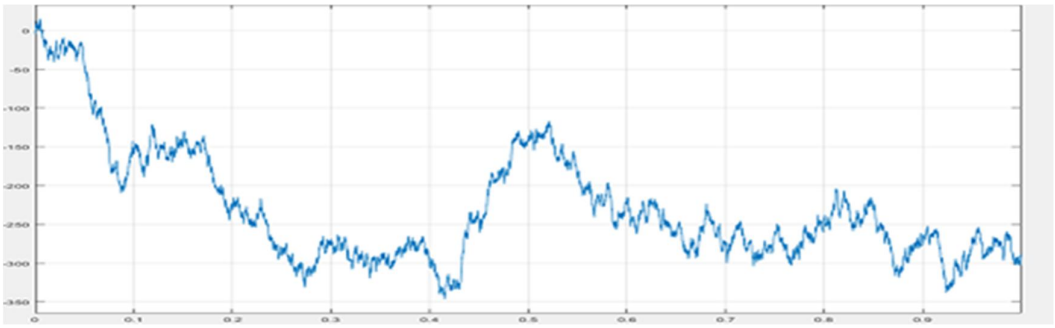

Fig 5 : Phase change of Redmi note 9 phone1

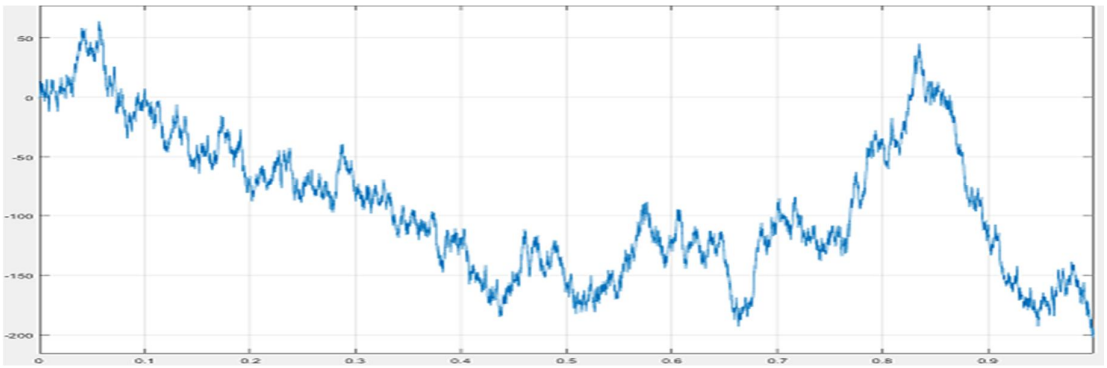

Fig 6 : Phase change of Redmi note 9 phone2

We have ploted center frequency vs ADC value phase change graph which is the normalized frequency graph. As from the graph we can see that even though we consider two phone of similar model and also pass the same signal from two phones there is a fluctuation in the signal which is shown from the graph.so this can be used for identification of individual devices.

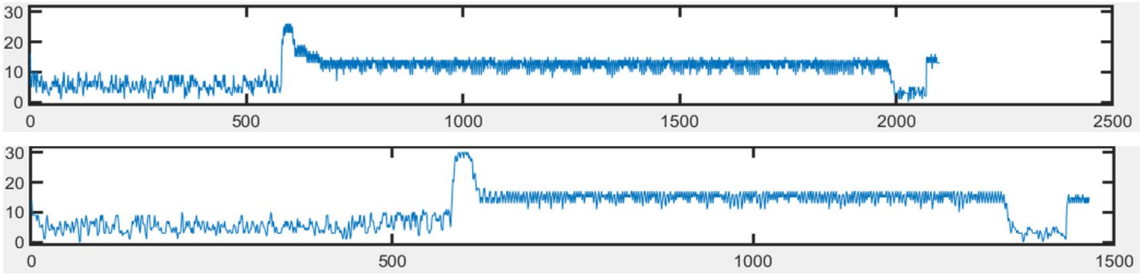

Fig 6 : RSSI vs Connection event graph

This are the two graph of RSSI value has been ploted with respect to connection event count.

IV. Feature Selection

For RF fingerprint feature extraction we need transient signal. This feature show performance depending upon the signal type and the feature set which we are using. In this we will extract feature from transient signal as it will be useful to get high classification performance. The transient signal show high classification performance because it has some characteristics which cannot be extracted easily. Therefore the Bluetooth signals which is transmitted can be used in frequency domain analysis . Different unique feature can be extracted through the transient based signal transformation in time and frequency. Some feature can be extracted directly from the data from the transient signal such as transient duration. Some of the important feature which will a robust feature in development of the machine learning model to get the highest accuracy found from the literature survey is Standard Deviation, Kurtosis, Skewness ,turn on transient phase of the signal. This are the tentative feature for RF fingerprinting.

As we are using MATLAB , there is an app name 'Diagnostic Feature Explorer' which will use to generate and rank the feature from our data. The feature ranking is necessary so as to select the most robust feature in our dataset. In this app we need an Ensemble data which is the collection of data in different scenarios and different condition. The data which we have ensembled it is in the following form. This data is under two condition.

Now this ensembled data is then given as a input to the Diagnostic Featurer explorer which is the used to generate time domain feature as well as spectral feature. This feature is then available for ranking. There is various ranking scheme such as T test, Wilcoxon test, Bhattacharya test, Anova test etc.

1	*707×1 table*	0
2	*707×1 table*	1

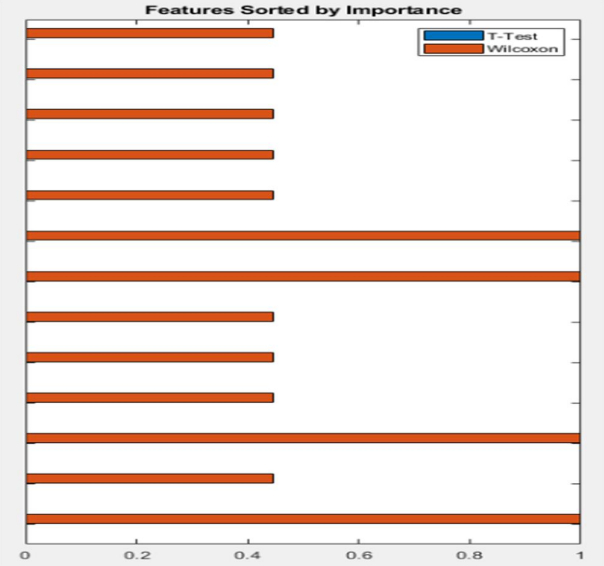

Fig 7 : Feature ranking

V. Conclusion

In this paper we have proposed a data collection method and then generation of fingerprinting from the data .We have explained how fingerprinting can help to detect the individual cell phone so that we can detect the relay attack .Further more work on fingerprint is in process and from the generated fingerprinting in future we will able to detect relay attack on the car by using machine learning model.The Development of machine learning model is also under process.

Reference

[1] A. M. Ali, E. Uzundurukan and A. Kara, "Assessment of Features and Classifiers for Bluetooth RF Fingerprinting," *in IEEE Access*, vol. 7, pp. 50524-50535, 2019

[2] Uzundurukan, E.; Dalveren, Y.; Kara, A."A Database for the Radio Frequency Fingerprinting of Bluetooth Devices". *Data* 2020, *5*, 55.

[3] Danev, Boris & Luecken, Heinrich & Capkun, Srdjan. (2022). Physical-layer Identification: Secure or not?.

[4] FLi, Jing & Dong, Yabo & Fang, Shengkai & Zhang, Haowen & Xu, Duanqing. (2020). User Context Detection for Relay Attack Resistance in Passive Keyless Entry and Start System

[5] Saeed Ur Rehman, Kevin W. Sowerby, Colin Coghill, Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers Journal of Computer and System Sciences

[6] M. Köse, S. Taşcioğlu and Z. Telatar, "RF Fingerprinting of IoT Devices Based on Transient Energy Spectrum," in *IEEE Access*, vol. 7, pp. 18715-18726, 2019.

[7] Y. Shi, K. Davaslioglu, Y. E. Sagduyu, W. C. Headley, M. Fowler and G. Green, "Deep Learning for RF Signal Classification in Unknown and Dynamic Spectrum Environments," *2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2019 .

[8] S. Riyaz, K. Sankhe, S. Ioannidis and K. Chowdhury, "Deep Learning Convolutional Neural Networks for Radio Identification," in *IEEE Communications Magazine*, vol. 56, no. 9, pp. 146-152, Sept. 2018.

[9] Kyungho Joo, Wonsuk Choi, Dong Hoon Lee," Hold the Door! Fingerprinting Your Car Keyto Prevent Keyless Entry Car Theft .

[10] Levi, Albert & Çetintas, Erhan & Aydos, Murat & Koc, Cetin & Çağlayan, Mehmet. (2004). Relay Attacks on Bluetooth Authentication and Solution

[11] Wu, Qingyang & Feres, Carlos & Kuzmenko, Daniel & Ding, Zhi & Yu, Zhou & Liu, Xin & Liu, Xiaoguang. (2018). Deep Learning Based RF Fingerprinting for Device Identification and Wireless Security. Electronics Letters

[12] M. I. AlHajri, N. T. Ali and R. M. Shubair, "A Machine Learning Approach for the Classification of Indoor Environments Using RF Signatures," *2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 2018

[13] Kim, G. , Lee, K. , Kim, S. and Kim, J. (2013) Vehicle Relay Attack Avoidance Methods Using RF Signal Strength. Communications and Network.