# PRIVACY PRESERVING LOCATION AUTHENTICATION PROTOCOLS FOR MOBILE PAYMENTS USING PHYSICAL LAYERED SIGNATURES

**PHASE I REPORT**

***Submitted by***

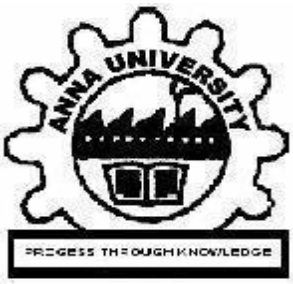
**THANGAPANDIAN B**
**2018252004**

***in partial fulfilment for the award of the degree of***

**MASTER OF ENGINEERING**

**IN**

**COMMUNICATION SYSTEMS**




**DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING**
**ANNA UNIVERSITY, CHENNAI**

**NOVEMBER 2019**

# ANNA UNIVERSITY, CHENNAI

## BONAFIDE CERTIFICATE

Certified that this Report titled "**PRIVACY PRESERVING LOCATION AUTHENTICATION PROTOCOLS FOR MOBILE PAYMENTS USING PHYSICAL LAYERED SIGNATURES**" is the bonafide work of **THANGAPANDIAN B (2018252004)** who carried out the work under my supervision. Certified further that to the best of my knowledge the work reported herein does not form part of any other thesis or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

**SIGNATURE**

**DR. S. MUTTAN**

Professor & Head

Department of ECE

Chennai – 25

**SIGNATURE**

**DR. K. GUNASEELAN**

Assistant Professor (Sr.Gr.)

Department of ECE

Chennai - 25

# ABSTRACT

Financial technology, often shortened to fintech, is the technology and innovation that aims to compete with traditional financial methods in the delivery of financial services. It is an emerging industry that uses technology to improve activities in finance. The use of smartphones for mobile banking, investing services and cryptocurrency are examples of technologies aiming to make financial services more accessible to the general public. Financial technology companies consist of both start-up's and established financial institutions and technology companies trying to replace or enhance the usage of financial services provided by existing financial companies. As such the security aspects of Fintech needs to be bolstered in a way such that the general public feels safe in using these mobile services for a better way of life.

Increasing Security always comes with a trade-off. In this project we try to increase security in mobile payment protocols with the least compromise in performance for the best improvement in security. One way to improve the security is by leveraging the location as a parameter to provide better security with minimal addition to computational complexity.

Work described in this project focuses on a mobile payment protocol called Secure Mutual Authentication Protocol (SMAP) and its integration with a Privacy Preserving Location Authentication (PriLA) Technique to create a modified protocol flow which is more secure compared to either of the above-mentioned techniques used independently. The newly modified protocol was tested for its Computational Complexity, Vulnerabilities and a complete Security Analysis was performed.

# ஆய்வுசுருக்கம்

நிதி தொழில்நுட்பம், பெரும்பாலும் ஃபிண்டெக்கிற்கு சுருக்கப்பட்டது, தொழில்நுட்ப சேவைகளை வழங்குவதில் பாரம்பரிய நிதி முறைகளுடன் போட்டியிடுவதை நோக்கமாகக் கொண்ட தொழில்நுட்பம் மற்றும் கண்டுபிடிப்பு. இது ஒரு வளர்ந்து வரும் தொழில், இது நிதியில் செயல்பாடுகளை மேம்படுத்த தொழில்நுட்பத்தைப் பயன்படுத்துகிறது. மொபைல் வங்கி, முதலீட்டு சேவைகள் மற்றும் கிரிப்டோகரன்சி ஆகியவற்றிற்கான ஸ்மார்ட்போன்களின் பயன்பாடு நிதி சேவைகளை பொது மக்களுக்கு அணுகுவதை நோக்கமாகக் கொண்ட தொழில்நுட்பங்களுக்கு எடுத்துக்காட்டுகள். நிதி தொழில்நுட்ப நிறுவனங்கள் தொடக்க மற்றும் நிறுவப்பட்ட நிதி நிறுவனங்கள் மற்றும் தொழில்நுட்ப நிறுவனங்கள் இரண்டையும் கொண்டிருக்கின்றன, தற்போதுள்ள நிதி நிறுவனங்களால் வழங்கப்படும் நிதி சேவைகளின் பயன்பாட்டை மாற்றவோ அல்லது மேம்படுத்தவோ முயற்சிக்கின்றன. எனவே, ஃபிண்டெக்கின் பாதுகாப்பு அம்சங்களை மேம்படுத்த வேண்டும், இது ஒரு சிறந்த வாழ்க்கை முறைக்கு இந்த மொபைல் சேவைகளைப் பயன்படுத்துவதில் பொது மக்கள் பாதுகாப்பாக உணர்கிறது.

பாதுகாப்பை அதிகரிப்பது எப்போதுமே ஒரு பரிமாற்றத்துடன் வருகிறது. இந்த திட்டத்தில், பாதுகாப்பில் சிறந்த முன்னேற்றத்திற்கான செயல்திறனில் குறைந்த சமரசத்துடன் மொபைல் கட்டண நெறிமுறைகளில் பாதுகாப்பை அதிகரிக்க முயற்சிக்கிறோம். கணக்கீட்டு சிக்கலுடன் குறைந்தபட்ச கூடுதலாக சிறந்த பாதுகாப்பை வழங்குவதற்கான இருப்பிடத்தை ஒரு அளவுருவாக மேம்படுத்துவதன் மூலம் பாதுகாப்பை மேம்படுத்துவதற்கான ஒரு வழி.

இந்த திட்டத்தில் விவரிக்கப்பட்டுள்ள பணிகள் பாதுகாப்பான பரஸ்பர அங்கீகார நெறிமுறை (SMAP) எனப்படும் மொபைல் கட்டண நெறிமுறை மற்றும் தனியுரிமையைப் பாதுகாக்கும் இருப்பிட அங்கீகாரம் (PriLA) நுட்பத்துடன் அதன் ஒருங்கிணைப்பு ஆகியவற்றில் கவனம் செலுத்துகிறது. நுட்பங்கள் சுயாதீனமாகப் பயன்படுத்தப்படுகின்றன. புதிதாக மாற்றியமைக்கப்பட்ட நெறிமுறை அதன் கணக்கீட்டு சிக்கலான தன்மை, பாதிப்புகள் ஆகியவற்றிற்காக சோதிக்கப்பட்டது மற்றும் முழுமையான பாதுகாப்பு பகுப்பாய்வு செய்யப்பட்டது.

# ACKNOWLEDGEMENT

The success and outcome of this project required a lot of guidance and assistance from many people and I am extremely privileged to have got this all along the completion of my project. All that I have done, is only due to such supervision and assistance and I would not forget to thank them.

I would like to express my sincere thanks to **Dr. S. MUTTAN,** Head of the Department and all the staff members in Department of Electronics and Communication, for their generosity and kind support during the period of study.

I consider myself fortunate to express my deep sense of gratitude to **Dr. K. GUNASEELAN**, Assistant Professor (Sr.GR), Department of ECE, for her guidance, valuable suggestions persistent encouragement, technical support and patience which made me to work in the right direction throughout this project.

I also thank my project coordinator **Dr. M. MEENAKSHI,** Professor, Department of ECE, for conducting periodic reviews that helped me in assessing my progress.

I would like to thank all the teaching and non-teaching staff members of Department of Electronics and Communication Engineering, for the help rendered during this project. I am very pleased to acknowledge my thanks to my family and friends for their moral support which helped me to bring out this work successfully.

**(THANGAPANDIAN B)**

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# LIST OF ABBREVIATIONS

| | |
|---|---|
| **PriLA** | Privacy Location Authentication |
| **SMAP** | Secure Mutual Authentication Protocol |
| **CSI** | Channel State Information |
| **CFO** | Carrier Frequency Offset |
| **AP** | Access Point |
| **MAC** | Medium Access Control |
| **SNR** | Signal to Noise Ratio |
| **ACK** | Acknowledgement |
| **Tx** | Transmitter |
| **Rx** | Receiver |

# LIST OF NOTATIONS

| Notation | Description |
|---|---|
| Fingerprint | Fingerprint identification |
| PIN | PIN code |
| $K_1$ | Private key |
| $K_2$ | Public key |
| $K_d$ | Key handle used for searching $K_2$ |
| RN | A random number generated by the device |
| M0 | Transaction information |
| M1 | Payment data |
| M2 | Transaction result |
| $C_s$ | Challenge value generated by the server |
| $S_m$ | Signature value operated by the device |
| XOR | Bitwise xor operation |
| $H()$ | Hash operation |

# CHAPTER I

# INTRODUCTION

## 1.1 MOTIVATION

The Internet has dramatically changed the face of the world. In this era, the Internet provides a variety of convenient services for individuals anywhere and anytime, having completely changed our daily lives, our ways of thinking, and the way we understand the world. With the development of mobile communication technology over time, many mobile Internet applications have become popular, thereby making us more informed and our activities more portable. In the mobile Internet field, the mobile phone has an indispensable role, and has become an inseparable life accessory for most individuals. Mobile phones maintain personal information and are used for both traditional communication as well as to interact in new ways with people and things. In addition, commerce is a necessary element of social stability and constitutes an inevitable part of our daily lives. The combination of smart phones and mobile Internet technology has effectively upgraded traditional offline transactions into networked, mobile, and more efficient exchanges.

Financial technology, often shortened to fintech, is the technology and innovation that aims to compete with traditional financial methods in the delivery of financial services. It is an emerging industry that uses technology to improve activities in finance. The use of smartphones for mobile banking, investing services and cryptocurrency are examples of technologies aiming to make financial services more accessible to the general public. Fintech applications are include

paying for water and electricity, public trips, online shopping, and many other things by mobile-payment methods Financial technology companies consist of both start-up's and established financial institutions and technology companies trying to replace or enhance the usage of financial services provided by existing financial companies.

Compared with traditional payment methods, mobile payment has the following features:

1. Digital transmission. Mobile payment uses advanced technology to digitally transmit financial transaction information, whereas the traditional payment method requires payment via the transfer of cash, notes, or bank statement.
2. Open payment environment. The mobile payment environment operates from an open system platform, whereas the traditional payment system operates in a relatively closed system.
3. Advanced means of communication. In mobile payment, the demands on hardware and software resources are high, but traditional payment uses traditional communication media, which are less demanding.
4. Other economic advantages. Mobile payment is convenient, fast, and efficient. Users simply use a networked tablet computer or mobile phone, thereby enjoying fewer geographical restrictions and the ability to complete the entire payment process in a very short period. Traditional payments, in contrast, involve cumbersome procedures and can be time consuming.

While mobile payment is popular because of its many advantages, unfortunately, it also faces many threats and security challenges. Mobile transactions face a range of security issues, such as the reliability of the transactions, the confidentiality of the data, the non-repudiation of transactions, and data integrity. In many parts of the world today, no standardized programs have been established for mobile payments. To ensure payment reliability, the trading environment must be reliable, and the transaction object must be true.

Confidentiality of data refers to the protection of the privacy of transaction information.

In addition, the transaction itself must be undeniable, which means that the participants are also undeniable, whereas data integrity refers to the prevention of malicious changes being made to the data during the transmission process. Several fraud problems have occasionally arisen with mobile payments in recent years, which seriously undermine the user experience. To a certain extent, fraud will also work against the popularity of the technology. More importantly, some security issues may provide opportunities for theft, thereby making the user vulnerable to huge financial losses due to mobile payment security issues. The occurrence of such events also increases the burden on society. Therefore, Security in the payment system is a major problem that must be solved.

A way to do this is to use a robust scheme which provides Authentication, Confidentiality, Integrity, Non-Repudiation, and Privacy of the User.

## 1.2 OBJECTIVE

Work in this report mainly focuses on the security of mobile-payment systems. To ensure the security of the online trading environment, Secure Mutual Authentication Protocol (SMAP) plays an important role in the payment process is considered. Note that traditional physical authentication devices such as USB keys, or similar devices produced by different organizations and which provide no unified interface standard, result in individuals carrying a variety of authentication devices, which is not only inconvenient but also full of risk. Our proposed protocol is based on the Universal 2nd Factor (U2F), which is an open standard that supports all certification services that meet these standards. In fact, a growing number of Internet services are beginning to support the two-step certification standard, which can identify and reject forged servers and counterfeit users. The Primary Objective of this work is,

- To enhance the security of SMAP protocol even further we combine it with a Privacy Preserving Location Based Authentication (PriLA) Scheme which is based on Physical Layered Signatures which in turn leads to a much more secure two-step authentication protocol.

And this PriLA uses Physical Layered Signatures like CSI and CFO to Authenticate the user while preserving the privacy of Location of the user. Here the location is associated to the channel conditions between user and server and not on the GPS location of the user. So, this protocol protects data, using the physical layer information and conventional cryptographic techniques which means a more robust scheme.

## 1.3 CONFIDENTIALITY

One of the main security aspects is ensuring the confidentiality of the transmitted data. Confidentiality is commonly used to describe the degree of protection in the transmitted data against eavesdroppers. Typically, confidentiality is achieved using encryption where a secret key is used to encrypt data at the transmitter and decrypt it at the legitimate receivers. Conventional encryption suffers from some practical challenges such as the complexity of the encryption algorithms and the signalling overhead required in key distribution/agreement protocols. Thus, encryption/decryption process represents a real challenge for resource-limited users.

## 1.4 AUTHENTICATION

Authentication is the process of recognizing a user's identity. It is the mechanism of associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user's information on a local operating system or within an authentication server. Different systems may require different types of credentials

to ascertain a user's identity. Three categories in which someone may be authenticated are: something the user knows, something the user is, and something the user has.

## 1.5 WIRELESS SECURITY CHALLENGES

As, all mobile payments are over a wireless channel we must face the security risks of communication over a wireless channel. Security is an implicit part of any communication system that is relied upon for the transmission of private information. Consequently, the reliability to share secret information in the presence of malicious attackers is critically important. From a general perspective, security is concerned with unauthorized users trying to access, forge or modify messages intended for legitimate receivers. Wireless communications are based on electromagnetic waves using radio frequencies (RF) propagating through open space, which provides the freedom of user mobility and the flexibility of data transmission, but also brings significantly more security challenges than traditional wired communications. Therefore, secure wireless communication becomes critical for wireless data transmission.

There are many factors contributing to the increasing security challenges in wireless communications. Primarily, the broadcast nature of the wireless medium makes transmitted signals available to any receiver within the transmission range, which leads to easy access to adversaries. Moreover, the mechanisms of high-level security in a wired network cannot be directly applied in wireless scenarios. Additionally, limited processing power is incurred by the limited space, cost and power constraints of wireless devices. Considering these essential limitations of wireless communications, security mechanisms for wireless systems should be developed to address increasing threats.

## 1.6 PHYSICAL LAYER SECURITY SCHEMES

Information security is critical for any communication systems. In wireless communications, spoofing is a severe security threat due to the broadcast nature of radio signal propagation, in which adversaries attempt to impersonate the legitimate user within a network in order to gain illegitimate advantages. In order to defend systems against spoofing attacks, the receiving end should be equipped with authentication and confidentiality mechanism. By exploiting the advantages of securing wireless transmissions at the physical layer, a variety of physical layer authentication schemes have been proposed by using the inherent properties of wireless channels or the imperfections of hardware devices.

Physical layer security, which exploits physical link properties, is a promising paradigm to provide energy-efficient security solutions and enhance the security performance of wireless communications systems. Security from the information-theoretic perspective was pioneered by Shannon, who introduced the definition of perfect secrecy and theoretically characterized that the fundamental ability of the physical layer can provide secure communications. Physical layer security techniques are classified into three major categories based on the wireless channel, RF-DNA and diversity technique, respectively.

The fundamental principle behind channel based physical layer security is that the spatial, spectral and temporal properties of the wireless fading channel have natural randomness and they are rapidly decorrelated between different geographic locations. Consequently, the properties of the channel link between legitimate terminals are only available to the intended receiver but cannot be duplicated by adversaries. Physical layer security techniques for wireless communications can prevent malicious attacks without upper layer data encryption.

## 1.7 LOCATION AUTHENTICATION

` Location-based authentication is a special procedure to prove an individual's identity. Authenticity on appearance simply by detecting its presence at a distinct location. To enable location-based authentication, a special combination of objects is required. The individual that applies for being identified and authenticated must present a sign of identity. The individual has to carry at least one human authentication factor that may be recognized on the distinct location. The distinct location must be equipped with a resident means that is capable to determine the coincidence of individual at this distinct location.

Once we can authenticate the location of the user, we can provide services based on the location such services are called Location-based services (LBS), they use real-time geo-data from a mobile device or Smartphone to provide information, entertainment or security. Some services allow consumers to "check in" at restaurants, coffee shops, stores, concerts, and other places or events [23]. Location-based services use a Smartphone's GPS technology to track a person's location, if that person has opted-in to allow the service to do that. After a Smartphone user opts-in, the service can identify his or her location down to a street address without the need for manual data entry.

LBS's have been slowly rising in Popularity and Companies have found several ways to use a device's location such as:

1. Store locators: Using location-based intelligence, retail customers can quickly find the nearest store location.
2. Proximity-based marketing: Local companies can push ads only to individuals within the same geographic location
3. Travel information: LBS can deliver real-time information, such as traffic updates or weather reports, to the Smartphone so the user can plan accordingly.

4. Mobile workforce management: For logistics-dependent companies that employ individuals out in the field or at multiple locations, an LBS allows employees to check in at a location using their mobile device

LBS's can be made use of, in many more ways and in a vast variety of fields.

## 1.8 LOCATION PRIVACY

Location privacy refers to the ability of an individual to move in public areas with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use. To avoid location forgery, an essential step is location authentication, which verifies the truthfulness of the reported location data. An intuitive approach is to equip provider with localization capability, which, however, falls short due to the following two limitations. First, there are places such as coffee shops and stores where the number of provider-trusted APs is not enough to perform localization. Second, the growing privacy threats of sharing location information via LBS have been widely concerned. Such privacy threats come from the fact that many untrusted Wi-Fi infrastructures aggressively collect the location data. Although mobile users can secure their location data via encryption, their location information is still at high risk of being leaked due to the broadcast nature of wireless medium. Adversary can easily infer the targeted user's physical location by collaboratively eavesdropping frames over the air from several sniffers (e.g., untrusted APs). Previous research shows that one can determine a node with meter/centimetre level resolution using several receivers. Being aware of such risks, mobile users may be reluctant to use LBS applications.

## 1.9 STRUCTURE OF THE REPORT

The Report consists of the following chapters.

1. The first chapter of this report gives the motivation and Introduction about Mobile Payments, its advantages and security needs & security goals – confidentiality and authentication, location privacy, location-based security schemes and the objective of the project.
2. The second chapter of this report presents a Literature Survey on various mobile Payment protocols, their performance measures, working principles and review of similar works.
3. The third chapter of this report deals with Methodology and Implementation of newly proposed protocol.
4. The fourth chapter of this report discusses about the proposed protocol's Performance, Simulation and the Results.
5. The fifth chapter of this report contains the conclusion of this work and the future work which must be carried out for Phase – II.

# CHAPTER II

# LITERATURE SURVEY

## 2.1 SECURE MUTUAL AUTHENTICATION PROTOCOL FOR MOBILE PAYMENTS

With the increasing popularity of fintech, i.e., financial technology, the e-commerce market has grown rapidly in the past decade, such that mobile devices enjoy unprecedented popularity and are playing an ever-increasing role in e-commerce. This is especially true of mobile payments, which are attracting increasing attention. However, the occurrence of many traditional financial mishaps has exposed the challenges inherent in online authentication technology that is based on traditional modes of realizing the healthy and stable development of mobile payment. In addition, this technology ensures user account security and privacy. In this paper, they propose a Secure Mutual Authentication Protocol (SMAP) based on the Universal 2nd Factor (U2F) protocol for mobile payment. To guarantee reliable service, they use an asymmetric cryptosystem for achieving mutual authentication between the server and client, which can resist fake servers and forged terminals. Compared to the modes currently used, the proposed protocol strengthens the security of user account information as well as individual privacy throughout the mobile-payment transaction process. Practical application has proven the security and convenience of the proposed protocol. mobile payment can be a double-edged sword. On one hand, it provides convenience in almost every respect to its users, such as for traveling, shopping, and paying fees. On the other hand, hostile attacks can harm the user account and result in great financial

loss. In this paper, they have found the proposed SMAP to work well in protecting the security of the user's account and improving the payment experience with low time consumption. In addition, this protocol architecture is based on U2F, which provides a unified payment model, with no need for the use of various payment tools, which will greatly contribute to the development of payment technology.

## 2.2 PRIVACY-PRESERVING LOCATION AUTHENTICATION IN WI-FI NETWORKS USING FINE-GRAINED PHYSICAL LAYER SIGNATURES

Privacy-preserving location authentication can be realized within existing Wi-Fi-based LBS systems by exploiting physical layer (PHY) signatures in Wi-Fi preambles. To achieve this goal, PriLA, a Privacy-Preserving Location Authentication system in orthogonal frequency division multiplexing (OFDM) based Wi-Fi networks (e.g., IEEE 802.11a/g/n/ac) is introduced. This system allows the LBS provider to successfully conduct authentication while and meanwhile guaranteeing location privacy preservation for all mobile users against adversaries. PriLA exploits carrier frequency offset (CFO) and multipath, which can be obtained via Wi-Fi preambles. In communication systems, CFO and multipath are detrimental, while PriLA leverages them for authentication and privacy-preservation. PriLA takes advantage of the channel reciprocity property and uses CFO together with channel state information (CSI) to generate CFO patterns that are exclusively known by the transmission pair. To defend against adversaries with localization capability, PriLA uses CFO pattern to secure users' IDs starting from the handshake (or association) phase. As such, the adversaries cannot link a frame to a certain user, or infer the presence of a user, and thus fail to localize a user via localization. To enable authentication without performing localization, PriLA leverages users' multipath profiles, which can be extracted from CSI using multiple antennas. They have prototyped PriLA to demonstrate its feasibility and merits. PriLA is a clean-slate design that is transparent to upper

layer protocols and can be integrated into OFDM-based Wi-Fi devices without hardware modifications. With those features, they believe that PriLA can be easily applied to existing LBS systems with a slight upgrade.

## 2.3 LIGHT WEIGHT AND PRIVACY PRESERVING AUTHENTICATION PROTOCOL FOR MOBILE PAYMENTS IN THE CONTEXT OF IOT

The widespread use of smart devices attracts much attention on the research for a mobile payment protocol in the context of the Internet of Things (IoT). However, payment trust and user privacy still raise critical concerns to the application of mobile payments since existing authentication protocols for mobile payments either suffer from the heavy workload on a resource-limited smart device or cannot provide user anonymity in the mobile payment. To address these challenges elegantly, this paper presents a lightweight and privacy-preserving authentication protocol for mobile payment in the context of IoT. First, they put forward a unidirectional certificateless proxy re-signature scheme, which is of independent interest. Based on this signature scheme, this paper, then, gives a new mobile payment protocol that for the first time not only achieves anonymity and unforgeability but also leaves low resource consumption on smart devices. In the proposed protocol, the efficiency is notably improved by placing the most computational cost on Pay Platform (usually with abundant computational power) instead of lightweight mobile devices. Moreover, by considering that the Pay Platform and Merchant Server needs to perform computation for each transaction, the idea of batch-verification has been adopted to mitigate the overhead for millions of users at the Pay Platform and Merchant Server to address the scalability issue. Through the formal security analysis presented in this paper, the proposed protocol is proved to be secure under the extended CDH problem. In addition, the performance evaluation shows that the proposed protocol is feasible and efficient for the resource-limited smart devices in the IoT. To summarise they have presented a lightweight and anonymous authentication protocol for mobile

payment by using a new certificateless unidirectional signature scheme. To the best of our knowledge, this is the first transaction protocol that achieves user anonymity, unforgeability, certificateless and low resource cost on resource limited smart device. Furthermore, the newly proposed certificateless unidirectional signature scheme, which is proven secure under the extended CDH assumption by using random oracle model, is also of independent interest. According to the results of our experiments, they can observe that our mobile payment transaction is very efficient and highly practical.

## 2.4 CSI-BASED INDOOR LOCALIZATION

Indoor positioning systems have received increasing attention for supporting location-based services in indoor environments. Wi-Fi-based indoor localization has been attractive due to its open access and low-cost properties. However, the distance estimation based on received signal strength indicator (RSSI) is easily affected by the temporal and spatial variance due to the multipath effect, which contributes to most of the estimation errors in current systems. In this work, they analyse this effect across the physical layer and account for the undesirable RSSI readings being reported. They explore the frequency diversity of the subcarriers in orthogonal frequency division multiplexing systems and propose a novel approach called FILA, which leverages the channel state information (CSI) to build a propagation model and a fingerprinting system at the receiver. They implement the FILA system on commercial 802.11 NICs, and then evaluate its performance in different typical indoor scenarios. The experimental results show that the accuracy and latency of distance calculation can be significantly enhanced by using CSI. FILA can significantly improve the localization accuracy compared with the corresponding RSSI approach. RSSI-based schemes have been widely used to provide location-aware services in WLAN. However, in this paper, they observe that RSSI is roughly measured and easily affected by the multipath effect which is unreliable. They then use the fine-grained information, that is, CSI, which

explores the frequency diversity characteristic in OFDM systems to build the indoor localization system FILA. In FILA, they process the CSI of multiple subcarriers in a single packet as effective CSI value $CSI_{eff}$ and develop a refined indoor radio propagation model to represent the relationship between $CSI_{eff}$ and distance. Based on the $CSI_{eff}$, they then design a new fingerprinting method that leverages the frequency diversity. To demonstrate the effectiveness of FILA, they implemented it on the commercial 802.11n NICs. They then conducted extensive experiments in typical indoor environments and the experimental results show that the accuracy and speed of distance calculation can be significantly enhanced by using CSI. In their work, they just use the simplest trilateration method to illustrate the effectiveness of CSI in indoor localization.

## 2.5 TOWARD PRIVACY PRESERVING AND COLLUSION RESISTANCE IN A LOCATION PROOF UPDATING SYSTEM

Today's location-sensitive service relies on user's mobile device to determine the current location. This allows malicious users to access a restricted resource or provide bogus alibis by cheating on their locations. To address this issue, they propose A Privacy-Preserving Location proof Updating System (APPLAUS) in which collocated Bluetooth enabled mobile devices mutually generate location proofs and send updates to a location proof server. Periodically changed pseudonyms are used by the mobile devices to protect source location privacy from each other, and from the untrusted location proof server. They also develop user-centric location privacy model in which individual users evaluate their location privacy levels and decide whether and when to accept the location proof requests. In order to defend against colluding attacks, they also present between ranking-based and correlation clustering-based approaches for outlier detection Extensive experimental results show that APPLAUS can effectively provide location proofs, significantly preserve the source location privacy, and effectively detect colluding attacks. In this paper, they proposed a privacy-

preserving location proof updating system called APPLAUS, where collocated Bluetooth enabled mobile devices mutually generate location proofs and upload to the location proof server. They use statistically changed pseudonyms for each device to protect source location privacy from each other, and from the untrusted location proof server. They also develop a user-centric location privacy model in which individual users evaluate their location privacy levels in real time and decide whether and when to accept a location proof exchange request based on their location privacy levels. To the best of our knowledge, this is the first work to address the joint problem of location proof and location privacy. To deal with colluding attacks, they proposed betweenness ranking based and correlation clustering-based approaches for outlier detection. Extensive experimental and simulation results show that APPLAUS can provide real-time location proofs effectively. Moreover, it preserves source location privacy and it is collusion resistant.

## 2.6 TRAFFIC SIGNATURE-BASED MOBILE DEVICE LOCATION AUTHENTICATION

Spontaneous and robust mobile device location authentication can be realized by supplementing existing 802.11x access points (AP) with small cells. They show that by transferring network traffic to a mobile computing device associated with a femtocell while remotely monitoring its ingress traffic activity, any internet-connected sender can verify the cooperating receiver's location. they describe a prototype non cryptographic location authentication system they constructed and explain how to design both voice and data transmissions with distinct, discernible traffic signatures. Using both analytical modelling and empirical results from their implementation, they demonstrate that these signatures can be reliably detected even in the presence of heavy cross-traffic introduced by other femtocell users.

They have proposed and demonstrated a novel approach to infrastructure-based location authentication that operates in a spontaneous, transaction-oriented fashion. Their approach strives to be well aligned with the evolving needs of internet location-based application providers, and particularly their desire to authenticate new users on-the-spot. They introduced techniques to use voice calls to authenticate voice-only phone users, and data transfers to authenticate smartphone users, and explored a diverse set of traffic signals that can authenticate users rapidly and reliably. Yet no single query can authenticate a mobile device user's location with certainty, particularly in the presence of adversaries. While they have studied the performance of each of the proposed traffic signatures in isolation, they also anticipate that multiple techniques will be combined – and repeated over the duration of a call – to permit the authenticator to achieve her desired confidence in the authentication at a cost of additional time, bandwidth and complexity.

Their system exploits mobile-operator technology without involving the operator directly in a transaction. Yet they believe that more robust authentications can be achieved with the mobile operator's active involvement. Operators control the infrastructure, have preferential network vantage points, and can create easily discernible authentication fingerprints.

## 2.7 PUZZLE: A SHAPE BASED SECRET SHARING APPROACH BY EXPLOITING CHANNEL RECIPROCITY IN FREQUENCY DOMAIN

In this paper they propose a shape-based approach in frequency domain to extract a shared key by exploiting the observation that wireless channel is reciprocal due to multi-path fading. Unlike the traditional quantization approach in time domain, no training sequences or predetermined pulses are needed to be transmitted in our approach. The correlated power spectral density of the transmitted packets served as the common random source between Alice and Bob. They use Lower smoothing to mitigate measurement errors and interference and

then use pattern matching to encode the shape of the spectrum. They name the technique as Puzzle for secrets are generated by finding right pieces (shape patterns) and then putting them together. Implementation in software defined radios (SDR) demonstrates the feasibility of extracting a 6-bit secret per measurement with an average bit mismatching rate 5% in a 20 MHz band. Experiments show that with eavesdropper nearby, the leaked information of each secret bit generated by Puzzle is about 0.05 bit, which is low in comparison with a RSSI-based method ASBG.

## 2.8 SECRET KEY EXTRACTION FROM WIRELESS SIGNAL STRENGTH IN REAL ENVIRONMENTS

They evaluate the effectiveness of secret key extraction, for private communication between two wireless devices, from the received signal strength (RSS) variations on the wireless channel between the two devices. They use real world measurements of RSS in a variety of environments and settings. The results from our experiments with 802.11-based laptops show that 1) in certain environments, due to lack of variations in the wireless channel, the extracted bits have very low entropy making these bits unsuitable for a secret key, 2) an adversary can cause predictable key generation in these static environments, and 3) in dynamic scenarios where the two devices are mobile, and/or where there is a significant movement in the environment, high entropy bits are obtained fairly quickly. Building on the strengths of existing secret key extraction approaches, they develop an environment adaptive secret key generation scheme that uses an adaptive lossy quantizer in conjunction with Cascade-based information reconciliation and privacy amplification. Our measurements show that our scheme, in comparison to the existing ones that they evaluate, performs the best in terms of generating high entropy bits at a high bit rate. The secret key bit streams generated by our scheme also pass the randomness tests of the NIST test suite that they conduct. They also build and evaluate the performance of secret key extraction

using small, low power, hand-held devices—Google Nexus One phones—that are equipped 802.11 wireless network cards. Last, they evaluate secret key extraction in a multiple input multiple output (MIMO)-like sensor network testbed that they create using multiple TelosB sensor nodes. We find that our MIMO-like sensor environment produces prohibitively high bit mismatch, which we address using an iterative distillation stage that we add to the key extraction process. Ultimately, we show that the secret key generation rate is increased when multiple sensors are involved in the key extraction process.

## 2.9 GROUP SECRET KEY GENERATION VIA RECIEVED SIGNAL STRENGTH: PROTOCOL, ACHIEVABLE RATE & IMPLEMENTATION

Secret key generation among wireless devices using physical layer information of radio channel has been an attractive alternative for ensuring security in mobile environments. Received Signal Strength (RSS) based secret key extraction gains much attention due to its easy accessibility in wireless infrastructure. However, the problem of using RSS to generate keys among multiple devices to ensure secure group communication in practice remains open. In this work, they propose a framework for collaborative key generation among multiple wireless devices leveraging RSS. To deal with mobile devices not within each other's communication range, they employ relay nodes to achieve reliable key extraction. To enable secure group communication, two protocols are developed to perform collaborative group key generation via star and chain topologies respectively. They further provide the theoretic analysis on the achievable secrecy rate for both star and chain topologies in the presence of an eavesdropper. Our prototype development using MICAz motes and extensive experiments using fading trend based key extraction demonstrate the feasibility of using RSS for group key generation in both indoor and outdoor environments, and concurrently achieving a lower bit mismatch rate compared to existing studies.

# CHAPTER III

# METHODOLOGY & IMPLEMENTATION

## 3.1 METHODOLOGY

Idea is to Strengthen Authentication Phase of the Secure Mutual Authentication Protocol (SMAP) with Privacy Preserving Location Authentication Technique (PriLA). Privacy Preserving Location Authentication Technique (PriLA) promises the following,

1. Privacy
2. Anonymity
3. Unforgeability

The Secure Mutual Authentication Protocol (SMAP) protocol is redesigned, such that instead of conventional Authentication techniques used in the Secure Mutual Authentication Protocol (SMAP) protocol we also make use of Privacy Preserving Location Authentication Technique (PriLA) to also authenticate the location of the user. And provide a two-level authentication for Better Security. SMAP has two phases the user verification and Payment Authentication our goal is to make it a two-step authentication by introducing Location authentication after user verification the proceeding to Payment Authentication, so the High-level protocol flow and its required parameters are Illustrated in Fig. 1

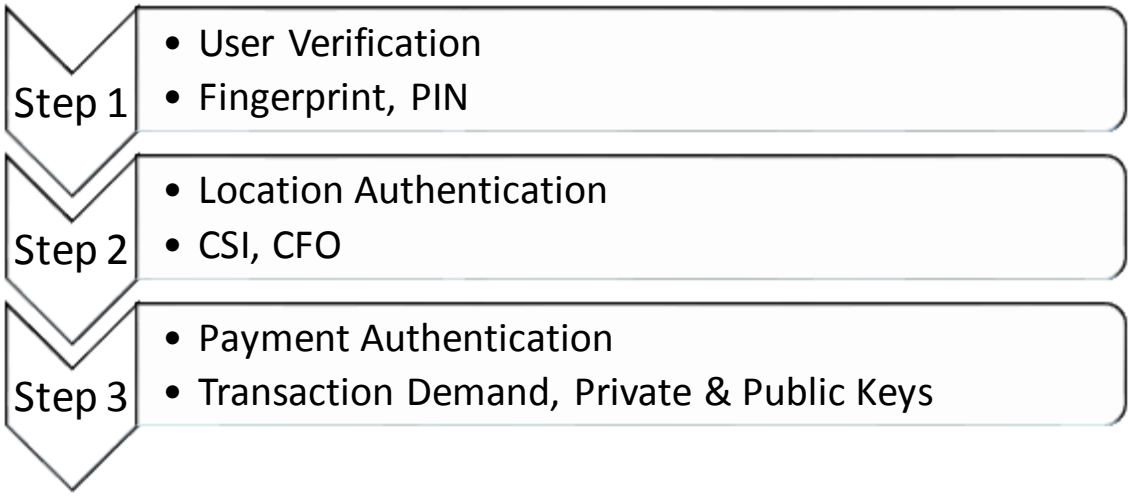



Figure 1 - High Level Protocol Flow

As shown in Fig. 1 the Protocol Authenticates the Authorized user for the Mobile Payment Transaction.

To Give a Better understanding of things it would be better to show a High-level flow individual protocols and the general overview of a LBS. As by Authenticating the location of the user we have converted the usual mobile transaction into a Location Based Service. The Overview of a Generalized LBS is illustrated in Fig. 2

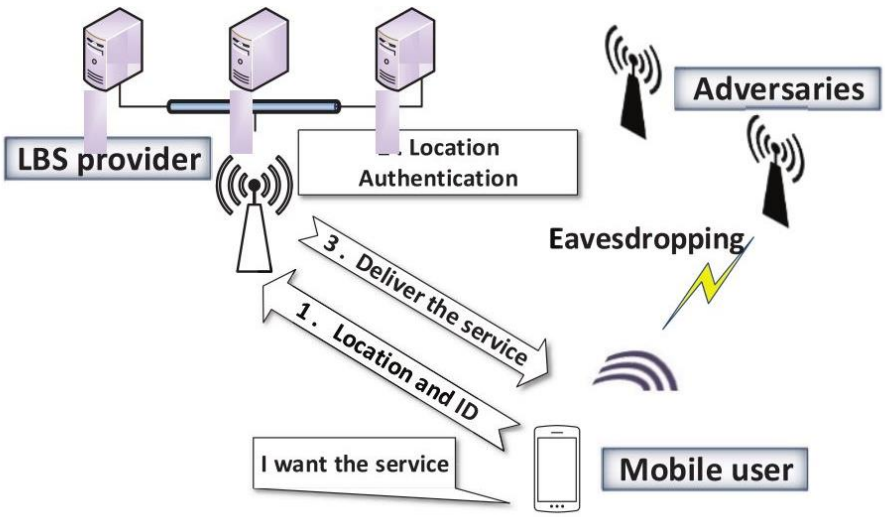



Figure 2 - Overview of Generalized LBS

As Shown in Fig. 2 The fundamental difference between a normal service and a location-based service, obviously is the fact that the user gets the service depending on the location parameter as well. This can act as extra layer of security at a very low computational complexity as location data is generally hard to Spoof or forge.

Next, we can look at the High-level overviews of the two separate protocols we are integrating for better security, Namely – SMAP and PriLA.

### 3.1.1 SMAP

SMAP is based on the theory of the U2F mechanism to achieve secure authentication between the user and website. An asymmetric cryptosystem in this SMAP during the mutual authentication between mobile terminals (e.g., a mobile phone) and the website. The protocol is divided into two phases—online registration and online authentication.

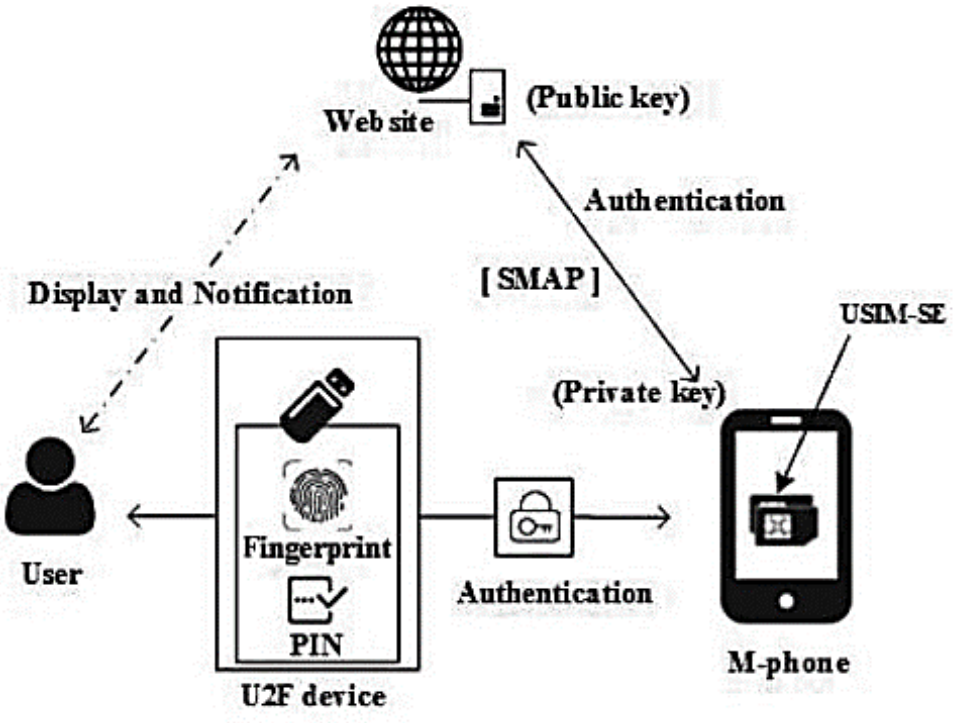



Figure 3 - High-level SMAP Protocol Flow

SMAP is based on the theory of the U2F mechanism to achieve secure authentication between the user and website. Fig. 3 shows the overall workflow of the proposed protocol architecture. The precondition for the smooth operation of this protocol is that the U2F device has built-in support in web browsers. We use an asymmetric cryptosystem in this SMAP during the mutual authentication between mobile terminals (e.g., a mobile phone) and the website. The protocol is divided into two phases—online registration and online certification.

During registration with an online service, the user's client device (mobile phone) creates a new key pair. A private key is retained in the device locally and a public key is registered in the website with the online service. Authentication is performed by the client device—it proves to the service that it possesses the private key by signing a challenge sent from the website. The client's private key can be used only after it is unlocked locally on the device by the user. That is, only a valid user can access the private key, which is guaranteed via the successful authentication exchange between the user and the device. The local unlock is accomplished by a user-friendly and secure action such as swiping a finger, entering a PIN, inserting a second factor device, or pressing a button. As illustrated in Fig. 3, the authentication process in this system is mutual. In the mobile payment environment, this intact protocol has two steps: registration and authentication. The first can be regarded as an initialization step, which provides a channel for both the server and user to store some cryptographic information for use in the next phase. Cryptography is used in the authentication process to ensure the reliability of both the server and client, thereby guaranteeing security. In addition, a Secure Element (SE) is embedded in the USIM card, which is responsible for identification and computation.

### 3.1.2 PriLA

The crux of PriLA is to facilitate the LBS provider to authenticate users' location by exploiting multipath profiles while preserving mobile users' location privacy by encrypting the location reports using fine-grained PHY information. The LBS server and a mobile user follow the protocol described in Fig. 4.

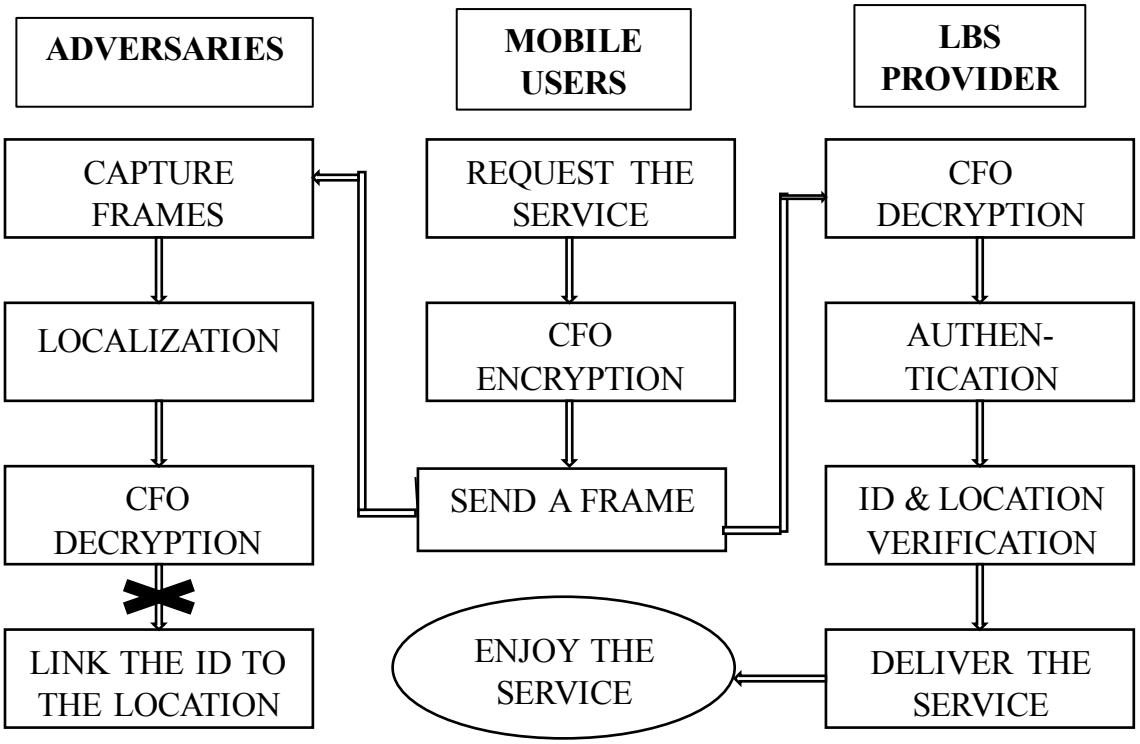



Figure 4 - High-Level PriLA Protocol Flow

First, the mobile user requests the service by exchanging handshake frames with the provider's AP. Then, both the mobile user and the provider extracts CSI and CFO information from the preambles to generate a secret key, which is used to encrypt the following frames sent by the user. After receiving the encrypted frames, the provider decrypts the frames using the CSI and CFO information obtained in the handshake frames, and then extracts the user's ID (MAC address) and location information from the frames. Afterwards, the provider uses the CSI obtained from the user's frames to construct a multipath profile, which is compared with multipath profiles stored at the provider for location authentication. After verifying the reported location, the provider delivers the service to the user.

## 3.2 IMPLEMENTATION

From the High-Level Protocol flow shown in Fig.1, now we can see how each of those steps were implemented namely,

1. User Verification
2. Location Authentication
3. Payment Authentication

Now we shall explore in great depth about how each of these steps function and how are they implemented and how they lead to the next step till the end of the protocol.

### 3.2.1 USER VERIFICATION

Before introducing the details of the workflow, we first explain the notations used, as shown in Table 1.

Table 1 - Summary of Notations Used in User Verification

| Notation | Description |
|---|---|
| Fingerprint | Fingerprint identification |
| PIN | PIN code |
| $K_1$ | Private key |
| $K_2$ | Public key |
| $K_d$ | Key handle used for searching $K_2$ |
| RN | A random number generated by the device |
| M0 | Transaction information |
| M1 | Payment data |
| M2 | Transaction result |
| $C_s$ | Challenge value generated by the server |
| $S_m$ | Signature value operated by the device |
| XOR | Bitwise xor operation |
| $H()$ | Hash operation |

In this phase, the user must choose an available U2F authenticator that is compatible with the online service's acceptance policy. Then, the user unlocks the U2F authenticator to reach a mobile client using a fingerprint reader, a button on a second-factor device, a securely entered PIN, or other similar method. An asymmetric cryptosystem is used, as noted above, for the user's device to create a new public/private key pair that is unique to the local device, the online server, and the user's account. The public key is sent to the online service (website) and is associated with the user's account. The private key and any information regarding the local authentication method (such as biometric measurements) will always remain in the device.

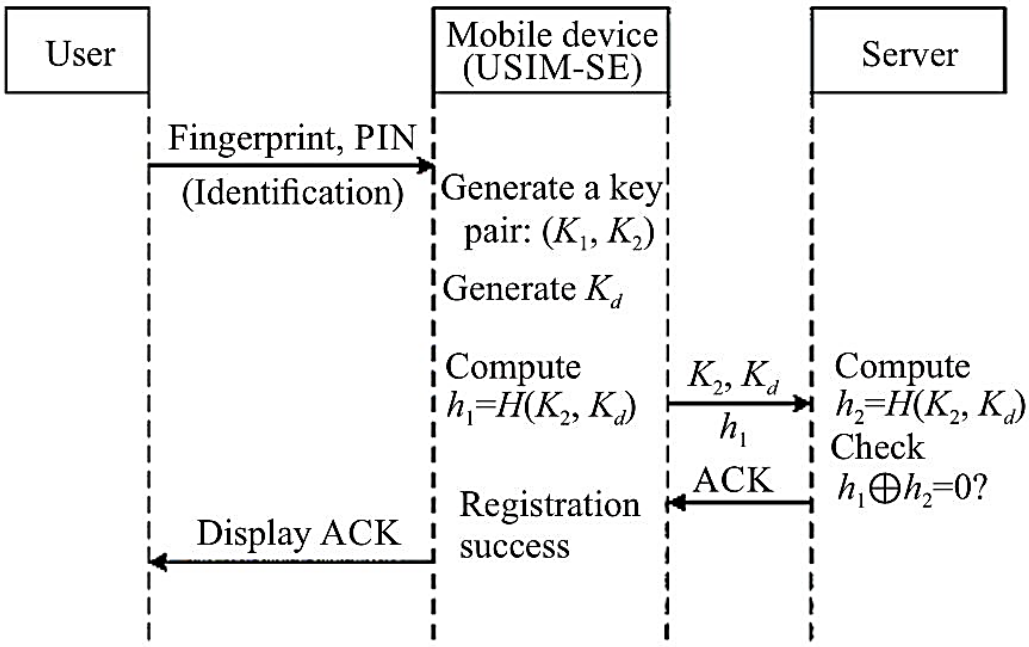



Figure 5 - User Verification Phase

The integrated registration procedure, as shown in Fig. 5, involves the following interactive steps:

*Step 1*: User mobile phone: Establishes an identification between the user and the mobile device with a fingerprint, PIN, or other similar method.

*Step 2:* Mobile phone: The USIM card with the embedded SE module in the mobile device generates a pair of keys. $K_1$, $K_2$ for the local device and the online server. And then the SE module creates the $K_d$. A hash value of $h_1 = H(K_2, K_d)$ is locally computed.

*Step 3:* Mobile phone server: The mobile phone stores the private key in the local device and sends the public key, the key handle, and their hash values to the server.

*Step 4:* Server: At this end, the $K_2$ and $K_d$ are stored, then the server computes the hash value $h_2 = H(K_2, K_d)$, and conducts an XOR operation. using $h_1$. If the result is not zero, this indicates that the information sent from the mobile device to the server has been changed, so the registration fails. Otherwise, the registration is successful, and the server sends an acknowledgment (ACK) response to the mobile device.

*Step 5:* User mobile phone: Upon viewing the ACK response, the user unlocks the device using one of the methods listed above.

In this registration phase, as shown in Fig. 5, we can see that all the preparatory work is completed and ready for the next phase. The first step guarantees that the user can access the mobile device by the way of fingerprint or PIN code. The public key $K_2$, which is sent to the server and pertains to the user's account $K_d$, is used for searching $K_2$ based on the private key $K_1$. At the server end, the binary XOR operation between the calculated hash value $h_2$ and the received hash value $h_1$ ensures that the data sent from the mobile device to the server is secure. If the result of the XOR operation is zero, this means that the values $h_1$ and $h_2$ are equal, which indicates that the registration keys have not been falsified. If ok, the ACK response is sent to the mobile device and is displayed to the user. At this point, the registration has been completed smoothly.

### 3.2.2 LOCATION AUTHENTICATION

After User Verification is successful, For Location Authentication it can be summarised in a single Handshake phase flow diagram Fig.6, which explains how the user and the service provider exchange CSI and generate their keys and Authenticate Location information with the generated keys.

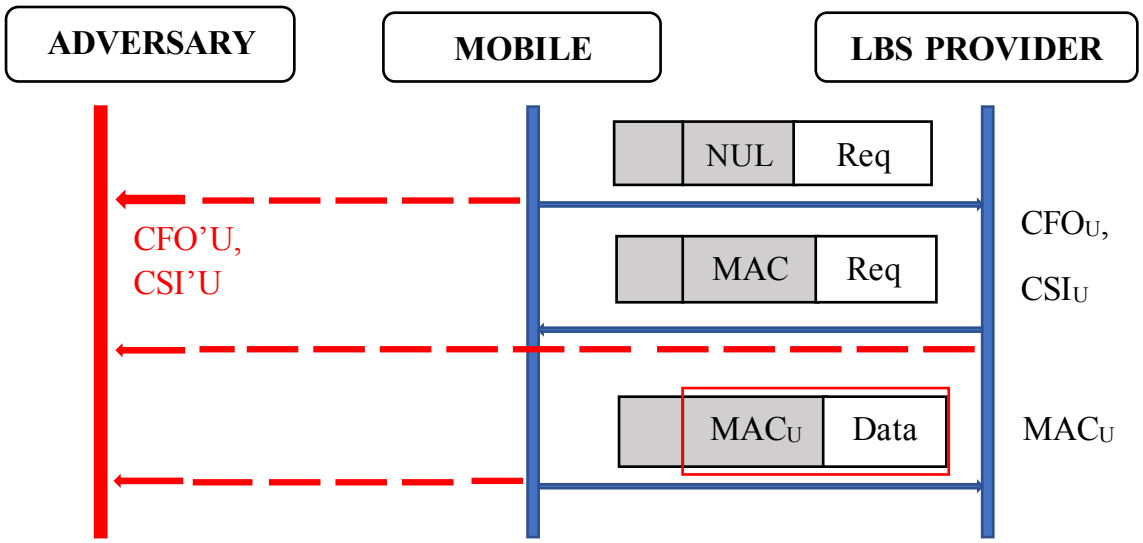



Figure 6 - Secure Handshake Protocol of PriLA

As depicted in Fig. 6, the request frame sets the transmitter address as "NULL" to hide the user's MAC address from adversaries. The provider extracts the CSI information and phase from the preamble. Then, the provider returns an acknowledge frame (ACK) to the user. Data is modulated using adaptive modulation process and MAC of the user is encrypted using CFO Injection. The user extracts the CSI information from the ACK and uses the CSI information to encrypt the subsequent frames. The provider extracts and then finds the matched CSI information based on previously logged mappings. Due to reciprocity of a wireless link, the phase and CSI information obtained by the user and the provider is (theoretically) identical.

Therefore, the provider can use the phase and CSI information obtained at the AP side to decrypt the frame. On the other hand, even if the adversaries can

eavesdrop all frames sent by the user and the provider, they cannot acquire the MAC address of the user. The Algorithm employed in both the user and the service provider to extract key from CSI values is Shown Below,

***Algorithm: CFO Encryption & Decryption***

---

***Initialization***

*Step 1:* Initialise k – [ ];

*Step 2:* Compute the differential CSI vector, $[d_1,.....,d_n]$

where $d_i = c_{i+1} - c_i \quad ,\forall_i = 1,.....,n$

*Step 3:* Put the differential CSI values into different buckets one by one following the rule,

$d_i \rightarrow$ ceil(i/L)$^{th}$

*Step 4*: Find the maximum and minimum differential CSI values $d_{max}$ and $d_{min}$.

*Step 5:* Generate four shape pattern vectors

$$v00 = [\frac{d_{min}}{n}, ..., \frac{id_{min}}{n}, ..., \frac{Ld_{min}}{n}],$$

$$v01 = [\frac{Ld_{min}}{n}, ..., \frac{id_{min}}{n}, ..., \frac{d_{min}}{n}],$$

$$v10 = [\frac{d_{max}}{n}, ..., \frac{id_{max}}{n}, ..., \frac{Ld_{max}}{n}],$$

$$v11 = [\frac{Ld_{max}}{n}, ..., \frac{id_{max}}{n}, ..., \frac{d_{max}}{n}],$$

***Key Generation***

*Step 6:* for each bucket

*Step 7*: Compute Frechet distances (Appendix B) between the bucket and the four shape pattern vectors

*Step 8:* Find the vector $v_i$ with the smallest distance

*Step 9:* Add the corresponding bits to k = [k i]

*Step 10*: end for

*Step 11*: return k

***CFO Injection***

*Step 12*: Generate a vector of CFOs of length, floor ( $\frac{2n}{ML}$ )
by multiply each M bits of K with singular values.

*Step 13:* Hash each generated CFO.

*Step 14:* for i = 1 to S do

*Step 15*: Compute the index j of CFO used for injection: j = i mod floor( $\frac{2n}{ML}$ )

*Step 16*: Inject the $j^{th}$ CFO value to the $i^{th}$ symbol;

*Step 17*: end for

---

Since k is the private message merely shared between the communication pair, the adversaries have no way to guess the generated CFO pattern. All further Handshake packets are protected by injecting the CFO vector as per the algorithm such that only the user and the LBS Service Provider can decrypt the encrypted message with the CFO vector. Which is the same for User and the LBS provider because of channel reciprocity.

Therefore, once the LBS provider decrypts User ID and Location And if the ID is verified Then their Location is also Authenticated as the Keys for Encryption/Decryption are generated from the CSI between User and LBS provider at that location. An adversary with different location i.e. different CSI will Have Different Key so He will not be Able to Decrypt the Message (Users Location And ID) Therefore, User ID and Location are Privacy-Preserved.

### 3.2.3 PAYMENT AUTHENTICATION

Once Both the User was verified and the Location is Authenticated only then will the protocol move on to the Next step which is the payment Authentication.

Some relevant information will be sent to the user's own account during the User Verification procedure like the Keys that were shared are stored for this stage of Authentication. In addition, if the user wants to be assured of a good online shopping experience, the Payment Authentication process is necessary and will play an important role.

Before introducing the details of the workflow, we first explain the notations used, as shown in Table 2.

Table 2 – Summary of Notations Used in Payment Authentication

| Notation | Description |
|---|---|
| Fingerprint | Fingerprint identification |
| PIN | PIN code |
| $K_1$ | Private key |
| $K_2$ | Public key |
| $K_d$ | Key handle used for searching $K_2$ |
| RN | A random number generated by the device |
| M0 | Transaction information |
| M1 | Payment data |
| M2 | Transaction result |
| $C_s$ | Challenge value generated by the server |
| $S_m$ | Signature value operated by the device |
| XOR | Bitwise xor operation |
| $H()$ | Hash operation |

This process involves the use of the asymmetric cryptosystem mechanism to perform information exchange, as well as a mutual authentication process, in which user-initiated transaction information and the online payment service information are strictly compared. When their consistency is confirmed, only then will payment occur. If the information is inconsistent, this indicates that the transaction has been tampered with, and the user can directly end the transaction. This certification process is effective for

helping users to avoid phishing sites. As shown in Fig. 7, the authentication process is divided into six steps.

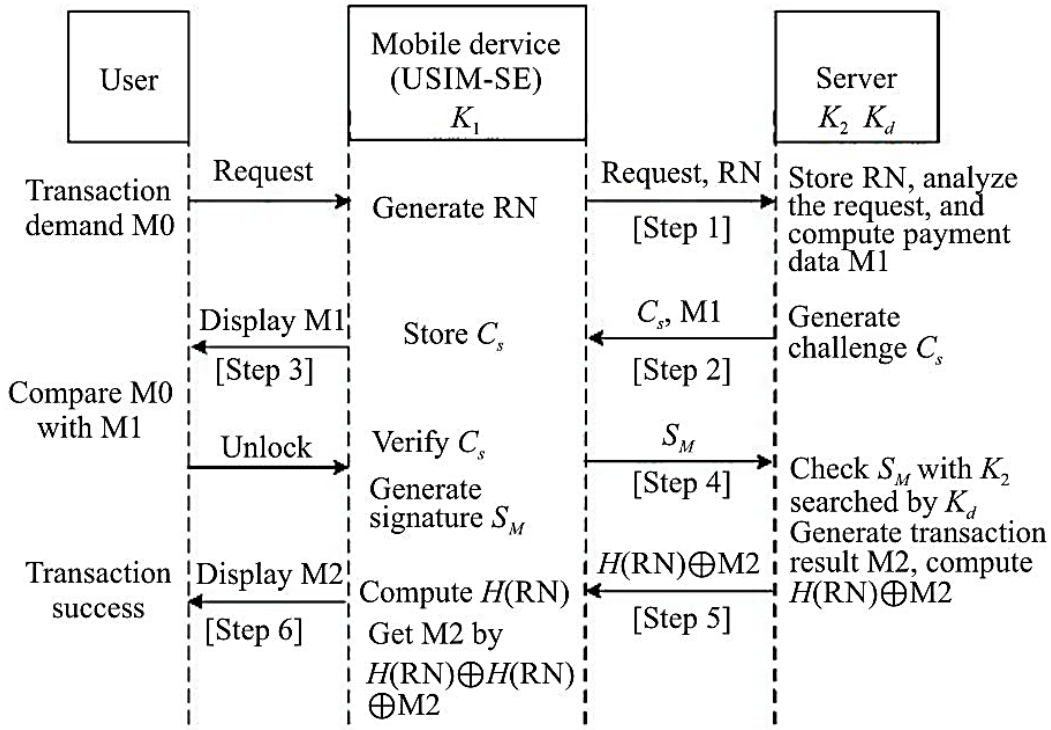



Figure 7 - Payment Authentication Phase

When registration is complete, the private key is stored in the SE module in the mobile device, whereas the public key and key handle are stored in the online server. When a user performs an online mobile payment, the entire transaction also comprises six steps, the details of which are as follows:

*Step 1* The user initiates an online transaction by sending a request to the mobile device. Based on this request, the mobile device (USIM-SE) generates a Random Number (RN) locally, and then sends both the request and the RN to the server.

*Step 2* After receiving and storing the RN, the server analyses the transaction request, transforms it into payment data, and computes it correctly, which is denoted as M1. Next, the server generates a challenge $C_s$ based on the

public key $K_1$ that had been stored earlier during registration. Then, the server sends the challenge $C_s$ and the M1 to the mobile device.

*Step 3* $C_s$ is stored in mobile device (USIM-SE). The payment data M1 is displayed to the user via a popup or other similar method on the screen. Based on the M1, the user can compare the payment data with the previous transaction information M0 created by the user's own demand. If they do not match, this indicates that the transaction request has been falsified, so the user can stop the transaction to avoid any financial loss from a wrong payment. However, if M1 matches M0, this confirms that the transaction data is unchanged and the transaction payment data is correct, so the user can unlock the SE by fingerprint, simplified PIN code, or other similar method.

*Step 4* After being unlocked by a valid user, the SE will verify the challenge $C_s$ previously stored locally. Then, the SE generates a signature $S_M$ with the local private key $K_1$ to respond to the challenge $C_s$ and the $S_M$ will be sent to the server.

*Step 5* The server searches the public key $K_2$ based on the key handle $K_d$, and uses it to verify the signature $S_M$. If successful, the server will generate the transaction result, denoted by M2, then compute the value H(RN)+M2 and send it to the mobile device (USIM-SE).

*Step 6* Compute H(RN) with the local RN in SE and obtain the M2 by H(RN)+H(RN)+M2. Then, the mobile device displays the M2 transaction result to the user. The authentication process is then complete and the whole transaction has been smoothly executed.

# CHAPTER IV

# RESULTS & DISCUSSIONS

## 4.1 SIMULATION TOOL & PERFORMANCE METRICS

The Simulation Tool Used for This Project is MATLAB.

The Primary focus of this project is to improve security of Mobile Transactions with the Least Compromises.

Any Protocol needs some metrics to measure performance/compare with exiting protocols in terms of Merits.

The Four Main Performance Metrics for this Protocol Are,

1. Transaction Time
2. Leakage
3. Mismatch
4. Adversary BER Performance

These Measurements were done in MATLAB using all 512-bit Values (for BITXOR simplicity) and Asymmetric Cryptosystem as RSA and Hash is SHA512.

### 4.1.1 TRANSACTION TIME

This is end-to-end time duration for each phase, and everything combined into a whole protocol.

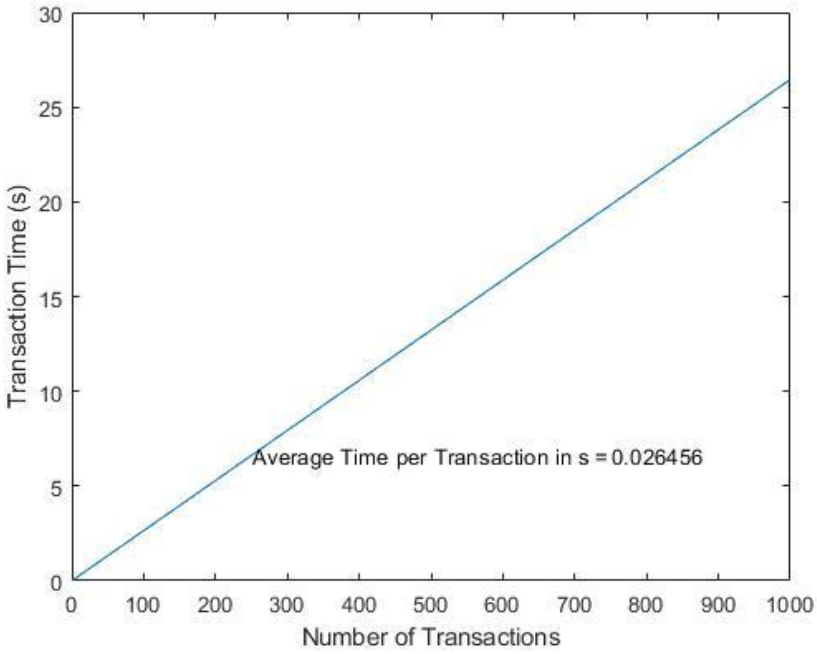



Figure 8 - User Verification Time per Transaction

In Fig.8, we can see the Average time taken for User verification per transaction is roughly 26 ms.

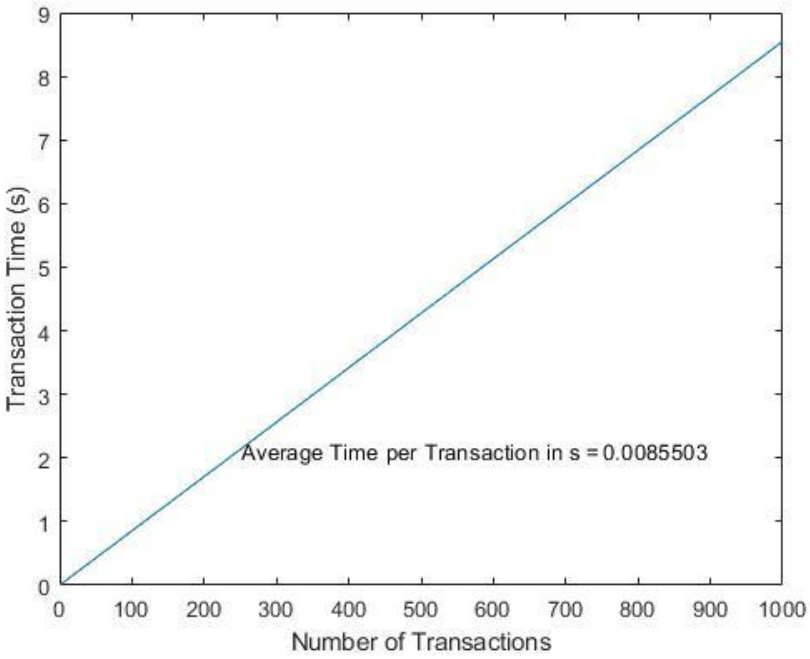



Figure 9 - Location Authentication Time per Transaction

In Fig. 9, we can see the Average time taken for Location Authentication per transaction is roughly 4 ms. (Here the Graph shows 8ms as it's done on both Server and the user side for just one person its half the value)

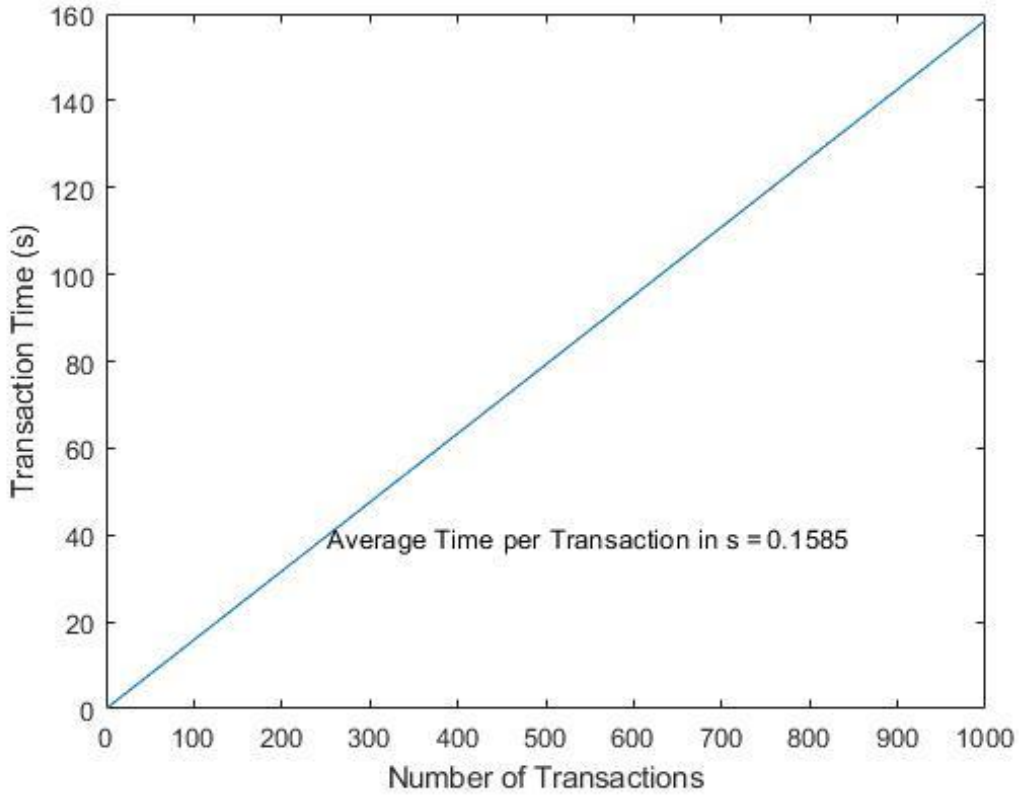



Figure 10 - Payment Authentication Time per Transaction

In Fig. 10, we can observe that Average time taken for Payment Authentication per transaction is 158.5 ms. Most of this time delay can be attributed to the Actual transaction by the merchant (in simulation attributed by 100 – SHA-512 Hash functions – to compensate actual transaction).

Finally, in Fig. 11, we can see the comparison between Vanilla SMAP and the newly Modified SMAP+PriLA to directly see the difference in transaction time for the new improved levels of security.

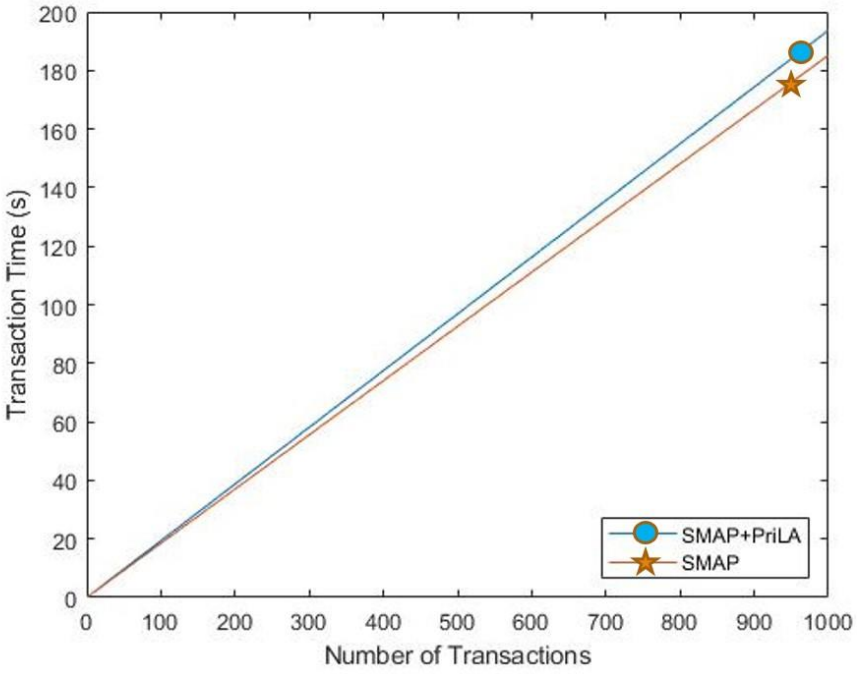



Figure 11 - SMAP Vs SMAP+PriLA

### 4.1.2 LEAKAGE

- Ratio of matched bits between user / provider and adversary.
- Encryption scheme with lower leakage is more secure.

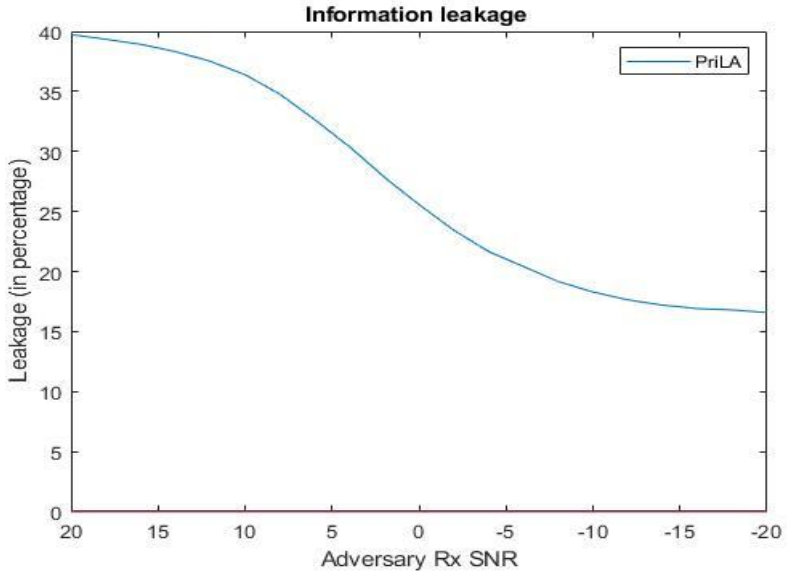



Figure 12 – Security Analysis - Leakage

From Fig 12, we can see the distance between the adversary and the user/provider is modelled as Rx SNR. Based on that even in the worst case this is only leaking about 40% information.

### 4.1.3 MISMATCH

- Ratio of number of bits unmatched between the secret key independently generated by USER and PROVIDER to the total number of bits.
- Measures the robustness of encryption scheme.
- Low Mismatch provides more security.

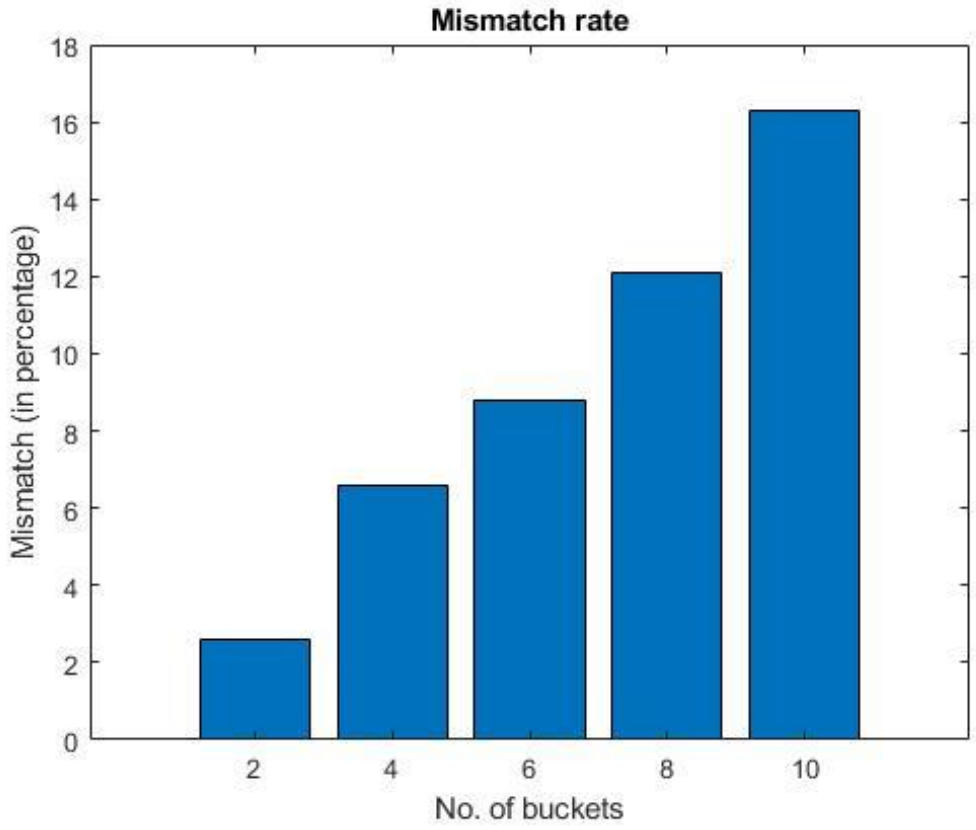



Figure 8 – Security Analysis - Mismatch Rate

From Fig 13 we can Observe As the number of Buckets increases the Mismatch also increases. The reason is that when the number of buckets is large, the entropy of bucket is quite small, implying low uncertainty in the bits generated

by buckets. Hence, the security level of PriLA in the case of large number of buckets is low.

### 4.1.4 ADVERSARY Rx BER PERFORMANCE

Here the adversaries are modelled in two ways,

1. Dumb Adversary
2. Smart Adversary

**Dumb Adversary:**

When the Adversary is generating keys at Random and they have no knowledge about the user/ provider pair in general.

**Smart Adversary:**

When the Adversary is generating keys with the knowledge of user/provider pair and has some knowledge of the channel which he can leverage to perform a better attack on the Transaction by user/provider.

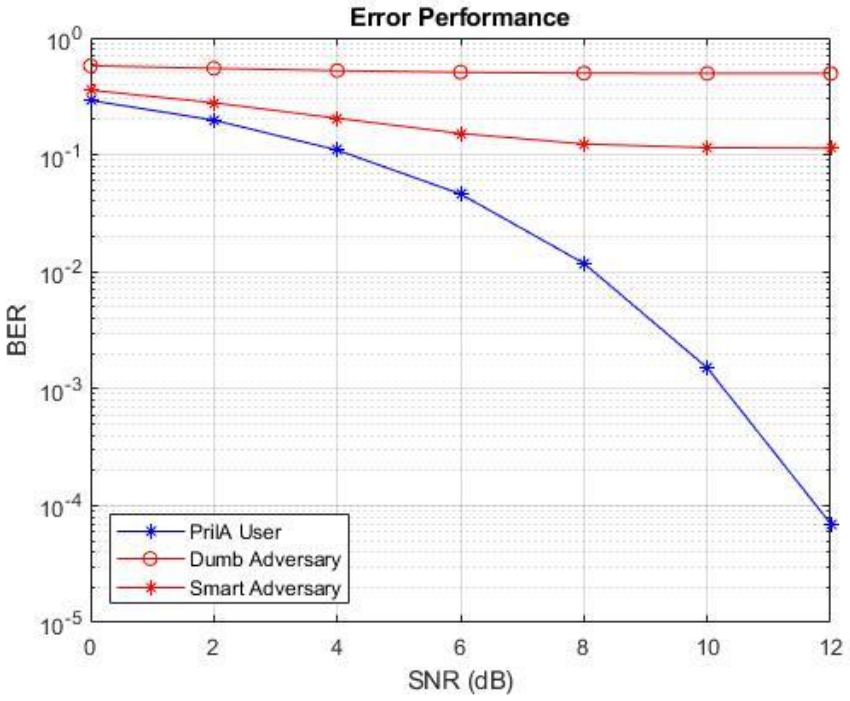



Figure 9 - Adversary Rx BER Performance

From Fig.14, we can observe that for the Dumb adversary the error performance stays at 0.5 regardless of increase SNR (here it corresponds to distance from the user/provider) this can be explained easily by the random generation of his Key.

For the Smart Adversary the performance is better than that of the Dumb Adversary but it's nowhere near acceptable performance because it is barely at 0.1 even at the highest SNR which is not acceptable performance for any system.

The Protocol has been Implemented and simulated for different metrics too gauge performance and tested for Security Vulnerabilities. And Based and Observations the Protocol was fine tuned for Optimal Performance.

# CHAPTER V

# CONCLUSION & FUTURE WORK

## 5.1 CONCLUSION

A modified mobile payment protocol from Secure Mutual Authentication Protocol (SMAP) and its integration with a Privacy Preserving Location Authentication (PriLA) Technique to create a more secure protocol compared to either of the above-mentioned techniques used independently. The newly modified protocol was tested for its Computational Complexity, Vulnerabilities and a complete Security Analysis was performed. It provides better security at the cost of Transaction time and Computational Complexity. Because of very flexible protocol it can be integrated with existing Wi-Fi networks with very little change to Hardware.

## 5.2 FUTURE WORK

This protocol can be Extended for the Concept of IoT with special restraints in mind specific to low power IoT devices. Some of the Heavier Calculations and Power consuming Tasks Would Have to be simplified while not compromising security.

## REFERENCES

[1]. Kai Fan, Hui Li, Wei Jiang, Chengsheng Xiao and Yintang Yang, (2018) "Secure Authentication Protocol for Mobile Payment", Tsinghua Science and Technology. Volume: 23, Issue: 5, Pages: 610 – 620

[2]. Wei Wang, Yingjie Chen and Qian Zhang (2016), "Privacy-Preserving Location Authentication in Wi-Fi Networks Using Fine-Grained Physical Layer Signatures", IEEE Transactions on Wireless Communications Volume: 15, Issue: 2.

[3]. Yanan Chen, Weixiang Xu, Li Peng and Hao Zhang (2019), "Light-Weight and Privacy-Preserving Authentication Protocol for Mobile Payments in the Context of IoT ", IEEE Access Security and Privacy for Cloud and IoT Volume: 7, Pages: 15210 – 15221.

[4]. Z. Zhang, L. Zhou, and X. Zhao (2013), "On the validity of geosocial mobility traces," in Proc. ACM HotNets, pp. 1–7.

[5]. W. Wang and Q. Zhang (2015), "Toward long-term quality of protection in mobile networks: A context aware perspective," IEEE Wireless Commun., vol. 22, no. 4, pp. 34–40.

[6]. K. Wu, J. Xiao, Y. Yi, D. Chen, X. Luo, and L. M. Ni (2013), "CSI-based indoor localization," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 7, pp. 1300-1309.

[7]. J. Xiong and K. Jamieson (2013), "Arraytrack: A fine-grained indoor location system," in Proc. USENIX Symp. Netw. Syst. Des. Implement. (NSDI), pp. 71–84.

[8]. V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi (2008), "Location-based trust for mobile user-generated content: Applications, challenges and implementations," in Proc. ACM HotMobile, pp. 60–64.

[9]. S. Saroiu and A. Wolman (2009), "Enabling new mobile applications with location proofs," in Proc. ACM HotMobile, p. 3.

[10]. M. Talasila, R. Curtmola, and C. Borcea (2012), "Link: Location verification through immediate neighbors knowledge," in Proc. Mobile Ubiquitous Syst. Comput. Netw. Serv., pp. 210–223.

[11]. J. Brassil, P. Manadhata, and R. Netravali (2014), "Traffic signature-based mobile device location authentication," IEEE Trans. Mobile Comput., vol. 13, no. 9, pp. 2156–2169.

[12]. Z. Zhu and G. Cao (2013), "Toward privacy preserving and collusion resistance in a location proof updating system," IEEE Trans. Mobile Comput., vol. 12, no. 1, pp. 51–64.

[13]. J. Wang and D. Katabi (2013), "Dude, where's my card? RFID positioning that works with multipath and non-line of sight," in Proc. ACM SIGCOMM, pp. 51–62.

[14]. K. G. Shin, X. Ju, Z. Chen, and X. Hu (2012), "Privacy protection for users of location-based services," IEEE Wireless Commun., vol. 19, no. 1, pp. 30-39.

[15]. C.-Y. Chow, M. F. Mokbel, and T. He (2011), "A privacy-preserving location monitoring system for wireless sensor networks," IEEE Trans. Mobile Comput., vol. 10, no. 1, pp. 94–107.

[16]. X.-Y. Li and T. Jung (2013), "Search me if you can: Privacy-preserving location query service," in Proc. IEEE INFOCOM, pp. 2760–2768.

[17]. J. Terry and J. Heiskala (2002), OFDM Wireless LANs: A Theoretical and Practical Guide. Indianapolis, IN, USA: Sam.

[18]. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput, IEEE Std 802.11n, 2009, pp. 1–565.

[19]. J. Fang et al. (2013), "Fine-grained channel access in wireless LAN," IEEE/ACM Trans. Netw., vol. 21, no. 3, pp. 772–787.

[20]. T. S. Rappaport et al. (1996), Wireless Communications: Principles and Practice. Englewood Cliffs, NJ, USA: Prentice-Hall, vol. 2.

[21]. Y. Qiao, K. Srinivasan, and A. Arora (2014), "Puzzle: A shape-based secret sharing approach by exploiting channel reciprocity in frequency domain," in Proc. USENIX Symp. Netw. Syst. Des. Implement. (NSDI), pp. 1–14.

[22]. S. N. Premnath et al. (2013), "Secret key extraction from wireless signal strength in real environments," IEEE Trans. Mobile Comput., vol. 12, no. 5, pp. 917–930.

[23]. H. Liu, J. Yang, Y. Wang, Y. Chen, and C. E. Koksal (2014), "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," IEEE Trans. Mobile Comput., vol. 13, no. 12, pp. 2820– 2835.

[24]. L. Sweeney (2002), "k-Anonymity: A model for protecting privacy," Int. J. Uncertainty Fuzziness Knowl. Based Syst., vol. 10, no. 5, pp. 557–570.

[25]. C. Dwork, F. McSherry, K. Nissim, and A. Smith (2006), "Calibrating noise to sensitivity in private data analysis," Theory Cryptogr., vol. 3876, pp. 265–285.

[26]. T. Eiter and H. Mannila (1994), "Computing discrete Fréchet distance," Tech. Rep. CD-TR 94/64, Information Systems Department, Technical University of Vienna.

[27]. S. Salvador and P. Chan (2007), "Toward accurate dynamic time warping in linear time and space," Int. Data Anal., vol. 11, no. 5, pp. 561–580.

# APPENDIX A

## TERMINOLOGY

Some Important terms & their Definitions,

- Confidentiality - Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it: Access must be restricted to those authorized to view the data in question.

- Integrity - involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people.

- Location Authentication - merely ensures that the individual is who he or she claims to be but says nothing about the access rights of the individual. In this case we Authenticate the Location instead of Identity.

- Location Privacy - is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively here we don't want everyone to be aware of our Physical Location.

- Physical Layer Information – Physical layer is the lowest layer. It deals with transmitting bit by bit information over the channel. Here we are most interested in the detrimental features of the physical layer like carrier frequency offset (CFO), Channel state Information (CSI) etc.

- Carrier Frequency Offset (CFO) - occurs when the local oscillator signal for down-conversion in the receiver does not synchronize with the carrier signal contained in the received signal. This phenomenon can be attributed to two important factors: frequency mismatch in the transmitter and the receiver oscillators; and the Doppler effect as the transmitter or the receiver is moving.

- Channel State Information (CSI) - refers to known channel properties of a communication link. This information describes how a signal propagates from the transmitter to the receiver and represents the combined effect of, for example, scattering, fading, and power decay with distance

- Signature - is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid signature, where the prerequisites are satisfied, gives a recipient very strong reason to believe that the message was created by a known sender (authentication), and that the message was not altered in transit (integrity).

# APPENDIX B

## FRECHET DISTANCE [26]

- The Fréchet distance is a measure of similarity between two curves, P and Q.
- It is defined as the minimum length enough to join two points travelling along different directions
- The rate of travel for either point may not necessarily be uniform.
- Walking your Dog – Fréchet Distance is the minimum leash length that permits such a walk