**IOT SECURITY ENHANCEMENT USING PHYSICAL LAYER SIGNATURES**

# PHASE I REPORT

***Submitted by***

**NARAYANAN B(2016105053)**

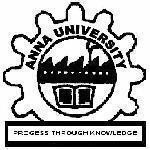
**ASHOK KUMAR M(2016105513)**

**VENKAT KRISHNAN (2016105077)**

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

# BACHELOR OF ENGINEERING IN ELECTRONICS

# AND COMMUNICATION ENGINEERING



**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 US” 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** | **SIGNATURE** |
| **DR. S. MUTTAN** | **DR. K. GUNASEELAN** |
| Professor & Head | Assistant Professor (Sr.Gr.) |
| Department of ECE | Department of ECE |
| Chennai – 25 | Chennai - 25 |

## ABSTRACT

Generating keys and Exchanging them with legitimate user is critical in secure communications. Due to the “open-air” nature, key distribution is more susceptible to attacks in wireless communications. An ingenious solution is to generate common secret keys by two communicating parties separately without the need of key exchange or distribution, and regenerate them on needs. Recently, it is promising to extract keys by measuring the random variation in wireless channels by two most popular channel parameters, i.e., channel state information and received signal strength. Through results collected from over a hundred tests, this project offers insights to the design of a secure and efficient key generation system and authentication between two communicating parties. The multipath effect in wireless channel and the movement of users/objects is essential and beneficial to key generation as it increases the channel randomness.

Authentication verifies the user identity and prevents malicious users from accessing the network. Secure transmission protects data integrity and confidentiality using encryption schemes .In this project, we propose an efficient Secret Key Extraction protocol from the channel state information(CSI), Authentication between two communicating parties by additional encryption using constellation rotation from generated key . A new system is proposed where the existing cryptographic securities are enhanced with the incorporation of **Physical layer signatures(PLS).** The principles, performance metrics, Authentication protocol, encryption using constellation rotation procedure and key generation procedure are comprehensively surveyed. The project concludes with some suggestions for future studies.

# 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 herguidance, 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**

## CHAPTER TITLE PAGE NO NO BONAFIDE CERTIFICATE ii

**ABSTRACT(Tamil) iii**  **ABSTRACT(English) v**

## ACKNOWLEDGEMENT vii

**TABLES OF CONTENT viii**

## LIST OF FIGURES xi

**LIST OF TABLES xii**

**LIST OF ABBREVIATION xiii**  **LIST OF SYMBOLS xiv**

## I INTRODUCTION 1

1.1 Motivation 1

1.2 Objective 2

1.3 Confidentiality 2

1.4 Authentication 5

1.5 Wireless Security Challenges 5

1.6 Physical Layer Security Schemes

1.7 Location Authentication 7

1.8 Location Privacy 8

1.9 Structure of the Report 9

## II LITERATURE SURVEY 10

2.1 Secure Mutual Authentication Protocol for 10

Mobile Payments

2.2 Privacy-Preserving Location Authentication 11 in Wi-Fi Networks Using Fine-Grained

Physical Layer Signatures

2.3 Light Weight and Privacy-Preserving 12 Authentication Protocol for Mobile Payments in the Context of IoT

2.4 CSI-based indoor localization 13

2.5 Toward privacy preserving and collusion 14 resistance in a location proof updating system

2.6 Traffic signature-based mobile device 15

location authentication

2.7 Puzzle: A Shape Based Secret Sharing 16 Approach by Exploiting Channel Reciprocity in Frequency Domain

2.8 Secret Key Extraction from Wireless Signal 17

Strength in Real Environments

2.9 Group Secret Key Generation via Received 18  Signal Strength: Protocol, Achievable Rates

& Implementation

## III METHODOLOGY IMPLEMENTATION 19

3.1 Methodology 19

3.1.1 SMAP 21

3.1.2 PriLA 23

3.2 Implementation 24

3.2.1 User Verification 24

3.2.2 Location Authentication 27

3.2.3 Payment Authentication 29 **IV**  **RESULTS & DISCUSSIONS 33**

4.1 Simulation Tool & Performance Metrics 33

4.1.1 Transaction Time 33

4.1.2 Leakage Rate 36

4.1.3 Mismatch Rate 37

4.1.4 Adversary Rx BER Performance 38

**V**  **CONCLUSION & FUTURE WORK 40**

5.1 Conclusion 40

5.2 Future Work 40

**REFERENCES 41**

**APPENDIX 45**

Appendix A - Terminology 45

Appendix B – Fréchet Distance 47

## 

## LIST OF FIGURES

**FIGURE DESCRIPTION PAGE**

**NO NO**

## LIST OF TABLES

**TABLE NO DESCRIPTION PAGE**

**NO**

## LIST OF ABBREVIATIONS

**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

**CHAPTER I**

### INTRODUCTION

#### 1.1 MOTIVATION

Due to the “open-air” nature, key distribution is more susceptible to attacks in wireless communications. Due to this underlying flaw in the key generation process and the fact that these keys are less random and predictable, there are many instances of forced entry on devices protected by these standards. Conventional schemes are based on complex mathematical problems and protocols. These schemes work well for devices having powerful capabilities, such as smartphones. IoT devices are lightweight devices which may not be able to support computationally complex algorithms needed to perform the complex cryptography. This calls for a new key generation method which is less complex, but at the same time secure is necessary to provide better security for such devices.

Physical layer security involves physical layer signatures which are very random and doesn’t involves complex mathematical computations. These signatures present an excellent quality of randomness and prove to be an ideal resource for secret key extraction.

A new system is proposed where the existing cryptographic securities are enhanced with the incorporation of physical layer signatures

#### 1.2 OBJECTIVE

• To develop a new secret key generation algorithm using physical layer signatures like CSI.

• To overcome key exchange, key distribution and key management overhead at legitimate users.

• To provide significant improvement in secrecy.

## 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.

**1.6 PHYSICAL LAYER SIGNATURES**

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 signaturess 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. One recent trend in this regard is to use physical-layer identification

For example, received signal strength (RSS) becomes a popular statistic of the radio channel and is used as the source of secret information shared between two parties . The variation over time of the RSS, caused by motion multipath fading, can be quantized and used for generating secret keys. Due to presence of noise and manufacturing variations, the generated secret keys might be different, which are corrected by information reconciliation. Finally, privacy amplification is introduced to convert this bit-string into a uniformly distributed string to make it secure enough. However, RSS cannot work well in stationary scenarios due to infrequent and small scale variations in the channel measurements. To address this issue, we propose a secret key extraction based on the inherent randomness of wireless channels. In current widely used IEEE 802.11n networks, data is modulated on multiple Orthogonal Frequency Division Multiplexing (OFDM) subcarriers simultaneously. Each network interface card (NIC) of the device can get a value of Channel State Information (CSI) which describes the current condition of the channel in each subcarrier Different from RSS, CSI is a fine-grained value derived from the physical layer. It consists of the attenuation and phase shift experienced by each spatial stream on every subcarrier in the frequency domain. In contrast to having only one RSS value per packet, NIC can obtain multiple CSI values at one time. CSI provides other attractive properties. First, it is very sensitive to location such that two closely-placed receivers have very different readings by the same sender. Second, its readings of a pair of sender and receiver have a strong correlation. Third, it presents an excellent quality of randomness. Due to these characteristics, CSI is an ideal resource for secret key extraction.

### 1.5 KEY EXCHAGING TECHNIQUE CHALLENGES

The inherent broadcast nature of wireless communication allows transmissions to be received by any user within the range, resulting in attackers' ability to initiate various passive attacks such as eavesdropping, traffic analysis and monitoring,

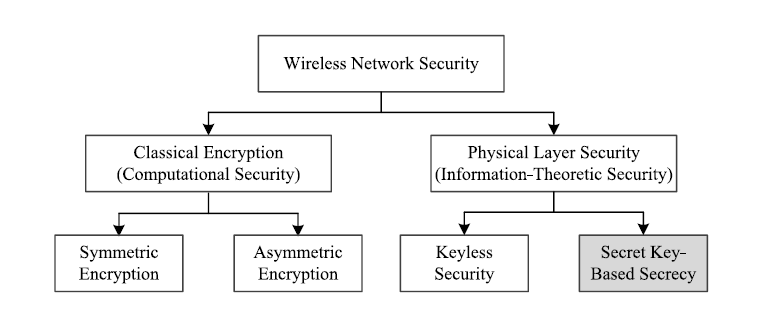
etc, or to execute active attacks like jamming, spoofing, modification, replaying and denial-of-service (DoS)attack ,etc .There has been extensive research interest to protect wireless transmission . Traditionally, the data is secured by

classic encryption schemes ,which work on the assumption that the algorithm is complex enough so that the time taken by eavesdroppers to crack the cryptographic system is much longer than the validity of the information itself,

therefore, the backward secrecy is guaranteed. As shown in ~~Fig. 1~~, classic encryption schemes consist of symmetric encryption schemes and asymmetric encryption schemes, depending on the keys that the two cryptographic parties

use. Symmetric encryption schemes use the same key and are usually employed for data protection thanks to their efficiency in data encryption. Asymmetric encryption schemes, also known as public key cryptography, use the same public

key but different private keys and are usually applied for key distribution.



Classic encryption schemes are faced with several vulnerabilities.

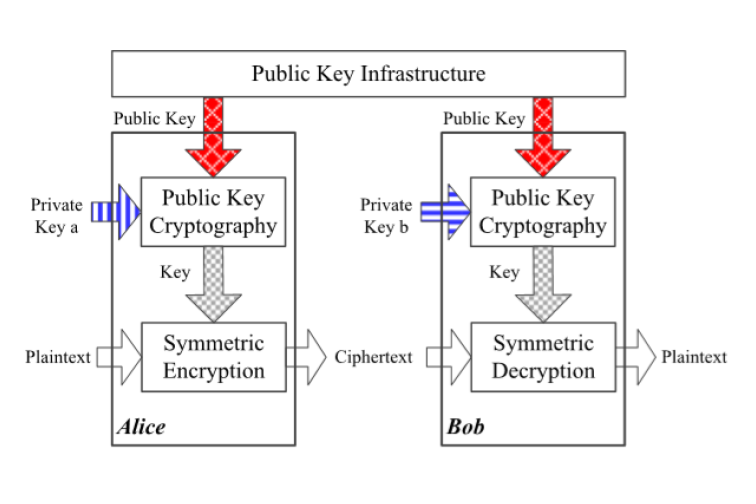
Take public key cryptography as an example. Firstly,it depends on the computational hardness of some mathematical problems, e.g., discrete logarithm. This computational security nature may not hold in future due to the rapid development of hardware technology. In addition, it requires a key management infrastructure which should be secured as well. This approach is therefore less attractive for many wireless sensor networks (WSNs) and ad hoc networks applications, because sensor nodes have limited computational capacity while ad hoc networks are decentralized.

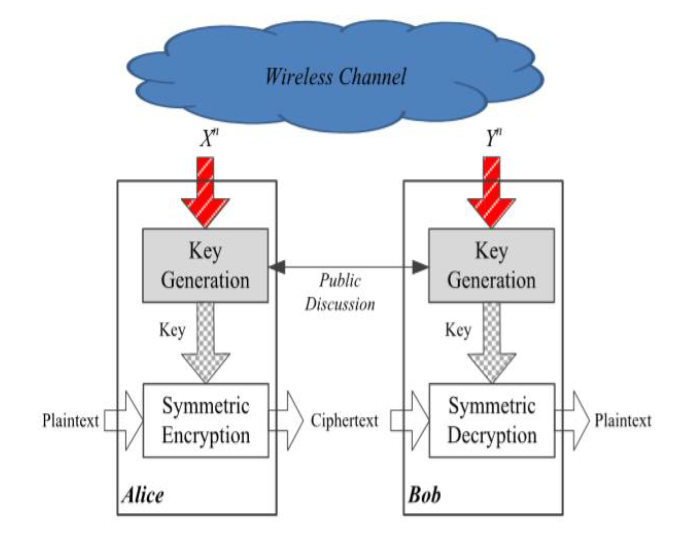
While classic encryption schemes are applied in the upper layers of the communication protocols, the physical layer can also be exploited to enhance wireless security. Physical layer security (PLS) schemes leverage unpredictable and random characteristics of wireless channels in order to achieve information theoretic-security. As shown in ~~Fig. 1~~, PLS schemes are composed of keyless security and secret key-based secrecy. Pioneered by Wyner's wiretap channel model, keyless security does not require keys for encryption but employs code design and channel properties of legitimate users and eavesdroppers to achieve secrecy . However, the legitimate users usually require full/part of instantaneous/statistical channel state information (CSI) of the eavesdroppers, which is not always available in practice and results in a very complex implementation. Secret key-based secrecy dated back as early as 1919 when the concept of one-time pad, also known as Vernam cipher ,was used to encrypt each message bit with a random secret key bit. Later on, Shannon laid the theoretical

basis for perfect secrecy .The message M is encoded into codeword C which does not reveal any information about the message, i.e.,

H(M /C) = H(M)

where H(.) denotes the entropy. This requires the information of the key sequence should be larger than, or at least equal to, the information of the message. One possible way to establish the key is to generate keys from the wireless channels.





However, in practice, it is very challenging, if not impossible, to efficiently establish random keys between legitimate users which cannot be reused.

Alternatively, a hybrid cryptosystem can be constructed by combining key generation and symmetric encryption, as illustrated in ~~Fig. 2b~~. The security level of the system is enhanced by replacing public key cryptography with key generation.

**1.7 KEY GENERATION**

Key generation exploiting unpredictable characteristics ofwireless channels is information-theoretically secure and has been an active research direction in physical layersecurity (PLS) **.**In this technique, two legitimate users,Alice and Bob, measure their common but noisy channel in analternate manner, through which they can get correlated butnot identical observations. Then they will quantize their correlatedanalog measurements into binary values separately, and their keys are usually not the same. Alice and Bob laterreach an agreement on the same key through informationreconciliation. Finally, they employ privacy amplifi**c**ationto remove the information revealed during the informationreconciliation **.**Therefore, key generation is able to establisha cryptographic key securely from the noisy observations.As one of the few implementable PLS techniques, key generationcan be constructed in current wireless devices. Many prototypes have been reported involving key extraction fromchannel state information (CSI) in IEEE 802.11n systems, ultra wideband (UWB) systems , andFM/TV systems , or from received signal strength (RSS)in IEEE 802.11 systems , IEEE 802.15.4 systems, and Bluetooth systems . The testbedsconsist of laptops, smartphones, customized platforms suchas universal software radio peripheral (USRP) , or anyother wireles**s** platform that can provide sufficient channelinformation.Key generation requires the channel to satisfy certainconditions with respect to temporal variation, channel reciprocity,and spatial decorrelation. Temporal variation is the main random source for key generation, which can be introduced by the movement of any users and/or objects in the wireless environment. It is feasible to exploit channel randomness in the frequency domain and spatial domain , but the randomness is limited and cannot be updated in a static environment. Experiments have been carried out in the indoor and outdoor environments and have shown that the mobility of users and/or objects is sufficient to introduce randomness .Channel reciprocity indicates that the signals at each end of the same link have identical statistical features, such as channel gains, phase shift, time delay, etc, which is the basis of key generation systems. Although there is ongoing research effort adopting full-duplex hardware most of the current commercial wireless devices work in half-duplex mode. Key generation usually works in time-division duplexing (TDD)

systems and slow fading channels. The conclusion from applying spatial decorrelation means that any eavesdropper located more than half-wavelength

away from legitimate users experiences uncorrelated fading. This property is highly influenced by the channel condition . In a rich multipath environment

the signal decorrelates when **d=0.4\*wavelength** of signal (approximately half-wavelength) , which is the theoretic basis of spatial decorrelation. Some experiments have been carried out to verify this property in UWB systems and IEEE 802.11g systems . In contrast, spatial decorrelation has also been found to not hold in some channel conditions by simulation and experiments . In this case, key generation cannot be deemed secure and requires special design consideration to combat eavesdropping when eavesdroppers are close to the legitimate users. In order to design an effective, workable, and secure key generation system, the above three principles, i.e., temporal variation, channel reciprocity, and spatial decorrelation, should be always satisfied. Although there have been a number of theoretical and experimental studies on these principles, to the best of the authors' knowledge, there is no thorough study examining the effects of environment conditions and channel parameters on the key generation. For example, channel reciprocity and spatial decorrelation in indoor environment by keys generated from channel impulse response (CIR) in a UWB system and from RSS in an IEEE 802.11g system, respectively. However, key generation performance greatly depends on the channel conditions, such as the multipath level and dynamicity,

which has not been studied comprehensively yet. In addition, the channel parameter used for key generation also has an impact. For example, it has been reported that RSS-based key generation systems are subject to predictable channel

attacks while CSI-based systems are robust to such attacks.

## 1.8 ENCRYPTION USING CONSTELLATION ROTATION

### 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, its advantages and security needs & security goals – confidentiality and authentication, Physical layer signatures, key exchange challenge, key generation,
2. The second chapter of this report presents a Literature Survey on !!!!!!!!!!!!
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 works.

**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 ecommerce. 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 CSIeff and develop a refined indoor radio propagation model to represent the relationship between CSIeff and distance. Based on the CSIeff, 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 privacypreserving 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 infrastructurebased 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 lossyquantizer 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

**METHODOLOGY**

**KEY EXTRACTION:**

**CSI EXTRACTION:**

CSI values are discarded by the NIC by default which makes it difficult to be used for security purpose in normal devices. However, the Atheros NICs provides a feature by which the CSI values can be read if the kernel of the Linux OS is changed to the supported version. CSI dataset resources are available which can be used for time being. This gives us a set of values describing the channel such as the RSS, Bandwidth, No. of Antennae, CSI in binary format. This binary data must be converted to a suitable readable format and the desired CSI data can be extracted in the form of complex values. The magnitude of the CSI data in different packets are taken and used for quantization.

**QUANTIZATION**

Cryptographic applications require a binary sequence as the key, but the channel measurements are analog in nature. Quantization can be adopted to convert these analog measurements to digital ones, Ku. The bit-string should be

• Sufficient long, ranging from 128 bits to 512 bits being the length of keys commonly used in symmetric cipher

• Statistically random, resilient to statistical defeats that could be exploited by attackers.

Due to the random nature of CSI, the thresholds needed to quantize the data cannot be fixed in nature. An adaptive-thresholding technique is thus employed to calculate the thresholds keeping in mind that the quantisation thresholds must be tuned to guarantee the same proportion of ‘0’s and ‘1’s, which is an important feature for randomness.

**QUANTIZATION ALGORITHM**

**INPUT**: Absolute value of CSI, 𝑆 of length 𝑁, 𝐾𝑑,𝑖=1→𝑁

**OUTPUT**: 𝐾𝑢

**Step 1**: To find 𝑚𝑎𝑥 and 𝑚𝑖𝑛 of 𝑆

**Step 2**: To find quantization threshold by using 𝑞𝑡= 𝑚𝑎𝑥+ 𝑚𝑖𝑛2

**Step 3**: Compare 𝑆𝑖 with 𝑞𝑡

if 𝑆𝑖 > 𝑞𝑡 then 𝐾𝑑𝑖=1

else if 𝑆𝑖< 𝑞𝑡 then 𝐾𝑑𝑖=0

**Step 4**: Δ= 𝑞𝑡

**Step 5**: while(𝑛𝑜.𝑜𝑓 𝑧𝑒𝑟𝑜𝑠 𝑖𝑛 𝐾𝑑 ==𝑛𝑜. 𝑜𝑓 𝑜𝑛𝑒𝑠 𝑖𝑛 𝐾𝑑)

Δ= Δ2

if 𝑛𝑜.𝑜𝑓 𝑧𝑒𝑟𝑜𝑠 𝑖𝑛 𝐾𝑑 > 𝑁2

𝑞𝑡=𝑞𝑡− Δ

if 𝑛𝑜.𝑜𝑓 𝑜𝑛𝑒𝑠 𝑖𝑛 𝐾𝑑 > 𝑁2

𝑞𝑡=𝑞𝑡+ Δ

Compare 𝑆𝑖 with 𝑞𝑡

if 𝑆𝑖 > 𝑞𝑡 then 𝐾𝑑𝑖=1

else if 𝑆𝑖< 𝑞𝑡 then 𝐾𝑑𝑖=0

**Step 6**: 𝐾𝑢= 𝐾𝑑

**PRIVACY AMPLIFICATION**

We use SHA-256 to hash the bit streams, which is highly secure and most widely used of one-way functions. SHA-256 has the following feature: even a small change in the message will, with the overwhelming probability, result in a completely different hash. The CSI input samples are not always of the same length. An added advantage of using SHA-256 is that it always results in a 256-bit message digest which can be used for symmetric encryption

**AUTENDICATION:**

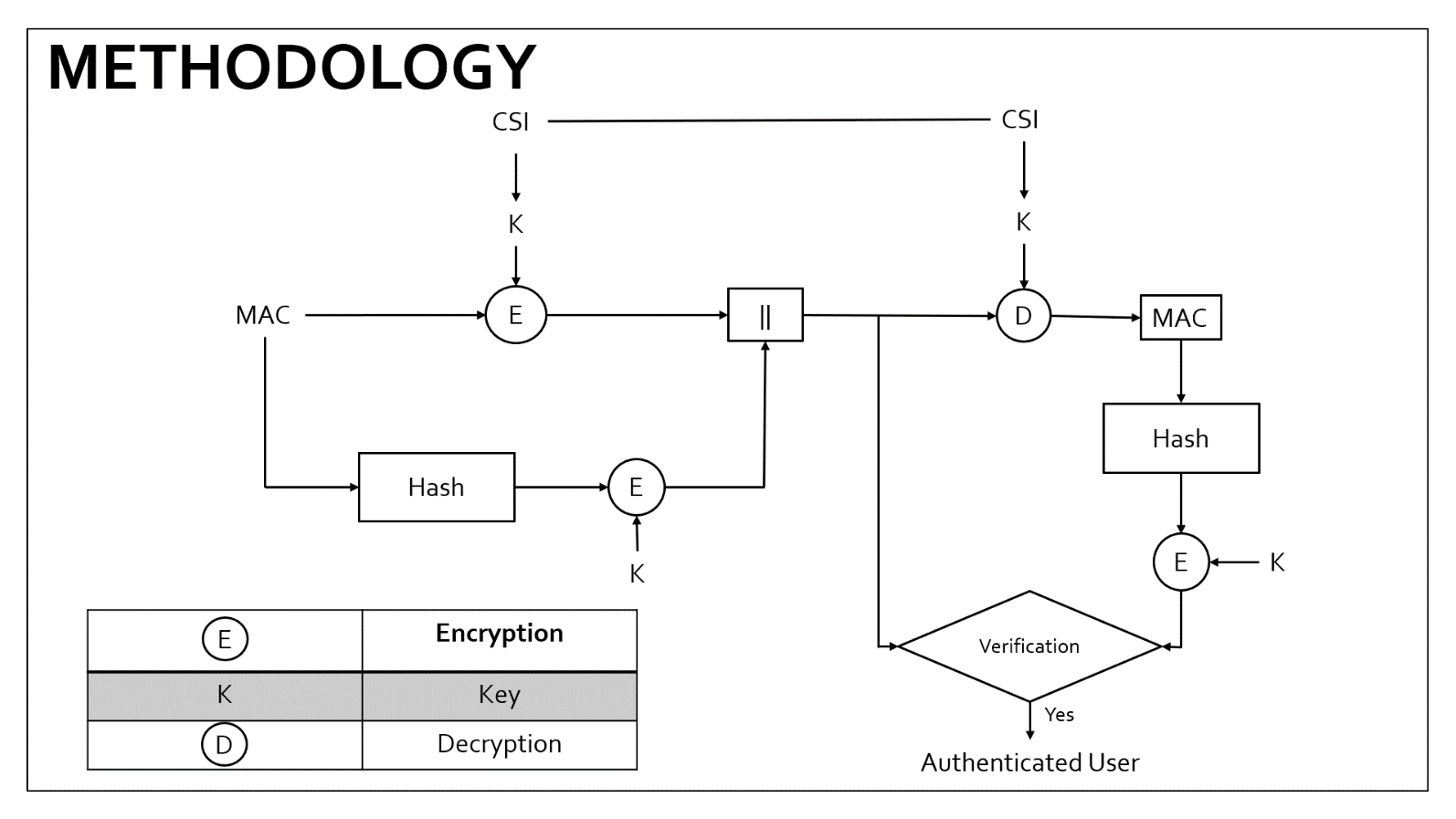


Figure 1 : Proposed methodology of authentication protocol

**ENCRYPTION**

This encryption technique is based on the constellation rotation in modulation techniques which enhances the security provided in the above layers. The constellation rotation requires a phase value to be calculated from the generated key. Every constellation symbol Sk is rotated by a unique angle α as

where,- Original constellation symbol

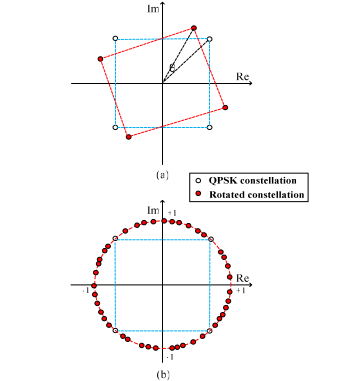
-Rotated constellation of 

Figure 2 : QPSK Constellation and possible rotation

**PHASE CALCULATION**

The phase calculation is used to generate an unique angle α with respect to the generated key.The 256 bit key is split into 8 bit words to find 32 phases α.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |

Figure 3: Representation of the 8-bit word from the 256-bit key

|  |  |
| --- | --- |
|  | Bits used to determine the quadrant of the phase |
|  | Sign Bits |
|  | Magnitude Bits |

**QUADRANT BITS**

|  |  |
| --- | --- |
| **a1** | **a2** |

The first two bits in the 8 bit word, called the **quadrant bits**are used to determine the quadrant of the required phase. The bits are converted to it’s decimal equivalent *i.* The base angle is then determined by

**SIGN BIT**

|  |
| --- |
| b |

 If **b is 0**, the constellation is rotated in the **anticlockwise** direction.If **b is 1**, the constellation is rotated in the **clockwise** direction.

**MAGNITUDE BITS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **C1** | **C2** | **C3** | **C4** | **C5** |

These 5 bits, called the **magnitude bits** are used to determine the position in the respective quadrant.The decimal equivalent is determined as *n* and the required magnitude can be equated as

Now, the unique angle is determined from the 8-bit word as

**DECRYPTION**

The original constellation symbol can be recovered as

where,- Original constellation symbol

- Rotated constellation of

The angle **α**is unique for every user as the CSI is unique. The resulting **α**varies even between the 32 words that makes the constellation rotation more random and more secure.

**CHAPTER IV**

### RESULTS & DISCUSSIONS

**CHAPTER V**

### CONCLUSION & FUTURE WORK

#### 5.1 CONCLUSION

#### 5.2 FUTURE WORK

.

### REFERENCES

**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.

.

* 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.
* 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

