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

PHASE I REPORT

Submitted by

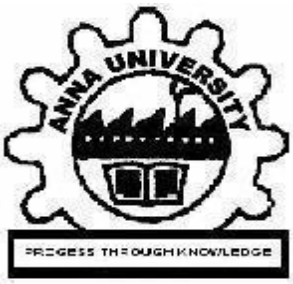
THANGAPANDIAN B
2018252004

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

CHAPTER NO	TITLE	PAGE 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 Mobile Payments	10

	2.2	Privacy-Preserving Location Authentication in Wi-Fi Networks Using Fine-Grained Physical Layer Signatures	11
	2.3	Light Weight and Privacy-Preserving Authentication Protocol for Mobile Payments in the Context of IoT	12
	2.4	CSI-based indoor localization	13
	2.5	Toward privacy preserving and collusion resistance in a location proof updating system	14
	2.6	Traffic signature-based mobile device location authentication	15
	2.7	Puzzle: A Shape Based Secret Sharing Approach by Exploiting Channel Reciprocity in Frequency Domain	16
	2.8	Secret Key Extraction from Wireless Signal Strength in Real Environments	17
	2.9	Group Secret Key Generation via Received Signal Strength: Protocol, Achievable Rates & Implementation	18
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 NO	DESCRIPTION	PAGE NO
1	High Level Protocol Flow	20
2	Overview of Generalized LBS	20
3	High Level SMAP Protocol Flow	21
4	High Level PriLA Protocol Flow	23
5	User Verification Phase	25
6	Secure Handshake Protocol of PriLA	27
7	Payment Authentication Phase	31
8	User Verification Time per Transaction	34
9	Location Authentication Time per Transaction	34
10	Payment Authentication Time per Transaction	35
11	SMAP Vs SMAP+PriLA	36
12	Security Analysis - Leakage	36
13	Security Analysis - Mismatch Rate	37
14	Adversary Rx BER Performance	38

LIST OF TABLES

TABLE NO	DESCRIPTION	PAGE NO
1	Summary of Notations Used in User Verification	24
2	Summary of Notations Used in Payment Authentication	30

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