SECURE AUTHENTICATION SCHEMES FOR ROAMING SERVICE IN GLOBAL MOBILITY NETWORKS

Thesis

Submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

by

K S SUVIDHA

DEPARTMENT OF MATHEMATICAL & COMPUTATIONAL SCIENCES

NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA

SURATHKAL, MANGALORE - 575025

February, 2021

Dedicated to
My Family

DECLARATION

By the Ph.D. Research Scholar

I hereby declare that the Research Thesis entitled **SECURE AUTHENTICATION SCHEMES FOR ROAMING SERVICE IN GLOBAL MOBILITY NETWORKS** which is being submitted to the **National Institute of Technology Karnataka, Surathkal** in partial fulfillment of the requirements for the award of the Degree of **Doctor of Philosophy** in **Mathematical and Computational Sciences** is a bonafide report of the research work carried out by me. The material contained in this Research Thesis has not been submitted to any University or Institution for the award of any degree.

K S Suvidha

Reg. No.: 155035 MA15F03

Department of Mathematical and Computational Sciences

Place: NITK, Surathkal.

Date: 17 February 2021

CERTIFICATE

This is to certify that the Research Thesis entitled **SECURE AUTHENTICATION SCHEMES FOR ROAMING SERVICE IN GLOBAL MOBILITY NETWORKS** submitted by **K S Suvidha**, (Reg. No.: 155035 MA15F03) as the record of the research work carried out by her, is accepted as the Research Thesis submission in partial fulfilment of the requirements for the award of degree of **Doctor of Philosophy**.

(Dr. R Madhusudhan)
Research Supervisor

Chairman - DRPC

ACKNOWLEDGMENT

First and foremost, I would like to express my sincere gratitude to my thesis advisor, Dr. R. Madhusudhan for his support. His encouragement and guidance have helped me to pursue my research work.

I also thank my RPAC members Dr. Srinivasa Rao Kola., Department of MACS, Dr. Suprabha K. R., School of Management, National Institute of Technology Karnataka, Surathkal. I would like to take this opportunity to express my heart filled thanks to Prof. Shyam. S. Kamath, Head of the department, Mathematical and Computational Sciences, for his valuable technical inputs given to pursue my research work. His encouragement and guidance have helped me immensely all the time. I also extend my sincere thanks to Prof. B. R. Shankar for his guidance and advice during my Ph.D program. I would like to express my heart filled thanks to all the professors of MACS department for helping me at various stages of my Ph.D. It is my pleasure to thank all my friends and co-scholars who shared their valuable time with me. I would like to record special thanks to Dr. Shridhar. G. Domanal, Full Stack Developer IBM, Bangalore-India, for all the valuable inputs. Without his guidance none of this would have been possible.

Finally, I would like to express my deep gratitude to my father Shashikant. Y. Korwar, mother Indira. Korwar and my brothers K. S. ShreeHarsha and K. S. Shubham and acknowledge with pleasure that without their love, affection, moral support and care, it would never have been possible for me to pursue my research.

Place: NITK, Surathkal K S Suvidha

Date: 17 February 2021

ABSTRACT

Distribution of resources and services via open network has become the latest trend in information technology. In the open network, hackers can easily obtain the communication data. Therefore, open network demands the security to protect data and information. Hence, network security is the most important requirement in an open network. In the security system, authentication plays a major role. User authentication is a central component of any security infrastructure. Other security measures depend upon verifying the identity of the sender and receiver of information. Authorization grants privileges based upon identity. Audit trails would not provide accountability without authentication. Confidentiality and integrity are broken if we can't reliably differentiate an authorized entity from an unauthorized entity. Remote user authentication is a mechanism to identify the remote users over an insecure communication network. In remote user authentication, password authentication is the simplest method to authenticate the user. But, the limitations in the password authentication approach leads towards the development of two-factor authentication. There are hundreds of remote user authentication schemes have been proposed by many researchers. None of the schemes achieve all the security goals and many schemes fail to provide security against various attacks. Even though some of the schemes provide the security, they are not efficient in terms of computation and communication cost. Hence, it is necessary to design an efficient and secure authentication scheme.

This thesis aims to provide efficient and secure remote user authentication schemes in distributed systems and networks. There are many factors involved in authentication schemes and these factors use the characteristics of the password, smart card and biometric. This research concentrates on cryptanalysis and improvements of the smart card based two-factor remote user authentication schemes. Till date, many smart card based remote user authentication schemes have been proposed. But, every scheme has its security flaws. None of the schemes have succeeded to achieve all the security requirements and goals. Also, many schemes do not provide a strong formal proof to prove the security of the scheme. In this thesis, cryptanalysis of the recently proposed remote user authentication schemes has been done to identify the vulnerabilities. New schemes have been proposed to overcome the identified security flaws. Security of

the proposed schemes has been formally analyzed using BAN logic. Furthermore, the proposed schemes have been simulated using Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. Through this simulation, it has been ensured that the proposed scheme is secure against active and passive attacks. Using NS 2 simulator, the performance metrics such as throughput, end to end delivery and packet delivery ratio are calculated for the proposed scheme.

In the literature study, it is observed that to avoid the replay attack, many remote user authentication schemes depend on clock synchronization. But the clock synchronization has its own disadvantages. Also, the schemes, which are independent of clock synchronization are vulnerable to replay attack. To fix these weaknesses, a novel authentication scheme has been proposed. By employing the Elliptic Curve Diffie-Hellman (ECDH) key exchange algorithm, the proposed scheme resists the replay attack. Through the security analysis, it is proved that the scheme achieves all the security goals and resists well-known attacks like insider attack, offline password guessing attack, etc. The proposed scheme security have been analyzed using BAN logic and simulated in AVISPA tool. Through these results, it is ensured that the proposed scheme resists all security attacks.

The contributions of this thesis is to the improve the security of the existing authentication schemes. In particular, this research analyzes the Gope and Hwang, Fan Wu et al. and Lee et al.'s schemes. However, the analyzed schemes have many security flaws like fail to provide user anonymity and forward secrecy, vulnerable to the stolen smart card attack, insider attack, guessing attack etc. Based on the analysis, this research proposes improved schemes to overcome the identified weaknesses. Furthermore, a novel authentication scheme has been proposed to resist security attacks. Finally, the thesis presents concluding remarks and discusses the future scope.

Keywords: Network Security, Authentication, Smart Card, Two-factor Authentication, Cryptography, Security, GLOMONET, Mobile cloud computing, NS2, BAN logic.

Table of Contents

List of Figures

List of Tables

Acronyms

1. GLOMONET - GLObal MObility NETwork
2. GSM- Global System for Mobile communications.
3. SG - Security Goals
4. SR - Security Requirement
5. ID, U, PW - Identity, User and Password
6. OFMC - On Fly Model Checker
7. CL-Atse - Constraint Logic based Attack Searcher
8. HLPSL - High Level Protocol Specification Language
9. AVISPA - Automated Validation of Internet Security Protocols and Applications
10. AES - Advanced Encryption Standard
11. SHA - Secure Hash Algorithm
12. SHA 1 - Secure Hash Algorithm 1
13. DES - Data Encryption Standard
14. IDEA - International Data Encryption Algorithm
15. SM2 - Public key cryptographic algorithm based on elliptic curves
16. RSA - Rivest Shamir Adleman
17. ECC - Elliptic Curve Cryptography

CHAPTER 1

Introduction

1.1 Overview of Network Security

The Internet has become an integral part of everyday life. With the rapid development of the Internet technology, people can access any service from any place and at any time. Major commercial organizations, educational institutes, governments and individuals depend upon the Internet for providing their services. Most of the information exchange will be done through the Internet. Nowadays the number of threats are rising, hacker tools are becoming more sophisticated and powerful. If the network is not secure then the rate of unauthorized access, use, alteration, theft or physical damage to an object that maintaining high confidential information will increase. Therefore, in the present situation, it is important to provide security against numerous malicious users and attackers. They not only disrupt the services but also can steal the sensitive information. Therefore network security has become more important to every user of the Internet.

According to NIST (National Institute of Standards and Technology) computer security is the protection afforded to the network environment in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources. Network security uses the same basic set of controls as computer security (Guttman and Roback, 1995).

Most definitions of network security have the intent to consider the security of the network as a whole, rather than as an endpoint issue. A comprehensive network security plan must encompass all the elements that make up the network and provide five

important services:

1. *Authentication:* Authentication is a service which provides a system with the capability to verify that a user is the one who claims to be authenticated based on what the user is, knows, and has.

2. *Access Control:* In network security, access control is the ability to limit and control the access to host systems and applications via communication link.

3. *Data Confidentiality:* Data confidentiality ensures that the information transmitted across the network is accessible only by the intended recipients.

4. *Data Integrity:* The integrity service protects data against the active threats such as those that may alter data. It ensures that a message has not been modified in transit. It is an assurance of the exactness of received data from the authorized user.

5. *Non Repudiation:* This is a security service that provides proof of origin and delivery of service and/or information. It ensures that the originator of the message cannot deny that he/she sent the message.

1.2 Overview of Authentication

Authentication is a basic unit of network security. According to Kizza (2009) authentication is a service used to identify a user. User authentication is a central component of any security infrastructure. Other security measures depend upon verifying the identity of the sender and receiver of information. Authorization grants privileges based upon identity.

There are three types of authentication methods. They are single-factor authentication that are based on password, two-factor authentication based on smart card and password, three-factor authentication based on password, smart card and biometrics like the fingerprint, iris scan based authentication (Karuppiah and Saravanan, 2015). Out of these methods, password authentication is the simplest and widely used authentication method in current technology. But some vulnerabilities affect the security of the

password authentication system. Weak password entropy which makes the password vulnerable for guessing attack. Periodic change of password is necessary to protect passwords from guessimg attack.

The problems idintified in the password authentication made an approach to introduce the smart cards authentication. There are many reasons to use the smart card, but the main reasons are the built-in security features and cost. Due to low cost, the portability, efficiency, and the cryptographic capacity, smart cards have been widely adopted in many E-Commerce applications and network security protocols. In this thesis, we have designed authentication protocols and given the cryptographic methods to protect the smart card paramaters. Our work mainly focuses on two factor authentication schemes. More information about two factor authentication schemes is given in further sections and chapters.

1.3 Smart card authentication

The smart card is a type of chip-based identification card. Its characteristic feature is, an integrated circuit embedded in the card, which has a component for transmitting, storing and processing the data. Data can be transmitted using either contact on the surface of the card or electromagnetic fields without any contact.

1.3.1 Smart card authentication system model

The traditional model of smart card based remote user authentication system is consists of three phases, (1) registration phase, (2) login and authentication phase and (3) password change phase. In the registration phase, the user selects the identity (ID), password (PW) and submit it to the server. After submission of user credentials, server issues the smart card to the user. Registration phase of smart card authentication system is shown in Figure 1.1.

In login and authentication phase, a user inserts the smart card into the card reader and enters ID and PW. The smart card computes login message and sends it to the server S. On the server side, S receives login message and verifies it. Server rejects the login message if the ID and PW are wrong. Otherwise it provides the service to the user.

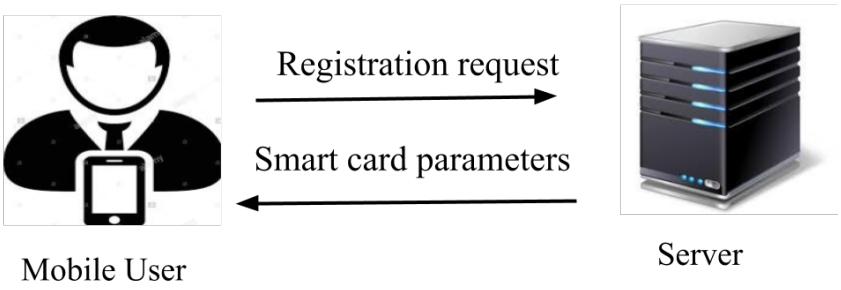

Figure 1.1 Registration phase of smart card authentication system

During the password change phase, the user can change his/her password. This can be done locally or interaction with the server. The login and authentication phase of smart card authentication system is shown in Figure 1.2.

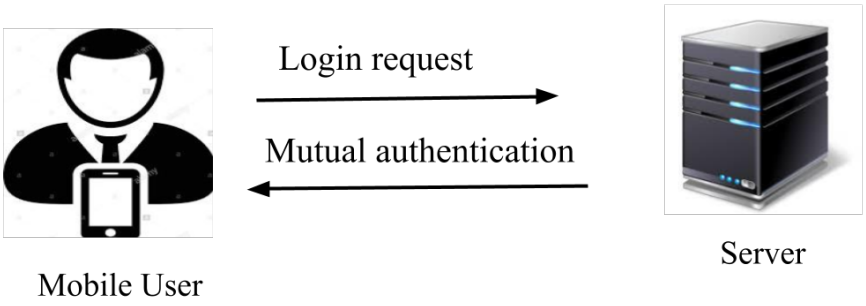

Figure 1.2 login and authentication phase of smart card authentication system

1.3.2 Global Mobility Network

A mobility network provides roaming service that permits mobile subscriber to access the services provided by the home agent in a foreign network (Suzuki and Nakada, 1997; Karuppiah and Saravanan, 2015). To provide global roaming service for a mobile user, authentication is an essential requirement and challenging task. User authentication scheme involves three entities: Mobile User (MU), a Foreign Agent (FA) and a Home Agent (HA). A user of a specific network can roam anywhere in the world and he/she can access the desired services through foreign agents in the foreign networks (Jiang et al., 2013). The scenario of privacy preserving scheme for roaming service in global mobility networks is shown in Figure 1.3.

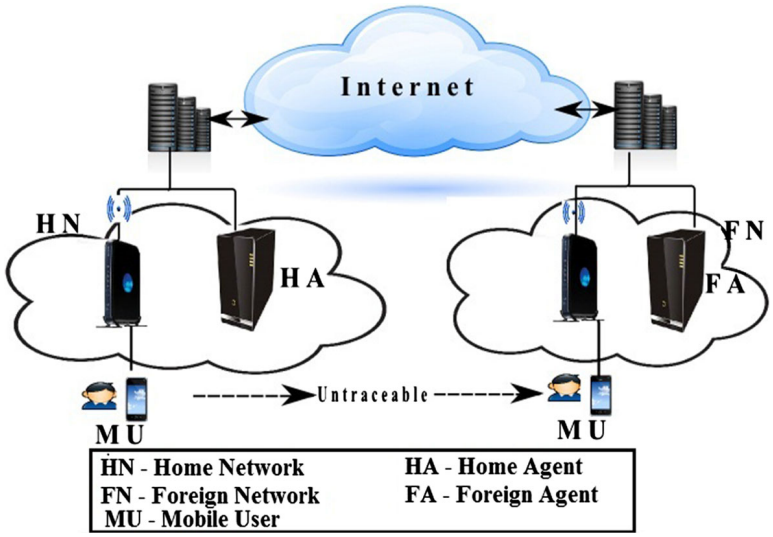

Figure 1.3 Scenario of user authentication for roaming service

When a mobile user roams into a foreign network, the foreign agent authenticates roaming user with the assistance of home agent (Jiang et al., 2013). During roaming process in global mobile networks, privacy protection is challenging and essential requirement. The identity of mobile users should be protected, which is known as user anonymity and his/her location activities should be kept secret, which is known as user untraceability.

The main security concerns in mobile networks are user anonymity, integrity, availability, confidentiality and mutual authentication of entities involved in communication. Only authorised mobile users have to access the desired services from service provider of mobile network. As the concern for privacy increases in our lives, user anonymity has become a vital security property in various WSN (Wireless Sensor Network) applications as well as in many other applications like location based services, e-voting, mobile roaming services etc. In the absence of user anonymity, users may have experienced problems like lost their personal information, took advantage of their visibility online including hijacked email and social media accounts. However, an attacker may steal information such as credit card information. Therefore, the user authentication protocol should have the ability to protect against various attacks in wireless and mobile networks.

The security breaches in this environment occurs as follows: A passive attacker can

eavesdrop the messages transmitted between MU and FA by intercepting the communication channel. This violates the message confidentiality. An active attacker may impersonate MU and FA to get services from HA. The secure data transmission is required between MU, FA and HA. Therefore, encryption mechanisms are necessary to encrypt the messages. In this regard, a symmetric/single key cryptography is more efficient than public key algorithms due to the power constraints of mobile devices.

1.4 Two factor authentication schemes

Authentication is proving the identity of oneself. Providing security to user authentication is the key issue that has to be addressed in GLOMONET. During communication, each entity has to mutually authenticate each other to establish a secure communication, hence mutual authentication plays a crucial role while designing an authentication scheme.

Many two-factor secure authentication schemes are proposed in GLOMONET to address the security issues but none of the schemes so far proposed could resist all the security issues and achieve security goals. Hence, the aim of this research is to propose a secure authentication scheme, which addresses all the security challenges and achieves all the security goals.

With the increased use of smartphones, mobile networks are increasingly pervasive. Mobile networks use electromagnetic waves i.e radio waves as transmission media to transmit the data. Since the messages transmitted through radio waves are vulnerable to interception, providing security to the data in mobile networks and achieving network security goals such as confidentiality, integrity and availability becomes vital (Kuo et al., 2014). Literature survey (Bellare et al., 2000; Wang et al., 2012) presents the seminal work on how an adversary is modelled to have full access on the communication channel, i.e he/she can intercept the login messages exchanged between the three communicating entities MU, FA and HA, by intercepting the messages, adversary can perform operations like insertion, deletion and modification of the messages, then he/she can retransmit the modified messages to one of the entities. Hence, while designing the two factor authentication schemes, one of the crucial goals is to achieve mutual

authentication. Each entity involved in the communication must prove its authenticity before providing the services.

However, the literature survey (Kim et al., 2012; Kocher et al., 1998; Messerges et al., 2002; Nohl et al., 2008) presents the seminal work on how the parameters stored in the smart card can be extracted by the methods like power analysis, reverse engineering etc.,. In case, the mobile user's smart card is lost or stolen, attacker can breach the security of the smart card and extract the parameters. Hence, the main goal is to protect the offline password guessing attack. Even with the smart card breach, attacker must not be successful in launching the password guessing attacks. It is also essential for any two factor authentication scheme not to maintain a verifier table in the server side containing user related critical information like user identity and password. In case any scheme does, such schemes do not preserve user anonymity (Wang et al., 2015). The verifier table must contain only the secret keys of the MU, HA and FA. If the server is compromised and the secret keys are revealed by an adversary, the revealed secret keys should not contribute in predetermining the session keys of the proposed scheme. This is one of the security requirements that has to be achieved by any scheme. This property is termed as perfect forward secrecy.

1.4.1 Security requirements and goals

Liao et al. (2006) proposed a set of ten requirement for evaluation of smart card security. They assumed that these requirements provides proper security to the smart card based authentication schemes. Yang et al. (2006) made an argument over Liao et al.'s criteria. and proposed a new set of five criteria as a solution. But, Yang et al.'s criteria set was bit more theoretical and difficult to adopt in real applications. Later, Tsai et al. (2006) presented another group of security property. This has nine security requirement and ten desirable features, which are based on the tamper resistant assumptions. Ambiguities and redundancies are identified in previous criteria by Madhusudhan and Mittal (2012). They also proposed new set of nine security requirements and ten security goals. In Table 1.1 illustrates the security attacks and goals that an ideal authentication scheme should withstand and achieves respectively.

Table 1.1 Evaluation criteria set

Security Requirements		Security Goals	
SR1	Robust against Denial of Service (DoS) attack	SG1	No password verification table
SR2	Robust against Impersonation attack	SG2	Freely password selection
SR3	Robust against Parallel session attack	SG3	No Password reveal
SR4	Robust against Password guessing attack	SG4	Password dependent
SR5	Robust against Replay attack	SG5	Mutual authentication
SR6	Robust against Smart card loss attack	SG6	Session key agreement
SR7	Robust against Stolen verifier attack	SG7	Perfect forward secrecy
SR8	Robust against Reflection attack	SG8	User anonymity
SR9	Robust against Insider attack	SG9	Smart card revocation
		SG10	Quick wrong password detection

1.5 Research objectives

Our research fulfills the following objectives:

1. Researchers have developed many two factor authentication schemes for GLOMONET. However, with the thorough literature survey, it is observed that the authentication schemes developed are susceptible to several security attacks and also the schemes could not achieve few security goals. The aim of this research is to overcome the security weaknesses of current authentication schemes in global mobility networks and achieve the security goals, so that the scheme will be more secure over insecure communication channel.

2. The second objective of this research is to propose a novel scheme, which is simple, secure, lightweight and more suitable for low-power and resource limited mobile environments.

3. The third objective is to simulate the proposed protocol to formally verify whether the proposed protocol is secure against security attacks using widely accepted tool AVISPA.

1.6 Organization of the thesis

The organization of the thesis is as follows.

Chapter 1, provides an overview of authentication in global mobility networks. The prominent applications of authentication, security attacks and requirements for roaming service in mobile networks has been discussed. Further, the motivation and objectives of this research have been addressed.

Chapter 2, explains the literature survey done on various two factor authentication schemes developed for roaming services in global mobility networks, which are useful for performance comparison with our proposed schemes in these areas.

In **Chapter 3**, the basic concepts of cryptography and its primitives such as Exclusive-OR operation, one-way hash function, and private and public key algorithms are presented. Further, this chapter comprise the mathematical preliminaries required to develop and analyse the authentication protocols for roaming service in global mobility networks such as Diffie-Hellman key exchange, Discrete Logarithmic Problem (DLP) and Elliptic Curve Cryptosystem (ECC).

In **Chapter 4**, the cryptanalysis of Gope and Hwang (2016a) scheme has been done. With the thorough cryptanalysis of their scheme, we have proved that their scheme is vulnerable to various security attacks like stolen smart card, offline password guessing, MU impersonation and replay attack. Further, their scheme fails to achieve security goals like user anonymity and perfect forward secrecy. To overcome the security attacks of their scheme and to achieve the security goals, a new scheme has been proposed. Through the rigorous informal and formal security analysis, we have demonstrated that the proposed scheme is secure against the security attacks. Furthermore, we have simulated the proposed scheme using widely accepted AVISPA (Automated Validation of Internet Security Protocols and Applications) tool. With the simulated result of the proposed scheme, we show that the proposed scheme is secure against active

and passive security attacks. Additionally, the proposed scheme is compared with Gope and Hwang scheme and other related schemes in terms of performance, computational cost and communication overhead. In comparison with other schemes, the proposed scheme is efficient and robust. This makes the proposed scheme suitable for practical implementation.

In **Chapter 5**, Wu et al. (2016) scheme has been reviewed. They claimed that their scheme is resilient to several attacks. However, with thorough cryptanalysis of their scheme, we have proved that their scheme is vulnerable to several attacks. To overcome these security issues, a new scheme is proposed. The proposed scheme resists security attacks like impersonation, replay, stolen smart card, offline password guessing, stolen verifier and insider attack. The proposed scheme also achieves security goals like perfect forward secrecy, mutual authentication, local password verification, no time synchronization, user anonymity and user friendliness. Furthermore, we have simulated the proposed scheme using widely accepted AVISPA (Automated Validation of Internet Security Protocols and Applications) tool. With the simulated results of the proposed scheme, we show that the proposed scheme is secure against active and passive security attacks. Additionally, the proposed scheme is compared with Fan Wu et al.'s scheme and other existing schemes in terms of performance, computational cost and communication overhead. In comparison with the other schemes, the proposed scheme is light-weight and robust. This makes the proposed scheme suitable for practical implementation.

Chapter 6, attempts to develop security architecture for GSM networks. Two factor authentication scheme is developed to address the security features such as user anonymity and privacy preservation during roaming scenario in GLObal MObility NETwork. While roaming MU needs to access the services of the FA, FA grants the service request only to the authenticated MU. To verify the authenticity of the MU, FA sends the service request of MU to HA. HA verifies the authenticity of the MU after which FA allows the MU to access the services. The entire communication during roaming is carried over insecure channel due to this, security concern is raised. The main objective of the proposed protocol is to secure the channel and to over come all active and

passive security attacks. Since, the protocol is designed for mobile networks, it should be light weight with less communication cost, one such protocol has been proposed in this chapter. The proposed protocol is light weight with less communication cost. The proposed protocol is simulated using NS2.35 simulator and the performance metrics such as throughput, end to end delivery and packet delivery ratio are computed. Additionally the proposed protocol addresses the active and passive security attacks that exists in cellular networks which is formally verified using AVISPA tool. The protocol is efficient in terms of computational and communication cost. The proposed scheme is robust and practically implementable.

In **Chapter 7**, we have developed the security framework for mobile cloud computing environment. Integration of mobile networks with cloud computing platform led to development of mobile cloud computing. Since the communication between mobile devices and the cloud computing occur over wireless medium, securing the network becomes paramount. With the thorough literature survey, we found that many two factor authentication schemes proposed so far to preserve user anonymity are vulnerable to various security attacks, they also had shortcomes to achieve security goals. To overcome the issues related to the two factor authentication schemes in mobile cloud computing, a new scheme is proposed. Furthermore, we have simulated the proposed scheme using widely accepted AVISPA (Automated Validation of Internet Security Protocols and Applications) tool. With the simulated result of the proposed scheme, we show that the proposed scheme is secure against active and passive security attacks. Additionally, the proposed scheme is compared with Gope and Hwang's scheme and other related schemes in terms of computational cost and communication overhead. The proposed scheme is efficient, robust and suitable for practical implementation.

Chapter 8, concludes the thesis with the summary of contributions of research and future work.

CHAPTER 2

Literature Survey

2.1 Related work

Hwang and Yang (1995) proposed a scheme to secure communication in mobile networks, their proposed scheme claims that the secure communication is provided over teleconference by sharing a common secret key. Hwang (1999) further worked on the same topic, securing teleconference and proposed a new scheme. Buttyan et al. (2000) proposed a new scheme on authentication protocols. The proposed scheme explained about the various security attacks that the authentication schemes designed for GLOMONETs are vulnerable. Hwang and Chang (2003) reviewed Hwang and Yang (1995) and Buttyan et al. (2000) authentication schemes and proposed a new scheme to provide secure and efficient authentication scheme.

Zhu and Ma (2004) also reviewed authentication schemes designed for GLOMONET, with the thorough understanding of the authentication schemes designed so far, they pointed out that the authentication schemes are failing to preserve user anonymity.

Later Lee et al. (2006) reviewed Zhu and Ma (2004) authentication scheme. The study revealed that their scheme is susceptible to forgery attack and mutual authentication. To improvise their scheme Lee et al. (2006) came up with a new scheme. Later, Wei et al. (2006) reviewed Lee et al. (2006) scheme. With the thorough understanding of their scheme, Wei et al. found that their scheme failed to preserve user anonymity and untraceability. Further, they stated that their scheme also suffered from password guessing attack. To improvise the scheme and to enhance the performance, Wei et al. (2006) came up with a new scheme. Wu et al. (2008) reviewed Lee et al. (2006). The

study revealed that their scheme failed to preserve user anonymity. To preserve user anonymity and other security requirements, Wu et al. came up with a new scheme. Chang et al. (2009) reviewed Lee et al. (2006). To achieve better performance, Chang et al. came up with a new scheme. Later, Youn et al. (2009) reviewed Chang et al. (2009). With the thorough cryptanalysis, Youn et al. proved that their scheme failed to achieve security goals like user anonymity and perfect forward secrecy. Further the scheme is also vulnerable to replay attack. To achieve the security goals and requirements, Youn et al. proposed a new scheme. Xu and Feng (2009) reviewed Wu et al. (2008). With the careful analysis, they found that the scheme is not resilient to preserve user anonymity and replay attack. To achieve better performance Xu and Feng (2009) came up with new scheme. He et al. (2011) reviewed Wu et al. (2008). However with the rigorous cryptanalysis, they found that the scheme failed to withstand security attacks like replay and impersonation attack. They further added that the scheme is not resilient to preserve user anonymity. He et al. (2011) came up with a new authentication scheme to eliminate these security issues. Later, Xu et al. (2011) reviewed Lee et al. (2006).

Li and Lee (2012) reviewed He et al. (2011) scheme. The study revealed that their scheme is non resilient to preserve user anonymity, they also stated their scheme failed to achieve perfect forward secrecy and the designed scheme was not user friendliness. Li and Lee (2012) came up with a new scheme to resolve these security issues. Mun et al. (2012) reviewed Wu et al. (2008) scheme. With the thorough cryptanalysis, they found that their scheme is irresistible to achieve perfect forward secrecy, further they also stated that the scheme suffered from password guessing attack. To enhance the security of their scheme and to provide better performance, Mun et al. (2012) came up with a new scheme. Kim and Kwak (2013) reviewed Mun et al. (2012), Wu et al. (2008) and Lee et al. (2006) schemes. With the thorough understanding of these schemes, Kim et al. found that these schemes are non resilient to preserve user anonymity. They further stated that these schemes suffered from the security attacks like replay, man in the middle and password guessing attack, these schemes also failed to achieve perfect forward secrecy. Kim and Kwak (2013) came up with a new scheme to eliminate these

security weaknesses. Xie et al. (2013) reviewed Chen et al.'s Chen et al. (2011) scheme and stated that their scheme lacks in privacy protection, user-friendliness, no perfect forward secrecy and unfair session key generation. To eliminate these security weaknesses Chen et al. (2011) and Xie et al. (2013) proposed a new scheme. Zhou and Xu (2011) reviewed Chang et al. (2009). They stated that the scheme could not preserve user anonymity and could not resist attack against confidentiality. To remedy these security attacks Zhou and Xu (2011) proposed a scheme.

Jiang et al. (2013) reviewed He et al. (2011). The study revealed that their scheme suffered from the security attacks and goals like replay, insider, offline password guessing attack and perfect forward secrecy. To eliminate all these security weaknesses Jiang et al. have proposed a new scheme. Further, Wen et al. (2013) reviewed Jiang et al. (2013). They stated that the Jiang et al.'s scheme is susceptible to security attacks like stolen-verifier attack, spoofing attack, replay attack and denial of service attack. To eliminate all these security attacks, Wen et al. (2013) proposed a new scheme. Li et al. (2013) worked on chaotic maps based user authentication and privacy preserving scheme against DoS attacks in pervasive and ubiquitous computing environments.

He et al. (2015) reviewed Kumar et al. (2012) and proved that their scheme is susceptible to the security attacks like offline password guessing attack, insider attack and user anonymity. To overcome these security limitations, they have proposed a new scheme.

Karuppiah et al. (2017) reviewed Kang et al. (2011) and proved that their scheme could not protect user anonymity. They further stated that their scheme is susceptible to the security attacks like offline password guessing and impersonation attack. They also proved that their scheme does not provide password change option and there is no local password verification. To overcome all these security flaws Karuppiah et al. proposed a new scheme Karuppiah et al. (2017). Li et al. (2017) reviewed Liu and Chung (2017) and proved that the scheme is vulnerable to security attacks like password disclosure attacks, replay attacks, sense data disclosure attacks, sense data forgery attacks, stolen smart attacks and offline password guessing attacks. To overcome these attacks, they have proposed a new scheme.

Further, Li et al. (2017) reviewed Karuppiah and Saravanan (2015) scheme and stated that their scheme could not achieve perfect forward secrecy and the session key is known by HA. Their scheme does not provide session key update phase. Their scheme uses timestamp mechanism. However in a large scale network clock synchronisation is a thorny problem. To resist all these security flaws Xiong Li et al. proposed a new scheme. Later, Li et al. (2018c) reviewed Gope and Hwang (2016a) and proved that their scheme does not provide local password verification, their scheme is also susceptible to denial of service attack. They further stated that their scheme achieves no perfect forward secrecy, their is also no option to update the session key. Further, they also stated that their session key is known to HA. They further added that in their scheme HA is loaded with heavy key management. To overcome all these security flaws Li et al. (2018c) proposed a new scheme. Later, Gope et al. (2018) proposed an anonymous and expeditious mobile user authentication scheme for GLOMONET environments.

Madhusudhan and Suvidha (2017a) have reviewed Gope and Hwang (2016a) thoroughly and pointed out that their scheme is vulnerable to several security attacks like stolen smart card attack, offline password guessing attack, replay attack and forgery attack. They further proved that their scheme failed to preserve confidentiality and also could not protect user anonymity. To eliminate these security flaws they proposed a new scheme.

Later, Madhusudhan and Suvidha (2017b) have reviewed Lee et al. (2017) and proved that their scheme is susceptible to the security attacks like replay, impersonation and man in the middle attack. They further stated that their scheme achieves no perfect forward secrecy and they also stated that their scheme does not provide local password verification to change the password. To overcome all these security flaws, they proposed a new scheme.

Mahmood et al. (2018) reviewed Lu et al. (2016) and proved that in Lu et al.'s proposed scheme a secret key is computed by server which can be revealed by an adversary. They further stated that their scheme could not protect user anonymity and traceability. Their scheme is also susceptible to stolen smart card attack. To overcome all these security issues Mahmood et al. proposed a new scheme. Later, Meshram et al.

(2018) proposed Chebyshev chaotic map-based ID-based cryptographic model using subtree and fuzzy-entity data sharing for public key cryptography in Global Mobility Networks. Li et al. (2018b) proposed design and implementation of SM2-based security authentication scheme with the key agreement for smart grid communications. SM2 is a asymmetric cryptographic algorithm which is based on elliptic curves cryptography (ECC). Later, Xu et al. (2018) reviewed Gope and Hwang (2016b) and proved their scheme is susceptible to replay attack and further stated that their scheme suffers from storage overhead and also computational burden. To overcome these security issues, a new scheme is proposed by Xu et al. (2018). Later, Banerjee et al. (2018) proposed design of an anonymity preserving group formation based authentication protocol.

Li et al. (2018a) reviewed Farash and Attari (2014) and proved that their scheme is vulnerable to password disclosure attacks, user impersonation attacks and offline password guessing attacks. Mir et al. (2015) reviewed Das (2015) and proved that the scheme is vulnerable to security attacks like not providing the protection of user anonymity, stolen smart card attacks, offline password guessing attacks, online password guessing attacks, many logged-in usersâĂŹ attack and known session-specific temporary information attack. Chen and Lee (2015) reviewed Lee et al. (2011) and proved that their scheme is vulnerable to two factor secuirty problem and masquerade attack. To overcome these attacks, they have proposed a new scheme.

CHAPTER 3

Cryptographic Primitives and Mathematical Preliminaries

3.1 Introduction

This chapter presents some cryptographic primitives and mathematical preliminaries required to design and analyse the authentication protocols for roaming service in global mobility networks. Initially, the properties of XOR and one-way hash function are described. Then, the Diffie-Hellman key exchange, Discrete Logarithmic Problem, Computational Diffie-Hellman Problem, Elliptic Curve Cryptosystem (ECC) have been discussed in brief.

3.1.1 Basic concepts

1. Cryptography: The art of encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form.

2. Encryption: The process of converting plaintext to cipher text using a key.

3. Decryption: The process of converting cipher text to plaintext using a key.

4. Cryptanalysis: The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. It is also called codebreaking

3.2 Cryptographic primitives

In order to ensure the secrecy and efficiency of the authentication system, the cryptographers prefer to use lightweight and low-cost cryptographic primitives like XOR, secure hash functions, and symmetric crypto operations.

3.2.1 EXCLUSIVE-OR cipher:

In cryptography, the simple EXCLUSIVE-OR algorithm has the successive additive principles:

$A \oplus A = 0$

$A \oplus 0 = A$

$A \oplus (B \oplus C) = (A \oplus B) \oplus C$

$(B \oplus A) \oplus A = B \oplus 0 = B$

3.2.2 Hash function:

A secure hash function accepts the string of variable length as an input and produces the fixed length output known as hash value (Ha, 2015). In cryptography, the secure one-way hash function has the following properties:

1. The output is deterministic, that is, the same hash value is produced for the same message.

2. For given input message M its very easy to compute H(M), but its computationally infeasible to obtain M from given H(M). This property is known as one-way property.

3. Its very difficult to find the pair of input A and B such that $H(A) = H(B)$ such a pair is known as a hash collision.

4. If the input message is altered even slightly, the hash digest should change significantly.

Hash functions are used to generate Message Authentication Code (MAC), in order to verify the integrity of a message. The Secure Hash Algorithm (SHA) the standard

has algorithms with varying lengths of digest produced. According to (FIPS, 1995), SHA-1 with a 160-bit length is most widely used in the cryptographic applications.

3.3 Private and public key algorithms

Private and public key algorithms In private key algorithms, the encryption and decryption keys are same and known both to sender and receiver. Some of the well-known examples of private key algorithms are DES, AES, IDEA etc. In public key algorithms, the encryption and decryption system uses two keys, a public key known to everyone and a private or secret key known only to the recipient of the message. The popular public key algorithms are RSA, ECC etc.

3.4 Diffie-Hellman key exchange

The Diffie-Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel (Diffie and Hellman, 1976). The procedure of D-H key exchange protocol is described below:

1. Alice generates two primes p, q and computes $n = pq$. After that he chooses a group G, an element $g \in G$ with order $q^{'}$.

2. Subsequently, Alice selects the private key $S_{HA} = a(< q^{'})$ and computes the public key $P_{HA} = g^{a} mod p^{'}$ then sends it to the Bob.

3. Similarly, Bob picks the private key $S_{FA} = b(< q^{'})$ and finds a corresponding public key $P_{FA} = g^{b} mod p^{'}$ to the Alice.

4. Alice computes the shared secret $K_{FH} = P_{FA}^{b} mod p^{'}$ from Bob's public lic key. In a similar way, Bob also computes $K_{FH} = P_{HA}^{b} mod p^{'}$ from Alice public key.

3.4.1 Discrete Logarithmic problem

Consider a generator g of Z_p^* and a large prime p. Assume $X = g^{x} mod p$. It is trivial to compute $X = g^{x} mod p$, when the values p, x and g are known. However, it is infeasible to compute x with the values p, X, and g due to the factoring of primes (ElGamal, 1984).

3.4.2 Computational Diffie-Hellman problem

Consider a group G with order q. The Computational Diffie-Hellman problem states that, given g, g^x, g^y for a generator g and nonce $x, y \in \{1, 2, ..., q-1\}$, it is impractical to calculate the value g^{xy} (Diffie and Hellman, 1976).

3.5 Elliptic curve cryptography

This section defines elliptic curve properties and, its application in the area of cryptography and network security.

3.5.1 Elliptic curve over a finite field

Considering a set of elliptic curve points $E_p(a,b)$ over E_p, which is defined by the equation: $y^2 = x^3 + ax + b \mod p$, where $a, b \in F_p$ and $4a^3 + 27b^2 \mod p \neq 0$. $E_p(a,b)$ forms a commutative or an abelian group under addition modulo p operation.

3.5.2 ECC encryption and decryption

The ECC cryptosystem first encrypts the plaintext message M to be sent as an elliptic curve point $P_M \in E_p(a,b)$. This point P_M will be encrypted as a ciphertext and then subsequently decrypted. The user selects a private and public key pair such that private-key $d \in Z_P^*$ and the public-key is calculated as $e = d.G$ where $Z_P^* = \{1, 2, ..., p-1\}$ and G is a base point on $E_p(a,b)$. The procedure of ECC encryption and decryption is outlined below:

- ECC encryption: The user picks a nonce $n \in Z_P^*$. The corresponding cipher text C_M for the plain text P_M is a pair of points C_1 and C_2

  $C_M = (C_1, C_2)$

  $C_1 = n.G$

  $C_2 = P_M + n.e.$

  Then, the encrypted cipher C_M is send to the receiver.

- ECC decryption: To decrypt the plaintext P_M , the receiver computes:

  $C_2(d.C_1) = (P_M + n.e)(d.(n.G)) = P_M + n.e - n.e = P_M.$

Here, d and e are private and public key of the receiver.

3.5.3 Elliptic curve discrete logarithm problem (ECDLP)

Given an elliptic curve E defined over a finite prime field F_p, a point $P \in E(F_p)$ of order n and a point $Q \in E(F_p)$, it is hard to compute integer $0 \leq \alpha \leq n-1$, such that $Q = \alpha P$.

3.5.4 Elliptic curve Diffie-Hellman problem (ECDHP)

Given an elliptic curve E defined over a finite prime field F_p and points $P, \alpha P, \beta P \in E(F_p)$ it is difficult to compute $\alpha\beta P$, without the knowledge of $\{\alpha, \beta\}$ (Koblitz et al., 2000).

3.5.5 Summary

In this chapter, a brief review of cryptography and its primitives such as Exclusive-OR operation, one-way hash function, and private and public key algorithms are presented. In addition, the mathematical preliminaries required to design and analyse the authentication protocols for roaming service, which includes Diffie-Hellman key exchange, discrete logarithmic problem and ECC cryptosystems have been discussed.

CHAPTER 4

A Secure User Anonymity and Authentication Scheme Using AVISPA for GLOMONET

4.1 Introduction

This chapter explains about the cryptanalysis done on Gope and Hwang's scheme. With the thorough cryptanalysis of their scheme, we explored that their scheme is vulnerable to various security attacks like stolen smart card, password guessing etc. which are briefly described in section 4.3. An efficient and robust scheme is proposed to eliminate the vulnerabilities that are found in Gope and Hwang's scheme.

Recently in 2016, Gope and Hwang have reviewed He et al. (2011). They stated that the scheme is vulnerable to forgery attack. They further claimed that the scheme failed to preserve user anonymity. They also claimed that their scheme lacks in practicality and achieved no perfect forward secrecy. To eliminate all the security weaknesses found in their scheme, they proposed an efficient scheme. With the thorough analysis of Gope and Hwang's scheme, we proved that their scheme is vulnerable to various security attacks like stolen smart card, offline password guessing, MU impersonation and replay attack. We further proved that their scheme does not protect user anonymity and fails to achieve perfect forward secrecy.

The remainder of this chapter is organized as follows. Gope and Hwang's scheme is analyzed thoroughly which is outlined in section 4.2. Section 4.3 illustrates the cryptanalysis part. The proposed scheme is explained in Section 4.4. Detailed description of the formal security analysis using BAN logic is explained in section 4.5. Formal security verification of the proposed scheme using AVISPA tool is illustrated in section

4.6. Performance comparison based on functionality of the security properties, computational cost and communication overhead of the proposed scheme is compared with the other existing schemes and it is described in section 4.7. Section 4.8 concludes the chapter.

4.2 Review of Gope and Hwang scheme

This section explains about the scheme Gope and Hwang (2016a) in detail. Notations and their representation used in this paper are defined in Table 4.1.

Table 4.1 Notations and their representation

Notation	Representation
MU	Mobile User
FA	Foreign Agent
HA	Home Agent
ID_M	MU's identity
PW_M	MU's password
AID_M	MU's one time alias identity
PID	MU's pseudo identity
ID_h	HA's identity
ID_f	FA's identity
ID_{HA}	HA's identity
ID_{FA}	FA's identity
SK	Session key exchanged with FA and MU
K_{uh}	Encryption key
K_{fh}	FA and HA's shared secret key
$Trseq$	Track sequence number
ID_{MU}	Identity of the MU
PW_{MU}	Password of the MU
X	Secret key of HA
T	Time-stamp
$\triangle$T	Time-delay

4.2.1 Registration phase

MU submits his/her ID_M over secure channel to HA. HA receives the login request, after that, HA generates random number n_h, server generates random number r_j. HA computes $K_{uh} = h(ID_M||n_h) \oplus ID_h$. Pseudo-identities $ID_s, PID = pid_1, pid_2, ...$, where for each $pid_j \in PID$ are generated by HA server computes $pid_j = h(ID_M||r_j||K_{uh})$, HA generates unique Tr_{seq}, a 64-bit sequence number and a random no. m that is assigned to $Tr_{seq} = m$, a copy of Tr_{seq} is stored in HA database, before sending to the MU. All these parameters $\{ID_M, K_{uh}, Tr_{seq}\}$ are stored in the database for future reference. After that, HA submits the smart card $\{K_{uh}, PID, Tr_{seq}, h(.)\}$ to the MU. After receiving the smart card, MU selects his/her own password PW_M. MU computes $K^*_{uh} = K_{uh} \oplus h(ID_M||PW_M)$, $PID^* = PID \oplus h(ID_M||PW_M)$. MU replaces K_{uh} with K^*_{uh} and PID is replaced with PID^*. Finally, the smart card contains the parameters $\{K^*_{uh}, PID^*, Tr_{seq}, h(.)\}$.

4.2.2 Mutual authentication and key agreement phase

The authentication process is explained below in detailed steps:

1. $M_1 = \{AID_M, \{N^{'}_m||P\}_{E_{K_{uh}}}, Tr_{seq}(\text{if required}), ID_h\}$. The smart card computations, where N_m and $N^{'}_m$ are the smart card random numbers $p = N_m \oplus N^{'}_m$
   $K_{uh} = K^*_{uh} \oplus h(ID_M||PW_M)$, $AID_M = h(ID_M||K_{uh}||N_m||Tr_{seq})$, where Tr_{seq} is a track sequence no. of 64-bit. Hence MU forms message M_1 and submits to FA. In case connection is lost, then MU needs to compute $pid_j = pid^*_j \oplus h(ID_M||PW_M)$ and assign $AID_M = pid_j$. In such case user need not send any Tr_{seq} in M_1.

2. $M_2 = \{AID_M, \{N^{'}_m||P\}_{E_{K_{uh}}}, Tr_{seq}, \{N^{'}_f||Q\}_{E_{K_{fh}}}, V_1\}$. FA accepts the message M_1 from MU, two random no.'s N_f and $N^{'}_f$ are generated by FA. FA calculates
   $Q = N_f \oplus N^{'}_f$, $V_1 = h(M_1||K_{fh}||N_f) \oplus Q$. FA submits the message M_2 to the HA.

3. $M_3 = \{x, Tr_{seq}, y, V_2, V_3\}$.
   After accepting M_2 from FA, HA checks for track sequence number Tr_{seq} whether it is valid or not, then decrypts $\{N^{'}_m||P\}_{E_{K_{uh}}}\}, \{N^{'}_f||Q\}_{E_{K_{fh}}}\}$. HA computes
   $N_m = P \oplus N^{'}_m, N_f = P \oplus N^{'}_f$ and verifies the parameters $\{V_1, AID_M\}$. If valid then

HA computes $x = \{N_m||N_f\}_{E_{K_{fh}}}$, $V_2 = h(x||K_{fh}||N_f)$, $y = h(N_m||K_{uh}||ID_M) \oplus N_f$, $Tr = h(K_{uh}||ID_M||N_m) \oplus Tr_{seq_{new}}$, $V_3 = h(y||N_m^{'}||K_{uh}||Tr)$. Finally forms message M_3 and sends to FA. In case if HA cannot find Tr_{seq} in M_1, then HA will check for the parameter AID_M and tries to recognize the pid_j in AID_M, if valid then HA authenticates MU or else terminates the request.

4. $M_4 = \{y, Tr, V_3\}$ On receiving M_3, FA first decrypts x and verifies N_f and checks for the integrity of value x. If verified successfully, then FA computes $SK = N_m \oplus N_f$. Forms message M_4 and submits to the MU.

5. After accepting the message M_4, integrity is checked by the MU by computing $V_3^* = h(y||N_m^{'}||K_{uh}||Tr)$ and checks whether received $V_3 \stackrel{?}{=} V_3^*$. If true mobile user MU computes $N_f = h(N_m||ID_M||K_{uh}) \oplus y$ $Tr_{seq_{new}} = h(K_{uh}||ID_M||N_m) \oplus Tr$ $SK = N_m \oplus N_f$. Thus MU and FA are mutually authenticated with each other.

4.2.3 Password renewal phase

Whenever MU wants to update his old password with new password, MU needs to insert his smart card into the device and input his ID_M, old password PW_M and new password PW_M^*. Thereafter, smart card will derive $K_{uh} = K_{uh}^* \oplus h(ID_M||PW_M)$, $PID = PID^* \oplus h(ID_M||PW_M)$ and then computes K_{uh}^{**}=$K_{uh} \oplus h(ID_M||PW_M^*)$, $PID^{**} = PID^* \oplus h(ID_M||PW_M^*)$. Finally K_{uh}^* will be replaced with K_{uh}^{**} and PID^* will be replaced with PID^{**} in smart card for future communication.

4.3 Cryptanalysis of Gope and Hwang scheme

With the thorough understanding of Gope and Hwang's scheme, the following attacks which are listed below are found.

4.3.1 User anonymity is not preserved

Gope and Hwang explained that during registration phase, MU sends ID_M. HA stores the ID_M for future communication in its database. An insider attacker who has the admin privileges to the database can easily reveal ID_M identity of the MU as it is saved

in plain text form. This becomes the security flaw for not protecting the user anonymity. Therefore, user anonymity is not preserved.

4.3.2 Vulnerable to stolen smart card attack

In case, the admin who have the access privileges to the database acts as an inside attacker and reveal the security parameters ID_M, K_{uh}, these parameters are not hashed, instead they are stored in plain text. This makes the attacker to easily compute the following along with the security parameters $\{ID_M, K_{uh}\}$ and the stolen smart card with the parameters $\{K^*_{uh}, PID^*, Tr_{seq}, \text{h(.)}\}$.

1. $K^*_{uh} = K_{uh} \oplus h(ID_M||PW_M)$
   $h(ID_M||PW_M) = K^*_{uh} \oplus K_{uh}$
   $PID^{'} = PID^* \oplus h(ID_M||PW_M)$. During connection loss, a pseudo identity PID is used by the MU, to establish the connection with the HA, based on PID, HA validates the authenticity of the MU.

2. During mutual authentication and key agreement phase, if an adversary intercepts the message $M_1 = \{AID_M, \{N^{'}_m||P\}_{E_{K_{uh}}}, Tr_{seq}(\text{if required}), ID_h\}$ exchanged over insecure channel and assigns $AID^*_M = PID^{'}$, attacker modifies the message $M^{'}_1 = \{AID^*_M, \{N^{'}_m||P\}_{E_{K_{uh}}}, Tr_{seq}(\text{if required}), ID_h\}$ and sends it to FA, FA sends it to HA. HA on receiving the message $M^{'}_1$ checks for the value of $PID^{'}$ which is saved in its database and verifies that the received AID^* matches to the value of saved $PID^{'}$ and confirms that message has come from a legal MU. This leads the attacker to successfully impersonate a MU, thus results in accessing the FA services during roaming. Therefore the scheme is non resilient to stolen smart card attack.

4.3.3 Perfect forward secrecy is not achieved

During mutual authentication and key agreement phase, the messages transmitted between MU, FA and HA are carried through insecure channel. The messages are exchanged between the three entities via insecure channel, these messages can be easily intercepted by an attacker. With the interception of these messages, an attacker will be able to reveal the session key. Hacking session key is briefly explained in below steps.

1. The security parameters ID_M, K_{uh} of HA stored in the database are revealed by an insider attacker who has the admin privileges to the HA's database.

2. During mutual authentication and key agreement phase, an attacker intercepts the messages exchanged between MU and FA.
   $M_1 = \{AID_M, \{N_m^{'}||P\}_{E_{K_{uh}}}, Tr_{seq}(\text{if required}), ID_h\}$ and $M_4 = \{y, Tr, V_3\}$.

3. After the reveal of the secret parameter K_{uh}, attacker will be able to decrypt $\{N_m^{'}||P\}_{D_{K_{uh}}}$ and obtain the values $N_m^{'}, P$. Then he/she can compute $N_m = P \oplus N_m^{'}$.

4. The message $M_4 = \{y, Tr, V_3\}$, and the random no. N_f contributes in computing $N_f = y \oplus h(N_m||ID_M||K_{uh})$.

5. The computed values of N_m, N_f, lets attacker to compute for the session key $SK = N_m \oplus N_f$. Session key is used for encrypting data that are transmitted over insecure channel, with the hack of the session key, attacker can keep track of all the messages that are exchanged between three entities. This makes the scheme non resilient towards perfect forward secrecy.

4.3.4 Vulnerable to offline password guessing attack

With the revealing of the parameters ID_M and K_{uh} stored in HA's database by an insider attacker and with the stolen smart card parameters $\{K_{uh}^*, PID^*, Tr_{seq}, h(.)\}$. An attacker will be able to compute $K_{uh}^{**} = K_{uh} \oplus h(ID_M||PW_M^{'})$, where $PW_M^{'}$ is a password guessed by an attacker and verifies whether $K_{uh}^{**} \stackrel{?}{=} K_{uh}^*$. If it matches, then an attacker who has guessed the password $PW_M^{'}$ is the correct password. If not, then the attacker keeps repeating the computation, assuming different values until K_{uh}^{**} is equal to K_{uh}^*. Thus the scheme is non resilient to offline password guessing attack.

4.3.5 Vulnerable to replay attack

1. The secret key K_{uh} which is stored in HA's database can be easily revealed by an insider attacker. If the smart card personalised with $\{K_{uh}^*, PID^*, Tr_{seq}, h(.)\}$ is stolen and falls in the hands of an attacker, then attacker will be able to compute $K_{uh}^* = K_{uh} \oplus h(ID_M||PW_M)$, $h(ID_M||PW_M) = K_{uh}^* \oplus K_{uh}$, $PID^{'} = PID^* \oplus h(ID_M||PW_M)$.

2. During mutual authentication and key agreement phase, with the interception of the message $M_1 = \{AID_M, \{N_m^{'}||P\}_{E_{K_{uh}}}, Tr_{seq}(\text{if required}), ID_h\}$ exchanged via insecure channel attacker sets $AID_M^* = PID^{'}$, then he/she can replay this message by computing $M_1^{'} = \{AID_M^*, \{N_m^{'}||P\}_{E_{K_{uh}}}, Tr_{seq}(\text{if required}), ID_h\}$ to FA.

3. On receiving the message $M_1^{'} = \{AID_M^*, \{N_m^{'}||P\}_{E_{K_{uh}}}, Tr_{seq}(\text{if required}), ID_h\}$ from MU, two random no.'s N_f, $N_f^{'}$ are generated by FA. FA computes $Q = N_f \oplus N_f^{'}$, $V_1 = h(M_1^{'}||K_{fh}||N_f) \oplus Q$. After that FA submits the message $M_2 = \{AID_M^*, \{N_m^{'}||P\}_{E_{K_{uh}}}, Tr_{seq}, \{N_f^{'}||Q\}_{E_{K_{fh}}}, V_1\}$ to HA. HA verifies for AID_M^* by mapping it with the PID that is stored in database, if the match holds true, HA assumes that an adversary to be a legitimate MU. This makes the scheme vulnerable to replay attack. Therefore, the scheme is non resilient to replay attack.

4.3.6 Vulnerable to MU impersonation attack

The messages that are transmitted over insecure channel are encrypted using the secret key K_{uh}. In Gope and Hwang's scheme, HA's database stores the secret key K_{uh}.

1. An insider attacker who has the access privilege to the HA's database can easily reveal the secret key K_{uh}, which lets the user to decrypt all the intercepted messages. For illustration consider $M_1 = \{AID_M, \{N_m^{'}||P\}_{E_{K_{uh}}}, Tr_{seq}(\text{if required}), ID_h\}$ transmitting over insecure channel can be intercepted by an attacker, along with the revelation of the the secret key K_{uh}, $\{N_m^{'}||P\}$ can be decrypted by obtaining the values of $N_m^{'}$ and P. where $P = N_m \oplus N_m^{'}$, with the parameters P, $N_m^{'}$ attacker can compute $N_m = P \oplus N_m^{'}$ and replay the message $M_1^{'}$ to FA.

2. After the arrival of the message $M_1^{'}$ from MU, two random no.'s $N_f, N_f^{'}$ are generated by FA. FA computes $Q = N_f \oplus N_f^{'}, V_1 = h(M_1||K_{fh}||N_f) \oplus Q$. FA submits message $M_2 = \{AID_M, \{N_m^{'}||P\}_{E_{K_{uh}}}, Tr_{seq}, \{N_f^{'}||Q\}_{E_{K_{fh}}}, V_1\}$ to HA. HA verifies for AID_M by comparing it with the stored value of PID in its database. Obviously, both are equal to each other. Thus an attacker will be successful in impersonating the legal MU. Therefore, the scheme is non resilient to impersonation attack.

4.4 Proposed scheme

The proposed scheme is divided into three phases, they are: registration phase that is carried over secure channel, login and authentication phase is carried over insecure channel and password change phase, which provides local password verification for the MU. Diffie and Hellman (1976) key agreement protocol is used to compute the secret key between FA and HA to achieve mutual authentication in the proposed scheme. The proposed scheme is simulated using AVISPA tool. Each phase is explained in detail below.

4.4.1 Registration phase

During the registration phase, MU is free to choose his/her identity ID_{MU} and password PW_{MU}. After choosing ID_{MU} and PW_{MU}, MU submits the chosen ID_{MU} and PW_{MU} to HA through secure channel. HA receives the request from MU. After that HA computes $K1 = h(ID_{MU}||X)$, X is a long term secret key of HA. $S = h(ID_{MU}||PW_{MU}) \oplus K1$. HA stores K1 in it's database. HA sends the smart card with the parameters $\{S, ID_{HA}, h(.)\}$ to the MU. Registration phase of the proposed scheme is presented in Figure 4.1.

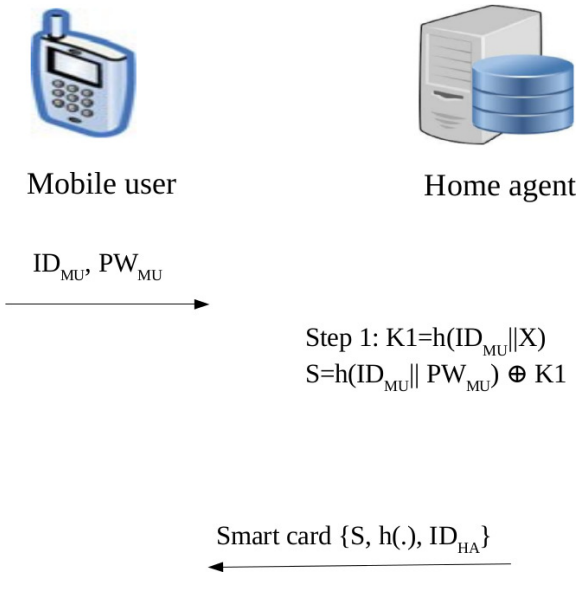

Figure 4.1 Registration phase

4.4.2 Login and authentication phase

Login and authentication phase is presented in Figure 4.2. The detailed description of the steps are stated below:

1. Smart card is inserted into the smart card terminal by the MU. Smart card terminal asks for the input of ID_{MU} and password PW_{MU} of the MU. After entering, the smart card computes $K1^* = S \oplus h(ID_{MU}||PW_{MU})$, $S^* = K1^* \oplus h(ID_{MU}||PW_{MU})$, verifies if $S^* \stackrel{?}{=} S$. If verified, random number N_m is generated by the smart card. Smart card computes $K = S \oplus h(ID_{MU}||PW_{MU})$, $L = K \oplus N_m$, $P = h(L||ID_{HA})$. Finally MU forms message $M_1 = \{P, N_m, ID_{HA}\}$, message M_1 is then transmitted to FA.

2. $M_2 = \{P, N_m, ID_{HA}, N_f, ID_{FA}\}$. After receiving the message $M_1 = \{P, N_m, ID_{HA}\}$ from MU. FA generates random number N_f and forms message $M_2 = \{P, N_m, ID_{HA}, N_f, ID_{FA}\}$, where ID_{FA} is the identity of the FA and sends to HA.

3. $M_3 = \{Q, ID_{HA}\}$. After receiving the message $M_2 = \{P, N_m, ID_{HA}, N_f, ID_{FA}\}$. HA computes $L^* = K1 \oplus N_m$, $P^* = h(L^*||ID_{HA})$. HA verifies whether $P^* \stackrel{?}{=} P$. If holds true, MU authenticity is verified. HA computes $SK = h(K1||N_m||N_f||ID_{MU}||ID_{FA}||ID_{HA})$, $Q = SK \oplus h(K_{HF}||N_f||ID_{FA})$. HA forms message $M_3 = \{Q, ID_{HA}\}$ and sends it to FA.

4. $M_4 = \{T, N_f, ID_{FA}\}$. On receiving the message $M_3 = \{Q, ID_{HA}\}$ from HA, FA computes $SK = Q \oplus h(K_{HF}||N_f||ID_{FA})$, $Q^* = SK \oplus h(K_{HF}||N_f||ID_{FA})$. Checks whether $Q^* \stackrel{?}{=} Q$. If true, FA computes $R = SK \oplus h(N_m||ID_{FA})$, $T = R \oplus h(N_m||N_f)$, and forms message $M_4 = \{T, N_f, ID_{FA}\}$ and sends it to MU.

5. On receiving the message, $M_4 = \{T, N_f, ID_{FA}\}$ from FA. MU computes $R^* = T \oplus h(N_m||N_f)$, $SK = R \oplus h(N_m||ID_{FA})$, $SK^* = h(K1||N_m||N_f||ID_{MU}||ID_{FA}||ID_{HA})$. Verify if $SK^* \stackrel{?}{=} SK$. If it holds, then FA is authenticated and message comes from trusted HA.

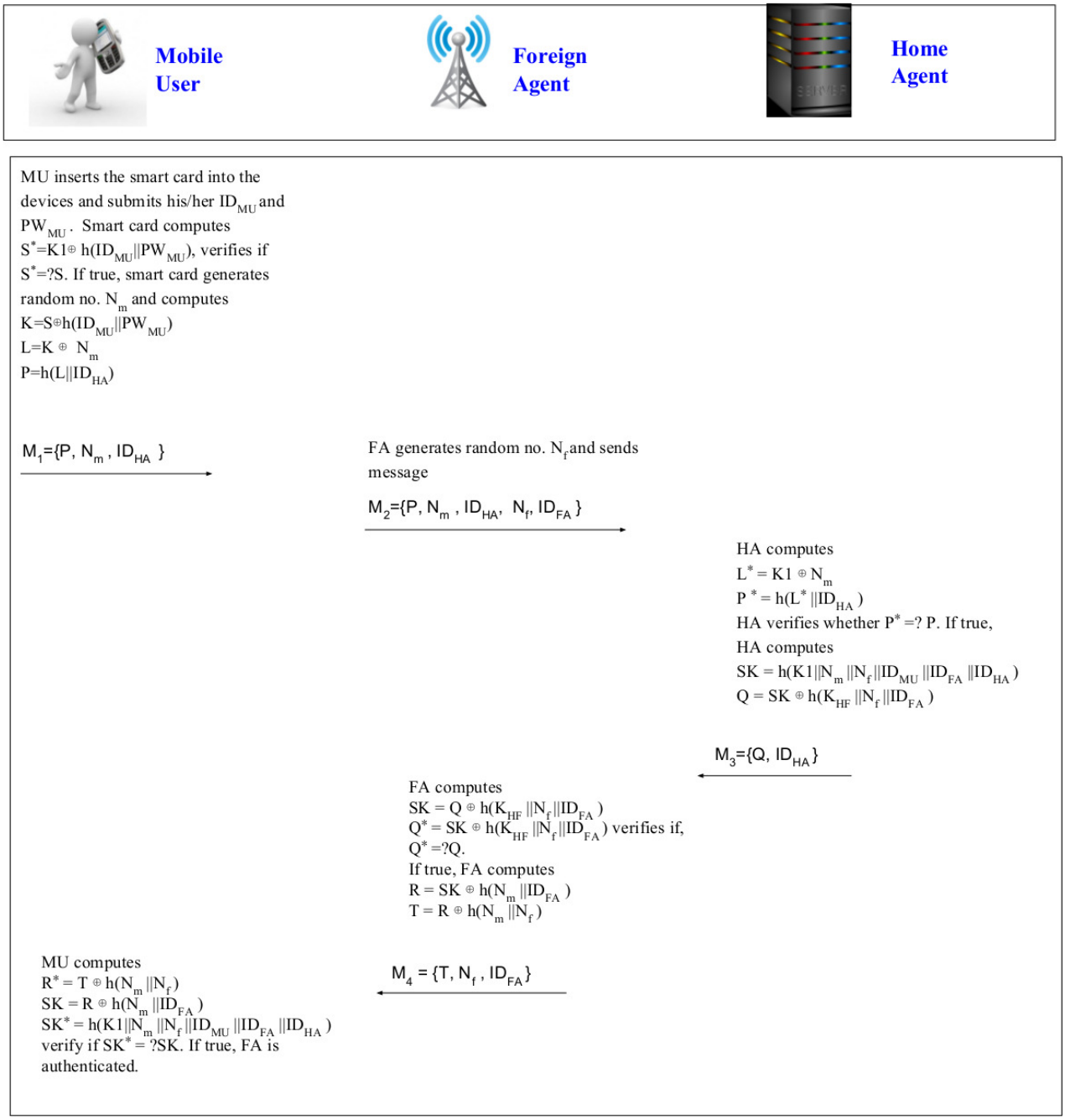

Figure 4.2 Login and authentication phase

4.4.3 Password change phase

During the password change phase, terminal allows the MU to change the current password PW_{MU}^{old} with the new password PW_{MU}^{new}, MU has to insert his/her smart card in to the terminal. After inserting MU has to provide his/her credentials to the terminal. Once the MU enters ID_{MU} and current password PW_{MU}^{old}, terminal processes the information. Then the smart card computes $K1^* = S \oplus h(ID_{MU}||PW_{MU}^{old})$, $S^* = K1^* \oplus h(ID_{MU}||PW_{MU}^{old})$ and checks if it matches with the value $S^* \stackrel{?}{=} S$. After validating, the MU will be able to update the current password PW_{MU}^{old} with the new password PW_{MU}^{new}. The smart card asks the MU to enter the new password PW_{MU}^{new}. After that the smart card computes $S^* = h(ID_{MU}||PW_{MU}^{new}) \oplus K1$. The parameter S which is stored in smart card is replaced with S^*.

4.5 Security analysis

This section explains how the proposed scheme is resilient towards some of the security attacks and goals which are described below. To prove the correctness of the proposed scheme, we use BAN logic (Burrows et al., 1988; Chen, 2013). BAN logic is a formal tool that enables to analyse the correctness of an authentication protocol. It includes mutual authentication and key distribution. The notations P and Q denote principals: X and Y denote statements; and K is the cryptographic key. Table 4.2 provides the meaning for the BAN logic symbols.

Table 4.2 Notations used in BAN logic

Notation	Definition
$P\| \equiv X$	P believes X: P would be entitled to believe X.
$P \lhd X$	P sees X: P can receive and read X
$P\| \sim X$	P said X: P once said X
$P\| \Rightarrow X$	P controls X: P has jurisdiction over X
$\#(X)$	Fresh (X): The formula X is fresh
$\langle X \rangle_y$	X is integrated with y; y should be kept secret
$P \overset{K}{\leftrightarrow} Q$	K is used as a shared key between P and Q for secure communication
$P \overset{y}{\rightleftharpoons} Q$	The formula y is shared between two principals P and Q

Logic postulates of BAN logic

1. Message meaning rule for shared secrets: $\frac{P|\equiv Q \overset{y}{\rightleftharpoons} P, P \triangleleft \langle X \rangle_y}{P|\equiv Q|\sim X}$

2. Nonce-verification rule: $\frac{P|\equiv \#(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$

3. Jurisdiction rule: $\frac{P|\equiv Q|\Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$

4. Receiving rule: $\frac{P \triangleleft (X,Y)}{P \triangleleft X}$ and $\frac{P \triangleleft \langle X \rangle_y}{P \triangleleft X}$

5. Freshness-propagation rule: $\frac{P|\equiv \#(X)}{P|\equiv \#(X,Y)}$

6. Session-key rule: $\frac{P|\equiv \#(K), P|\equiv Q|\equiv X}{P|\equiv P \overset{K}{\leftrightarrow} Q}$

We summarize the proposed protocol in the following generic form:

1. Message M1. $MU \rightarrow FA : \{P, N_m, ID_{HA}\} = \{h(L||ID_{HA}), N_m, ID_{HA})\}$

2. Message M2. $FA \rightarrow HA : \{P, N_m, ID_{HA}, N_f, ID_{FA}\} = \{h(L||ID_{HA}), N_m, ID_{HA}, N_f, ID_{FA}\}$

3. Message M3. $HA \rightarrow FA : \{Q, ID_{HA}\} = \{SK \oplus h(K_{FH}||ID_{FA}), ID_{HA}\}$, where $SK = h(K1||N_m||N_f||ID_{MU}||ID_{FA}||ID_{HA})$

4. Message M4. $FA \rightarrow MU : \{T, N_f, ID_{FA}\} = \{R \oplus h(N_m||N_f), N_f, ID_{FA}\}$.

The generic form of the proposed protocol is transformed into idealized form (Chang and Cheng, 2011). K_m, K_f are the secret parameters of MU and FA respectively used for hashing conventions.

I_1. $MU \rightarrow FA : \langle N_m \rangle_{K_m}$

I_2. $FA \rightarrow HA : \langle N_m \rangle_{K_m}, \langle N_f \rangle$

$I_3.\ HA \rightarrow FA : \langle N_m \rangle_{K_m}, \langle N_f \rangle_{K_f}$

$I_4.\ FA \rightarrow MU : \langle N_m \rangle_{K_m}, \langle N_f \rangle_{K_f}$

Following assumptions were made to analyze the proposed protocol

$A_1.\ MU| \equiv MU \overset{K1}{\rightleftharpoons} HA$

$A_2.\ HA| \equiv MU \overset{K1}{\rightleftharpoons} HA$

$A_3.\ FA| \equiv FA \overset{K_{fh}}{\rightleftharpoons} HA$

$A_4.\ HA| \equiv FA \overset{K_{fh}}{\rightleftharpoons} HA$

$A_5.\ HA| \equiv \#(N_{mMU})$

$A_6.\ MU| \equiv \#(N_{mMU})$

$A_7.\ HA| \equiv \#(N_{f_{FA}})$

$A_8.\ FA| \equiv \#(N_{f_{FA}})$

$A_9.\ HA| \equiv MU| \Rightarrow N_{mMU}$

$A_{10}.\ MU| \equiv HA| \Rightarrow N_{mMU}$

$A_{11}.\ HA| \equiv FA| \Rightarrow N_{f_{FA}}$

$A_{12}.\ FA| \equiv HA| \Rightarrow N_{f_{FA}}$

4.5.1 User anonymity

User anonymity is an important security service required to ensure that the identity of the mobile user is not disclosed.

Proposition 4.5.1. User anonymity is preserved.

Proof: If an adversary intercepts the message $M1 = \{P, N_m, ID_{HA}\}$ transmitting on public channel along with the stolen smart card parameters $\{S, ID_{HA}, h(.)\}$. Adversary can compute

1. $P \oplus S = h(L||ID_{HA}) \oplus h(ID_{MU}||PW_{MU}) \oplus h(ID_{MU}||X)$

2. $h(h(ID_{MU}||X) \oplus N_m||ID_{HA}) \oplus h(ID_{MU}||PW_{MU}) \oplus h(ID_{MU}||X)$

BAN Logic Postulates

1. $MU| \equiv MU \overset{K1}{\rightleftharpoons} HA$

2. $HA| \equiv MU \overset{K1}{\rightleftharpoons} HA$

With all the above computations, still adversary will not be successful in extracting the identity ID_{MU} of the mobile user. Thus the proposed scheme provides user anonymity.

4.5.2 Mutual authentication and session key establishment

In roaming scenario, the three communicating entities MU, FA and HA must authenticate to each other to communicate with each other. To achieve mutual authentication between FA and HA, Diffie and Hellman (1976) key agreement protocol is used, using this protocol, the secret key K_{FH} is computed. The secret key is shared between FA and HA.

Lemma 1: In the proposed scheme, HA authenticates the MU and the FA.
Proof: MU and FA generates random no.s N_m and N_f respectively. The following beliefs verifies that HA can authenticate both MU and FA.

B1: $HA| \equiv N_m$

B2: $HA| \equiv N_f$

For B1, the steps are stated below:

S1: HA sees $\langle N_m \rangle_{K_m}$. (Using I_2 and receiving rule)

S2: HA believes MU said N_m. (Using I_2 and receiving rule)
$HA| \equiv MU| \sim N_m$.

S3: HA believes MU believes N_m. (Using A_5, S2 and nonce-verification rule)
$HA| \equiv MU \equiv N_m$.

S4: HA believes N_m.

$HA| \equiv N_m$. (Using A_9, S3 and jurisdiction rule). Thus HA verifies legality of MU.

Detailed steps for B2 are listed below:

S5: HA sees N_f. (Using I_2 and receiving rule)

$HA \lhd N_f$

S6: HA believes FA said N_f. (Using A_7, S5 and message meaning rule)

$HA| \equiv FA| \sim N_f$

S7: HA believes FA believes N_f. (Using A_8, S6 and nonce-verification rule)

$HA| \equiv FA \equiv N_f$.

S8: HA believes N_f. (Using A_7, S_7 and jurisdiction rule)

$HA| \equiv N_f$

Lemma 2: Authentication of MU and FA to HA.

Proof: In the proposed scheme, HA after receiving N_m and N_f random no.'s from MU and FA sends back to the MU and FA. The following assumptions are made, to authenticate MU and FA by HA:

B3: $FA \equiv N_f$

B4: $MU \equiv N_m$

For B3, the steps are listed below:

S9: FA sees $\langle N_f \rangle_{K_f}$. Using I_3 and receiving rule.

$FA \lhd \langle N_f \rangle_{K_f}$

S10: FA believes HA said N_f. Using S9 and message meaning rule.

$FA| \equiv HA| \sim N_f$

S11: FA believes HA believes N_f. Using A_7, S10 and message meaning rule.

$FA| \equiv HA| \equiv N_f$

S12: FA believes N_f; that is, $FA| \equiv N_f$. Using A_7, S11 and the jurisdiction rule. Therefore, the FA can authenticate the HA.

For B4, the main steps of the proof are similar as follows:

S13: MU sees $\langle N_m \rangle_{K_m}$. Using I_4 and receiving rule.
$MU \lhd \langle N_m \rangle_{K_m}$

S14: MU believes HA said N_m. Using S13 and message meaning rule.
$MU| \equiv HA| \sim N_m$

S15: MU believes HA believes N_m. Using A_5, S14 and message meaning rule.
$MU| \equiv HA| \equiv N_m$

S16: MU believes N_m; that is, $MU| \equiv N_m$. Using A_6, S15 and the jurisdiction rule. Therefore, the MU can authenticate the HA.

Lemma 3: In the proposed scheme MU and FA can mutually authenticate each other and share established session key.

Proof: On receiving the message, $M_4 = \{T, N_f, ID_{FA}\}$ from FA. MU computes $R^* = T \oplus h(N_m||N_f)$, $SK = R \oplus h(N_m||ID_{FA})$, $SK^* = h(K1||N_m||N_f||ID_{MU}||ID_{FA}||ID_{HA})$. Verify if $SK^* \stackrel{?}{=} SK$, if true then FA is authenticated and message comes from trusted HA. Hence the proposed scheme mutually authenticates all the three communicating entities in GLOMONETs.

4.5.3 Perfect forward secrecy is achieved

Suppose an adversary who is secretly listening to the communication intercepts the messages $M_2 = \{P, N_m, ID_{HA}, N_f\}$, $M_3 = \{Q, ID_{HA}\}$ and $M_4 = \{T, N_f, ID_{FA}\}$. With the parameter Q, N_f and ID_{FA} he/she will not be successful in hacking the SK, to get the session key he/she must compute $Q = SK \oplus h(K_{HF}||N_f||ID_{FA})$. In order to get $SK = Q \oplus h(K_{HF}||N_f||ID_{FA})$ he/she must know the secret key K_{HF} that is shared between HA and FA and the secret key is computed using Diffie-Hellman key exchange protocol

due to the protocol complexity, it is impossible for an adversary to hack the session key. Hence the scheme provides security to the disclosure of the session key.

$$\frac{P|\equiv Q \overset{y}{\rightleftharpoons} P, P \lhd \langle X \rangle_y}{P|\equiv Q|\sim X}$$

4.5.4 Security against offline password guessing attack

The smart card with the parameters $\{S, h(.), ID_{HA}\}$ gets stolen and falls in the hand of an adversary. He/she tries to reveal the PW_{MU}. Adversary has the parameter S, to reveal the password PW_{MU}, he/she tries to compute $S = K1 \oplus h(ID_{MU}||PW_{MU})$, $K1 = h(ID_{MU}||X)$, X is a secret key of HA. To compute K1, he/she should know the value of ID_{MU} and X. The complexity of guessing the two parameters precisely becomes impossible for an adversary. In the proposed scheme PW_{MU} is concatenated with the ID_{MU} of the MU and hashed, hence the two parameters ID_{MU} and PW_{MU} has to be guessed precisely, which becomes impossible for an adversary. Therefore, the proposed scheme provides security against offline password guessing attack.

4.5.5 Security against MU impersonation attack

If an adversary, tries to impersonate the legal MU by intercepting the message $M_2 = \{P, N_m, ID_{HA}, N_f, ID_{FA}\}$ and sending it as $M_2^{'}$ to HA. After the arrival of the message $M_2^{'}$, HA computes $L^* = K1 \oplus N_m$, $P^* = h(L^*||ID_{HA})$. HA verifies whether $P^* \stackrel{?}{=} P$. If it does not hold, the request is terminated by HA. Thus the proposed scheme provides security against MU impersonation attack.

4.5.6 Security against replay attack

The two messages $M_1 = \{P, N_m, ID_{HA}\}$, and $M_2 = \{P, N_m, ID_{HA}, N_f, ID_{FA}\}$ that are transmitted over the insecure channel. With the interception of these two messages, if he/she tries to send the modified message $M_2^{'}$ to HA. Adversary fails to replay the message as the messages carry random numbers N_m of the MU and N_f of the FA. Random number changes for every session. Suppose, if an adversary sends the modified message $M_2^{'}$ to HA. On receiving the message $M_2^{'}$, HA computes $L^* = K1 \oplus N_m$, $P^* = h(L^*||ID_{HA})$. HA verifies whether $P^* \stackrel{?}{=} P$. If it does not hold, the request is terminated by HA. Hence the scheme provides protection against replay attack.

4.5.7 Security against stolen smart card attack

The smart card with the parameters $\{S, h(.)\}$ gets stolen and falls in the hand of an adversary, with the stolen card he/she can listen to the communication channel and tries to eavesdrop the messages $M_1 = \{P, N_m, ID_{HA}\}$, $M_2 = \{P, N_m, ID_{HA}, N_f, ID_{FA}\}$ and $M_3 = \{Q, ID_{HA}\}$. After that, he/she can compute the following values based on the parameters, which he/she has investigated during interception $K1 = h(ID_{MU}||X)$, X is a secret value of HA. K1 value can be computed only by the authorised mobile user that is $K1 = h(ID_{MU}||X)$. To compute K1, he/she should guess the two unknown parameters ID_{MU} and X precisely, which becomes impossible for an adversary. Hence even with the stolen card parameters and the intercepted messages, adversary will not be able to arrive neither at the ID_{MU} of the MU nor the long term secret key X of the HA. Thus the proposed scheme is secure against stolen smart card attack.

4.6 Formal security verification using avispa tool

To provide the results of the formal security verification of the proposed scheme, AVISPA tool is used. Acronym AVISPA stands for Automated Validation of Internet Security Protocols and Applications, the proposed scheme is simulated and verified against the active and passive security attacks. Firstly, the AVISPA tool is introduced, secondly, the implementation details of the proposed scheme using AVISPA is presented and finally the output of the simulation is presented.

4.6.1 Overview of AVISPA

AVISPA is a tool, which is widely accepted for the verification of the cryptographic protocols. One of the major advantages of this AVISPA tool is that, the same protocol specification can be verified by different verification techniques. The cryptographic protocol is written in HLPSL. HLPSL (High Level Protocol Specification Language) is an expressive, modular, role-based, formal language. The cryptographic protocol written in HLPSL, is first converted into Intermediate Format (IF) by the HLPSL2IF translator. Later this IF is executed by the back-ends that AVISPA tool uses. Back-end tools supported by AVISPA are On-the-Fly Model-Checker (OFMC), Constraint Logic based

Attack Searcher (CL-AtSe), SAT-based Model-Checker (SATMC) and Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP). Detailed description of these four back-ends is given in (von Oheimb, 2005). AVISPA tool uses OFMC/CL-AtSe back-end to execute IF which is then converted to Output Format (OF). OF includes the sections which are explained in detail below.

1. SUMMARY: It summarises about the executed protocol safe or unsafe property, safe signifies that the tested protocol is safe and unsafe signifies that the tested protocol is insecure.

2. DETAILS: This section gives details about the conditions that are used in test to make the protocol safe or unsafe.

3. PROTOCOL: This section provides the name of the protocol that is to be tested.

4. GOAL: Test's goal is specified in this section.

5. BACKEND: Back-end name that is used to execute the test is specified in this section.

6. COMMENTS and STATISTICS: This sections demonstrates the attacker simulation if the test is unsafe.

4.6.2 HLPSL Implementation

HLPSL uses three basic roles: mobileuser played_by MU, foreignagent played_by FA homeagent played_by HA. The three supporting roles used in the HLPSL implementation are: environment, session and role. The HLPSL implementation details of mobile user's registration phase and login and authentication phase of the proposed scheme is presented in Fig. 4.3. HLPSL implementation for the foreignagent role is presented in Fig. 4.4. HLPSL implementation for the homeagent role is presented in Fig. 4.5. HLPSL implementation for the session role is presented in Fig. 4.6. HLPSL implementation for the goal and environment role is presented in Fig. 4.7. Output of the program is presented in Fig. 4.8.

```
role mobileuser(MU, HA, FA : agent,
SKmuha: symmetric_key,
H: hash_func,
SND, RCV: channel(dy))

played_by MU
Def=

local State :nat,
IDmu, PWmu, S, X, NM, NF, K1, IDha, IDfa, R, T, K, P, Kfh,
L, SK :text

const nm,nf,s1,s2,s3,s4 : protocol_id
init State := 1

transition
1. State = 1 ∧RCV(start) =|>
State' := 2 ∧SND(IDmu_Skmuha)

∧SND(PWmu_Skmuha)

∧secret(IDmu,s1,MU,HA)

∧secret(PWmu,s2,MU)

2. State = 2
∧RCV (H(IDmu.X).xor(H(IDmu.PWmu),
H(IDmu.X))_SKmuha) =|>

State' := 3∧secret(X,s3,HA)
∧secret(Kfh,s4,FA)

∧NM' := new()

∧K' :=xor(xor(H(IDmu.PWmu), H(IDmu.X)), H(IDmu.Pwmu))

∧L' :=xor(xor(xor(H(IDmu.PWmu), H(IDmu.X)),
H(IDmu.PWmu)), NM')

∧P' :=H(xor(xor(xor(H(IDmu.PWmu),H(IDmu.X)),
H(IDmu.PWmu)), NM').Idha)

%send login request M1={P, NM, IDha} to the FA
∧SND(P'.NM.Idha)

%Authentication phase
%Receive message M4={T, NF, IDfa}
3. State = 4 ∧RCV(xor(xor(xor(H(K1.NM.NF.IDmu.IDfa.IDha),
H(NM.IDfa)), H(NM.NF))) =|>

State' := 5
∧R':=xor(xor(xor(H(K1.NM.NF.IDmu.IDfa.IDha),H(NM.IDfa)),
H(NM.NF)),H(NM.NF))

∧SK' :=xor(H(K1.NM.NF.IDmu.IDfa.IDha), H(NM.IDfa))
end role
```

Figure 4.3 HLPSL implementation for the mobileuser role

```
role foreignagent(MU, HA, FA : agent,
SKmuha: symmetric_key,
H: hash_func,
SND, RCV: channel(dy))

played_by FA

def=
local State :nat, IDmu, PWmu, S, X, NM, NF, K1, IDha, IDfa,
R, T, K, P, Q, SK, Kfh, M2 :text

const nm,nf,s1,s2,s3,s4 : protocol_id

init State := 0
transition
%Login phase
% Receive login request M1={P, NM, IDha} from MU

1. State = 0 ∧RCV(H(xor(xor(xor(H(IDmu.X),H(IDmu.Pwmu)),
H(IDmu.Pwmu)),
NM).IDha)) =|>

State' :=1 ∧secret(IDmu,s1,MU,HA)

∧secret(PWmu,s2,MU)
∧secret(X,s3,HA)
∧secret(Kfh,s4,FA)

∧ NF' := new()
%send message M2={P, NM, IDha, NF, IDfa} to HA

∧SND(H(xor(xor(xor(IDmu.X),H(IDmu.Pwmu)),H(IDmu.Pwmu)),
NM).NM.Idha.NF.Idfa)

%FA freshly generated random no. Nf for HA
%Reccieve message M3={Q, IDha} from HA

2. State=2 ∧RCV(xor(H(K1.NM.NF.IDmu.IDfa.IDha), H(Kfh.NF.Idfa)).
IDha) =|>

State' :=3 ∧SK' :=xor(xor(H(K1.NM.NF.Idmu.Idfa.Idha),H(Kfh.NF.Idfa)),
H(Kfh.NF.Idfa))

∧R' := xor(H(K1.NM.NF.IDmu.IDfa.IDha),H(NM.IDfa))
∧T' :=xor(xor(H(K1.NM.NF.IDmu.IDfa.IDha),H(NM.IDfa)), H(NM.NF))
%FA sends message M4={T, NF, IDfa} to MU

∧SND(xor(xor(H(K1.NM.NF.Idmu.Idfa.Idha),H(NM.Idfa)),
H(NM.NF)).NF.Idfa)

end role
```

Figure 4.4 HLPSL implementation for the foreignagent role

```
role homeagent(MU, HA, FA : agent,
SKmuha: symmetric_key,
H: hash_func,
SND, RCV: channel(dy))

played_by HA

Def=

local State :nat,

IDmu, PWmu, S, X, NM, NF, K1, IDha, IDfa, R, T, K,

 P, Q, SK, Kfh :text

const nm,nf,s1,s2,s3,s4 : protocol id

init State := 0

transition
1. State = 0 ∧RCV(IDmu.PWmu_SKmuha) =|>

State' := 3 ∧secret(IDmu,s1,MU,HA)

∧secret(PWmu,s2,MU)

∧K1' := H(IDmu.X)
∧S' := xor(H(IDmu.PWmu), H(IDmu.X))

∧secret(X, s3, HA)

∧secret(Kfh, s4, FA)

%send smart card to MU securely

∧SND(S.H_SKmuha)
% Authentication phase
%Receive message M2={P, NM, IDha, NF, Idfa}

2. State = 3 ∧RCV(H(xor(xor(xor(H(IDmu.PWmu),
H(IDmu.X)), H(IDmu.PWmu)), NM').Idha).NM.
IDha.NF.IDfa) =|>

State' := 4 ∧SK := H(K1.NM.NF.IDmu.IDfa.IDha)
∧Q' :=xor(H(K1.NM.NF.Idmu.Idfa.Idha),
H(Kfh.NF.Idfa))

∧ SND(Q'.Idha)

end role
```

Figure 4.5 HLPSL implementation for the homeagent role

```
role session(MU,HA,FA : agent,
SKmuha: symmetric_key,
H: hash_func)

def=
local SD1, SD2, SD3, RV1, RV2, RV3 : channel(dy)

Composition

mobileuser(MU,HA,FA,Skmuha,H,SD1,RV1)

/\ foreignagent(MU,HA,FA,Skmuha,H,SD2,RV2)

/\ homeagent(MU,HA,FA,Skmuha,H,SD3,RV3)

end role
```

Figure 4.6 HLPSL implementation for the session role

```
role environment()

def=
const mu, fa, ha : agent,
skmuha: symmetric_key,
h : hash func,
idha, idfa,p : text,

mu_fa_nm,fa_ha_nf: protocol id,
s1,s2,s3,s4 : protocol id

intruder_knowledge=mu,fa,ha,h,idha,idfa,p

composition

session(mu, ha, fa, skmuha, h)

∧session(i, ha, fa, skmuha, h)
∧session(mu, i, fa, skmuha, h)

∧session(mu, ha, i, skmuha, h)

end role

goal
secrecy_of s1, s2, s3, s4

authentication_on mu_fa_nm
authentication_on fa_ha_nf

end goal

environment()
```

Figure 4.7 HLPSL implementation for the goal and environment role

```
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/span/testsuite/results/aina.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.04s
visitedNodes: 8 nodes
depth: 3 plies
```

Figure 4.8 Result of the analysis using OFMC backend

4.7 Performance analysis and comparison

This section evaluates performance of the proposed scheme with the others schemes like Gope and Hwang (2016a), Wu et al. (2016) and Lee et al. (2017) in terms of security and functional features, computational costs and communication costs.

4.7.1 Comparison of security and functional features

Table 4.3 Functionality comparison

Security Requirements	**Proposed Scheme**	A	B	C
User anonymity is protected	✓	×	×	✓
Mutual authentication is achieved	✓	✓	✓	✓
Security against insider attack	✓	✓	×	✓
Security against off-line password guessing attack	✓	×	×	✓
Security against replay attack	✓	×	×	×
Perfect forward secrecy achieved	✓	×	✓	×
Security against stolen-verifier attack	✓	×	✓	✓
Local password verification achieved	✓	✓	✓	×
Fair Key Agreement achieved	✓	×	✓	×
No time synchronization	✓	✓	✓	✓
User friendliness	✓	✓	✓	×

A: Gope and Hwang (2016a), *B*: Wu et al. (2016), *C*: Lee et al. (2017)

It is clearly evident from Table 4.3 that the related schemes failed to resist security attack like replay attack. Fan Wu et al.'s scheme could not protect user anonymity and could not resist security attacks like insider attack and offline password guessing attack. Lee et al.'s scheme could not achieve security goals like perfect forward secrecy, local password verification and fair key agreement. Their scheme failed to resist the insider attack. Gope and Hwang scheme could not protect user anonymity and failed to achieve security goals like perfect forward secrecy, fair key agreement. They also failed to resist security attacks like offline password guessing attack, stolen verifier attack and replay attack. Whereas, the proposed scheme achieves all the security goals and resists all the security attacks. In comparison with other schemes the proposed scheme resists the

active security attacks which is presented in simulation results using AVISPA tool. The proposed scheme also resists the security attacks like offline password guessing attack, stolen smart card attack, impersonation attack and replay attack. Thus, our scheme achieves all the desirable security functionality features.

4.7.2 Comparison of computational costs

Table 4.4 summarizes the computational cost of the registration phase of the proposed scheme along with the other schemes namely Gope and Hwang scheme Fan Wu et al.'s scheme and Lee et al.'s scheme.

Table 4.4 Computational cost comparison for registration phase

Entities	**Proposed Scheme**	**Gope and Hwang (2016a)**	**Wu et al. (2016)**	**Lee et al. (2017)**
C_{MU}	$0T_h$+$0T_{\oplus}$+$0T_{\|\|}$	$2T_h$+$2T_{\oplus}$+$2T_{\|\|}$	$2T_h$+$1T_{\oplus}$+$2T_{\|\|}$	$1T_h$+$2T_{\oplus}$
C_{HA}	$2T_h$+$1T_{\oplus}$+$2T_{\|\|}$	$3T_h$+$2T_{\oplus}$+$3T_{\|\|}$	$3T_h$+$2T_{\oplus}$+$4T_{\|\|}$	$3T_h$+$2T_{\oplus}$+$1T_{\|\|}$

Table 4.5 summarizes the computational cost of the login and authentication phase of the proposed scheme. Computational cost is calculated based on the number of operations used by MU, FA and HA respectively during communication. Hash functions are denoted as T_h. XOR operations are denoted as $T_{\oplus}$. Concatenation operations are denoted as $T_{||}$. C_{MU}, C_{FA}, C_{HA} represents the computations of MU, FA and HA respectively. The total number of operations used by Gope and Hwang to design an authentication scheme are 15 T_h, 16 $T_{\oplus}$ and 31 $T_{||}$. The total number of operations used by Fan Wu et al. to design an authentication scheme are 31 T_h, 17 $T_{\oplus}$ and 74 $T_{||}$. The total number of operations used by Lee et al. to design an authentication scheme are 30 T_h, 18 $T_{\oplus}$ and 28 $T_{||}$. Whereas, the proposed scheme uses 16 T_h, 13 $T_{\oplus}$ and 27 $T_{||}$. The proposed scheme requires lesser computations when compared with other schemes. Thus, the proposed scheme operates in less communication cost.

Table 4.5 Computational cost comparison for login and authentication phase

Entities	**Proposed Scheme**	**Gope and Hwang (2016a)**	**Wu et al. (2016)**	**Lee et al. (2017)**
C_{MU}	$7T_h$+$6T_{\oplus}$+$11T_{||}$	$6T_h$+$6T_{\oplus}$+$6T_{||}$	$10T_h$+$8T_{\oplus}$+$21T_{||}$	$11T_h$+$9T_{\oplus}$+$8T_{||}$
C_{FA}	$4T_h$+$4T_{\oplus}$+$6T_{||}$	$1T_h$+$3T_{\oplus}$+$2T_{||}$	$5T_h$+$1T_{\oplus}$+$16T_{||}$	$8T_h$+$3T_{\oplus}$+$9T_{||}$
C_{HA}	$3T_h$+$2T_{\oplus}$+$8T_{||}$	$3T_h$+$3T_{\oplus}$+$18T_{||}$	$11T_h$+$5T_{\oplus}$+$31T_{||}$	$7T_h$+$2T_{\oplus}$+$10T_{||}$

4.7.3 Comparison of communication costs

Table 4.6 Communication overhead comparison of the proposed scheme with other schemes

Scheme	Handshakes	Communication overhead
Proposed scheme	4 messages	2080 bits
Gope and Hwang (2016a)	4 messages	2688 bits
Wu et al. (2016)	4 messages	5696 bits
Lee et al. (2017)	5 messages	2400 bits

Table 4.6 summarizes about handshakes and communication overhead between the proposed scheme and other schemes, namely Gope and Hwang scheme, Fan Wu et al.'s scheme and Lee et al.'s scheme for login and authentication phase. We assume that the SHA-1 hash function requires 160-bits (Eastlake 3rd and Jones, 2001). Time-stamp requires 32 bits, user identity requires 160 bits, random numbers/nonce requires 160 bits. In the proposed scheme the login message $M_1 = \{P, N_m, ID_{HA}\}$ requires (160+160+160)=480 bits, $M_2 = \{P, N_m, ID_{HA}, N_f, ID_{FA}\}$ requires (160+160+160+160+ 160)=800 bits, $M_3 = \{Q, ID_{HA}\}$ requires (160+160)=320 bits and $M_4 = \{T, N_f, ID_{FA}\}$ requires (160+160+160)=480 bits. Thus the computational overhead of the proposed scheme is 480+800+320+480=2080 bits. Gope and Hwang's scheme requires total 2688 bits. Fan Wu et al.'s scheme requires total 5696 bits and Lee et al.'s scheme requires total 2400 bits. Thus the proposed scheme takes less communication overhead compared to other schemes. Hence the proposed scheme is more suitable for the practical implementation.

4.8 Summary

In this chapter, with the thorough cryptanalysis of Gope and Hwang's scheme, we are able to prove the scheme is vulnerable to many security attacks, further their scheme also fails to achieve some of the security goals. To improvise their scheme and to provide better security, a new scheme is proposed. The proposed scheme is resilient to the security attacks like MU impersonation, stolen smart card, offline password guessing and replay attack. The proposed scheme also achieves the security goals like user anonymity, perfect forward secrecy and mutual authentication. Secret key is computed using Diffie-Hellman key exchange protocol, this secret key is exchanged between the two entities FA and HA during communication to authenticate each other. The proposed scheme is proved using BAN logic. Furthermore, the proposed scheme is simulated using AVISPA tool to formally verify whether the proposed scheme is secure against active and passive security attacks. In comparison with the computational cost and communication overhead of the proposed scheme with the other related schemes such as Gope and Hwang's scheme, Fan Wu et al.'s scheme and Lee et al.'s scheme, the proposed scheme operates with less cost and less communication overhead. Therefore, the proposed scheme is more robust and practically implementable.

CHAPTER 5

ES-AKA: An Efficient and Secure Authentication and Key Agreement Protocol for GSM Network

5.1 Introduction

In this chapter, Fan Wu et al.'s scheme on user authentication has been reviewed, with the thorough cryptanalysis of their scheme we proved that their scheme is vulnerable to replay attack, insider attack, stolen smart card attack, offline password guessing attack and impersonation attack. Further, their scheme could not protect user anonymity. To overcome these security issues, we have proposed a new scheme.

The remainder of this chapter is organized as follows. Section 5.2 reviews Fan Wu et al.'s scheme. Cryptanalysis of Fan Wu et al.'s scheme is explained in section 5.3. An enhanced and secure two-factor user authentication scheme for roaming service in global mobility networks is proposed in Section 5.4. In Section 5.5, security analysis of the proposed scheme is described. Section 5.6 shows the simulation results of the proposed scheme using formal verification AVISPA tool. In section 5.7, the performance of the new proposed scheme is compared with the Fan Wu et al.'s scheme and other existing schemes. Section 5.8 concludes the chapter.

5.2 Review of Fan Wu et al.'s scheme

Fan Wu et al. (2016) proposed a novel two factor authenticaion scheme. Their scheme consists of 3 phases, namely registration phase, mutual authentication and key agreement and password renewal phase. The notations and cryptographic functions used in

this paper are defined in Table 5.1.

5.2.1 Registration phase

1. MU chooses his/her identity ID_{MU} and password PW_{MU}. Then he/she generates a random number b_{MU}, calculates $HPW_{MU} = h(PW_{MU}||b_{MU})$ and sends $\{ID_{MU}, HPW_{MU}\}$ to HA via secure channel.

2. After receiving $\{ID_{MU}, HPW_{MU}\}$ from MU, HA stores ID_{MU} in its database and generates a pseudo random string PID_{MU} corresponding to ID_{MU}. Then it computes $B_1 = h(PID_{MU}||ID_{HA}||x) \oplus HPW_{MU}$
   $B_2 = h(ID_{MU}||x) \oplus h(ID_{MU}||HPW_{MU})$. Smart card is personalised with the parameters $\{B_1, B_2, PID_{MU}, ID_{HA}\}$. HA sends smart card to MU via secure channel.

3. On receiving the smart card, MU computes
   $B_3 = h(ID_{MU}||PW_{MU}) \oplus b_{MU}$. Finally B_3 is stored in the smart card.

Table 5.1 Notations and cryptographic functions

Symbol	Definition
MU	Mobile User
FA	Foreign Agent
HA	Home Agent
ID_{MU}	MU's identity
PW_{MU}	MU's password
ID_{HA}	HA's identity
ID_{FA}	FA's identity
SK	Session key between FA and MU
K_{fh}	Secret key shared between the FA and HA
$E_k(.)$	The symmetric encryption function with the key k
$D_k(.)$	The symmetric decryption function with the key k
P	Large prime number
X	Secret key of HA
x	HA's secret key of Fan Wu et al.'s scheme
N_m	Random number of MU
b_{MU}	Random number of MU
N_f	Random number of FA
Z_N^*	$Z_N^* \stackrel{def}{=} \{x \in Z_N : gcd(x,N) = 1\}$ = elements of Z_N with multiplicative inverses.

5.2.2 Mutual authentication and key agreement(MAKA)

MU inserts his/her ID_{MU} and PW_{MU} into the smart card terminal and smart card generates a random numbers N_m and $\alpha \in Z_n^*$. Smart card terminal computes the following

1. $b_{MU} = B_3 \oplus h(ID_{MU}||PW_{MU})$
   $HPW_{MU} = h(PW_{MU}||b_{MU})$
   $C_1 = B_1 \oplus HPW_{MU} \oplus N_m$
   $C_2 = h(N_m||PID_{MU}||ID_{HA}) \oplus ID_{MU}$
   $C_3 = \alpha P$
   $C_4 = h(N_m||PID_{MU}||ID_{MU}||C_3)$.
   After computations, MU submits the message $M_1 = \{PID_{MU}, C_1, C_2, C_3, C_4, ID_{HA}\}$ to FA.

2. On receiving the message M_1 from MU. FA generates the random numbers N_f and $\beta \in Z_n^*$ and computes the following
   $C_5 = \beta P$
   $C_6 = E_{K_{fh}(N_f)} \oplus h(C_3||C_5)$
   $C_7 = h(PID_{MU}||C_1||C_2||C_3||C_4||C_5||N_f)$.
   FA sends the message $M_2 = \{PID_{MU}, C_1, C_2, C_3, C_4, C_5, C_6, C_7, ID_{FA}\}$ to HA.

3. HA after receiving the message
   $M_2 = \{PID_{MU}, C_1, C_2, C_3C_4, C_5, C_6, C_7,$
   $ID_{FA}\}$ from FA, computes the following
   $N_m = C_1 \oplus h(PID_{MU}||ID_{HA}||x)$
   $ID_{MU} = C_2 \oplus h(N_m||PID_{MU}||ID_{HA})$.
   Searches for ID_{MU} in its database. Verifies if
   $C_4 \stackrel{?}{=} h(N_m||PID_{MU}||ID_{MU}||C_3)$. If it is true, HA decrypts
   $N_f = D_{K_{fh}}(C_6 \oplus h(C_3||C_5))$ and verifies if
   $C_7 \stackrel{?}{=} h(PID_{MU}||C_1||C_2||C_3||C_4||C_5||N_f)$.
   If it is true, HA further generates PID_{MU}^{new} a new pseudo identity for MU and computes $C_8 = h(ID_{MU}||x)$
   $C_9 = h(PID_{MU}^{new}||ID_{HA}||x)$

$C_{10} = C_9 \oplus h(C_8||N_m)$

$C_{11} = h(C_8||C_3||C_5||N_m) \oplus PID_{MU}^{new}$

$C_{12} = h(C_9||N_m||ID_{MU}||PID_{MU}||PID_{MU}^{new}||ID_{HA})$

$C_{13} = h(K_{fh}||N_f||C_3||C_5||ID_{FA}||ID_{HA})$.

HA forms a message $M_3 = \{C_{10}, C_{11}, C_{12}, C_{13}\}$ and submits it to FA.

4. On receiving message $M_3 = \{C_{10}, C_{11}, C_{12}, C_{13}\}$ from HA, FA verifies if $C_{13} \stackrel{?}{=} h(K_{fh}||N_f||C_3||C_5||ID_{FA}||ID_{HA})$. If it is true, FA computes the session key as follows $SK_{FA} = h(C_3||C_5||\beta C_3)$

   $C_{14} = h(SK_{FA}||PID_{MU}||ID_{HA})$ and sends the message $M_4 = \{C_5, C_{10}, C_{11}, C_{12}, C_{14}\}$ to MU.

5. After receiving message

   $M_4 = \{C_5, C_{10}, C_{11}, C_{12}, C_{14}\}$ from FA, smart card computes the following

   $C_{15} = B_2 \oplus h(ID_{MU}||HPW_{MU})$

   $C_{16} = C_{10} \oplus h(C_{15}||N_m)$

   $PID_{MU}^{new} = C_{11} \oplus h(C_{15}||C_3||C_5||N_m)$.

   Verifies if $C_{12} \stackrel{?}{=} h(C_9||N_m||ID_{MU}||PID_{MU}||PID_{MU}^{new}||ID_{HA})$.

   If it is true, smart card computes the session key as follows

   $SK_{MU} = h(C_3||C_5||\alpha C_5)$. Verifies if $C_{14} \stackrel{?}{=} h(SK_{MU}||PID_{MU}||ID_{HA})$. If it holds true, then smart card computes

   $B_1^{new} = C_{16} \oplus HPW_{MU}$. $\{B_1, PID_{MU}\}$ is updated with $\{B_1^{new}, PID_{MU}^{new}\}$.

5.2.3 Password renewal phase

1. After MU inserts ID_{MU} and PW_{MU} into the smart card terminal, the terminal calculates b_{MU} and HPW_{MU} as illustrated in MAKA phase. Random number N_m is selected and the data C_1, C_2, C_{15} and $C_{17} = h(N_m||PID_{MU}||ID_{MU}||C_{15})$ are computed. Finally MU submits $M_5 = \{PID_{MU}, C_1, C_2, C_{17}\}$ to HA along with the request for password change.

2. On receiving M_5, HA computes for N_m and ID_{MU} and verifies if the received ID_{MU} is stored in its database or not, if it exists, C_7 is calculated and $C_{17} \stackrel{?}{=}$

$h(N_m||PID_{MU}||ID_{MU}||C_7)$ is verified. If it is true, a random string PID_{MU}^{new} is generated by HA and the following calculations are done

$C_9, C_{18} = h(N_m||ID_{MU}||PID_{MU}||C_7) \oplus PID_{MU}^{new}$

$C_{19} = h(C_7||N_m||PID_{MU}^{new}||ID_{MU}) \oplus C_9$

$C_{20} = h(C_7||N_m||PID_{MU}^{new}||C_9||ID_{MU})$.

Finally HA submits message $M_6 = \{C_{18}, C_{19}, C_{20}\}$ to MU.

3. Now the smart card calculates

$PID_{MU}^{new} = C_{18} \oplus h(N_m||ID_{MU}||PID_{MU}||C_{15})$

$C_{21} = C_{19} \oplus h(C_{15}||N_m||PID_{MU}^{new}||ID_{MU})$ and verifies whether,

$C_{20} \stackrel{?}{=} h(C_{15}||N_m||PID_{MU}^{new}||C_{21}||ID_{MU})$. If it holds true, MU inputs a new password PW_{MU}^{new} and then smart card generates a new random number b_{MU}^{new} and computes the following

$HPW_{MU}^{new} = h(PW_{MU}^{new}||b_{MU}^{new})$

$B_1^{new2} = C_{21} \oplus HPW_{MU}^{new}$

$B_2^{new} = C_{14} \oplus h(ID_{MU}||HPW_{MU}^{new})$.

$B_3^{new} = h(ID_{MU}||PW_{MU}^{new}) \oplus b_{MU}^{new}$.

Finally the smart card with the parameters $\{PID_{MU}, B_1, B_2, B_3\}$ are replaced with $\{PID_{MU}^{new}, B_1^{new}, B_2^{new}, B_3^{new}\}$.

5.3 Cryptanalysis of Fan Wu et al.'s scheme

In this section cryptanalysis of Fan Wu et al.'s scheme has been done.

5.3.1 User anonymity is not protected

In Fan Wu et al.'s scheme during the registration phase, MU sends the message $\{ID_{MU}, HPW_{MU}\}$ to HA via secure channel. On receiving the message, HA stores the identity of the mobile user ID_{MU} in its database. One of the basic design goals of the two factor authentication schemes in GLOMONET is not to maintain the verifier table in the server. User specific information like $\{ID_{MU}, PW_{MU}\}$ should not be stored in the verifier table. The reason being, in case the server's verifier table is compromised, adversary can easily reveal user related information, such schemes does not achieve the

desirable security attribute user anonymity. Therefore, we conclude that Fan Wu et al.'s scheme does not achieve user anonymity.

5.3.2 Vulnerable to stolen smart card attack

In this attack, if MU's Smart Card (SC) is stolen or lost and falls in the hands of an adversary, he/she can extract the parameters $\{B_1, B_2, B_3, PID_{MU}, ID_{HA}\}$ stored in the SC as described in the literatures (Kim et al., 2012; Kocher et al., 1998; Messerges et al., 2002; Nohl et al., 2008). Fan Wu et al.'s scheme stores user specific information ID_{MU} in the verifier table as discussed in section 5.3.1. In case, the server is compromised adversary can easily reveal ID_{MU}. With the available SC parameters $\{B_1, B_2, B_3, PID_{MU}, ID_{HA}\}$ and ID_{MU}. Adversary computes $b'_{MU} = B_3 \oplus h(ID_{MU}||PW^*_{MU})$. Adversary can guess the password PW^*_{MU} within the password space $|D_{pw}| = 10^6$ (Bonneau, 2012). Having obtained the random number b'_{MU}, he/she computes $B^*_3 = b'_{MU} \oplus h(ID_{MU}||PW^*_{MU})$. Verifies if $B^*_3 \stackrel{?}{=} B_3$. If it holds true, guessed password is the real password. Thus with the stolen SC, the password of the mobile user can be revealed. In the second scenario, during the MAKA phase adversary who has control over the communication channel can intercept the login messages (Bellare et al., 2000; Wang et al., 2012). By intercepting the login message $M_1 = \{PID_{MU}, C_1, C_2, C_3, C_4, ID_{HA}\}$. Adversary computes $HPW_{MU} = h(PW^*_{MU}||b'_{MU})$, $N_m = B_1 \oplus HPW_{MU} \oplus C_1$ $C_4 = h(N_m||PID_{MU}||ID_{MU}||C_3)$. By computing the parameter C_4 adversary can impersonate a valid MU by sending message M_1, HA validates the authenticity of the MU based on the parameter C_4. Thus with the stolen or lost SC adversary can reveal the password PW_{MU} of the mobile user and also can impersonate a valid MU. Therefore Fan Wu et al.'s scheme is vulnerable to stolen smart card attack.

5.3.3 Vulnerable to offline password guessing attack

Adversary can launch the offline password guessing attack by possessing the MU's Smart Card (SC) either by stealing or finding the lost SC. Adversary can extract the SC parameters $\{B_1, B_2, B_3, PID_{MU}, ID_{HA}\}$ discussed in section 5.3.2 and reveals the parameter ID_{MU} discussed in section 5.3.1. With the available parameters adversary computes

1. $b_{MU}^{'} = B_3 \oplus h(ID_{MU}||PW_{MU}^{*})$.
   Adversary can guess the password PW_{MU}^{*} within the password space $|D_{pw}| = 10^6$. Having obtained the random number $b_{MU}^{'}$, he/she computes

2. $B_3^{*} = b_{MU}^{'} \oplus h(ID_{MU}||PW_{MU}^{*})$.
   Verifies if, $B_3^{*} \stackrel{?}{=} B_3$. If does not holds true go back to step 1.

3. Else, repeat steps 1-2, until the correct password is found. The correct password is found only if the verification in step 2 holds true.

The running time of the aforementioned attack procedure is $\mathcal{O}(|D_{pw}| * 2T_h)$, where T_h is running time for hash function. The time to recover MU's password PW_{MU} is a linear function of $|D_{pw}|$. Hence this attack is quiet effective. Thus Fan Wu et al.'s scheme is vulnerable to offline password guessing attack.

5.3.4 Vulnerable to impersonation attack

An adversary can impersonate a valid mobile user by leaking out the real identity of the mobile user ID_{MU} that is stored in HA's database as discussed in section 5.3.1. By extracting the stolen smart card parameters $\{B_1, B_2, B_3, PID_{MU}, ID_{HA}\}$ and eavesdropping the login messages $M_1 = \{PID_{MU}, C_1, C_2, C_3, C_4, ID_{HA}\}$ and
$M_2 = \{PID_{MU}, C_1, C_2, C_3, C_4, C_5, C_6, C_7, ID_{FA}\}$ transmitted on the public channel during MAKA phase. Adversary computes the following

1. $b_{MU}^{'} = B_3 \oplus h(ID_{MU}||PW_{MU}^{*})$, where PW_{MU}^{*} is the guessed password trails made by an adversary, for every guessed PW_{MU}^{*}, a random number $b_{MU}^{'}$ is obtained, which is used to compute $HPW_{MU} = h(PW_{MU}^{*}||b_{MU}^{'})$
   $N_m = C_1 \oplus B_1 \oplus HPW_{MU}$
   $C_4^{'} = h(N_m||PID_{MU}||ID_{HA})$, where ID_{HA} is taken from the stolen smart card and then verifies if $C_4^{'} \stackrel{?}{=} C_4$. If it is true, then adversary has guessed the password correctly. Otherwise, he/she will repeat for the password trails. After that new random number $N_m^{'}$ is chosen by an adversary. He/she computes
   $C_1^{*} = B_1 \oplus HPW_{MU} \oplus N_m^{'}$
   $C_2^{*} = h(N_m^{'}||PID_{MU}||ID_{HA}) \oplus ID_{MU}$

$C_4^* = h(N_m^{'}||PID_{MU}||ID_{HA})$ adversary sends message
$M_1^{'} = \{PID_{MU}, C_1^*, C_2^*, C_3, C_4^*, ID_{HA}\}$ to FA, FA sends it to HA. On receiving the message $M_1^{'}$. HA computes $N_m^{'} = C_1^* \oplus h(PID_{MU}||ID_{HA}||x)$
$ID_{MU} = C_2^* \oplus h(N_m^{'}||PID_{MU}||ID_{HA})$ and searches for ID_{MU} in its database.
Verifies if $C_4^* \stackrel{?}{=} h(N_m^{'}||PID_{MU}||ID_{HA})$. Obviously both are equal. Hence HA believes that an adversary is a valid mobile user. In case of FA, adversary can compute the following to impersonate a FA.

2. $E_{K_{fh}}(N_f) = C_6 \oplus h(C_3||C_5)$.

3. Adversary computes C_7^* with all the parameters available from the message M_2 and inserts the obtained value $E_{K_{fh}}(N_f)$ into C_7^*, computed as
$C_7^* = h(PID_{MU}||C_1||C_2||C_3||C_4||C_5||E_{K_{fh}}(N_f))$. Adversary generates the message $M_2^{'} = \{PID_{MU}, C_1, C_2, C_3, C_4, C_5, C_6, C_7^*, ID_{FA}\}$ and sends it to the HA. On receiving the message $M_2^{'}$, HA computes $E_{K_{fh}}(N_f) = C_6 \oplus h(C_3||C_5)$. Verifies if $C_7^* \stackrel{?}{=} h(PID_{MU}||C_1||C_2||C_3||C_4||C_5||C_6||C_7||E_{K_{fh}}(N_f))$ and believes it to be a valid FA. Hence the scheme is not resistant to the impersonation attack.

5.3.5 Vulnerable to replay attack

During the MAKA phase, adversary who listens to the communication on the public channel can eavesdrop the messages $M_1 = \{PID_{MU}, C_1, C_2, C_3, C_4, ID_{HA}\}$ and $M_2 = \{PID_{MU}, C_1, C_2, C_3, C_4, C_5, ID_{FA}\}$ transmitting on the public channel. Values HPW_{MU}, N_m and $N_m^{'}$ are calculated in section 5.3.4. With these values adversary computes the following. $C_1^* = B_1 \oplus HPW_{MU} \oplus N_m^{'}$
$C_2^* = h(N_m^{'}||PID_{MU}||ID_{HA}) \oplus ID_{MU}$
$C_4^* = h(N_m^{'}||PID_{MU}||ID_{HA})$. He/she replays the message
$M_1^{'} = \{PID_{MU}, C_1^*, C_2^*, C_3, C_4^*, ID_{HA}\}$ and sends it to FA, FA sends it to HA. On receiving the message $M_1^{'}$, HA proceeds with its computations to verify the authenticity of the MU. $N_m^{'} = C_1^* \oplus h(PID_{MU}||ID_{HA}||x)$
$ID_{MU} = C_2^* \oplus h(N_m^{'}||PID_{MU}||ID_{HA})$ and searches for ID_{MU} in its database and verifies if $C_4^* \stackrel{?}{=} h(N_m^{'}||PID_{MU}||ID_{HA})$. It holds true, thus HA believes that the message is received from an authorised MU. Therefore Fan Wu et al.'s scheme cannot resist the

replay attack.

5.3.6 Vulnerable to insider attack

In Fan Wu et al.'s scheme during the registration phase, MU sends HPW_{MU} to HA over secure channel. Suppose an insider who is authorised to use computers and networks of the server acts as an adversary, then he/she can easily steal the MU's password PW_{MU}. To obtain PW_{MU} from HPW_{MU} which is computed as $HPW_{MU} = h(PW_{MU}||b_{MU})$, adversary exhaustively chooses the random number b'_{MU} for every guessed password PW^*_{MU} within the password space $|D_{pw}| = 10^6$ (Bonneau, 2012). By launching offline dictionary attack adversary guesses the password PW^*_{MU} and chooses a random number b'_{MU}. For for every guessed PW^*_{MU} and b'_{MU} adversary uses the hash function and computes HPW^*_{MU}. Verifies if $HPW^*_{MU} \stackrel{?}{=} HPW_{MU}$. If it holds true, then the guessed PW^*_{MU} and b'_{MU} are the real values. Thus an adversary will be successful in revealing the password. Therefore, Fan Wu et al.'s scheme is vulnerable to insider attack.

5.4 Proposed scheme

The proposed scheme involves three entities Mobile User (MU), Foreign Agent (FA) and Home Agent (HA) and communication between these three entities are carried in four phases. They are: initialization phase, registration phase, authentication and key agreement phase and password change phase. The proposed scheme makes use of Diffie-Hellman key exchange protocol (Diffie and Hellman, 1976) to compute secret key K_{fh} exchanged between FA and HA. The proposed scheme also uses of elliptic curve cryptography. The domain parameters $\{E_{(F_p)}, G, a, b, p\}$ of the elliptic curve cryptography are shared among the three communicating entities. A brief introduction to ECC is as follows.

5.4.1 Initialization phase

1. HA chooses its random number r_h and computes its secret key $X = r_h P$. HA stores $\{r_h, P, N\}$ in its database, where N is a large prime number.

2. During initialization phase, MU and HA shares symmetric encryption key E_k over secure channel.

3. Each foreign network participating in the communication submits its ID_{FA} to HA over secure channel.

4. On receiving ID_{FA}, HA computes SK_{FA} using Diffie-Hellman key exchange protocol. HA sends SK_{FA} to FA over secure channel.

5. Each foreign agent stores the secret key SK_{FA} computed by HA.

5.4.2 Registration phase

The registration phase is illustrated in the Fig. 5.1.

Mobile User **HomeAgent**

Step 1: MU chooses his/her own $\{ID_{MU}, PW_{MU}\}$

$\{ID_{MU}\}$ →

Step 2 : $A_1 = h(ID_{MU} || X) \oplus N$

Smart card $\{A_1, E_{Fp}, p, G, ID_{HA}\}$ ←

Step 3 : $A_2 = h(h(ID_{MU}) \oplus h(PW_{MU}))$.

Finally MU inserts A_2 into the smart card .

Smart card is now personalised with the parameters $\{A_1, A_2, ID_{HA}, E_{Fp}, p, G, h(.)\}$

Figure 5.1 Registration phase

1. MU chooses his/her identity ID_{MU} and password PW_{MU} and sends $\{ID_{MU}\}$ to HA.

2. HA on receiving ID_{MU} from MU, computes $A_1 = h(ID_{MU}||X) \oplus N$, where N is a large prime number and X is secret key of HA. HA sends the Smart Card (SC) personalised with the parameters $\{A_1, E_{F_p}, p, G, ID_{HA}\}$ to MU.

3. MU on receiving the SC with the parameters $\{A_1, E_{F_p}, p, G, ID_{HA}\}$, computes $A_2 = h(h(ID_{MU}) \oplus h(PW_{MU}))$. Stores A_2 into the smart card. Finally the SC contains $\{A_1, A_2, E_{F_p}, p, G, ID_{HA}\}$.

5.4.3 Mutual authentication and key agreement phase (MAKA)

The MAKA phase is illustrated in the Figure 5.2.The steps involved in the MAKA phase are as follows.

1. When MU inserts the smart card into the smart card reader, he/she inputs the login credentials $\{ID_{MU}, PW_{MU}\}$. Smart card generates two random numbers $R_m \in Z_n^*, N_{mu}$ and computes $A_2^* = h(h(ID_{MU}) \oplus h(PW_{MU}))$.
   Verifies if $A_2^* \stackrel{?}{=} A_2$ is true or not, if it is true the authenticity of the MU is verified and proceeds further for computations. Else, terminates the request.
   $C_1 = E_k(ID_{MU})$
   $C_2 = R_m P$
   $C_3 = h(A_1||C_1||C_2) \oplus N_{mu}$.
   Finally MU sends the message $M_1 = \{C_1, C_2, C_3, ID_{HA}\}$ to FA.

2. On receiving the message
   $M_1 = \{C_1, C_2, C_3, ID_{HA}\}$ from MU, FA generates two random numbers $R_f \in Z_n^*, N_{fa}$ and computes
   $C_4 = R_f P$
   $C_5 = E_{K_{fh}}(N_{fa})$
   $C_6 = h(C_1||C_2||C_3||C_4||C_5||K_{fh})$.
   Finally, FA sends the message $M_2 = \{C_1, C_2, C_3, C_4, C_5, C_6, ID_{FA}\}$ to HA.

3. On receiving the message
   $M_2 = \{C_1, C_2, C_3, C_4, C_5, C_6, ID_{FA}\}$ from FA. HA decrypts $D_k(E_k(ID_{MU}))$ using decryption key D_k, extracts ID_{MU}. HA computes
   $A_1 = h(ID_{MU}||X) \oplus N$
   $N_{mu} = C_3 \oplus h(A_1||C_1||C_2)$.
   Verifies if $C_3 \stackrel{?}{=} h(A_1||C_1||C_2) \oplus N_{mu}$. If it is true, HA authenticates MU and

Mobile User

Foreign Agent

Home Agent

Generate two random no.'s N_{mu} , $R_m \in Z_n^*$

$A_2^* = h(h(ID_{MU}) \oplus h(PW_{MU}))$. If $A_2^* \stackrel{?}{=} A_1$

$C_1 = E_k(ID_{MU})$

$C_2 = R_m \; P$

$C_3 = h(A_1 || C_1 || C_2) \oplus N_{mu}$

$M_1 = \{C_1, C_2, C_3, ID_{HA}\}$ →

FA generates two random numbers $N_{fa}, R_f \in Z_n^*$ and computes

$C_4 = R_f \; . \; P$

$C_5 = E_{Kfh}(N_{fa})$

$C_6 = h(C_1 || C_2 || C_3 || C_4 || C_5 || K_{fh})$

$M_2 = \{C_1, C_2, C_3, C_4, C_5, C_6, ID_{FA}\}$ →

HA decrypts $D_k(E_k(ID_{MU}))$ using key D_k and extracts ID_{MU}. HA computes

$A_1 = h(ID_{MU} || X) \oplus N$

$N_{mu} = C_3 \oplus h(A_1 || C_1 || C_2)$ and verifies if

$C_3^* \stackrel{?}{=} h(A_1 || C_1 || C_2) \oplus N_{mu}$. If true, HA authenticates MU and computes

$N_{fa} = D_{Kfh}(C_5)$

$C_6 \stackrel{?}{=} h(C_1 || C_2 || C_3 || C_4 || C_5 || K_{fh})$. If true, HA authenticates FA and computes

$C_8 = h(h(ID_{MU} || N_{mu}) || C_2 || ID_{HA})$

$C_9 = h(K_{fh} || N_{fa} || ID_{FA} || ID_{HA} || C_2 || C_4)$

$M_3 = \{C_8, C_9, ID_{HA}\}$ ←

$C_9 \stackrel{?}{=} h(K_{fh} || N_{fa} || ID_{FA} || ID_{HA} || C_2 || C_4)$.

If true, FA computes

$SK = R_f \; . \; C_2$

$C_{10} = h(C_2 || C_4 || SK)$.

$M_4 = \{C_4, C_8, C_{10}, ID_{HA}\}$ ←

$C_8 \stackrel{?}{=} h(h(ID_{MU} || N_{mu}) || C_2 || ID_{HA})$.

If true, MU computes the session key

$SK = R_m \; C_4$

$C_{10} \stackrel{?}{=} h(C_2 || C_4 || SK)$. If true, MU mutually authenticates FA.

Figure 5.2 Mutual authentication and key agreement phase

further computes $N_{fa} = D_{K_{fh}}(C_5)$

$C_6 \stackrel{?}{=} h(C_1||C_2||C_3||C_4||C_5||K_{fh})$. If it is true, HA confirms that the message has come from the trusted FA. HA further computes

$C_8 = h(h(ID_{MU}||N_{mu})||C_2||ID_{HA})$

$C_9 = h(K_{fh}||N_{fa}||ID_{FA}||ID_{HA}||C_2||C_4)$.

Finally, HA sends the message $M_3 = \{C_8, C_9, ID_{HA}\}$ to FA.

4. FA on receiving the message

   $M_3 = \{C_8, C_9, ID_{HA}\}$ from HA will verify for

   $C_9 \stackrel{?}{=} h(K_{fh}||N_{fa}||ID_{FA}||ID_{HA}||C_2||C_4)$.

   If it is true, FA authenticates HA and computes

   $SK = R_f C_2$

   $C_{10} = h(C_2||C_4||SK)$.

   Finally, FA sends the message $M_4 = \{C_4, C_8, C_{10}, ID_{HA}\}$ to MU.

5. MU on receiving the message

   $M_4 = \{C_4, C_8, C_{10}, ID_{HA}\}$ from FA verifies if

   $C_8 \stackrel{?}{=} h(h(ID_{MU}||N_{mu})||C_2||ID_{HA})$.

   If it is true, MU computes the session key,

   $SK = R_m C_4$ and verifies if

   $C_{10} \stackrel{?}{=} h(C_2||C_4||SK)$. If it is true, MU mutually authenticates FA.

5.4.4 Password change phase

MU inputs his/her login credentials $\{ID_{MU}, PW_{MU}\}$. Smart card computes $A_2^* = h(h(ID_{MU}) \oplus h(PW_{MU}^{old}))$. Verifies if $A_2^* \stackrel{?}{=} A_2$ is true or not, if it is true the authenticity of the MU is verified. Else, the password update request is terminated. If the MU, wants to update his/her old password PW_{MU}^{old} with the new password PW_{MU}^{new}, MU computes $A_2^{'} = h(h(ID_{MU}) \oplus h(PW_{MU}^{new}))$. Finally replaces the parameter A_2 with $A_2^{'}$. The smart is now personalised with the parameters $\{A_1, A_2^{'}, E_{F_p}, p, G, ID_{HA}\}$.

5.5 Security analysis

In this section, security analysis of the proposed scheme is explained.

5.5.1 User anonymity is protected

It is imperative for the two factor authentication schemes designed in GLOMONET to protect the user identity one of the crucial security properties. To achieve user anonymity one of the main basic design goal of two factor authentication schemes is not to maintain password verifier table. The server shall only keep the secret keys of MU, FA or HA. Servers should not store any critical user specific information like $\{ID_{MU}, PW_{MU}\}$ in the verifier table, such schemes achieves no user anonymity. The proposed scheme stores no such critical user specific information in the server's database. Suppose during the MAKA phase, an adversary who have control over the insecure communication channel between the three communicating entities MU, FA and HA intercepts the login messages $M_1 = \{C_1, C_2, C_3, ID_{HA}\}$ and $M_2 = \{C_1, C_2, C_3, C_4, C_5, C_6, ID_{FA}\}$, with these login messages adversary can get the parameters $\{C_1, C_3\}$, which are computed as $C_1 = E_k(ID_{MU})$ $C_3 = h(A_1||C_1||C_2) \oplus N_{mu}$. To extract ID_{MU} from C_1 adversary must know the decryption key. The symmetric encryption key E_k is known only to HA and MU. With the C_3 parameter it is difficult for an adversary to compute $A_1 = h(ID_{MU}||X) \oplus N$ as it is difficult to arrive at the secret key X of HA due to Elliptic curve discrete logarithm problem (ECDLP). Therefore, we conclude that the proposed scheme protects user anonymity.

5.5.2 Resistant to the replay attack

During the MAKA phase, the messages exchanged between the entities MU, FA and HA are transmitted over public channel. An adversary who has control over the insecure communication channel can insert, delete and modify the transmitted messages over the public channel. With the interception of the messages $M_1 = \{C_1, C_2, C_3, ID_{HA}\}$ and $M_2 = \{C_1, C_2, C_3, C_4, C_5, C_6, ID_{FA}\}$, if an adversary tries to replay the message M_1 by retransmitting the same message as $M_1^{'}$ to FA for accessing the FA services. FA on receiving the message $M_1^{'}$ computes for $C_4 = R_f P$, $R_f \in Z_n^*$, $C_{10} = h(C_2||C_4||SK)$. FA sends the message $M_4 = \{C_4, C_8, C_{10}, ID_{HA}\}$ to MU. Even after obtaining the parameters $\{C_4, C_{10}\}$, adversary will not be able to compute $SK = R_m C_4$. For every new session the fresh random numbers $\{R_f^{new}, R_m^{new}\} \in Z_n^*$ are generated by FA and MU respectively,

hence it is difficult to compute the session key for an adversary by knowing the parameters C_2, C_4. An adversary cannot arrive at the random numbers $\{R_f, R_m\}$ of $\{C_4, C_2\}$ respectively due to the complexity of Elliptic curve discrete logarithm problem (ECDLP). Besides, we did not use the timestamp mechanism. Therefore, the proposed scheme can avoid replay attack without suffering from synchronization problem of clock.

5.5.3 Resistant to offline password guessing attack

The proposed scheme allows the MU to freely choose his/her PW_{MU}, the passwords chosen by the MU are low entropy and are susceptible to password guessing attacks. In the case of offline password guessing attack, an adversary gets the lost Smart Card (SC) or he/she has stolen the SC. The SC is subjected to SC breach. Adversary will be successful in revealing the parameters $\{A_1, A_2, E_{F_p}, p, G, ID_{HA}\}$ stored in the SC. With the available parameters $\{A_1, A_2\}$ attacker tries to extract PW_{MU} from the parameter A_2. But A_2 is computed as $A_2 = h(h(ID_{MU}) \oplus h(PW_{MU}))$. It is difficult to guess a pair of identity and password $\{ID_{MU}, PW_{MU}\}$ within the identity space $|D_{id}| = 10^6$ and password space $|D_{pw}| = 10^6$. For their exists, $\frac{|D_{id} * D_{pw}|}{2^8} \approx 2^{32}$ candidates of $\{ID_{MU}, PW_{MU}\}$ pairs. The proposed scheme uses the hash function of 256 bit length, n=8. Therefore, we conclude that the proposed scheme is resilient to the offline password guessing attack.

5.5.4 Resistant to stolen smart card attack

When the mobile user's Smart Card (SC) is lost or stolen by an adversary, he/she can extract the SC parameters. With the available SC parameters, adversary can launch the attacks to guess the MU's password and update the password, further he/she can impersonate a valid MU using the SC. In the proposed scheme the SC is personalised with the parameters $\{A_1, A_2, E_{F_p}, p, G, ID_{HA}\}$. By extracting the parameters $\{A_1, A_2\}$ from SC, adversary tries to compute $A_2 = h(h(ID_{MU}) \oplus h(PW_{MU}))$. To arrive at A_2, he/she must guess $\{ID_{MU}, PW_{MU}\}$. If an adversary tries to guess $\{ID_{MU}, PW_{MU}\}$ by offline dictionary attack, he/she fails to arrive at either ID_{MU} or PW_{MU}. Next with the available parameter A_1, adversary tries to compute $A_1 = h(ID_{MU}||X) \oplus N$, where X is the server's secret key computed as $X = r_h P$. It is difficult for an adversary to compute

for X due to the complexity of Elliptic curve discrete logarithm problem (ECDLP). Even if he/she makes guessing trials for ID_{MU} within the $|D_{id}| = 10^6$ which denotes the size of the identity space, arriving at X and N is difficult, which make it difficult for an adversary to compute A_1 with the three unknown values ID_{MU}, X and N. Thus it is difficult for an adversary to guess the pair of $\{ID_{MU}, PW_{MU}\}$. To impersonate a valid MU, during the MAKA phase adversary intercepts the login message $M_1 = \{C_1, C_2, C_3, ID_{HA}\}$ sends it to HA. On receiving the message M_1. HA verifies if $C_3 \stackrel{?}{=} h(A_1||C_1||C_2) \oplus N_{mu}$. If it is true, HA authenticates MU. Therefore, it is difficult for an adversary to forge the values from the available parameters in the message M_1, due to the fact that the proposed scheme uses elliptic curve cryptography and symmetric encryption for the computations. Thus, adversary fails to impersonate a valid MU. Hence the proposed scheme is resilient to the stolen smart card attack.

5.5.5 Resistant to stolen verifier attack

The proposed scheme does not store any critical user specific information like $\{ID_{MU}, PW_{MU}\}$ in the server. In other words, the proposed scheme does not maintain password verifier table in the server. An adversary who tries to steal the plain text passwords or hashed password stored in the password verifier table to impersonate as valid MU, will find no password verification table stored in the server. Thus the proposed scheme is resilient to the stolen verifier attack.

5.5.6 Resistant to impersonation attack

To impersonate a valid MU, adversary needs to generate the login message $M_1 = \{C_1, C_2, C_3, ID_{HA}\}$ and send it to HA. However, adversary can intercept the login messages during MAKA phase as discussed in section 5.5.2 and generates the message M_1. Even after obtaining the message M_1, it is difficult for an adversary to obtain the values with the available parameters in the message M_1. For instance, he/she cannot extract the ID_{MU} from the parameters C_1 and A_1 from C_3 which is discussed in Section 5.5.1. If an adversary retransmits the message M_1 to HA. On receiving the message M_1. HA verifies if $C_3 \stackrel{?}{=} h(A_1||C_1||C_2) \oplus N_{mu}$. If it is true, HA authenticates MU. Thus the proposed scheme is resilient to impersonation attack.

5.5.7 Mutual authentication is achieved

In the proposed scheme mutual authentication is provided between MU FA and HA. All the three entities involved in the communication achieve mutual authentication during the MAKA phase by exchanging the login messages $\{M_1, M_2, M_3\}$. MU sends the login message $M_1 = \{C_1, C_2, C_3, ID_{HA}\}$ to HA. On receiving the message M_1, HA computes $A_1 = h(ID_{MU}||X) \oplus N$, $N_{mu} = C_3 \oplus h(A_1||C_1||C_2)$. Verifies if $C_3 \stackrel{?}{=} h(A_1||C_1||C_2) \oplus N_{mu}$. If it is true, HA authenticates MU. It is not easy for an adversary to forge the value A_1 as discussed in section 5.5.1. FA sends the message $M_2 = \{C_1, C_2, C_3, C_4, C_5, C_6, ID_{FA}\}$ to HA. HA on receiving the message M_2 computes $C_6 \stackrel{?}{=} h(C_1||C_2||C_3||C_4||C_5||K_{fh})$. If it holds true, HA authenticates FA. FA shares the secret key K_{fh} with the HA, hence it is difficult for an adversary to compute for C_6 and to send it to the HA. HA sends the message $M_3 = \{C_8, C_9, ID_{HA}\}$ to FA, FA computes $C_9 \stackrel{?}{=} h(K_{fh}||N_{fa}||ID_{FA}||ID_{HA}||C_2||C_4)$. If it is true, FA authenticates HA. FA then sends the message M_3 to MU. MU on receiving M_3 verifies if $C_8 \stackrel{?}{=} h(h(ID_{MU}||N_{mu})||C_2||ID_{HA})$. If it holds true, MU mutually authenticates HA. Only the authenticated HA can compute for ID_{MU} by decrypting $D_k(E_k(ID_{MU}))$, since the encryption key is shared only between MU and HA. Thus we conclude that the proposed scheme achieves mutual authentication.

5.5.8 Perfect forward secrecy is achieved

Perfect forward secrecy is a security feature that has to be achieved by the authentication schemes designed in GLOMONET. Even with the revelation of the server's secret key, there has to be an assurance that the session key cannot be compromised. In the proposed scheme session key is computed as $SK = R_m R_f P$, where $\{R_m, R_f\}$ are the random numbers of MU and FA respectively. Even if the private keys of (MU, FA and HA) are compromised by an adversary, he/she will not be able to compute SK due to the complexity of ECDLP and ECDHP. Thus the proposed scheme achieves perfect forward secrecy.

5.5.9 Local password verification achieved

The proposed scheme provides local password verification by allowing the mobile users to insert their smart card into the terminal and then the valid MU, enters his/her lo-

gin credentials $\{ID_{MU}, PW_{MU}\}$. After that, smart card computes $A_2^* = h(h(ID_{MU}) \oplus h(PW_{MU}))$. Verifies if $A_2^* \stackrel{?}{=} A_2$ is true or not, if it is true the authenticity of the MU is verified and allows the mobile users to request for the FA's services. Thus the proposed scheme achieves local password verification to prevent the unauthorised access.

5.5.10 Resistant to insider attack

During the registration phase, MU does not send any password related information to the HA. In that case, the attacker who has the admin privileges to access the HA's database, cannot get any password related information to steal the password. Thus the proposed scheme is resistant to insider attack.

5.5.11 No time synchronization

The proposed scheme does not make use of time stamps, instead random numbers are used to thwart replay attack. Use of time stamps creates a lot of synchronization problems due to the fact that all the hardware clocks are imperfect, the local clock of the users device may drift away from the server in time. It is observed that time stamps should not be used in large distributed networks to avoid synchronization problems. Thus the proposed scheme does not time synchronization.

5.5.12 User friendliness

The proposed scheme allows the mobile users to freely choose their $\{ID_{MU}, PW_{MU}\}$. If mobile users need to update their old password PW_{MU}^{old} with new password PW_{MU}^{new}, they can update locally without the intervention of HA. Updating the old password with the new password is discussed in section 5.4.4. For the valid MU password changing is secure and hassle free process. Thus the proposed scheme achieves user friendliness.

5.6 Formal security verification using avispa tool

Using the widely accepted AVISPA tool, the proposed scheme is simulated and verified against the active and passive security attacks. Firstly, the AVISPA tool is introduced, secondly, the implementation details of the proposed scheme using AVISPA is presented and finally the output of the simulation is presented.

5.6.1 HLPSL Implementation

```
% OFMC
% Version of 2006/02/13

SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/span/span/testsuite/results/fanwu.if

GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS

 parseTime: 0.00s
 searchTime: 0.06s
 visitedNodes: 8 nodes
 depth: 3 plies
```

Figure 5.3 Output analysis using OFMC back-end

```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/fanwu.if

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS
Analysed  : 3 states
 Reachable  : 0 states
 Translation: 0.04 seconds
 Computation: 0.00 seconds
```

Figure 5.4 Output analysis using CL-AtSe back-end

AVISPA tool is used to formally verify the safety of our protocol against several security threats under OFMC and CL-AtSe back end. The implementation phase of the proposed protocol is done using HLPSL considering the Dolev-Yao threat model to reflect the properties of an insecure channel among MU, FA and HA. A symmetric key is used to implement the secure channel during registration phase of our protocol. Two insecure channels are considered: between MU and FA, and between FA and HA. We have fixed four secrecy goals and two authentication goals namely, secrecy of ID_{MU}, secrecy of PW_{MU}, secrecy of X, secrecy of K_{fh}. HLPSL uses three basic roles: mobileuser played_by MU, foreignagent played_by FA homeagent played_by HA. The three supporting roles used in the HLPSL implementation are: environment, session and role. Output of the program using OFMC back end is presented in Fig. 5.3. Output of the program using CL-AtSe back end is presented in Fig. 5.4. The proposed protocol remains SAFE under Dolev-Yao channel and achieves all the specified secrecy and authentication goals with a search time of 0.06s using OFMC back end and 0.04s using

CL-AtSe back end.

5.7 Performance analysis and comparision

This section evaluates the performance of the proposed scheme with the Gope and Hwang (2016a) scheme, Wu et al. (2016) scheme and Lee et al. (2017) scheme in terms of security attacks and security goals an ideal authentication scheme designed for GLOMONET should achieve.

Table 5.2 Functionality comparison

Security Requirements	**Proposed scheme**	**A**	**B**	**C**
User anonymity is protected	✓	×	✓	×
Mutual authentication is achieved	✓	✓	✓	✓
Security against insider attack	✓	✓	✓	×
Security against off-Line password guessing attack	✓	×	✓	×
Security against replay attack	✓	×	×	×
Security against stolen-verifier attack	✓	✓	✓	✓
Security against impersonation attack	✓	×	×	×
Perfect forward secrecy achieved	✓	×	×	✓
Security against stolen smart card attack	✓	×	✓	×
Local password verification achieved	✓	✓	×	✓
No time synchronization	✓	✓	✓	✓
User friendliness	✓	✓	×	✓

A: Gope and Hwang (2016a), *B*: Wu et al. (2016), *C*: Lee et al. (2017)

It is clearly evident from Table 5.2 that the compared schemes failed to resist security attack like replay attack. Fan Wu et al.'s scheme could not protect user anonymity and could not resist security attacks like insider attack, impersonation attack, stolen smart card, offline password guessing and replay attack. Lee et al.'s scheme could not achieve security goals like perfect forward secrecy and local password verification. Their scheme failed to resist the security attacks like replay attack and impersonation attack. Gope and Hwang scheme could not protect user anonymity and failed to achieve security goals like perfect forward secrecy. They also failed to resist security attacks like offline password guessing attack, stolen smart card attack, impersonation and replay attack. The proposed scheme achieves all the security goals and resists all the security attacks.

Table 5.3 Computational cost comparison

Entities	**Proposed Scheme**	**Gope and Hwang (2016a)**	**Wu et al. (2016)**	**Lee et al. (2017)**
C_{MU}	$10T_h$+$3T_{\oplus}$+$7T_{\|\|}$	$8T_h$+$8T_{\oplus}$+$8T_{\|\|}$	$12T_h$+$9T_{\oplus}$+$23T_{\|\|}$	$12T_h$+$11T_{\oplus}$+$8T_{\|\|}$
C_{FA}	$3T_h$+$0T_{\oplus}$+$12T_{\|\|}$	$1T_h$+$3T_{\oplus}$+$2T_{\|\|}$	$5T_h$+$1T_{\oplus}$+$16T_{\|\|}$	$8T_h$+$3T_{\oplus}$+$9T_{\|\|}$
C_{HA}	$8T_h$+$4T_{\oplus}$+$19T_{\|\|}$	$6T_h$+$5T_{\oplus}$+$21T_{\|\|}$	$14T_h$+$7T_{\oplus}$+$35T_{\|\|}$	$10T_h$+$4T_{\oplus}$+$11T_{\|\|}$
Total	21 T_h + 7 $T_{\oplus}$ + 38 $T_{\|\|}$	$15T_h$+$16T_{\oplus}$+$31T_{\|\|}$	31 T_h + 17 $T_{\oplus}$ + 74 $T_{\|\|}$	30 T_h + 18 $T_{\oplus}$ + 28 $T_{\|\|}$

Table 5.3 summarizes the computational cost of the proposed scheme with the schemes such as Gope and Hwang (2016a), Wu et al. (2016) and Lee et al. (2017). Computational cost is calculated based on the number of operations used by MU, FA and HA respectively during communication. Hash functions are denoted as T_h. XOR operations are denoted as $T_{\oplus}$. Concatenation operations are denoted as $T_{||}$. C_{MU}, C_{FA}, C_{HA} represents the computations of MU, FA and HA respectively. The total number of operations used by Gope and Hwang's scheme to design an authentication scheme are 15 T_h, 16 $T_{\oplus}$ and 31 $T_{||}$. The total number of operations used by Fan Wu et al.'s scheme to design an authentication scheme are 31 T_h, 17 $T_{\oplus}$ and 74 $T_{||}$. The total number of operations used by Lee et al.'s scheme to design an authentication scheme are 30 T_h, 18 $T_{\oplus}$ and 28 $T_{||}$. Whereas, the proposed scheme uses 21 T_h, 7 $T_{\oplus}$ and 38 $T_{||}$. Compared

to Fan Wu et al.'s scheme the proposed scheme requires less computational cost. With less computational cost, the proposed scheme is able to resist all the security attacks and achieves all the security goals which are listed in Table 5.2.

Table 5.4 summarizes the efficiency of the proposed scheme and the other schemes such as Gope and Hwang (2016a); Lee et al. (2017); Wu et al. (2016). The cryptographic operations required in registration phase, login and authentication phase and password change phase are tabulated in Table 5.4. The notations used are: HF : Hash function, E/D : Encryption/Decryption and PM : Point Multiplication.

Table 5.4 Efficiency comparison

Scheme / Phase	Proposed scheme			Gope and Hwang		Fan Wu et. al.			Lee et. al.	
Operations	HF	E/D	PM	HF	E/D	HF	E/D	PM	HF	E/D
Registration phase	4	0	0	4	0	5	0	0	4	0
Login and authentication phase	17	4	4	11	4	26	2	4	26	0
Password change phase	6	0	0	4	1	11	0	0	4	3
Total no. of operations	27	4	4	19	5	42	2	4	34	3

Table 5.5 summarizes the time taken (ms) by cryptographic functions to perform the operations (Wu et al., 2018). The hardware and software requirements to perform the operations are CPU: Intel(R) Core TM i7-4710HQ, 2.50 GHz. OS: Ubuntu 16.10 64-bit Memory:8 GB. Software: NetBeans 8.2, MIRACL C/C++ Library. Security level: 1024/1024 bits in a cyclic group G, 160-bit point in F_p, AES, SHA-2 (256 bits).

Table 5.5 Referred cryptographic operations (ms)

Symbol	Meaning	Time cost(ms)
T_e	Time of a modular exponentiation in a cyclic group	2.080552
T_m	Time of a scalar multiplication on ECC	0.298595
T_s	Time of an average average symmetric encryption/decryption	0.020206
T_h	Time of Sha2-256	0.003997

Table 5.6 summarizes the performance comparison, in terms of time complexities

with the proposed scheme and other schemes. Time complexities are calculated based on the time taken by the cryptographic operations t_h, t_m, t_s. The proposed scheme requires less time compared to Fan Wu et al.'s scheme.

Table 5.6 Performance comparison

Phase	Time in ms			
	Proposed Scheme	**Gope and Hwang (2016a)**	**Wu et al. (2016)**	**Lee et al. (2017)**
Registration phase	0.015988	0.015988	0.019985	0.015988
Login phase	1.343153	0.124791	1.338714	0.103922
Password change phase	0.023982	0.036194	0.043967	0.076606
Total	1.383123	0.176973	1.402666	0.196516

Table 5.7 Communication overhead comparison between the proposed scheme and other schemes

Scheme	Handshakes	Communication overhead
Proposed scheme	4 messages	3520 bits
Gope and Hwang (2016a)	4 messages	2688 bits
Wu et al. (2016)	4 messages	5696 bits
Lee et al. (2017)	5 messages	2400 bits

Table 5.7 compares the communication overhead between the proposed scheme and the other schemes such as Gope and Hwang (2016a); Lee et al. (2017); Wu et al. (2016). SHA-1 hash function requires 160-bits (Eastlake 3rd and Jones, 2001). Time-stamp requires 32 bits, user identity requires 160 bits, random numbers/nonce requires 160 bits, 160 bits; $x.P$ (ECC point (x_P, y_P)): 320 bits; 128-bit ciphertext for 128-bit plaintext block using symmetric encryption/decryption (using AES-128) (Banerjee et al., 2018). In the proposed scheme the login message $M_1 = \{C_1, C_2, C_3, ID_{HA}\}$ requires (160+320+160+160)=800 bits, $M_2 = \{C_1, C_2, C_3, C_4, C_5, C_6, ID_{FA}\}$ requires (160+320+160+320+160+160+160)=1440 bits, $M_3 = \{C_8, C_9, ID_{HA}\}$ requires (160+160+160)=480 bits and $M_4 = \{C_4, C_8, C_{10}, ID_{HA}\}$ requires (320+160+160+160)=800 bits. Thus, the computational overhead of the proposed scheme is 800+1440+480+800=3520 bits. However, when compared to Fan Wu et al.'s scheme the communication overhead of the

proposed scheme is less. Hence the proposed scheme is more suitable for the practical implementation.

5.8 Summary

In this chapter, we have proved that the Fan Wu et al.'s scheme is insecure and has failed to resist security attacks like replay attack, insider attack, stolen smart card attack, offline password guessing attack and impersonation attack. We further prove that their scheme could not protect user anonymity. To eliminate these security attacks, we have proposed an enhanced secure authentication scheme. The proposed scheme has made use of elliptic curve cryptography problem to compute session key. Due to the complexity of the algorithm, it is infeasible for an adversary to compute the session at a definite time interval, which makes the proposed scheme possible to achieve perfect forward secrecy. Diffie-Hellman key exchange protocol is used to achieve mutual authentication between FA and HA. Additionally, the proposed scheme is simulated using AVISPA tool to formally verify that the proposed scheme is secure against active and passive attacks. Furthermore, the performance analysis of the proposed scheme proves that the scheme is lightweight and suitable for practical implementation.

CHAPTER 6

ECC Based Authentication and Key Agreement Protocol to avoid replay attack in GSM Network

6.1 Introduction

GLObal MObility NETworks (GLOMONET) provide roaming service to mobile users. This network facilitates the roaming service for mobile users and has three entities involved in the communication. They are Mobile User (MU), the Foreign Agent (FA) and the Home Agent (HA). In a roaming scenario, MU can access the services provided by HA in FA. While accessing services offered by HA in FA, MU has to prove its authenticity to FA, that will be later verified by HA.

Authentication is proving the identity of oneself. Providing security to user authentication is the key issue that has to be addressed in GLOMONET. During communication, each entity has to mutually authenticate each other to establish a secure communication, hence mutual authentication plays a crucial role while designing an authentication scheme.

Security is the major challenge to address in wireless comunications due to the broadcast nature and the limited bandwidth. Mobile networks use electromagnetic waves i.e radio waves as transmission media to transmit the data. Since the messages transmitted through radio waves are vulnerable to interception, providing security to the data in mobile networks and achieving network security goals such as confidentiality, integrity and availability becomes vital (Kuo et al., 2014). Literature survey (Bellare et al., 2000; Wang et al., 2012) presents the seminal work on how an adversary is mod-

elled to have full access on the communication channel, i.e he/she can intercept the login messages exchanged between the three communicating entities MU, FA and HA, by intercepting the messages, adversary can perform operations like insertion, deletion and modifying the messages, then he/she can retransmit the modified messages to one of the entities. Hence, while designing the two factor authentication schemes one of the crucial goals is to achieve mutual authentication. Each entity involved in the communication must prove its authenticity before providing the services. In the two factor authentication schemes mobile users possess both password and smart card.

The literature survey (Kim et al., 2012; Kocher et al., 1998; Messerges et al., 2002; Nohl et al., 2008) presents the seminal work on how the parameters stored in the smart card can be extracted by the methods like power analysis, reverse engineering etc.,. In case, the mobile user's smart card is lost or stolen, attacker can breach the security of the smart card and extract the parameters. Hence, the main goal is to protect the offline password guessing attack. Even with the smart card breach, attacker must not be successful in launching the password guessing attacks. It is also essential for any two factor authentication scheme not to maintain a verifier table in the server side containing user related critical information like user identity and password. In case any scheme does, such schemes do not preserve user anonymity (Wang et al., 2015). The verifier table must contain only the secret keys of the MU, HA and FA. If the server is compromised and the secret keys are revealed by an adversary, the revealed secret keys should not contribute in predetermining the session keys of the proposed scheme. This is one of the security requirements that has to be achieved by any scheme. This property is termed as perfect forward secrecy. Hence the aim of this chapter is to overcome the security challenges in the existing cellular networks.

6.1.1 Motivations and Contributions

With the advent of the new standards into the cellular system, there have been increased number of security attacks. Hence, the challenge is to overcome the security attacks. Securing the network and protecting the security features like authenticity, confidentiality and integrity is the key aspect of network security. There are various security attacks, vulnerabilities and privacy concerns at the media access control layer and phys-

ical layer that has to be addressed in cellular networks. To protect the voice and data over the wireless channel, traditional security architectures are used.

1. The proposed scheme provides security features as user identity management, mutual authentications between the network and the mobile user and securing communication channel.

2. Using the cryptographic techniques a secure light weight protocol is developed.

3. The proposed protocol is formally verfied using AVISPA tool. AVISPA tool is used to validate the resistance of the security attacks of the protocol.

4. Using NS2 simulator we have analysed the network performance metrics like throughput, end to end delivery and packet delivery ratio.

5. The proposed protocol operates with less computational cost and communication cost.

The remainder of this chapter is organized as follows. The proposed scheme is explained in section 6.2. In Section 6.3, security analysis of the proposed protocol are described. Formal verfication of the security protocol is expalined in section 6.4. Section 6.5 shows the simulation results of NS2.35 simulator. In Section 6.6, the performance of the proposed scheme is compared with the other related schemes. Section 6.7 concludes the paper.

6.2 Proposed scheme

The proposed scheme involves three entities Mobile User (MU), Foreign Agent (FA) and Home Agent (HA) and communication between these three entities are carried in four phases. They are: initialization phase, registration phase, authentication and key agreement phase and password change phase. The proposed scheme makes use of Diffie-Hellman key exchange protocol (Diffie and Hellman, 1976) to compute secret key K_{fh} exchanged between FA and HA. The proposed scheme also uses of elliptic curve cryptography. The domain parameters $\{E_{(F_p)}, G, a, b, p\}$ of the elliptic curve cryptography are shared among the three communicating entities. A brief introduction to ECC is as follows.

Notations used in the proposed scheme are shown in Table 6.1.

Table 6.1 Notations and cryptographic functions

Symbol	Definition
MU	Mobile User
FA	Foreign Agent
HA	Home Agent
ID_{MU}	MU's identity
PW_{MU}	MU's password
ID_{HA}	HA's identity
ID_{FA}	FA's identity
SK	Session key between FA and MU
K_{FH}	Secret key shared between the FA and HA
$E_k(.)$	The symmetric encryption function with the key k
$D_k(.)$	The symmetric decryption function with the key k
q	Large prime number
X	Secret key of HA
Z_N^*	$Z_N^* \stackrel{def}{=} \{x \in Z_N : gcd(x,N) = 1\}$ = elements of Z_N with multiplicative inverses.

6.2.1 Initialization phase

1. HA chooses its random number r_h and computes its secret key $X = r_h P$. HA stores $\{r_h, P, N\}$ in its database, where N is a large prime number.

2. During initialization phase, MU and HA shares symmetric encryption key E_k over secure channel.

3. On receiving ID_{FA}, HA computes SK_{FA} using Diffie-Hellman key exchange protocol. HA sends SK_{FA} to FA over secure channel.

4. HA and FA chooses two random numbers a, b and large prime number q over multiplicative group g. $a, b < q$. FA computes its public key $P_{FA} = g^b \mod q$ and HA computes its public key as $P_{HA} = g^a \mod q$. Both HA and FA share their public keys keeping private keys secret.

6.2.2 Registration phase

Registration phase of the proposed scheme is illustrated in Figure 6.1.

Mobile User

Home Agent

MU chooses login credentials $\{ID_{MU}, PW_{MU}\}$ and computes $(h(ID_{MU}||b||)$ where b is the random number of MU. computes

$M_1=(h(ID_{MU}||b)$

HA on receiving the message M_1, computes X=rP, where r is the random number and P is generator point on ECC. HA assigns counter value $Ctr_{MU}=1$ and stores ($(h(ID_{MU}||b||)$, Ctr_{MU}). HA computes

$A=h(h(ID_{MU}||b||)||X)$

$B=A\oplus g^a \bmod q$.

MU on receiving smart card, computes. $h(ID_{MU}||b||PW_{MU})$. MU stores $\{A, B, E_p, b\ Ctr_{MU}\}$ in to the smart card

Smart card $\{A, B, E_P, Ctr_{MU}\}$

Figure 6.1 Registration phase

1. MU chooses identity and password ID_{MU}, PW_{MU} of his/her own choice and submits $h(ID_{MU}||b)$ to the HA, where b is the random no. of the MU.

2. HA on receiving the request computes
   $X = rP$ where r is the random number chosen by the HA. P is the generator point on ECC. HA assigns the counter value $Ctr_{MU} = 1$ to HA and stores $(h(ID_{MU}||b), Ctr_{MU})$ in its database. HA computes $A = h(h(ID_{MU}||b)||X)$ $B = A \oplus g^a mod\ q$. HA issues the smart card with the parameters $\{A, B, Ctr_{MU}, E_p\}$to MU.

3. MU on receiving the smart card, computes
   $C = h(h(ID_{MU}||b||PW_{MU}))$. MU stores $\{A, B, C, Ctr_{MU}, b, E_p\}$ into the smart card.

6.2.3 Login and Mutual Authentication phase

Login and Mutual Authentication phase of the proposed scheme is illustrated in Figure 6.2.

1. MU inserts his/her login credentials ID_{MU}, PW_{MU} into the smart card terminal. Smart card computes $C^* = h(h(ID_{MU}||b||PW_{MU}))$. Verifies whether $C^* \stackrel{?}{=} C$. If true, smart card generates random number $\alpha \in Z_n^*$ and computes $C_1 = \alpha P$
   $P = E_k(h(ID_{MU}||b))$
   $D = C \oplus Ctr_{MU} \oplus C_1$
   $E = h(h(ID_{MU}||b)||D||Ctr_{MU}||ID_{HA}||T_1)$. MU forms the message
   $M_1 = \{P, D, E, C_1, T_1, Ctr_{MU}\}$ and sends to FA at T_1.

2. On receiving the message M_1 from MU, FA verifies if $\Delta T \leq T_2 - T_1$. If true, FA generates random number $\beta \in Z_n^*$ and computes $C_2 = \beta P$
   $F = h(D||C_1||E||T_1||T_2) \oplus g^b \mod q$. FA forms the message
   $M_2 = \{P, D, E, C_1, Ctr_{MU}, T_1, E_{K_{FH}}(F), C_2, T_2\}$ and sends to the HA at T_2.

3. HA on receiving
   $M_2 = \{P, D, E, C_1, Ctr_{MU}, T_1, E_{K_{FH}}(F), C_2, T_2\}$. HA verifies if $\Delta T \leq T_3 - T_2$. If true, HA decrypts $D_{K_{FH}}(F)$ using the shared secret key K_{FH} known only to FA and HA and reveals the parameter F. HA computes
   $F^* = h(D||C_1||E||T_1||T_2) \oplus g^{ab} \mod q$. Verifies if $F^* \stackrel{?}{=} F$. If true, HA mutually authenticates FA. Else, the request is terminated. HA decrypts $D_k(h(ID_{MU}||b))$ and reveals $h(ID_{MU}||b)$. HA verifies the obtained $h(ID_{MU}||b)$ with the stored value in its database. If both the values does not match, HA terminates the request. Otherwise, HA considers that a MU is legitimate. HA computes
   $E^* = h(h(ID_{MU}||b)||D||Ctr_{MU}||ID_{HA}||T_1)$. If true, HA authenticates MU and computes $G = h(C_2||T_3) \oplus g^a \mod q$
   $H = h(C_1||Ctr_{MU}||T_3)$. MU forms the message $M_3 = \{H, G, T_3\}$ to FA at T_3.

4. After receiving $M_3 = \{H, G, T_3\}$ at T_4 from HA, FA verifies if $\Delta T \leq T_4 - T_3$. If true, FA computes $G^* = h(C_2||T_3) \oplus g^{ab} \mod q$ and verifies if $G^* \stackrel{?}{=} G$. If holds true, FA mutually authenticates HA. FA computes $SK = h(C_1||C_2||\beta C_1)$
   $L = SK \oplus h(C_1||T_4)$. MU forms the message $M_4 = \{C_2, H, T_3, T_4, L\}$ at T_5 and sends to MU.

5. MU on receiving the message $M_4 = \{C_2, H, T_3, T_4, L\}$ at T_5 verifies if $\Delta T \leq T_5 -$

T_4. If true, MU computes $H^* = h(C_1||Ctr_{MU}||T_3)$. Verifies if $H^* \stackrel{?}{=} H$. If it holds true, MU authenticates HA. MU computes $SK = h(C_1||C_2||\alpha C_2)$

$L^* = SK \oplus h(C_1||T_4)$. Verifies if $L^* \stackrel{?}{=} L$. If true, MU mutually authenticates FA.

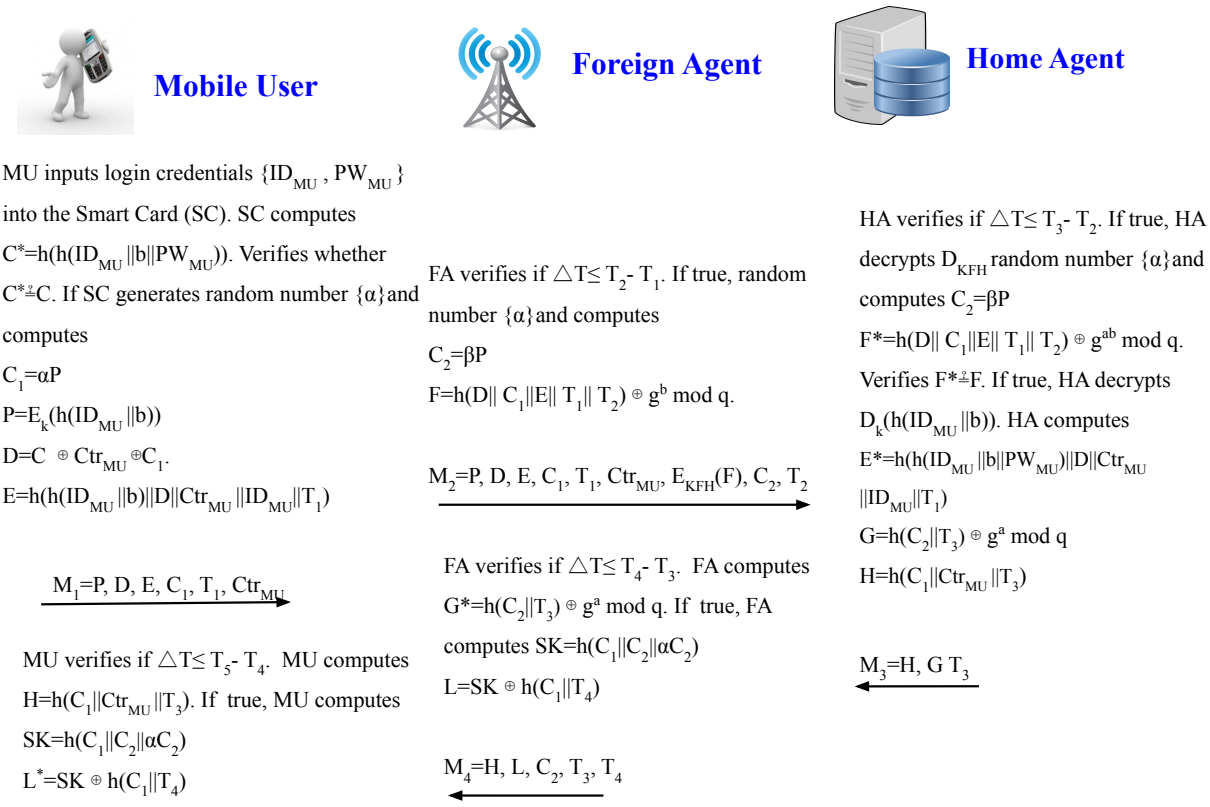

Figure 6.2 Login and Mutual Authentication phase

6.2.4 Password change phase

Procedure for password change phase is described in detail.

1. If a valid MU wants to change his/her password he/she is allowed to update their password such provision is made available in the proposed scheme. For the updation of old password to new password, MU is requested to enter his/her login credentials identity and password ID_{MU}, PW_{MU}^{old} into the smart card terminal. Smart card computes $C^* = h(h(ID_{MU}||b||PW_{MU}^{old}))$. Verifies if $C^* \stackrel{?}{=} C$. If true, MU is allowed to update their password. MU enters new password PW_{MU}^{new}. Smart computes $C^{'} = h(h(ID_{MU}||b||PW_{MU}^{new}))$.

2. Smart card replaces C with $C^{'}$ and stores $\{A, B, C^{'}, Ctr_{MU}, b, E_p\}$ in the smart card.

6.3 Security analysis

The proposed protocol resists active security attacks and passive security attacks. Active security like replay attack, masquerade attack and passive attacks like traffic analysis and eavesdropping. The proposed protocol also provides security features like user anonymity, mutual authentication and perfect forward secrecy. The proposed protocol resists some of the security attacks in cellular networks like insider attack, offline password guessing attack and forgery attacks.

6.3.1 User anonymity is protected

In the proposed scheme, the login message $M_1 = \{P, D, E, C_1, T_1, Ctr_{MU}\}$ carries the user sensitive information identity of the MU in the parameter P, which is computed as $P = E_k(h(ID_{MU}||b))$, where b is the random number chosen by the MU. In each session, user chooses a new random number. $\mathscr{A}$ cannot disclose the identity by eavesdropping the login message M_1 as the identity ID_{MU} is concatenated with the random number which is unknown to an $\mathscr{A}$ and the ID_{MU} is encrypted with the symmetric key E_k. The key is known only to HA and MU. The symmetric encryption algorithm used is blowfish of key size 64 bits. Hence, the proposed scheme is secure and protects user anonymity.

6.3.2 Resistant to replay attack

The proposed scheme uses time synchronisation mechanism during the communication between the three entities MU, FA and HA. Time synchronisation mechanism first validates the received login messages based on the time interval i,e $\Delta T \leq T_{arr} - T_{sent}$, where T_{arr} is the arrival time of the message and T_{sent} is the time at which the message was sent by the communicating entity. ΔT is the time interval at which the message should be received. If the delay is more than the expected time then the message request is terminated by the receiving entity. This way the replay attack can be resisted if $\mathscr{A}$ eavesdrops the message, modifies the same message and replays. Thus, the proposed scheme is resistant to the replay attack.

6.3.3 Resistant to insider attack

The proposed scheme allows the user to choose their own password freely. But during the registration phase, MU sends only identity of the MU ID_{MU} as $h(ID_{MU}||b)$, where b is the random number chosen by the MU. Password is not sent to the HA, this prevents the administrator of the HA's database from stealing the password. Thus, the approach used in the registration phase of the proposed scheme prevents insider attack.

6.3.4 Resistant to offline password guessing attack

In the proposed scheme, the smart card is personalised with the parameters $\{A,B,C,Ctr_{MU},b,E_p\}$. The parameter C contains the user sensitive information such as $\{ID_{MU},PW_{MU}\}$. The parameter C is computed as $C = h(h(ID_{MU}||b||PW_{MU}))$. With the reverse engineer method or power analysis method $\mathscr{A}$ leaks the parameters in the smart card. To obtain the real PW_{MU} $\mathscr{A}$ guesses the password $PW^{'}_{MU}$. With the guessed $PW^{'}_{MU}$ $\mathscr{A}$ computes $C^{'} = h(h(ID^{'}_{MU}||b||PW^{'}_{MU}))$, where $\{ID^{'}_{MU},PW^{'}_{MU}\}$ are the guessed pair of the identity and password of the MU. The parameter b is obtained from the smart card. $\mathscr{A}$ verifies if $C^{'} \stackrel{?}{=} C$. However, the probability that both the values matches is practically impossible due to the fact that both the $\{ID_{MU},PW_{MU}\}$ are concealed in hash functions and the result of the hash function is again hashed. The double hashing technique used in the proposed scheme resists collision and makes it difficult for $\mathscr{A}$ to guess the password. Thus, the proposed scheme is resistant to offline password guessing attack.

6.3.5 Resistant to stolen smart card attack

With the theft of the stolen smart card and the leakage of the smart card parameters $\{A,B,C,Ctr_{MU},b,E_p\}$, $\mathscr{A}$ launches the guessing attacks for the the two unknown pair ID_{MU},PW_{MU}. However, his/her efforts fails due to the fact that it is difficult to guess two unknown values. Additional to that ID_{MU},PW_{MU} which can be known from the parameter C is computed as $C = h(h(ID_{MU}||b||PW_{MU}))$. The pair $\{ID_{MU},PW_{MU}\}$ is concealed with two hash functions. Hence, it is difficult to guess the $\{ID_{MU},PW_{MU}\}$ pair. Thus, the proposed scheme is resistant to stolen smart card attack.

6.3.6 Resistant to forgery attacks

The three communicating entities MU, FA and HA in the proposed scheme share the secret keys E_k, K_{FH}, P_{HA} respectively to communicate with each other. To forge each of the messages $\{M_1, M_2, M_3, M_4\}$ transmitted over insecure channel is impossible as $\mathscr{A}$ fails to obtain the secret keys due to the complexity of the encryption algorithms used in the proposed scheme. Thus, the proposed scheme is resistant to forgery attack.

6.3.7 Security against traffic analysis or eavesdropping

Traffic analysis is a passive security attack, this type of attack is launched by an attacker by listening to the communication channel. This attack is similar to eavesdropping. Attackers perform traffic analysis to determine the location of the base station. Once the base station is located, the attacker can accurately launch a host of attacks against the base station such as jamming and eavesdropping. The proposed encrypts the data transmitting over insecure channel by using cryptographic techniques.

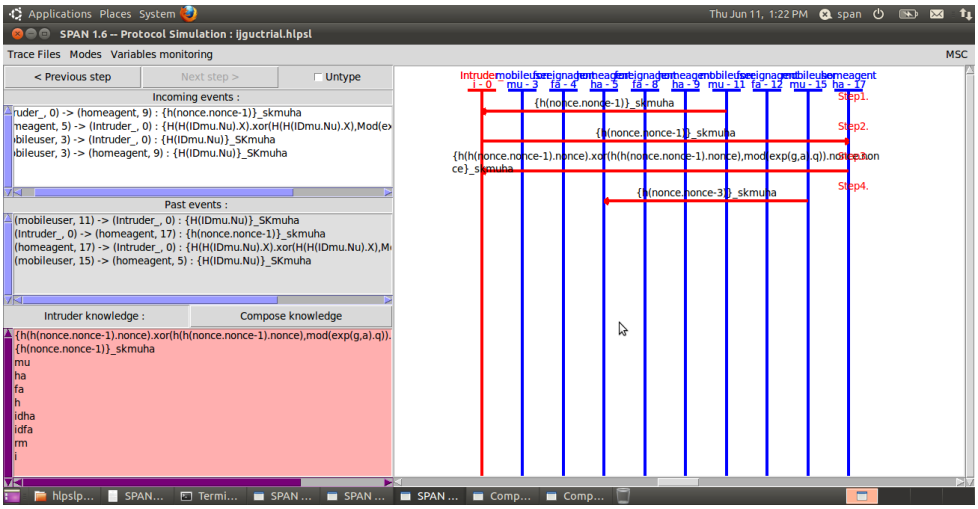

Figure 6.3 Message sequence chart

Fig. 6.3 refers to the message sequence chart (msc) of the proposed protocol. Message sequence chart is built using Security Protocol Animator (SPAN) for Avispa tool. The proposed protocol consists of three roles namely mobileuser, foreignagent and homeagent. In the MSC, intruder learns about the parameter as shown in Fig. 6.3. Intruder intercepts the communication channel to learn about the data. Since the pro-

posed protocol made use of cyptographic primitives the data available to intruder is in encrypted format. Thus, the proposed protocol provides security to traffic analysis and eavesdropping.

6.3.8 Perfect forward secrecy

The proposed scheme uses Elliptic Curve Cryptography (ECC) to compute the session keys. During the transmission of the login messages $\{M_1, M_2\}$ the parameters $\{C_1, C_2\}$ in the login messages are computed as $C_1 = \alpha P$, $C_2 = \beta P$. For every session, fresh values of $\{\alpha, \beta\}$ is generated. In case, if $\mathscr{A}$ records the previous session keys, its of no use because of the fact that for every session new session key is generated. Thus, the proposed scheme achieves perfect forward secrecy.

6.3.9 Mutual authentication is achieved

It is difficult for $\mathscr{A}$ to impersonate due to the fact that each communicating entity uses the secret key to mutually authenticate each other.

1. To impersonate MU

   On receiving the login message $M_1 = \{P, D, E, C_1, T_1, Ctr_{MU}\}$, HA decrypts the parameter P which is computed as $P = E_k(h(ID_{MU}||b))$. Decryption key D_k is known only to HA. Hence, it is difficult for $\mathscr{A}$ to impersonate a valid MU.

2. To impersonate FA

   During the communication FA and HA shares the secret key K_{FH}. HA validates the authenticity of the FA based on the login message
   $M_2 = \{P, D, E, C_1, Ctr_{MU}, T_1, E_{K_{FH}}(F), C_2, T_2\}$ in which FA encrypts the parameter F with the secret key K_{FH} as $E_{K_{FH}}(F)$ only the valid HA will be able to decrypt the message. Thus, it is impossible to impersonate as valid HA.

6.4 Formal security verification using avispa tool

To provide the results of the formal security verification of the proposed scheme, AVISPA tool is used. Acronym AVISPA stands for Automated Validation of Internet Security Protocols and Applications, the proposed scheme is simulated and verified against the

active and passive security attacks. The HLPSL implementation details of mobile user's registration phase and login and authentication phase of the proposed scheme is presented in Fig. 6.4. HLPSL implementation for the foreignagent role is presented in Fig. 6.5. HLPSL implementation for the homeagent role is presented in Fig. 6.6. HLPSL implementation for the session, goal and environment role is presented in Fig. 6.7. Output of the program using OFMC back-end is presented in Fig. 6.8. Output of the program using CL-Atse back-end is presented in Fig. 6.9.

```
role mobileuser(MU, HA, FA : agent,
            SKmuha: symmetric_key,
Ka, Kb: public_key,
            H,F,Mod: hash_func,
            SND, RCV: channel(dy))

played_by MU
def=
local State :nat,
 IDmu, IDha, PWmu, C,H1, C1,G, D, Ep, T1,T2, X, T3, T5, T4, C2, P, L, Ctr, A, B, E, Nu, NM, NF, NIDu, K, SK :text
const a,b,g,nm,nf,s1,s2,s3,s4 : protocol_id
  init  State := 1
  transition
    1.  State   = 1 /\ RCV(start)=|>
        State' := 2  /\ Nu' := new()
                  /\ NIDu' := H(IDmu.Nu')
                  /\ SND({H(IDmu.Nu')}_SKmuha)
          /\ secret(IDmu,s1,{MU,HA}) /\ secret(PWmu,s2,{MU}) /\ secret(X,s3,{HA}) /\ secret(K,s4,{FA})

% Receive the smart card  {A, B, CtrM U , Ep } from HA securely
    2.  State   = 2 /\ RCV ({H(H(IDmu.Nu').X).xor(Mod(exp(g,a),q))}_SKmuha) =|>
        State' := 3  /\ NM' := new()  /\ NF' := new()
/\ C' :=H(H(IDmu.Nu'.PWmu))
/\ C1' := F(NM'.P)
/\ P' := {H(IDmu.Nu')}_K
/\ D' := xor(xor(C',Ctr),C1')
/\ E' := H(H(IDmu.Nu').D'.Ctr.IDha.T1)
%send login request M1={P'.D'.E'.C1'.T1.Ctr} to the FA through open channel
/\ SND(P'.D'.E'.C1'.T1.Ctr)
/\ witness(MU,FA,nm,NM')

%Authentication phase
%Receive message M4 ={C2 , H, T3 , T4 , L} from FA via a public channel

 3. State = 3 /\ RCV(F(NF'.P).H(F(NM'.P).Ctr.T3).T3.T4.xor(H(F(NM'.P).F(NF'.P).NF'.F(NM'.P)), H(F(NM'.P).T4))) =|>

State' := 4 %/\ secret(X,s3,{HA}) /\ secret(K,s4,{FA})
           /\ SK' :=H(F(NM'.P).F(NF'.P).F(NM'.F(NF'.P)))
end role
```

Figure 6.4 Mobileuser role

```
role foreignagent(MU, HA, FA : agent,
              SKmuha: symmetric_key,
              Ka, Kb: public_key,
             H,F,Mod: hash_func,
        SND, RCV: channel(dy))
played_by FA
def=

  local State :nat,
 IDmu, IDha, PWmu, C,H1, C1, D, G,Ep, T1, X, T3, T5, T4, T2,C2, P, L, Ctr, A, B, E, Nu, NM, NF, NIDu, K, SK :text

const a,b,g,nm,nf,s1,s2,s3,s4 : protocol_id

  init  State := 0
  transition

%Login phase
% Receive login request M1 = {P, D, E, C1 , T1 , Ctr} from MU via open channel
    1.  State = 0 /\ RCV({H(H(IDmu.Nu'))}_K.xor(xor(H(H(IDmu.Nu'.PWmu)),Ctr),F(NM'.P)).
H(H(H(IDmu.Nu')).xor(xo(H(H(IDmu.Nu'.PWmu)),Ctr),F(NM'.P)).Ctr.IDha.T1).T1.Ctr) =|>

 State' := 1  /\ secret(IDmu, s1, {MU,HA}) /\ secret(PWmu, s2, {MU})
             /\ secret(K, s3, {FA,HA})  /\ secret(X, s3, {HA})
              /\ NF' := new()  /\ C2' := F(NF'.P)
             /\ F' := xor(H(xor(xor(H(H(IDmu.Nu'.PWmu)),Ctr),F(NM'.P)).F(NM'.P).H(H(IDmu.Nu').
xor(xor(H(H(IDmu.Nu'.PWmu)),Ctr),F(NM'.P)).Ctr.IDha.T1).T1.T2), Mod(exp(g,b),q))

% Send message M2 ={P, D, E, C1, Ctr, T1 , EK(F), C2 , T2 } to HA via a public channel to HA via open channel

/\ SND(F(NF'.P).{xor(H(xor(xor(H(H(IDmu.Nu'.PWmu)),Ctr),F(NM'.P)).F(NM'.P).H(H(IDmu.Nu').
xor(xor(H(H(IDmu.Nu'.PWmu)),Ctr),F(NM'.P)).Ctr.IDha.T1).T1.T2), Mod(exp(g,b),q))}_K.
{H(IDmu.Nu')}_K.xor(xor(H(H(IDmu.Nu'.PWmu)),Ctr),F(NM'.P)).
H(H(IDmu.Nu').xor(xor(H(H(IDmu.Nu'.PWmu)),Ctr),F(NM'.P)).Ctr.IDha.T1).F(NM'.P). Ctr. T1.T2 )

%Reccieve message M3 = {H, G, T3 } from HA
2. State=2 /\ RCV(H(F(NM'.P).Ctr.T3).xor(H(F(NF'.P).T3),Mod(exp(g,a),q))) =|>

 State' :=3 /\ SK' :=H(F(NM'.P).F(NF'.P).F(NF'.F(NM'.P)))
             /\ L' := xor(SK', H(F(NM'.P).T4))

%FA sends message M4={C2 , H1, T3 , T4 , L} to MU
/\ SND(F(NF'.P).xor(H(F(NM'.P).F(NF'.P).F(NF'.F(NM'.P))), H(F(NM'.P).T4)).H(F(NM'.P).Ctr.T3).T3.T4)
/\ witness(FA,HA,nf,NF')
end role
```

Figure 6.5 Foreignagent role

```
role homeagent(MU, HA, FA : agent,
               SKmuha: symmetric_key,
                Ka, Kb: public_key,
                H,F,Mod: hash_func,
        SND, RCV: channel(dy))
played_by HA
def=

local State :nat,
IDmu, IDha, PWmu, C,H1, C1,G, D, Ep, T1,T2, X, T3, T5, T4, C2, P, L, Ctr, A, B, E, Nu, NM, NF, NIDu, K,R, SK :text
const a,b,g,nm,nf,s1,s2,s3,s4 : protocol_id

init  State := 0

transition

   1.  State = 0 ∧ RCV({H(IDmu.Nu')}_SKmuha) =|>
       State' := 3   ∧ secret(X, s3, {HA}) ∧ secret(K, s4, {FA})
                  ∧ secret(IDmu,s1,{MU,HA}) ∧ secret(PWmu,s2,{MU})
              ∧ R' := new()
        ∧ X' := F(R'.P)
        ∧ A' := H(H(IDmu.Nu').X)
        ∧ B' := xor(A', Mod(exp(g,a),q))

%send smart card to MU securely

      ∧ SND({A'.B'.Ctr.Ep}_SKmuha)

% Authentication and key establishment phase with help of FA
% Receive message M2 ={P, D, E, C1 , CtrM U , T1 , EK_(F), C2 , T2 } from FA via a public channel

2. State = 3 ∧ RCV({H(IDmu.Nu')}_K.xor(xor(H(H(IDmu.Nu'.PWmu)),Ctr),F(NM'.P)).
H(H(IDmu.Nu').xor(xor(H(H(IDmu.Nu'.PWmu)),Ctr),F(NM'.P)).Ctr.IDha.T1).F(NM'.P).F(NF'.P).
{xor(H(xor(xor(H(H(IDmu.Nu'.PWmu)),Ctr),F(NM'.P)).F(NM'.P).H(H(IDmu.Nu').
xor(xor(H(H(IDmu.Nu'.PWmu)),Ctr),F(NM'.P)).Ctr.IDha.T1).T1.T2), Mod(exp(g,b),q))}_K.T1.T2.Ctr) =|>

         State' := 4  ∧ G' := xor(H(F(NF'.P).T3), Mod(exp(exp(g,b),a),q))
                    ∧ H1' := H(F(NM'.P).Ctr.T3)
% send message M3 = {H1, G, T3 }

              ∧ SND( H1'.G'.T3)

 end role
```

Figure 6.6 Homeagent role

```
role session(MU,HA,FA : agent,
        SKmuha: symmetric_key,
            Ka, Kb: public_key,
           H,F,Mod: hash_func)
 def=
local SD1, SD2, SD3, RV1, RV2, RV3 : channel(dy)
composition
mobileuser(MU,HA,FA,SKmuha,Ka,Kb,H,F,Mod,SD1,RV1)
/\ foreignagent(MU,HA,FA,SKmuha,Ka,Kb,H,F,Mod,SD2,RV2)
/\ homeagent(MU,HA,FA,SKmuha,Ka,Kb,H,F,Mod,SD3,RV3)
end role

role environment()
def=
 const mu, ha, fa : agent,
       skmuha: symmetric_key,
       ka, kb: public_key,
       h,f,mod : hash_func,
       idha, idfa,rm: text,
       mu_fa_nmu,fa_ha_nfa: protocol_id,
      s1,s2,s3,s4 : protocol_id

 intruder_knowledge={mu,ha,fa,h,idha,idfa,rm}

 composition

session(mu, ha, fa, skmuha,ka,kb, h,f,mod)
/\session(i, ha, fa, skmuha,ka,kb, h,f,mod)
/\session(mu, i, fa, skmuha,ka,kb, h,f,mod)
/\session(mu, ha, i, skmuha,ka,kb, h,f,mod)

end role

goal

secrecy_of s1
secrecy_of s2
secrecy_of s3
secrecy_of s4
authentication_on mu_fa_nmu
authentication_on fa_ha_nfa

end goal
environment()
```

Figure 6.7 Session and environment role

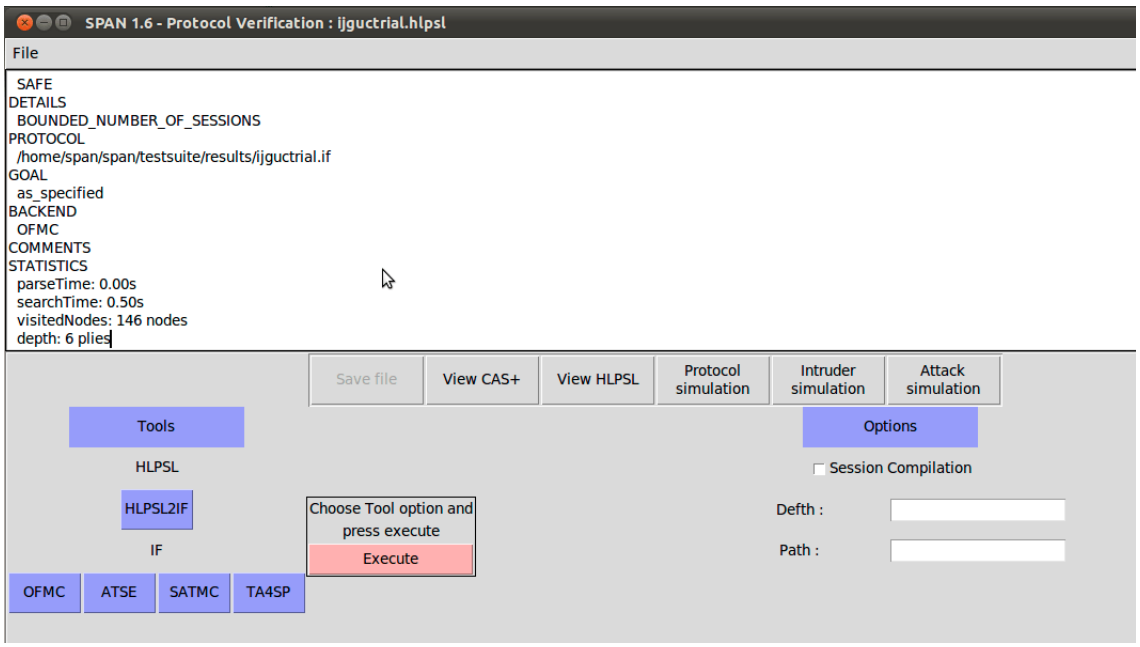

Figure 6.8 Output results using OFMC

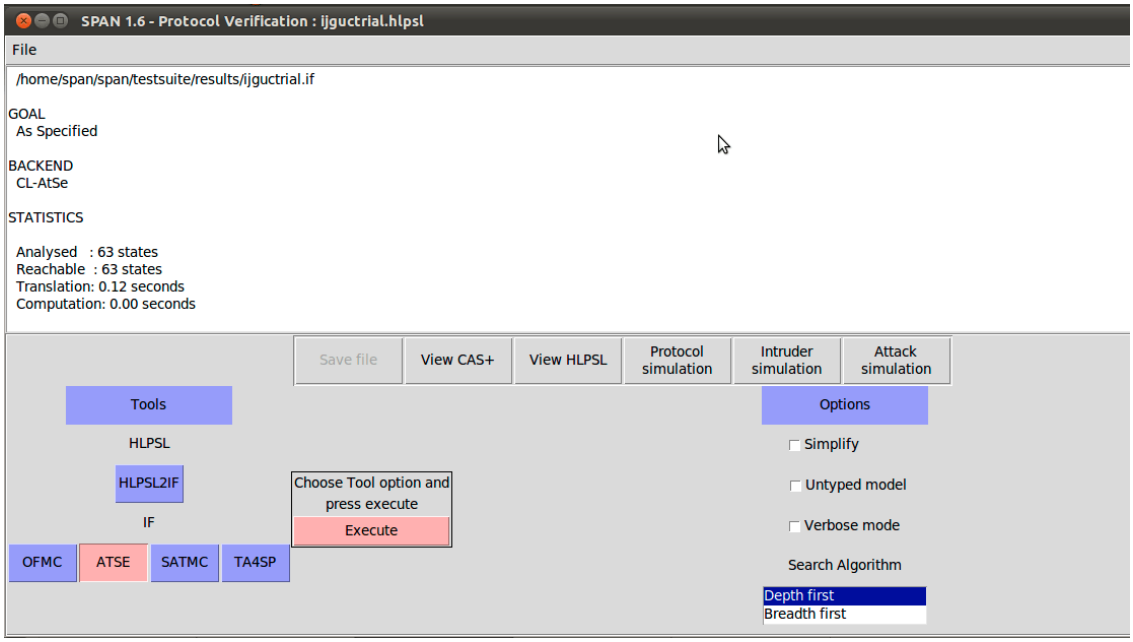

Figure 6.9 Output results using CL-Atse

It is evident from the results that the proposed authentication protocol is safe and satisfies the design goals for roaming service in mobility environments. Further, the proposed protocol is verified using security protocol animator (SPAN) tool (Glouche

et al., 2006) to detect and build a Message Sequence Chart (MSC) to represent the possible attacks and intruder activities.

6.5 Simulation using NS-2

In this section, we measure the network performance parameters of the proposed scheme. The proposed scheme is simulated using NS2.35 simulator. NS is a discrete event simulator primarily used for network related research purpose. NS provides support to simulate various protocols including routing protocols, TCP/UDP protocols over wired and wireless networks. Ad hoc, mobile and wireless sensor networks.

Table 6.2 Simulation metrics

Metric	Description
Tool	NS2.35
NS1, NS2, NS3, NS4	Network scenarios
Number of MU's	5, 10, 20, 30 in NS1, NS2, NS3, NS4
Mobility	10,20,30,40 mps
Simulation	15s
Platform	Ubuntu 16.04 LTS

Table 6.2 describes the simulation parameters used by NS2.35 simulator to simulate the proposed scheme. In the proposed scheme four network scenarios are considered. Network scenario 1 consists of 5 MU, 1 FA and 1 HA with the mobility speed of 10mps. Network scenario 2 consists of 10 MU, 1 FA and 1 HA with the mobility speed of 20mps. Network scenario 3 consists of 20 MU, 1 FA and 1 HA with the mobility speed of 30mps. Network scenario 4 consists of 30 MU, 1 FA and 1 HA with the mobility speed of 40mps.

The proposed scheme consists of four messages that are exchanged during login and mutual authentication phase in each network scenario between MU, FA and HA. Login message M_1 is of size 1088 bits and authentication messages $\{M_2, M_3, M_4\}$ are of size 1696, 352, 700 bits respectively.

6.5.1 Simulation environment

We have considered four global mobility network scenarios (NS) for the simulation.

1. NS1: Consists of 5MU'S, 1FA. 1HA with the mobility speed of 10mps.

2. NS2: Consists of 10MU'S, 1FA. 1HA with the mobility speed of 10mps.

3. NS3: Consists of 20MU'S, 1FA. 1HA with the mobility speed of 30mps.

4. NS4: Consists of 30MU'S, 1FA. 1HA with the mobility speed of 40mps.

6.5.2 Simulation results

During simulation, the network performance metrics such as throughput, end-to-end delivery and packet delivery ratio are analysed.

Impact on throughput

Network throughput (bps) is measured as the number of packets received successfully in a given time period. Throughput is calculated as:

$$Throughput = \frac{Received packets\ X\ Bit size\ of\ a\ packet}{Total time}.$$

Throughput calculated for different network scenarios is shown in Fig 6.10. Throughput increases with the increase in the number of mobile nodes. Since the number of messages exchanged will be more in case of huge MU'S communicating to the service provider network. Throughput for NS1, NS2, NS3 and NS4 are 401, 820, 1344 and 2211 bps respectively.

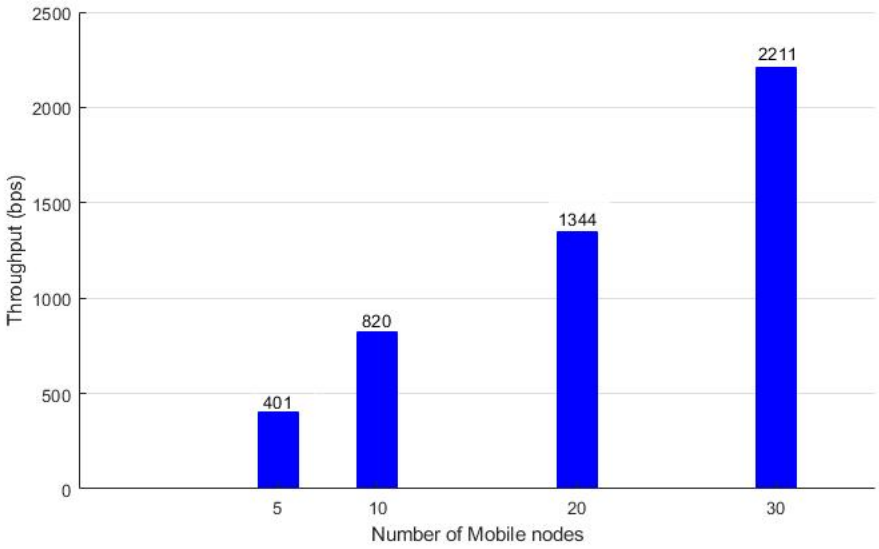

Figure 6.10 Throughput

Impact on End-to-End Delay (EED)

End-to-end delay refers to the time taken by the data packet that has to be sent across the network from source to destination. It can be computed as:

$$EED = \frac{T_{Rec} - T_{snd}}{T_P}.$$

where T_{Rec} is the time at which the packet is received and T_{snd} is the time at which the packet is sent. T_P is the total number of packets sent. The simulation result for NS1, NS2, NS3 and NS4 is shown in Fig. 6.11.

Impact on Packet Delivery Ratio (PDR)

Packet delivery ratio is the ratio of number of received packets to the number of sent. It can be computed as:

$$PDR = \frac{Received\,packets}{Sent\,packets}.$$

The simulation results for PDR under the network scenarios NS1, NS2, NS3 and NS4 is shown in Fig. 6.12. PDR decreases with the increase in the number of mobile

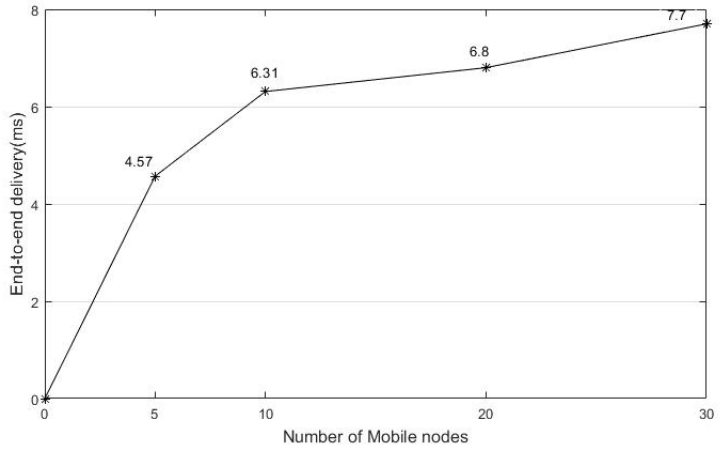

Figure 6.11 End-to-end delay

nodes. Since, the messages transmitted across the network are more in case of large MU's the packet drop will be more.

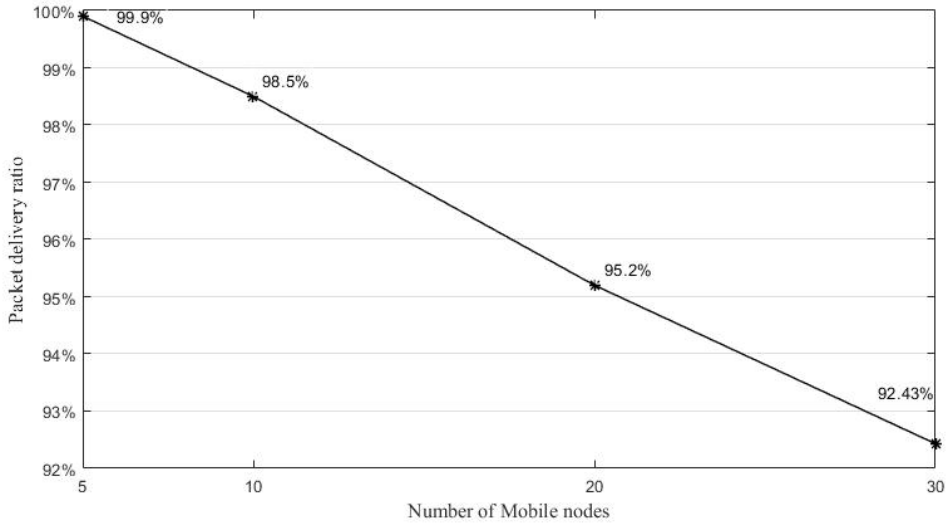

Figure 6.12 Packet delivery ratio

6.6 Performance analysis and comparison

This section evaluates performance of the proposed scheme with the Gope and Hwang's scheme (Gope and Hwang, 2016a), Fan Wu et al.'s scheme (Wu et al., 2016) and Lee et al.'s scheme (Lee et al., 2017) in terms of security and functional features, computational costs and communication costs.

6.6.1 Comparison of security and functional features

It is clearly evident from Table 6.3 that the related schemes failed to resist security attack like replay attack. Fan Wu et al.'s scheme could not protect user anonymity and could not resist security attacks like insider attack and offline password guessing attack.

Table 6.3 Functionality comparison

Security Requirements	**Proposed scheme**	**A**	**B**	**C**
User anonymity is protected	✓	×	✓	×
Mutual authentication is achieved	✓	✓	✓	✓
Security against insider attack	✓	✓	✓	×
Security against off-Line password guessing attack	✓	×	✓	×
Security against replay attack	✓	×	×	×
Security against stolen-verifier attack	✓	✓	✓	✓
Security against impersonation attack	✓	×	×	×
Perfect forward secrecy achieved	✓	×	×	✓
Security against stolen smart card attack	✓	×	✓	×
Local password verification achieved	✓	✓	×	✓
No time synchronization	✓	✓	✓	✓
User friendliness	✓	✓	×	✓

A: Gope and Hwang (2016a), *B*: Wu et al. (2016), *C*: Lee et al. (2017)

Lee et al.'s scheme could not achieve security goals like perfect forward secrecy, local password verification and fair key agreement. Their scheme failed to resist to the insider attack. Gope and Hwang scheme could not protect user anonymity and failed to achieve security goals like perfect forward secrecy, fair key agreement. They also failed to resist security attacks like offline password guessing attack, stolen verifier attack and replay attack. Whereas, the proposed scheme achieves all the security goals and resists all the security attacks. Thus, the proposed scheme achieves all the desirable security functionality features.

6.6.2 Comparison of computational costs and efficiency

Table 6.4 summarizes the computational cost of the proposed scheme along with the other schemes namely Gope and Hwang's scheme (Gope and Hwang, 2016a), Fan Wu et al.'s scheme (Wu et al., 2016) and Lee et al.'s scheme (Lee et al., 2017). Computational cost is calculated based on the number of operations used by MU, FA and HA respectively during communication. Hash functions are denoted as T_h. XOR operations are denoted as $T_{\oplus}$. Concatenation operations are denoted as $T_{||}$. C_{MU}, C_{FA}, C_{HA} represents the computations of MU, FA and HA respectively.

Table 6.5 summarizes the efficiency of the proposed scheme and the schemes Gope and Hwang (2016a); Lee et al. (2017); Wu et al. (2016). The cryptographic operations required in registration phase, login and authentication phase and password change phase are tabulated in Table 6.5. The notations used are: HF : Hash function, E/D : Encryption/Decryption, PM : Point Multiplication and ME : Modular exponentiation. Time complexities are calculated based on the time taken by the cryptographic operations t_h, t_m, t_s, t_e. Time taken by one hash function t_h is 0.003997 ms, time taken by one multiplicative function t_m is 0.298595 ms, time taken by symmetric encryption/decryption t_s is 0.020206 ms and t_e is 2.080552 ms (Wu et al., 2018). Based on these time results, time complexities for the proposed scheme is 10.007923ms and the other schemes are calculated as 0.176973 ms, 0.196516 ms and 1.402666 ms respectively. Though the proposed scheme takes more time than the other schemes it achieves better security compared to other schemes.

Table 6.4 Computational cost comparison

Entities	**Proposed Scheme**	**Gope and Hwang (2016a)**	**Wu et al. (2016)**	**Lee et al. (2017)**
C_{MU}	$11T_h$+$3T_{\oplus}$+$20T_{||}$	$8T_h$+$8T_{\oplus}$+$8T_{||}$	$12T_h$+$9T_{\oplus}$+$23T_{||}$	$12T_h$+$11T_{\oplus}$+$8T_{||}$
C_{FA}	$4T_h$+$3T_{\oplus}$+$8T_{||}$	$1T_h$+$3T_{\oplus}$+$2T_{||}$	$5T_h$+$1T_{\oplus}$+$16T_{||}$	$8T_h$+$3T_{\oplus}$+$9T_{||}$
C_{HA}	$7T_h$+$3T_{\oplus}$+$14T_{||}$	$6T_h$+$5T_{\oplus}$+$21T_{||}$	$14T_h$+$7T_{\oplus}$+$35T_{||}$	$10T_h$+$4T_{\oplus}$+$11T_{||}$
Total	$22T_h$+$9T_{\oplus}$+$42T_{||}$	$15T_h$+$16T_{\oplus}$+$31T_{||}$	$31T_h$+$17T_{\oplus}$+$74T_{||}$	$30T_h$+$18T_{\oplus}$+$28T_{||}$

Table 6.5 Efficiency comparison

Scheme / Phase	Proposed scheme				Gope and Hwang		Fan Wu et. al.			Lee et. al.	
Operations	HF	E/D	PM	ME	HF	E/D	HF	E/D	PM	HF	E/D
Registration phase	6	0	1	1	4	0	5	0	0	4	0
Login and authentication phase	18	4	4	3	11	4	26	2	4	26	0
Password change phase	4	0	0	0	4	1	11	0	0	4	3
Total no. of operations	28	4	5	4	19	5	42	2	4	34	3

6.6.3 Comparison of communication costs

Table 6.6 Communication overhead

Scheme	Handshakes	Communication overhead
Proposed scheme	4 messages	3836 bits
Gope and Hwang (2016a)	4 messages	2688 bits
Wu et al. (2016)	4 messages	5696 bits
Lee et al. (2017)	5 messages	2400 bits

Table 6.6 summarizes about the communication overhead between the proposed scheme and other schemes, namely Gope and Hwang's scheme (Gope and Hwang, 2016a), Fan Wu et al.'s scheme (Wu et al., 2016) and Lee et al.'s scheme (Lee et al., 2017) for login and authentication phase. The experimental results shows that the SHA-1 hash function requires 160-bits (Eastlake 3rd and Jones, 2001). Time-stamp requires 32 bits, user

identity, random numbers/nonce requires 160 bits, $x.P$ (ECC point (x_P, y_P)): 320 bits; 128-bit ciphertext for 128-bit plaintext block using symmetric encryption/decryption (using AES-128) (Banerjee et al., 2018). The proposed scheme yields better security compared to other schemes with the cost of 3836 bits.

6.6.4 Comparison of network performance metrics using NS2 tool

Network performance metrics like throughput, end to end delivery (eed) and packet delivery ratio (pdr) are calculated by carrying out the experiments in NS2 environment. The proposed scheme is compared with other schemes like Madhusudhan and Shashidhara (2019) and Madhusudhan and Shashidhara (2020) in terms of throughput, eed and pdr.

In table 6.7, the network scenarios with the number of MU, FA and HA are tabulated. To carry out the experiments in NS2 environment, network scenarios (NS) are created with MU, FA and HA based on which the performance metrics are calculated. In each NS, the number of MUs are increased to evaluate the load of the network.

Fig. 6.13 compares the throughput of the proposed scheme with other schemes. Fig. 6.14 compares the end to end delivery of the proposed scheme with other schemes. 6.15 compares the packet delivery ratio of the proposed scheme with other schemes.

Table 6.7 Network scenarios

Network Scenarios (NS)	Proposed scheme			Scheme A			Scheme B		
Entities	MU	FA	HA	MU	FA	HA	MU	FA	HA
NS1	5	1	1	4	1	1	4	1	1
NS2	10	1	1	7	1	1	8	4	1
NS3	20	1	1	8	2	1	12	4	1
NS4	30	1	1	0	0	0	0	0	0

A: Madhusudhan and Shashidhara (2019) *B*: Madhusudhan and Shashidhara (2020)

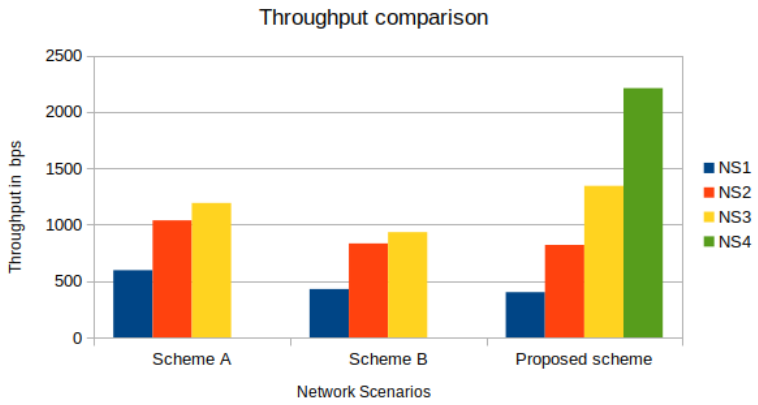

Figure 6.13 Throughput

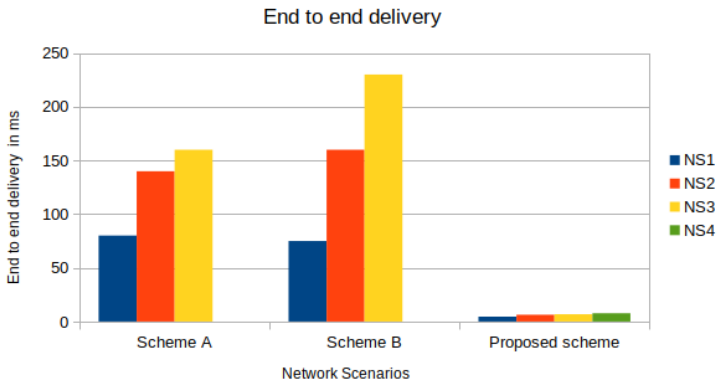

Figure 6.14 End to end delivery

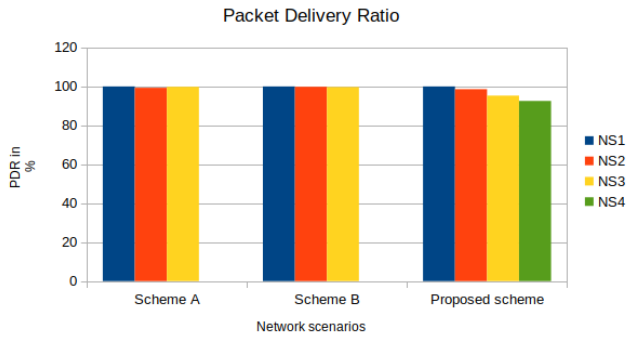

Figure 6.15 Packet delivery ratio

Scheme A: Madhusudhan and Shashidhara (2019)

Scheme B: Madhusudhan and Shashidhara (2020)

6.7 Summary

The proposed scheme designed for cellular networks is resistant towards the security attacks like replay, insider, offline password guessing, stolen smart card, traffic analysis, eavesdropping, impersonation and forgery attacks. The proposed scheme also achieves the security goals like perfect forward secrecy, mutual authentication and user anonymity. The proposed scheme is formally verfied using AVISPA tool. AVISPA tool is used to validate the resistance of the security attacks of the protocol. The proposed scheme is efficient in terms of computational and communication cost. With less communication overhead the proposed scheme achieves all the desirable security attributes. The proposed scheme is simulated using NS2.35 simulator and the performance metrics such as throughput, end to end delay and packet delivery ratio are computed. The computed results shows that the performance of the proposed scheme is highly efficient for practical use. Hence, the scheme is light weight and practically implementable.

CHAPTER 7

An Efficient Two Factor Authentication Scheme Providing Secure Communication in Evolved Packet System

7.1 Introduction

Cloud computing is an emerging technology which contains the applications, hardware and the systems software. Applications are delivered as services over the internet. Hardware and systems software are stored in the data centres and they are responsible for providing those services. The major role of cloud computing is that it offers the services to its users. The services offered by the cloud service providers are: Software as a Service (SaaS), Platform as a Service (PaaS) and infrastructure as a service (IaaS). Cloud computing is also known as on demand computing, utility computing or pay as you go computing (Choudhury et al., 2011).

The increased usage of mobile devices led the rapid development of mobile computing by increase in the number of applications in the mobile device. The applications targeted at mobile devices can be categorised into various fields such as entertainment, e-commerce, digital banking, health, games, social networking, travelling and news. All these applications can be browsed through mobile app download centers such as Apple's, iTunes, Android's playstore or Nokia's Ovi suite (Fernando et al., 2013). Mobile computing provides a tool for its users to access these applications irrespective of its user movement and location.

In mobile cloud computing, mobile users and service providers communicate with

each other over wireless medium. Since the communication takes place over wireless medium the communication channel is not secure and it is prone to many security attacks such as identity tracing, impersonation attack, replay attack, denial of service attack, offline password guessing attack, forgery attack etc. (Jegadeesan et al., 2019). Computing efficiency of the mobile devices are limited due to the limited bandwidth. Hence, it is important to design an efficient authentication scheme for mobile cloud computing. The entities involved in the communication are: Mobile User (MU), Trusted Third Party (TTP) and Service Provider (SP). Mobile users cannot store the information of all the service providers that are offering services to the mobile users due to its limited storage. Thus, authenticating SP becomes important to achieve mutual authentication. The main objective of this chapter is to achieve mutual authentication, preserve user identity and to protect data from breaching.

The remainder of this chapter is organised as follows. Section 7.2 briefs about the proposed scheme. Section 7.3 explains the security analysis of the proposed scheme. Section 7.4 illustrates about the simulation results of the proposed scheme using AVISPA tool. Section 7.5 explains about the performance enhancement of the proposed scheme. Section 7.6 concludes the chapter.

7.2 Proposed scheme

The proposed scheme is divided into three phases, they are: the registration phase that is carried over secure channel, login and authentication phase is carried over insecure channel and the password change phase. The proposed scheme makes use of Diffie and Hellman (1976) key exchange protocol to compute the secret key K_{HF} exchanged between TTP and SP. MU and SP exchange symmetric encryption key E_k to encrypt the messages. The proposed scheme makes use of elliptic curve cryptography (Koblitz et al., 2000). The domain parameters $\{E_{(F_p)}, G, a, b, p\}$ of the elliptic curve cryptography are shared among the three communicating entities. Notations used in this chapter are described in the table 7.1.

Table 7.1 Notations and cryptographic functions

Symbol	Definition
MU	Mobile User
FA	Foreign Agent
HA	Home Agent
ID_{MU}	MU's identity
PW_{MU}	MU's password
ID_{SP}	Service provider's identity
ID_{TTP}	Trusted third party identity
SK	Session key between FA and MU
K_{HF}	Secret key shared between the TTP and SP
$E_k(.)$	The symmetric encryption function with the key k
$D_k(.)$	The symmetric decryption function with the key k
P	Large prime number
Z_N^*	$Z_N^* \stackrel{def}{=} \{x \in Z_N : gcd(x,N) = 1\}$ = elements of Z_N with multiplicative inverses.

7.2.1 Registration phase

During the registration phase, MU is free to choose his/her identity ID_{MU}, password PW_{MU} and random number R_m. MU computes $PID_{MU} = h(h(PW_{MU}) \oplus h(R_m))$. After computation, MU submits the chosen ID_{MU} and PID_{MU} to the SP over secure channel. SP receives the request from MU. After that SP computes $K1 = h(ID_{MU}||X)$, X is secret key of SP computed as $X = R_hP$, where R_h is a random number chosen by the SP and P is a point on elliptic curve. SP further computes $S = h(ID_{MU}||PID_{MU})$. SP stores K1 in its database for future communication. SP sends the smart card with the parameters $\{S, ID_{SP}, h(.)\}$ to the MU. MU on receiving the smart card parameters, stores its random number R_m into the smart card. Smart card contains the parameters $\{S, ID_{SP}, R_m, h(.)\}$. Registration phase is illustrated in the Figure 7.1.

7.2.2 Login and authentication phase

Login and authentication phase is illustrated in the Figure 7.2.

1. Smart card is inserted into the smart card terminal by the MU. Smart card terminal asks for the input of ID_{MU} and password PW_{MU} of the MU. After entering

Mobile User

Service Provider

MU chooses his/her
identity ID_{MU} , password PW_{MU} and random number R_m .
MU computes
$PID_{MU} = h(h(PW_{MU}) \oplus h(Rm))$.
After computation, MU submits the chosen ID_{MU} and PID_{MU}
to the SP over secure channel.

$\{ID_{MU}, PW_{MU}\}$

After that SP computes
$K_1 = h(ID_{MU} || X)$, X is secret
key of SP computed as $X = R_h P$, where R_h is a random
number chosen by the SP and P is a point on elliptic curve.
SP further computes
$S = h(ID_{MU} || PID_{MU})$.
SP stores K1 in its database for future communication.
SP sends the smartcard with the parameters
{S, ID SP , h(.)} to the MU.

{S, ID SP , h(.)}

MU on receiving the smart card parameters, stores its random
number R_m into the smart card.
Smart card contains the parameters{S, ID SP, R_m , h(.)}.

Figure 7.1 Registration phase

the input, the smart card computes $S^* = h(ID_{MU}||h(h(PW_{MU}) \oplus h(R_m)))$, verifies whether $S^* \stackrel{?}{=} S$. If it holds true, random number N_m is produced by the smart card and computes $C_1 = N_m P$

$P = h(ID_{MU}||C_1||ID_{SP})$. Finally MU forms the message

$M_1 = \{P, E_k(ID_{MU}), C_1, ID_{SP}\}$, message M_1 is then transmitted to the TTP.

2. $M_2 = \{P, E_k(ID_{MU}), C_1, ID_{SP}, C_2, ID_{TTP}\}$.

   After receiving the message $M_1 = \{P, E_k(ID_{MU}), C_1, ID_{SP}\}$ from MU. TTP generates random number N_f and computes $C_2 = N_f P$ forms the message

   $M_2 = \{P, E_k(ID_{MU}), C_1, ID_{SP}, C_2, ID_{TTP}\}$, where ID_{TTP} is the identity of the TTP and sends to the SP.

3. $M_3 = \{Q, ID_{SP}\}$.

   After receiving the message $M_2 = \{P, E_k(ID_{MU}), C_1, ID_{SP}, C_2, ID_{TTP}\}$.

   SP decrypts $D_k(E_k(ID_{MU}))$ and reveals ID_{MU}. SP computes $P^* = h(ID_{MU}||C_1||ID_{SP})$. SP verifies whether $P^* \stackrel{?}{=} P$. If it holds true, MU authenticity is verified. SP computes $SK = h(C_1||C_2||ID_{MU}||ID_{TTP})$

   $Q = SK \oplus h(K_{HF}||C_2||ID_{TTP})$. SP forms message $M_3 = \{Q, ID_{SP}\}$ and sends it to the TTP.

4. $M_4 = \{T, N_f, ID_{TTP}\}$.

   On receiving the message $M_3 = \{Q, ID_{SP}\}$ from SP. TTP computes

   $SK = Q \oplus h(K_{HF}||N_f||ID_{TTP})$

   $Q^* = SK \oplus h(K_{HF}||N_f||ID_{TTP})$ checks whether $Q^* \stackrel{?}{=} Q$. If true, TTP computes

   $R = SK \oplus h(C_2||ID_{TTP})$

   $T = R \oplus h(C_1||C_2)$. Finally TTP computes the session key as $SK1 = h(C_1||C_2||N_f C_1)$ and forms message $M_4 = \{T, C_2, SK1, ID_{TTP}\}$ and sends it to the MU.

5. $M_4 = \{T, C_2, SK1, ID_{TTP}\}$

   On receiving the message from TTP. MU computes

   $R^* = T \oplus h(C_2||ID_{TTP})$

   $SK = R^* \oplus h(C_2||ID_{TTP})$

   $SK^* = h(C_1||C_2||ID_{MU}||ID_{TTP})$. Verifies if $SK^* \stackrel{?}{=} SK$.

If it holds true, then MU authenticates TTP and confirms that message comes from the trusted SP. Finally MU computes the session key as
$SK1 = h(C_1||C_2||N_mC_2)$.

7.2.3 Password change phase

During the password change phase, terminal allows the MU to change the current password PW_{MU}^{old} with the new password PW_{MU}^{new}, MU has to insert his/her smart card in to the terminal. After inserting MU has to provide his/her credentials to the terminal. Once the MU enters ID_{MU} and current password PW_{MU}^{old}, terminal processes the information. Then the smart card computes $S^* = h(ID_{MU}||h(h(PW_{MU}) \oplus h(R_m)))$, verifies whether $S^* \stackrel{?}{=} S$. After validating, the MU will be able to update the current password PW_{MU}^{old} with the new password PW_{MU}^{new}. The smart card asks the MU to enter the new password PW_{MU}^{new}. After that the smart card computes $S^{'} = h(ID_{MU}||h(h(PW_{MU}) \oplus h(R_m)))$. The parameter S which is stored in the smart card is replaced with $S^{'}$. The smart card contains the parameters $\{S^{'}, ID_{SP}, h(.)\}$.

7.3 Security analysis

In this section, the security analysis of the proposed scheme has been done.

7.3.1 User anonymity is protected

The proposed two factor authentication scheme for mobile cloud computing provides strong user anonymity in an efficient manner. During the registration phase of the proposed scheme, MU sends ID_{MU}, PID_{MU} to the service provider (SP). After receiving the request, SP computes $K_1 = h(ID_{MU}||X)$, X is secret key of SP computed as $X = R_hP$, where R_h is a random number chosen by the SP and P is a point on elliptic curve. SP stores K_1 in its database for future communication. Since ID_{MU} is concatenated with X the secret key of the SP which is computed using elliptic curve cryptography. Due to the complexity of ECC, it is difficult for an adversary to arrive at ID_{MU}. Given point P on elliptic curve E, it is difficult to compute $X = R_hP$, where R_h is a random number chosen by the SP.

Mobile User

Trusted Third Party (TTP)

Service Provider

After entering the input, the smart card computes

$S^* = h(ID_{MU} \| h(h(PW_{MU}) \oplus h(R_m)))$.

Verifies whether $S^* =? S$. If it holds true, random number N_m is generated by the smart card and computes

$C_1 = N_m P$

$P = h(ID_{MU} \| C_1 \| ID_{SP})$.

$M_1 = \{P, E_k (ID_{MU}), C_1, ID_{SP}\}$ →

After receiving the message M_1. TTP generates random number N_f and computes

$C_2 = N_f P$.

$M_2 = \{P, E_k (ID_{MU}), C_1, ID_{SP}, C_2, ID_{TTP}\}$ →

SP decrypts $D_k (E_k (ID_{MU}))$ and reveals ID_{MU}. SP computes

$P^* =? h(ID_{MU} \| C_1 \| ID_{SP})$.

SP verifies whether $P^* =? P$. If it holds true, MU authenticity is verified. SP computes

$SK = h(C_1 \| C_2 \| ID_{MU} \| ID_{TTP})$

$Q = SK \oplus h(K_{HF} \| C_2 \| ID_{TTP})$

← $M3 = \{Q, ID_{SP}\}$

TTP computes $SK = Q \oplus h(K_{HF} \| N_f \| ID_{TTP})$

$Q^* =? SK \oplus h(K_{HF} \| N_f \| ID_{TTP})$

checks whether $Q^* =? Q$. If true, TTP computes

$R = SK \oplus h(C_2 \| ID_{TTP})$

$T = R \oplus h(C_1 \| C_2)$.

Finally TTP computes the session key as

$SK_1 = h(C_1 \| C_2 \| N_f C_1)$

← $M4 = \{T, C_2, SK_1, ID_{TTP}\}$

MU computes

$R^* = T \oplus h(C_2 \| ID_{TTP})$

$SK = R^* \oplus h(C_2 \| ID_{TTP})$

$SK^* = ? h(C_1 \| C_2 \| ID_{MU} \| ID_{TTP})$.

Verifies if $SK^* = ?$ SK. If it holds true, then MU authenticates TTP. Finally MU computes the session key as

$SK1 = h(C_1 \| C_2 \| N_m C_2)$.

Figure 7.2 Login and authentication phase

7.3.2 Security against impersonation attack

The proposed scheme authenticates each entity involved in the communication based on the secret keys exchanged between the entities.

1. Impersonate as MU

   During the message transmission in login and authentication phase over wireless medium, MU sends the message $M_1 = \{P, E_k(ID_{MU}), C_1, ID_{SP}\}$ to the Third Trusted Party (TTP). If the messages are intercepted by an adversary and makes attempts to reveal ID_{MU} the identity of the MU is difficult. Due to the fact that the ID_{MU} is encrypted with the symmetric encryption key E_k which is known to MU and SP. Thus, it is difficult for an adversary to impersonate a valid MU.

2. Impersonate as Trusted Third Party (TTP)

   SP and TTP exchange the secret key K_{HF} to mutually authenticate each other. When TTP sends $M_3 = \{Q, ID_{SP}\}$ to SP, SP authenticates TTP based on the secret key K_{HF} exchanged between SP and TTP.

7.3.3 Security against replay attack

In replay attack, adversary retransmits the intercepted messages to one of the communicating entities involved in the communication. In the proposed scheme, this attack is not possible because of the fact that the message $M_2 = \{P, E_k(ID_{MU}), C_1, ID_{SP}, C_2, ID_{TTP}\}$ contains the parameters $\{C_1, C_2\}$ that are computed using random numbers of MU and TTP respectively. These random numbers chosen will different for each session. Due to the complexity of ECC adversary will not be successful in revealing the random numbers concealed in the parameter C_1, C_2. Thus, the proposed scheme is resistant to replay attack.

7.3.4 Security against offline password guessing attack

In the proposed scheme, the smart card is personalised with the parameters $\{S, ID_{SP}, h(.)\}$ where S is computed as $S = h(ID_{MU}||h(h(PW_{MU}) \oplus h(R_m)))$. If the smart card falls in the hands of an adversary with the power analysis technique adversary will be able to

obtain the parameters of the smart card. However, with the available parameters adversary will still fail to guess the password due to the complexity of one way hash function. To arrive at the correct password PW_{MU} adversary must guess the unknown parameter ID_{MU} of the MU. After guessing, hash function should be used to verify if the guessed pair of ID_{MU}, PW_{MU} is correct or not. This requires lot of time and the probability of guessing accurate pair of ID_{MU}, PW_{MU}. Therefore, the proposed scheme protects offline password guessing attack.

7.3.5 Security against insider attack

In the proposed scheme, MU registers to SP by sending its user credentials ID_{MU}, PID_{MU} where $PID_{MU} = h(h(PW_{MU}) \oplus h(R_m))$ over secure channel. Since the password is hashed and for the hashed password the XOR operation is performed, if an inside attacker wants to reveal the password it is impossible due to the complexity of the one way hash function. Thus, the proposed scheme provides security against insider attack.

7.3.6 Security against man in the middle attack

In cryptographic protocols, mutual authentication between both communication sides is the most effective prevention method to the man-in-the-middle attack. In the proposed scheme, during login and authentication phase the messages $\{M_1, M_2, M_3, M_4\}$ are transmitted over an insecure channel. Suppose, an adversary listening to this channel intercepts all the login messages and tries to impersonate a legitimate MU SP and TTP, he/she fails to do so, due to the fact that in login message $M_1 = \{P, E_k(ID_{MU}), C_1, ID_{SP}\}$ identity of the MU ID_{MU} is concealed with the symmetric encryption key E_k. Only the valid SP will be able to decrypt $D_k[E_k(ID_{MU}]$ with their decryption key D_k. With the interception of the message $M_3 = \{Q, ID_{SP}\}$ adversary cannot arrive at session key SK computed as $SK = h(C_1||C_2||ID_{MU}||ID_{TTP})$, $Q = SK \oplus h(K_{HF}||C_2||ID_{TTP})$. In conjunction with the secret key K_{HF} computed using Diffie-Hellman protocol, ECC is also used to compute session key. In such case, it is impossible for an adversary to steal the secret keys due to the complexity of ECC. Therefore, the proposed scheme actively thwarts man in the middle attack.

7.4 Formal security verification using avispa tool

To provide the results of the formal security verification of the proposed scheme, AVISPA tool is used. Acronym AVISPA stands for Automated Validation of Internet Security Protocols and Applications, the proposed scheme is simulated and verified against the active and passive security attacks.

Three roles are used while implementation. The role MU describes the entity MU, role foreignagent describes the role of TTP and the role homeagent describes the role of SP in the proposed scheme. The output of the simulation is presented in Fig. 7.3.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/wowmom.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.04s
  visitedNodes: 8 nodes
  depth: 3 plies
```

Figure 7.3 Result of the analysis using OFMC backend

7.5 Performance analysis and comparison

This section evaluates performance of the proposed scheme with the others schemes like Gope and Hwang (2016a), Wu et al. (2016) and Lee et al. (2017) scheme in terms of computational cost. Table 7.2 summarizes the computational cost of the proposed scheme with the others schemes like Gope and Hwang (2016a), Wu et al. (2016) and Lee et al. (2017). Computational cost is calculated based on the number of operations

used by the MU, TTP and SP respectively during communication. Hash functions are denoted as T_h. XOR operations are denoted as $T_{\oplus}$. Concatenation operations are denoted as $T_{||}$. C_{MU}, C_{TTP}, C_{SP} represents the computations of the MU, TTP and SP respectively.

Table 7.2 Computational cost comparison

Entities	**Proposed Scheme**	Gope and Hwang (2016a)	Wu et al. (2016)	Lee et al. (2017)
C_{MU}	$12T_h$+$3T_{\oplus}$+$10T_{||}$	$8T_h$+$8T_{\oplus}$+$8T_{||}$	$12T_h$+$9T_{\oplus}$+$23T_{||}$	$12T_h$+$11T_{\oplus}$+$8T_{||}$
C_{TTP}	$4T_h$+$4T_{\oplus}$+$8T_{||}$	$1T_h$+$3T_{\oplus}$+$2T_{||}$	$5T_h$+$1T_{\oplus}$+$16T_{||}$	$8T_h$+$3T_{\oplus}$+$9T_{||}$
C_{SP}	$5T_h$+$1T_{\oplus}$+$9T_{||}$	$6T_h$+$5T_{\oplus}$+$21T_{||}$	$14T_h$+$7T_{\oplus}$+$35T_{||}$	$10T_h$+$4T_{\oplus}$+$11T_{||}$
Total	$21T_h$+$8T_{\oplus}$+$27T_{||}$	$15T_h$+$16T_{\oplus}$+$31T_{||}$	$31T_h$+$17T_{\oplus}$+$74T_{||}$	$30T_h$+$18T_{\oplus}$+$28T_{||}$

Table 7.3 summarizes handshakes and the communication overhead between the proposed scheme and other schemes for login and authentication phase. We assume that the SHA-1 hash function requires 160-bits (Eastlake 3rd and Jones, 2001). Timestamp requires 32 bits, user identity requires 160 bits, random numbers/nonce requires 160 bits. In the proposed scheme the login message $M_1 = \{P, E_k(ID_{MU}), C_1, ID_{SP}\}$ requires (160+128+320+160)=768 bits. $M_2 = \{P, E_k(ID_{MU}), C_1, ID_{SP}, C_2, ID_{TTP}\}$ requires (160+128+320+160+320+160)=1248 bits, $M_3 = \{Q, ID_{SP}\}$ requires (160+160) =320 bits and $M_4 = \{T, C_2, SK1, ID_{TTP}\}$ requires (160+160+160+160)=640 bits. Thus the computational overhead of the proposed scheme is 768+1248+320+160+640=3136 bits. The proposed scheme is more suitable for the practical implementation.

Table 7.3 Handshakes/overhead comparison of the proposed scheme with other schemes

Scheme	Handshakes	Communication overhead
Proposed scheme	4 messages	3136 bits
Gope and Hwang (2016a)	4 messages	2688 bits
Wu et al. (2016)	4 messages	5696 bits
Lee et al. (2017)	5 messages	2400 bits

7.6 Summary

In this chapter, we have done rigorous study of the two factor authentication schemes in mobile cloud computing, the study led us to find out some of the security weaknesses which are to be addressed, while designing two factor authentication schemes. To provide better security, a new scheme is proposed. The proposed scheme is resilient to the security attacks like impersonation, offline password guessing replay attack and insider attack. The proposed scheme also achieves the security goals like user anonymity and mutual authentication. Secret key is computed using Diffie-Hellman key exchange protocol, this secret key is exchanged between the two entities TTP and SP during communication to authenticate each other. Furthermore the proposed scheme is simulated using AVISPA tool to formally verify whether the proposed scheme is secure against active and passive security attacks. In comparison with the computational cost and communication overhead of the proposed scheme with the others schemes such as Gope and Hwang's scheme, Fan Wu et al.'s scheme and Lee et al.'s scheme, the proposed scheme operates with less cost and the communication overhead is also less. Therefore, the proposed scheme is more robust and practically implementable.

CHAPTER 8

Conclusion and Future work.

8.1 Conclusion

This chapter summarizes the major contributions of the thesis. It also highlights the road-map for future research directions in the field of authentication in wireless and mobility environments.

8.1.1 Contributions

The contributions of the thesis are summarized as follows. We have analysed and proposed several authentication protocols for roaming service in global mobility networks, which are the following:

1. Researchers have developed many two factor authentication schemes for GLOMONET. However, with the thorough literature survey, it is observed that the authentication schemes developed are susceptible to several security attacks and also the schemes could not achieve few security goals. Through careful crypt-analysis, it has been identified several security weaknesses in Gope and Hwang (2016a), Lee et al. (2017) and Wu et al. (2016) authentication schemes. To overcome these security weaknesses, a secure and lightweight authentication scheme for roaming service in GLOMONET is proposed.

2. The proposed novel authentication scheme is formally verified against active and passive security attacks using widely accepted tool AVISPA.

3. The proposed scheme for GLOMONET measures the network performance met-

rics like throughput, end to end delay and packet delivery ratio using NS2 simulator.

The first contribution provided in **Chapter 4**, the cryptanalysis of Gope and Hwang (2016a) scheme has been done, with the thorough cryptanalysis of their scheme, we have proved that their scheme is vulnerable to various security attacks like stolen smart card, offline password guessing, MU impersonation and replay attack. Further, their scheme fails to achieve security goals like user anonymity and perfect forward secrecy. To overcome the security attacks of their scheme and to achieve the security goals, a new scheme has been proposed. Through the rigorous informal and formal security analysis, we have demonstrated that the proposed scheme is secure against the security attacks. Furthermore, we have simulated the proposed scheme using widely accepted AVISPA (Automated Validation of Internet Security Protocols and Applications) tool. With the simulated result of the proposed scheme, we show that the proposed scheme is secure against active and passive security attacks. Additionally, the proposed scheme is compared with Gope and Hwang scheme and other related schemes in terms of performance, computational cost and communication overhead. In comparison with other schemes, the proposed scheme is efficient and robust. This makes the proposed scheme suitable for practical implementation.

In the second contribution **Chapter 5**, Wu et al. (2016) scheme has been reviewed. They claimed that their scheme is resilient to several attacks. However, with thorough cryptanalysis of their scheme, we have proved that their scheme is vulnerable to several attacks. To overcome these security issues, a new scheme is proposed. The proposed scheme resists security attacks like impersonation, replay, stolen smart card, offline password guessing, stolen verifier and insider attack. The proposed scheme also achieves security goals like perfect forward secrecy, mutual authentication, local password verification, no time synchronization, user anonymity and user friendliness. Furthermore, we have simulated the proposed scheme using widely accepted AVISPA (Automated Validation of Internet Security Protocols and Applications) tool. With the simulated results of the proposed scheme, we show that the proposed scheme is secure against active and passive security attacks. Additionally, the proposed scheme is

compared with Fan Wu et al.'s scheme and other existing schemes in terms of performance, computational cost and communication overhead. In comparison with the other schemes, the proposed scheme is light-weight and robust. This makes the proposed scheme suitable for practical implementation.

In the third contribution **Chapter 6**, we have developed security architecture for GSM networks. Two factor authentication scheme is developed to address the security features such as user anonymity and privacy preservation during roaming scenario in GLObal MObility NETwork. While roaming MU needs to access the services of the FA, FA grants the service request only to the authenticated MU. To verify the authenticity of the MU, FA sends the service request of MU to HA. HA verifies the authenticity of the MU after which FA allows the MU to access the services. The entire communication during roaming is carried over insecure channel. Due to this, security concern is raised. The main objective of the proposed protocol is to secure the channel and to over come all active and passive security attacks. Since, the protocol is designed for mobile networks, it should be light weight with less communication cost, one such protocol has been proposed in this chapter. The proposed protocol is light weight with less communication cost. The proposed protocol is simulated using NS2.35 simulator and the performance metrics such as throughput, end to end delivery and packet delivery ratio are computed. Additionally, the proposed protocol addresses the active and passive security attacks that exists in cellular networks which is formally verified using AVISPA tool. The protocol is efficient in terms of computational and communication cost. The proposed scheme is robust and practically implementable.

The final contribution **Chapter 7**, we have developed the security framework for mobile cloud computing environment. Integration of mobile networks with cloud computing platform led to development of mobile cloud computing. Since the communication between mobile devices and the cloud computing occur over wireless medium, securing the network becomes paramount. With the thorough literature survey, we found that many two factor authentication schemes proposed so far to preserve user anonymity are vulnerable to various security attacks, they also had shortcomes to achieve security goals. To overcome the issues related to the two factor authentication schemes in

mobile cloud computing, a new scheme is proposed. Furthermore, we have simulated the proposed scheme using widely accepted AVISPA (Automated Validation of Internet Security Protocols and Applications) tool. With the simulated result of the proposed scheme, we show that the proposed scheme is secure against active and passive security attacks. Additionally, the proposed scheme is compared with Gope and Hwang's scheme and other related schemes in terms of computational cost and communication overhead. The proposed scheme is efficient, robust and suitable for practical implementation.

8.1.2 Future scope

This section suggests some directions for possible future works. Several research directions are worth investigating as follows.
One of the future research direction includes extending the proposed two factor authentication protocol to LTE-A cellular networks. The security concerns in the 5G architecture can be addressed as following

1. Two factor authentication schemes can be used to develop trust model for 4G-5G networks.

2. Two factor authentication schemes can be used in the security framework of the 5G networks to resist active and passive security attacks.

3. Two factor authentication schemes can be used to secure the communication between the mobile users, MEC servers and the core network.

BIBLIOGRAPHY

Banerjee, S., Odelu, V., Das, A. K., Chattopadhyay, S., Kumar, N., Park, Y., and Tanwar, S. (2018). Design of an anonymity-preserving group formation based authentication protocol in global mobility networks. *IEEE Access*, 6, 20673–20693.

Bellare, M., Pointcheval, D., and Rogaway, P. (2000). Authenticated key exchange secure against dictionary attacks. In *International conference on the theory and applications of cryptographic techniques*, 139–155. Springer.

Bonneau, J. (2012). The science of guessing: analyzing an anonymized corpus of 70 million passwords. In *2012 IEEE Symposium on Security and Privacy*, 538–552. IEEE.

Burrows, M., Abadi, M., and Needham, R. (1988). Authentication: A practical study in belief and action. In *Proceedings of the 2nd Conference on Theoretical Aspects of Reasoning about Knowledge*, 325–342. Morgan Kaufmann Publishers Inc.

Buttyan, L., Gbaguidi, C., Staamann, S., and Wilhelm, U. (2000). Extensions to an authentication technique proposed for the global mobility network. *IEEE Transactions on Communications*, 48(3), 373–376.

Chang, C. and Cheng, T. (2011). A robust and efficient smart card based remote login mechanism for multi-server architecture. *International Journal of Innovative Computing, Information and Control*, 7(8), 4589–4602.

Chang, C., Lee, C., and Chiu, Y. (2009). Enhanced authentication scheme with

anonymity for roaming service in global mobility networks. *Computer Communications*, 32(4), 611–618.

Chen, C. (2013). Improved efficient authentication scheme with anonymity in global mobility networks. *International Journal of Innovative Computing, Information, and Control*, 9(8), 3319–3339.

Chen, C., He, D., Chan, S., Bu, J., Gao, Y., and Fan, R. (2011). Lightweight and provably secure user authentication with anonymity for the global mobility network. *International Journal of Communication Systems*, 24(3), 347–362.

Chen, C.-T. and Lee, C.-C. (2015). A two-factor authentication scheme with anonymity for multi-server environments. *Security and Communication Networks*, 8(8), 1608–1625.

Choudhury, A. J., Kumar, P., Sain, M., Lim, H., and Jae Lee, H. (2011). A strong user authentication framework for cloud computing. In *Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific*, 110–115. IEEE.

Das, A. K. (2015). A secure and robust password-based remote user authentication scheme using smart cards for the integrated epr information system. *Journal of medical systems*, 39(3), 1–14.

Diffie, W. and Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, 22(6), 644–654.

Eastlake 3rd, D. and Jones, P. (2001). Us secure hash algorithm 1 (sha1). Technical report.

ElGamal, T. (1984). A public key cryptosystem and a signature scheme based on discrete logarithms, crypto 84 lncs. 196, 10–18.

Farash, M. S. and Attari, M. A. (2014). An efficient and provably secure three-party password-based authenticated key exchange protocol based on chebyshev chaotic maps. *Nonlinear Dynamics*, 77(1), 399–411.

Fernando, N., Loke, S. W., and Rahayu, W. (2013). Mobile cloud computing: A survey. *Future generation computer systems*, 29(1), 84–106.

FIPS, 180-1, P. (Apr. 1995). *Secure Hash Standard, U.S. Dept. Commerce, Nat. Inst. Standards Technol.,Washington, DC, USA*, 1–28.

Glouche, Y., Genet, T., Heen, O., and Courtay, O. (2006). A security protocol animator tool for avispa. In *ARTIST2 workshop on security specification and verification of embedded systems, Pisa*.

Gope, P. and Hwang, T. (2016a). An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks. *Journal of Network and Computer Applications*, 62, 1–8.

Gope, P. and Hwang, T. (2016b). Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks. *IEEE Systems Journal*, 10(4), 1370–1379.

Gope, P., Islam, S. H., Obaidat, M. S., Amin, R., and Vijayakumar, P. (2018). Anonymous and expeditious mobile user authentication scheme for glomonet environments. *International Journal of Communication Systems*, 31(2), 1–18.

Guttman, B. and Roback, E. A. (1995). *An introduction to computer security: the NIST handbook*. Diane Publishing.

Ha, J. (2015). An efficient and robust anonymous authentication scheme in global mobility networks. *International Journal of Security and Its Applications*, 9(10), 297–312.

He, D., Kumar, N., Chen, J., Lee, C.-C., Chilamkurti, N., and Yeo, S.-S. (2015). Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. *Multimedia Systems*, 21(1), 49–60.

He, D., Ma, M., Zhang, Y., Chen, C., and Bu, J. (2011). A strong user authentication scheme with smart cards for wireless communications. *Computer Communications*, 34(3), 367–374.

Hwang, K. and Chang, C. (2003). A self-encryption mechanism for authentication of roaming and teleconference services. *IEEE Transactions on Wireless Communications*, 2(2), 400–407.

Hwang, M. (1999). Dynamic participation in a secure conference scheme for mobile communications. *IEEE Transactions on Vehicular Technology*, 48(5), 1469–1474.

Hwang, M. and Yang, W. (1995). Conference key distribution schemes for secure digital mobile communication network. *IEEE J. Selected Areas Commun*, 13, 416–420.

Jegadeesan, S., Azees, M., Kumar, P. M., Manogaran, G., Chilamkurti, N., Varatharajan, R., and Hsu, C. H. (2019). An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications. *Sustainable Cities and Society*, 1–7.

Jiang, Q., Ma, J., Li, G., and Yang, L. (2013). An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. *Wireless Personal Communications*, 68(4), 1477–1491.

Kang, M., Rhee, H. S., and Choi, J. Y. (2011). Improved user authentication scheme with user anonymity for wireless communications. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 94(2), 860–864.

Karuppiah, M., Kumari, S., Li, X., Wu, F., Das, A. K., Khan, M. K., Saravanan, R., and Basu, S. (2017). A dynamic id-based generic framework for anonymous authen-

tication scheme for roaming service in global mobility networks. *Wireless Personal Communications*, 93(2), 383–407.

Karuppiah, M. and Saravanan, R. (2015). A secure authentication scheme with user anonymity for roaming service in global mobility networks. *Wireless Personal Communications*, 84(3), 2055–2078.

Kim, J. and Kwak, J. (2013). Secure and efficient anonymous authentication scheme in global mobility networks. *Journal of Applied Mathematics*, 2013(16), 1–13.

Kim, T. H., Kim, C., and Park, I. (2012). Side channel analysis attacks using am demodulation on commercial smart cards with seed. *Journal of Systems and Software*, 85(12), 2899–2908.

Kizza, J. M. (2009). *A guide to computer network security*. Springer.

Koblitz, N., Menezes, A., and Vanstone, S. (2000). The state of elliptic curve cryptography. In *Towards a quarter-century of public key cryptography*, 103–123. Springer.

Kocher, P., Jaffe, J., and Jun, B. (1998). Cryptography research. `http://www.cryptography.com/dpa/technical`.

Kumar, P., Lee, S.-G., and Lee, H.-J. (2012). E-sap: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. *Sensors*, 12(2), 1625–1647.

Kuo, W., Wei, H., and Cheng, J. (2014). An efficient and secure anonymous mobility network authentication scheme. *journal of information security and applications*, 19(1), 18–24.

Lee, C., Hwang, M., and Liao, I. (2006). Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Transactions on Industrial Electronics*, 53(5), 1683–1687.

Lee, C., Lai, Y., Chen, C., and Chen, S. (2017). Advanced secure anonymous authentication scheme for roaming service in global mobility networks. *Wireless Personal Communications*, 94(3), 1281–1296.

Lee, C.-C., Lin, T.-H., and Chang, R.-X. (2011). A secure dynamic id based remote user authentication scheme for multi-server environment using smart cards. *Expert Systems with Applications*, 38(11), 13863–13870.

Li, C. and Lee, C. (2012). A novel user authentication and privacy preserving scheme with smart cards for wireless communications. *Mathematical and Computer Modelling*, 55(1), 35–44.

Li, C.-T., Chen, C.-L., Lee, C.-C., Weng, C.-Y., and Chen, C.-M. (2018a). A novel three-party password-based authenticated key exchange protocol with user anonymity based on chaotic maps. *Soft Computing*, 22(8), 2495–2506.

Li, C.-T., Lee, C.-C., and Weng, C.-Y. (2013). An extended chaotic maps based user authentication and privacy preserving scheme against dos attacks in pervasive and ubiquitous computing environments. *Nonlinear Dynamics*, 74(4), 1133–1143.

Li, C.-T., Wu, T.-Y., Chen, C.-L., Lee, C.-C., and Chen, C.-M. (2017). An efficient user authentication and user anonymity scheme with provably security for iot-based medical care system. *Sensors*, 17(7), 1482.

Li, W., Li, R., Wu, K., Cheng, R., Su, L., and Cui, W. (2018b). Design and implementation of an sm2-based security authentication scheme with the key agreement for smart grid communications. *IEEE Access*, 6, 71194–71207.

Li, X., Niu, J., Kumari, S., Wu, F., and Choo, K. K. R. (2018c). A robust biometrics based three-factor authentication scheme for global mobility networks in smart city. *Future Generation Computer Systems*, 83, 607–618.

Liao, I. E., Lee, C. C., and Hwang, M. S. (2006). A password authentication scheme over insecure networks. *Journal of Computer and System Sciences*, 72(4), 727–740.

Liu, C.-H. and Chung, Y.-F. (2017). Secure user authentication scheme for wireless healthcare sensor networks. *Computers & Electrical Engineering*, 59, 250–261.

Lu, Y., Li, L., Peng, H., and Yang, Y. (2016). Robust anonymous two-factor authenticated key exchange scheme for mobile client-server environment. *Security and Communication Networks*, 9(11), 1331–1339.

Madhusudhan, R. and Mittal, R. (2012). Dynamic id based remote user password authentication schemes using smart cards: A review. *Journal of Network and Computer Applications*, 35(4), 1235–1248.

Madhusudhan, R. and Shashidhara, R. (2019). A secure anonymous authentication protocol for roaming service in resource-constrained mobility environments. *Arabian Journal for Science and Engineering*, 1–22.

Madhusudhan, R. and Shashidhara, R. (2020). Mobile user authentication protocol with privacy preserving for roaming service in glomonet. *Peer-to-Peer Networking and Applications*, 13(1), 82–103.

Madhusudhan, R. and Suvidha, K. (2017a). An efficient and secure user authentication scheme with anonymity in global mobility networks. In *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 19–24. IEEE.

Madhusudhan, R. and Suvidha, K. (2017b). An enhanced secure authentication scheme with user anonymity in mobile cloud computing. In *2017 International Conference on Public Key Infrastructure and its Applications (PKIA)*, 17–22. IEEE.

Mahmood, K., Naqvi, H., Alzahrani, B. A., Mehmood, Z., Irshad, A., and Chaudhry, S. A. (2018). An ameliorated two-factor anonymous key exchange authentication

protocol for mobile client-server environment. *International Journal of Communication Systems*, 31(18), 1–16.

Meshram, C., Obaidat, M. S., and Meshram, S. G. (2018). Chebyshev chaotic map-based id-based cryptographic model using subtree and fuzzy-entity data sharing for public key cryptography. *Security and Privacy*, 1(1), 1–9.

Messerges, T. S., Dabbish, E. A., and Sloan, R. H. (2002). Examining smart-card security under the threat of power analysis attacks. *IEEE transactions on computers*, 51(5), 541–552.

Mir, O., van der Weide, T., and Lee, C.-C. (2015). A secure user anonymity and authentication scheme using avispa for telecare medical information systems. *Journal of medical systems*, 39(9), 1–16.

Mun, H., Han, K., Lee, Y. S., Yeun, C. Y., and Choi, H. H. (2012). Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. *Mathematical and Computer Modelling*, 55(1), 214–222.

Nohl, K., Evans, D., Starbug, S., and Plotz, H. (2008). Reverse-engineering a cryptographic rfid tag. In *USENIX security symposium*, 28.

Suzuki, S. and Nakada, K. (1997). An authentication technique based on distributed security management for the global mobility network. *IEEE Journal on Selected Areas in Communications*, 15(8), 1608–1617.

Tsai, C. S., Lee, C. C., and Hwang, M. S. (2006). Password authentication schemes: Current status and key issues. *IJ Network Security*, 3(2), 101–115.

von Oheimb, D. (2005). The high-level protocol specification language hlpsl developed in the eu project avispa. In *Proceedings of APPSEM 2005 workshop*, 1–17.

Wang, D., He, D., Wang, P., and Chu, C. H. (2015). Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. *IEEE Transactions on Dependable and Secure Computing*, 12(4), 428–442.

Wang, D., Ma, C. g., Wang, P., and Chen, Z. (2012). Robust smart card based password authentication scheme against smart card security breach. *Cryptology ePrint Archive*, 439, 1–35.

Wei, Y., Qiu, H., and Hu, Y. (2006). Security analysis of authentication scheme with anonymity for wireless environments. In *2006 International Conference on Communication Technology*, 1–4. IEEE.

Wen, F., Susilo, W., and Yang, G. (2013). A secure and effective anonymous user authentication scheme for roaming service in global mobility networks. *Wireless personal communications*, 73(3), 993–1004.

Wu, C., Lee, W., Tsaur, W., et al. (2008). A secure authentication scheme with anonymity for wireless communications. *IEEE Communications Letters*, 12(10), 722–723.

Wu, F., Li, X., Xu, L., Kumari, S., and Sangaiah, A. K. (2018). A novel mutual authentication scheme with formal proof for smart healthcare systems under global mobility networks notion. *Computers & Electrical Engineering*, 68, 107–118.

Wu, F., Xu, L., Kumari, S., Li, X., Das, A. K., Khan, M. K., Karuppiah, M., and Baliyan, R. (2016). A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks. *Security and Communication Networks*, 9(16), 3527–3542.

Xie, Q., Bao, M., Dong, N., Hu, B., and Wong, D. S. (2013). Secure mobile user authentication and key agreement protocol with privacy protection in global mobility

networks. In *Biometrics and Security Technologies (ISBAST), 2013 International Symposium on*, 124–129. IEEE.

Xu, G., Liu, J., Lu, Y., Zeng, X., Zhang, Y., and Li, X. (2018). A novel efficient maka protocol with desynchronization for anonymous roaming service in global mobility networks. *Journal of Network and Computer Applications*, 107, 83–92.

Xu, J. and Feng, D. (2009). Security flaws in authentication protocols with anonymity for wireless environments. *ETRI journal*, 31(4), 460–462.

Xu, J., Zhu, W., and Feng, D. (2011). An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks. *Computer Communications*, 34(3), 319–325.

Yang, G., Wong, D. S., Wang, H., and Deng, X. (2006). Formal analysis and systematic construction of two factor authentication scheme (short paper). In *International Conference on Information and Communications Security*, 82–91. Springer.

Youn, T., Park, Y., and Lim, J. (2009). Weaknesses in an anonymous authentication scheme for roaming service in global mobility networks. *IEEE Communications Letters*, 13(7), 471–473.

Zhou, T. and Xu, J. (2011). Provable secure authentication protocol with anonymity for roaming service in global mobility networks. *Computer Networks*, 55(1), 205–213.

Zhu, J. and Ma, J. (2004). A new authentication scheme with anonymity for wireless environments. *IEEE Transactions on Consumer Electronics*, 50(1), 231–235.

LIST OF PUBLICATIONS:

Journal papers

- Madhusudhan, R and Suvidha K. (2019). A secure lightweight two-factor authentication scheme in global mobility networks. International Journal of Space-Based and Situated Computing, $9(2) : 109 - 123$. (ESCI Indexed)
  DOI: $10.1504/IJSSC.2019.104221$

- R Madhusudan and K S Suvidha. (2020). A Secure and Lightweight Authentication Protocol for Mobile User Preserving Privacy in Global Mobility Networks. Procedia Computer Science. $171(1) : 907 - 916$. (Scopus Indexed)
  DOI: $10.1016/j.procs.2020.04.098$

- R. Madhusudhan and K. S. Suvidha. (2021). Robust and Secure Authentication Protocol Protecting Privacy for Roaming Mobile User in Global Mobility Networks. International Journal of Grid and Utility Computing, $12(1) : 94 - 111$.
  DOI: $10.1504/IJGUC.2021.112488$

- R Madhusudan and K S Suvidha. An Enhanced and Secure Two-factor User Authentication Scheme for Roaming Service in Global Mobility Networks. Communicated to IEEE Transactions On Mobile Computing.
  (Decision: revise and resubmit).

- R Madhusudan and K S Suvidha. An Enhanced Secure Two Factor Authentication Scheme with Authenticated Key Establishment in Global Mobility Networks. Communicated to International Journal of Arabian Science and Engineering.
  (Under review).

Conference papers

- R. Madhusudhan and K. S. Suvidha (2017). "An efficient and secure user authentication scheme with anonymity in global mobility networks." In Advanced Information Networking and Applications Workshops (WAINA), 2017 31st International Conference on, pp. 19-24. IEEE.
  DOI: 10.1109/*WAINA*.2017.133.

- R. Madhusudhan and K. S. Suvidha (2017). "An enhanced secure authentication scheme with user anonymity in mobile cloud computing." In Public Key Infrastructure and its Applications (PKIA), 2017 International Conference on, pp. 17-22. IEEE.
  DOI: 10.1109/*PKIA*.2017.8278955.

- R. Madhusudhan and K. S. Suvidha(2019). An efficient two factor authentication scheme providing secure communication in mobile cloud computing. In 2019 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), pages 80-85. IEEE.
  DOI: 10.1109/*CCEM*48484.2019.00017.

BIO-DATA

Name	:	K S Suvidha
Email Id	:	suviks22@gmail.com
Mobile	:	+91-9880582391
Date of Birth	:	July 22, 1987
Address	:	D/o. S.Y. Korwar,
		# 016, Shashank aikya appartment,
		Ambabhavani temple, M S palya
		Bangalore - 560097.
		Karnataka, India.

Educational Qualifications:

Degree	Year of Passing	University
B.E.	2011	NMAMIT, Nitte, Mangaluru.
M. Tech.	2015	VTU University, Bangalore.