Robust and secure authentication protocol protecting privacy for roaming mobile user in global mobility networks

R. Madhusudhan* and K.S. Suvidha

Department of Mathematical and Computational Sciences,
National Institute of Technology Karnataka (Surathkal),
Karnataka, Mangalore, India
Email: madhurk96@gmail.com
Email: suviks22@gmail.com
*Corresponding author

Abstract: With the advent of new 5G technology there is a need to develop security architecture. Two factor authentication schemes are developed to address the security features such as user anonymity and privacy preservation during roaming scenario in GLObal Mobility NETwork. The entire communication during roaming is carried over insecure channel and owing to this, security concern is raised. The main objective of the proposed protocol is to secure the channel and to overcome all active and passive security attacks. The proposed protocol addresses the active and passive security attacks that exist in 5G cellular networks which are formally verified using AVISPA tool. 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. The protocol is efficient in terms of computational and communication cost. The proposed scheme is robust and practically implementable.

Keywords: GLOMONET; security; smartcard; ECC; timestamp; AVISPA, span; NS2; 4G; 5G; mobile edge computing.

Reference to this paper should be made as follows: Madhusudhan, R. and Suvidha, K.S. (2021) 'Robust and secure authentication protocol protecting privacy for roaming mobile user in global mobility networks', *Int. J. Grid and Utility Computing*, Vol. 12, No. 1, pp.94–111.

Biographical notes: R. Madhusudhan received his MTech degree in 2003 from NITK Surathkal, (A Deemed University) and PhD degree from IIT Roorkee in 2013. Currently, he is an Associate Professor in the Department of Mathematical and Computational Sciences at NITK, Surathkal, India. He teaches several courses such as Computer Networks, Internet Technology and Applications, Database Management Systems. He is Life Member of Computer Society of India and Indian Society for Technical Education. He is also a Member of ACM and IEEE. His current research includes network security, remote user authentication and mobile computation.

K.S. Suvidha received her BE degree in Information Science and Engineering from NMAM Institute of Technology Nitte in 2011 and MTech degree in Computer Science and Engineering from Visvesvaraya Technological University in 2015. Currently, she is an Assistant Professor in Ramaiah University of Applied Sciences and pursuing her PhD degree in the Department of Mathematical and Computational Sciences at National Institute of Technology Karnataka, Surathkal. Her research is focused on network security, remote user authentication, authentication protocols in mobile networks, mobile cloud security.

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.

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 (Karuppiah, M. and Saravanan, 2015). 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 article is to propose a secure authentication scheme, which addresses all the security challenges and achieves all the security goals.

5G are the next generation mobile wireless communications. 5G are the evolution over the 4G International Telecommunications Advanced Systems with many service capabilities. Ongoing research on 5G systems aims at various advanced characteristics such as higher capacity than current 4G and higher density of mobile broadband users and Device to Device (D2D) communications. The advanced features of 5G systems are as follows:

1–10 Gbps connectivity speed, provide lower latency of 1 ms, 100% network coverage, increase in the battery life for low power devices. To achieve these features in the 5G systems various technologies are applied to 5G systems such as Heterogenous Networks (HeNet), massive Multiple-Input Multiple-Output (MIMO), millimetre wave (mmWave), D2D communications, Software Defined Network (SDN), Network Functions Visualisation (NFV) and networking slicing. The new cellular architecture and the new technologies will impose various security challenges in the 5G system (Fang et al., 2017).

Security is the major challenge to address in wireless communications 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., 2018; 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 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 research article is to overcome the security challenges in the existing 5G system.

1.1 Motivations and contributions

With the advent of the new 5G system many technologies are developed to integrate into the 5G architecture to achieve 5G features. The development of the new technologies in 5G has led the security concerns. 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 physical layer that has to be addressed in cellular networks. To protect the voice and data over the wireless channel traditional security architectures are used. There is ongoing research work on security related to the technologies applied to LTE.

1 We have proposed the 4G-5G trust model to provide the security features to the LTE (Long Term Evolution) networks. 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 to provide security to the LTE networks.

3 The proposed protocol is formally verified 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 the paper is organised as follows. Section 2 provides the related work done on previous authentication schemes. Mobile edge computing architecture is explained in Section 3. The proposed scheme is explained in Section 4. 4G-5G trust model is explained in Section 5. In Section 6, security attacks and services of the proposed protocol are described. Formal verification of the security protocol is explained in Section 7. Section 8 shows the

simulation results of NS2.35 simulator. In Section 9, the performance of the proposed scheme is compared with the other related schemes. Section 10 concludes the paper.

2 Related work

Zhu and Ma (2004) also worked on authentication schemes designed for GLOMONET, with the thorough understanding of the authentication schemes, Zhu and Ma (2004) pointed out the authentication schemes are failing to preserve user anonymity.

Later, Lee et al. (2006) worked on Zhu and Ma (2004)authentication scheme. The study revealed that their scheme is susceptible to forgery attack and mutual authentication. To improvise Zhu and Ma's scheme, Lee et al. (2006) came up with a new scheme. Later, Wei et al. (2006) worked on Lee et al.'s (2006) scheme. With the thorough understanding of their scheme, Wei et al. found that their scheme failed to preserve user anonymity and untraceability. Further, Wei et al. also stated that their scheme 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) worked on Lee et al.'s scheme (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) worked on Lee et al.'s scheme (2006). To achieve better performance, Chang et al. came up with a new scheme. Later, Youn et al. (2009) worked on Chang et al.'s scheme (2009). To achieve the security goals and requirements, Youn et al. proposed a new scheme. In 2009, Xu and Feng (2009) worked on Wu et al.'s scheme (2008). To achieve better performance Xu and Feng (2009) came up with new scheme. He et al. (2011) worked on Wu et al.'s scheme (2008). To preserve user anonymity. He et al. (2011) came up with a new authentication scheme.

Li and Lee (2012) worked on He et al.'s (2011) scheme. Li et al. (2012) came up with a new scheme to resolve the security issues. Kim and Kwak (2013) worked on Mun et al. (2012), Wu et al. (2008) and Lee et al.'s (2006) schemes. With the thorough understanding of these schemes, Kim and Kwak found that these schemes are non-resilient to preserve user anonymity. Kim and Kwak (2013) came up with a new scheme to eliminate the security weaknesses.

Karuppiah et al. (2017) reviewed Miyoung Rhee's scheme (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 off-line 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. (2017) proposed a new scheme.

Further, Li et al. (2017) reviewed Karuppiah and Saravanan's scheme (2015) 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 Li et al. (2017) proposed a new scheme. Later, Li et al. (2018) reviewed Gope and Hwang's scheme (2016) 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, there 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. 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) reviewed Gope and Hwang's scheme (2016) 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) reviewed Lee et al.'s scheme (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.'s scheme (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. (2018) proposed a new scheme.

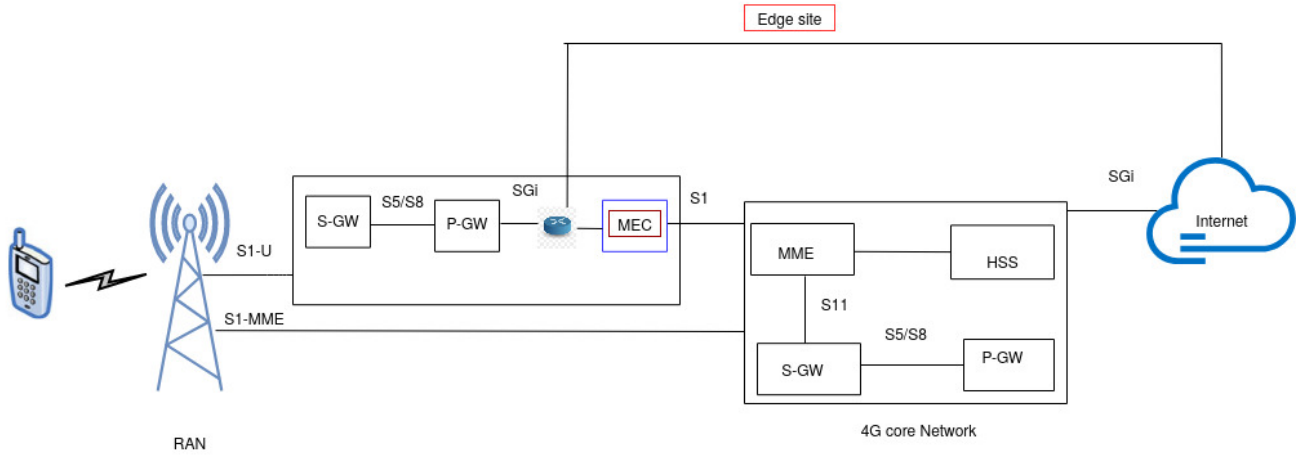
3 Mobile edge computing deployments in 4G and evolution towards 5G

The proposed scheme shows the compatibility of an European Telecommunications Standards Institute (ETSI) MEC system with 3 Generation Partnership Project (3GPP) 4G and 5G architectures.

The proposed scheme describes the potential deployment for operational 4G systems providing a technical insight of MEC operations under such scenarios showing how the creation of the mobile edge infrastructure in 4G can pave the way for 5G deployment.

Figure 1 shows the LTE 4G architecture. It is mainly divided into three main components. Firstly, the User Equipment (UE). Secondly, the Radio Access Network (RAN) and the third component is the Evolved Packet Core (EPC) the core network.

Figure 1 4G S-GW MEC deployment



The E-UTRAN (The access network) the architecture of Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) has been illustrated in the Figure 1. The E-UTRAN handles the radio communications between the mobile and the evolved packet core and just has one component, the evolved base stations, called eNodeB or eNB. Each eNB is a base station that controls the mobiles in one or more cells. The base station that is communicating with a mobile is known as its serving eNB. There are two main functions supported by eNB:

1 The eBN sends and receives radio transmissions to all the mobiles using the analogue and digital signal processing functions of the LTE air interface.

2 The eNB controls the low-level operation of all its mobiles, by sending them signalling messages such as handover commands.

Each eBN connects with the EPC the core network by means of the S1 interface.

The Evolved Packet Core (The core network) the architecture of Evolved Packet Core (EPC) has been illustrated in the Figure 1. The core network has four main components.

1 The Home Subscriber Server (HSS) component has been carried forward from UMTS and GSM and is a central database that contains information about all the network operator's subscribers.

2 The Packet Data Network (PDN) Gateway (P-GW) communicates with the outside world that is packet data networks PDN, using SGi interface. Each packet data network is identified by an access point name (APN). The PDN gateway has the same role as the GPRS support node (GGSN) and the Serving GPRS Support Node (SGSN) with UMTS and GSM.

3 The serving gateway (S-GW) acts as a router, and forwards data between the base station and the PDN gateway.

4 The Mobility Management Entity (MME) controls the high-level operation of the mobile by means of signalling messages and Home Subscriber Server (HSS).

3.1 MEC deployment as a middlebox

The deployment of MEC on LTE network is based on middlebox approach. MEC is connected to RAN through S1-U interface. MEC is deployed at RAN site. The MEC is connected to the eNB and the S-GW with the two NIC cards. The eNB sends the packets to the MEC's MAC address. MEC is assigned with the S-GW's IP address. The eNB considers MEC as its next hop, instead of the S-GW. The S-GW considers the MEC as a next hop to forward packets to the eNB via GTP tunnels.

GTP repackaging: UE's sends the IP packets over GTP tunnels to the eNB and S-GW. The transmitted packets are encapsulated into the GTP packets. The application servers that are hosted on MEC platform reads IP packets. Hence MEC decapsulates GTP packets to IP packets. The IP packets that should be transmitted over GTP tunnel should again be encapsulated into GTP packets and then transmit to the eNB. This GTP repackaging method requires identifying the tunnel ids associated with each UE. This can be done by maintaining a table with the entry of UE's IP address and its tunnel ID. With the help of the table MEC can formulate the correct GTP headers.

Traffic redirection via DNS: On receiving the IP packets from UE, MEC redirects it to its application servers using DNS service. DNS server returns the IP address of the MEC applications domain names. UE's applications can directly communicate with MEC's servers.

Edge cloud is applied to improve the network performance by reducing the communication delay. Central cloud is used to connect the edge clouds for data sharing and centralised control.

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: initialisation 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 $\left\{E_{(F_p)}, G, a, b, p\right\}$ of the elliptic curve cryptography are shared among the three communicating entities. A brief introduction to ECC is as follows.

Let F_p is a finite prime field, and p is a large prime number. The solutions $(x, y) \in Fp \times F_p$ of the equation $y^2 = x^3 + ax + b \bmod p$, where $a, b \in F_p$ and $4a^3 + 27b^2 \bmod p \neq 0$ which we call a non-singular elliptic curve, we ignore mod p in the later part along with so called point at infinity O forms a set E. An additional group G is a subgroup of E where its order is a large prime n, and P is a generator of group G. Elliptic Curve Discrete Logarithm Problem (ECDLP) Given an elliptic curve E defined over a finite prime field F_p, a point $P \in E\left(F_p\right)$ of order n and a point $Q \in E\left(F_p\right)$, it is hard to compute integer $0 \le \alpha \le n-1$, such that $Q = \alpha P$. Elliptic Curve Diffie-Hellman Problem (ECDHP). Given an elliptic curve E defined over a finite prime field F_p and points $P, \alpha P, \beta P \in E\left(F_p\right)$ it is difficult to compute $\alpha\beta P$, without the knowledge of $\{\alpha, \beta\}$ (Koblitz). Notations used in the proposed scheme are shown in Table 1.

Table 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^*	$\{1, 2, ..., n-1\}$ combined with multiplication of integers mod n, n is large prime number

4.1 Initialisation phase

Step 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.

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

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

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

4.2 Registration phase

- MU chooses identity and password ID_{MU}, PW_{MU} of his/her own choice and submits $h\left(ID_{MU} \| b\right)$ to the HA, where b is the random no. of the MU.
- 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 $\left(h\left(ID_{MU} \| b\right), Ctr_{MU}\right)$ in its database. HA computes
- $A = h\left(h\left(ID_{MU} \| b\right) \| X\right)$
- $B = A \oplus g^a mod\ q$. HA issues the smart card with the parameters $\left\{A, B, Ctr_{MU}, E_p\right\}$ to MU.
- MU on receiving the smart card, computes
- $C = h\left(h\left(ID_{MU} \| b \| PW_{MU}\right)\right)$. MU stores $\left\{A, B, C, Ctr_{MU}, b, E_p\right\}$ into the smart card.

4.3 Login and mutual authentication phase

- 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

$$C_1 = \alpha P$$

$$P = E_k\left(h\left(ID_{MU} \| b\right)\right)$$

$$D = C \oplus Ctr_{MU} \oplus C_1$$

$E = h\left(h\left(ID_{MU} \| b\right) \| D \| Ctr_{MU} \| ID_{HA} \| T_1\right)$. MU forms the message $M_1 = \left\{P, D, E, C_1, T_1, Ctr_{MU}\right\}$ and sends to FA at T_1.

- On receiving the message M_1 from MU, FA verifies if $\Delta T \le T_2 - T_1$. If true, FA generates random number $\beta \in Z_n^*$ and computes

$$C_2 = \beta P$$

$F = h(D \| C_1 \| E \| T_1 \| T_2) \oplus g^b \bmod q$. 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.

- 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 $\Delta T \le T_3 - T_2$. 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 $F^* = h(D \| C_1 \| E \| T_1 \| T_2) \oplus g^{ab} \bmod q$. 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. Else, 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

$$G = h(C_2 \| T_3) \oplus g^a \bmod q$$

$H = h(C_1 \| Ctr_{MU} \| T_3)$. MU forms the message $M_3 = \{H, G, T_3\}$ to FA at T_3.

- After receiving $M_3 = \{H, G, T_3\}$ at T_4 from HA, FA verifies if $\Delta T \le T_4 - T_3$. If true, FA computes

$G^* = h(C_2 \| T_3) \oplus g^{ab} \bmod q$ 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.

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

4.4 Password change phase

Procedure for password change phase is described in detail.

- 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 $C' = h(h(ID_{MU} \| b \| PW_{MU}^{new}))$.

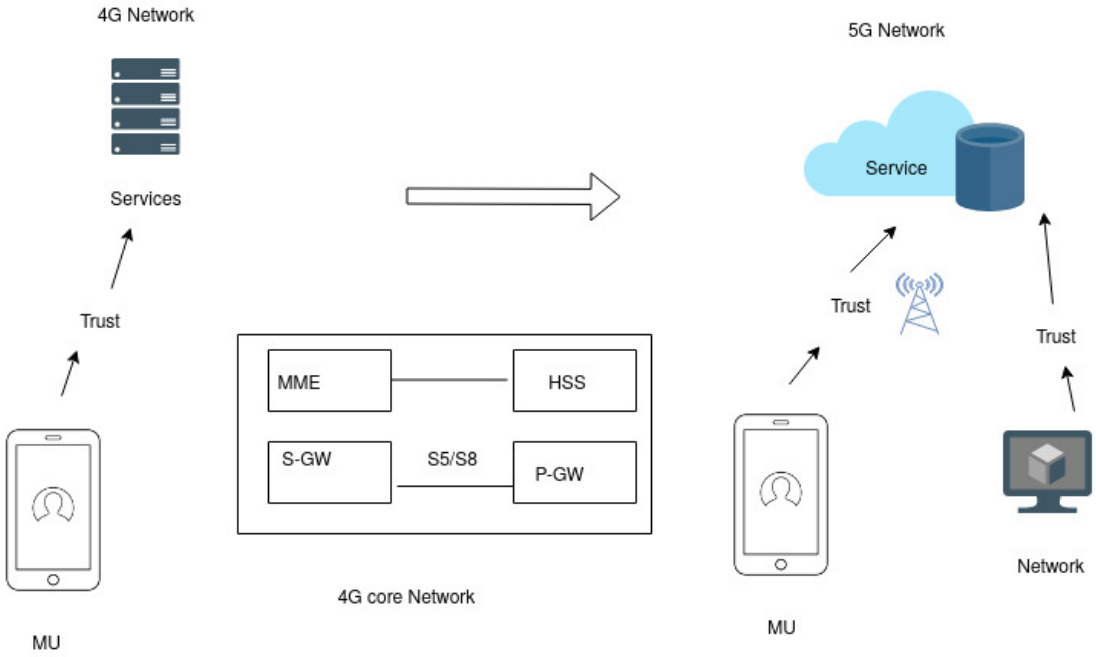
- Smart card replaces C with C' and stores $\{A, B, C', Ctr_{MU}, b, E_p\}$ in the smart card.

5 Proposed 4G-5G trust model

With the development of the new 5G networking paradigms, there exist the new security challenges and threats to address in the 5G system. To address these security issues a new security architecture should be introduced which works in compliance with the 5G paradigms. The trust models for the 4G-5G networks are presented in the Figure 2.

We have developed security architecture which can be integrated with the new 5G system. The proposed security architecture provides the security features like user identity management, mutual authentications between the communicating entities and Mobile User (MU), securing communication channel. Further, the proposed protocol resists the active and passive security attacks. Since mobile devices are energy constrained devices, lightweight authentication protocols have been designed. To provide security to the data, the proposed protocol uses cryptographic techniques like symmetric encryption and asymmetric encryption. The security algorithms used in the proposed protocol are Diffie-Hellman key exchange protocol, SHA-256 hash algorithm, Advanced Encryption Standard (AES) 128 bit. Public key cryptosystem like Elliptic Curve Cryptography (ECC). The proposed protocol provides security not only to the communicating entities but also to Mobile Edge Computing (MEC) servers and cloud servers.

Figure 2 4G-5G trust model



6 Security attacks and security services in 5G networks

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.

6.1 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 $P = E_k\left(h\left(ID_{MU} \| b\right)\right)$, where b is the random number chosen by the MU. In each session, user chooses a new random number. $\mathcal{A}$ 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 $\mathcal{A}$ 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.

6.2 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. $\Delta T \le T_{arr} - T_{sent}$, 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 $\mathcal{A}$ eavesdrops the message, modifies the same message and replays. Thus, the proposed scheme is resistant to the replay attack.

6.3 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 $h\left(ID_{MU} \| b\right)$, 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.

6.4 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 $C = h\left(h\left(ID_{MU} \| b \| PW_{MU}\right)\right)$. With the reverse engineer method or power analysis method $\mathcal{A}$ leaks the parameters in the smart card. To obtain the real PW_{MU} $\mathcal{A}$ guesses the password PW'_{MU}. With the guessed PW'_{MU} $\mathcal{A}$ computes $C' = h\left(h\left(ID'_{MU} \| b \| PW'_{MU}\right)\right)$, 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. $\mathcal{A}$ 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 $\mathcal{A}$ to guess the password. Thus, the proposed scheme is resistant to offline password guessing attack.

6.5 *Resistant to stolen smart card attack*

With the theft of the stolen smart card and the leakage of the smart card parameters $\{A, B, C, Ctr_{MU}, b, E_p\}$, $\mathcal{A}$ launches the guessing attacks for 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 $C = h\left(h\left(ID_{MU} \| b \| PW_{MU}\right)\right)$. 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.

6.6 *Resistant to forgery attacks*

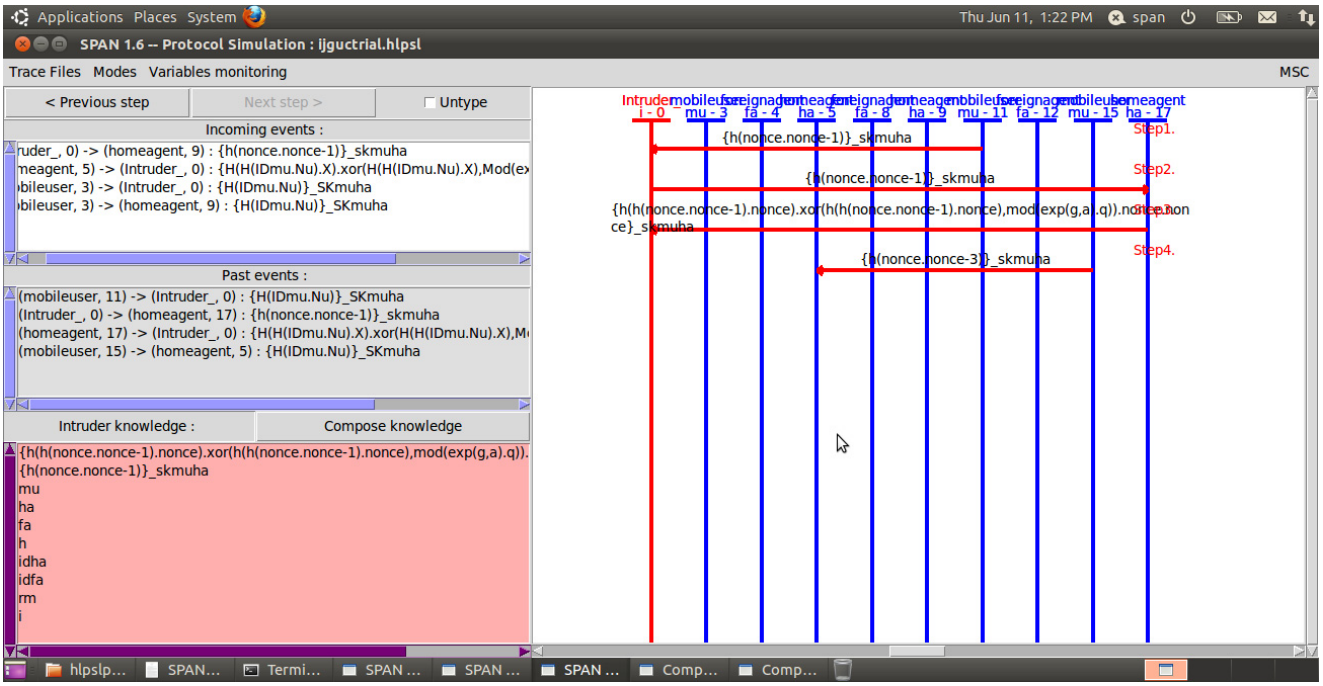
The three communicating entities MU, FA and HA in the proposed scheme share the secret keys E_k, K_{FH}, P_{HA} respectively to communicate with each other. To forge each of the messages $\{M_1, M_2, M_3, M_4\}$ transmitted over insecure channel is impossible as $\mathcal{A}$ fails to obtain the secret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

6.7 *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 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 mobile user, foreign agent and home agent. In the MSC intruder learns about the parameter as shown in Figure 3. Intruder intercepts the communication channel to learn about the data. Since the proposed protocol made use of cryptographic primitives the data available to intruder is in encrypted format. Thus, the proposed protocol provides security to traffic analysis and eavesdropping.

Figure 3 Message sequence chart



6.8 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 $\mathcal{A}$ 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.

6.9 Mutual authentication is achieved

It is difficult for $\mathcal{A}$ 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 $P = E_k\left(h\left(ID_{MU} \| b\right)\right)$. Decryption key D_k is known only to HA. Hence, it is difficult for $\mathcal{A}$ 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 $M_2 = \left\{P, D, E, C_1, Ctr_{MU}, T_1, E_{K_{FH}}\left(F\right), C_2, T_2\right\}$ in which FA encrypts the parameter F with the secret key K_{FH} as $E_{K_{FH}}\left(F\right)$ only the valid HA will be able to decrypt the message. Thus, it is impossible to impersonate as valid HA.

7 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.

7.1 Overview of AVISPA

AVISPA is a tool which is widely accepted for the verification of the cryptographic protocols. One of the major advantages of the AVISPA tool is that the protocol specification can be verified by different verification techniques. The cryptographic protocol is written in High Level Protocol Specification Language (HLPSL). HLPSL 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.

The HLPSL implementation details of mobile user's registration phase and login and authentication phase of the proposed scheme is presented in Figure 4. HLPSL implementation for the foreign agent role is presented in Figure 5. HLPSL implementation for the home agent role is presented in Figure 6. HLPSL implementation for the session, goal and environment role is presented in Figure 7. Output of the program using OFMC back-end is presented in Figure 8. Output of the program using CL-Atse back-end is presented in Figure 9.

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.

Figure 4 Mobile user role

```
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 5 Foreign agent 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 Home agent 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 7 Session and environment 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 8 Output results using OFMC

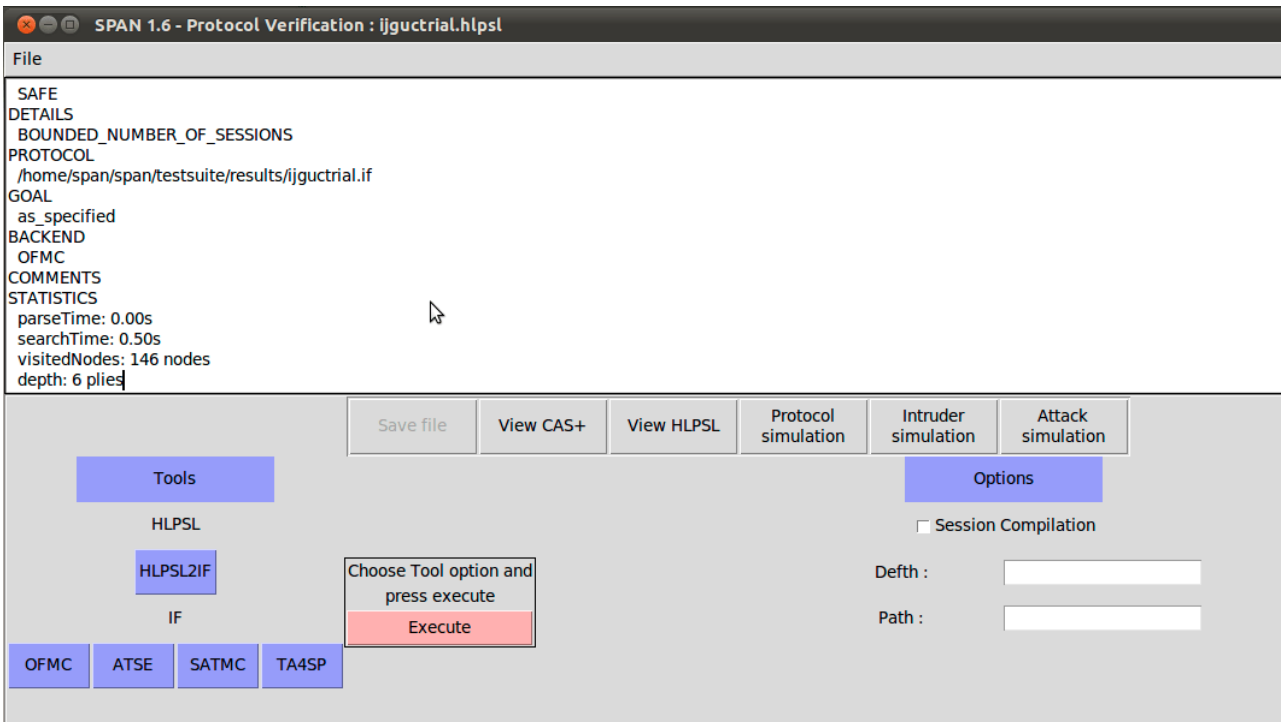
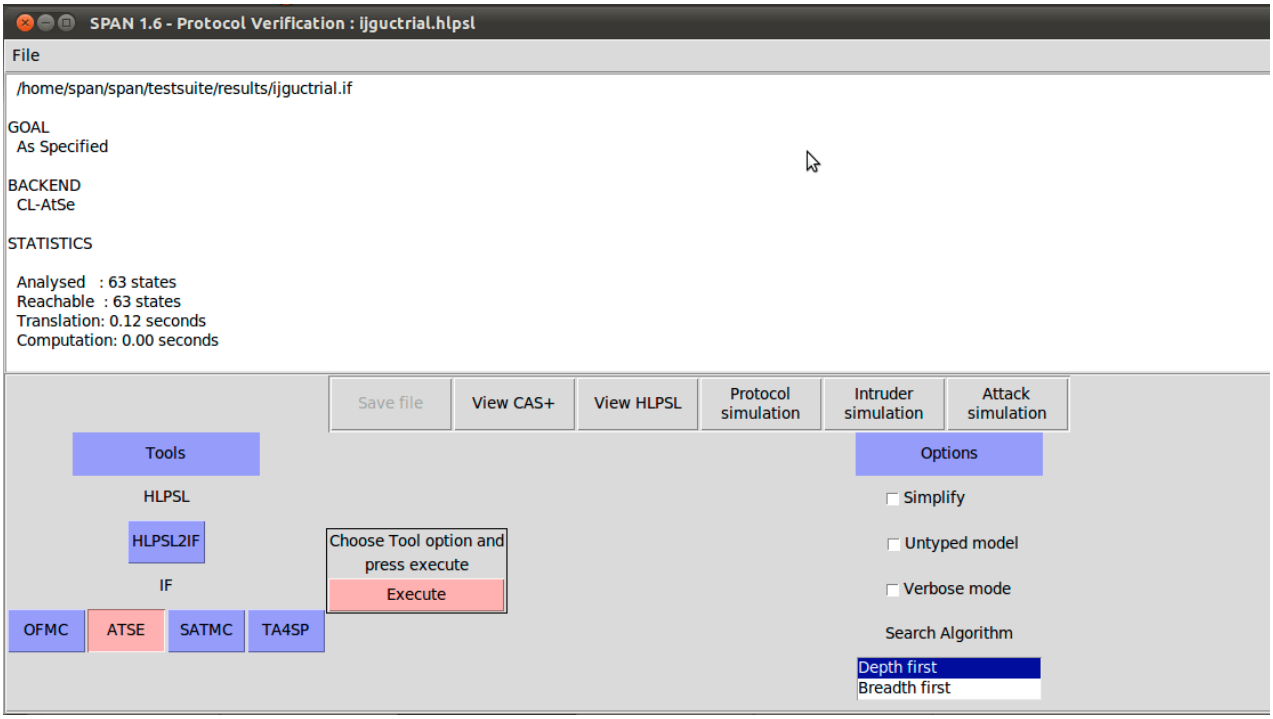


Figure 9 Output results using CL-Atse



8 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 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 10 mps. Network scenario 2 consists of 10 MU, 1 FA and 1 HA with the mobility speed of 20 mps. Network scenario 3 consists of 20 MU, 1 FA and 1 HA with the mobility speed of 30 mps. Network scenario 4 consists of 30 MU, 1 FA and 1 HA with the mobility speed of 40 mps.

Table 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	15 s
Platform	Ubuntu 16.04 LTS

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 and 700 bits, respectively.

8.1 Simulation environment

We have considered four global mobility Network Scenarios (NS) for the simulation.

1 *NS1*: Consists of 5MUs, 1FA. 1HA with the mobility speed of 10 mps.

2 *NS2*: Consists of 10MUs, 1FA. 1HA with the mobility speed of 10 mps.

3 *NS3*: Consists of 20MUs, 1FA. 1HA with the mobility speed of 30 mps.

4 *NS4*: Consists of 30MUs, 1FA. 1HA with the mobility speed of 40 mps.

8.2 Simulation results

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

8.2.1 Impact on throughput

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

$$Throughput = \frac{Receivedpackets\ X\ Bitsize\ of\ a\ packet}{Totaltime}$$

Throughput calculated for different network scenarios is shown in Fig 1. Throughput increases with the increase in the number of mobile nodes. Since the number of messages exchanged will be more in case of huge MUs communicating to the service provider network. Throughput for NS1, NS2, NS3 and NS4 are 401, 820, 1344 and 2211 bps, respectively.

8.2.2 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 Figure 11.

8.2.3 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:

$$PDR = \frac{Receivedpackets}{Sentpackets}$$

The simulation results for PDR under the network scenarios NS1, NS2, NS3 and NS4 is shown in Figure 12. PDR decreases with the increase in the number of mobile nodes. Since, the messages transmitted across the network are more in case of large MUs the packet drop will be more.

Figure 10 Throughput

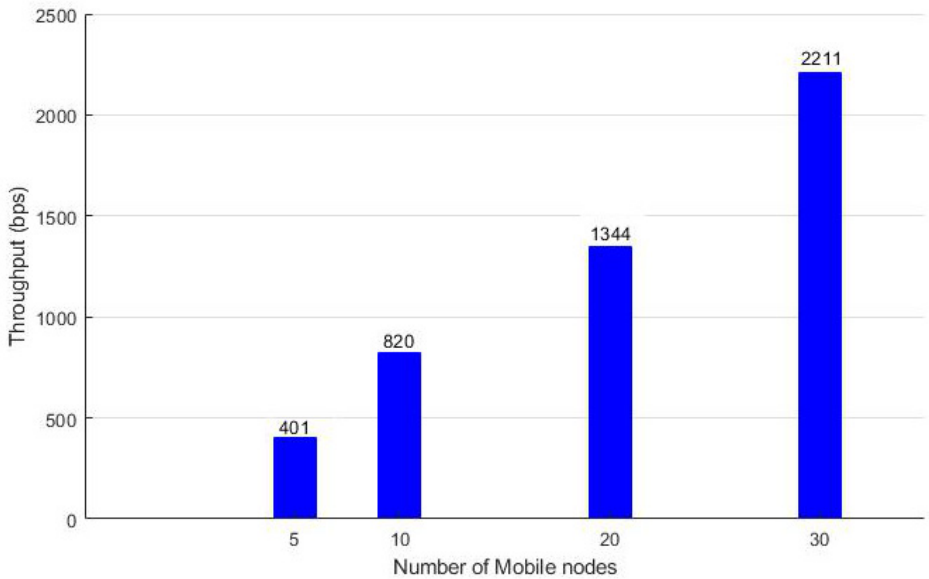


Figure 11 End-to-end delay

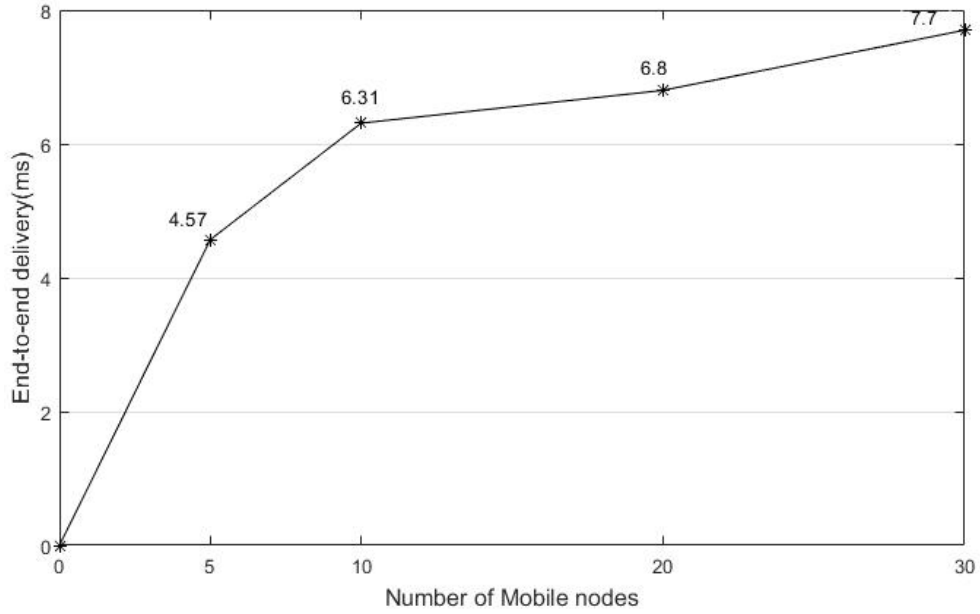
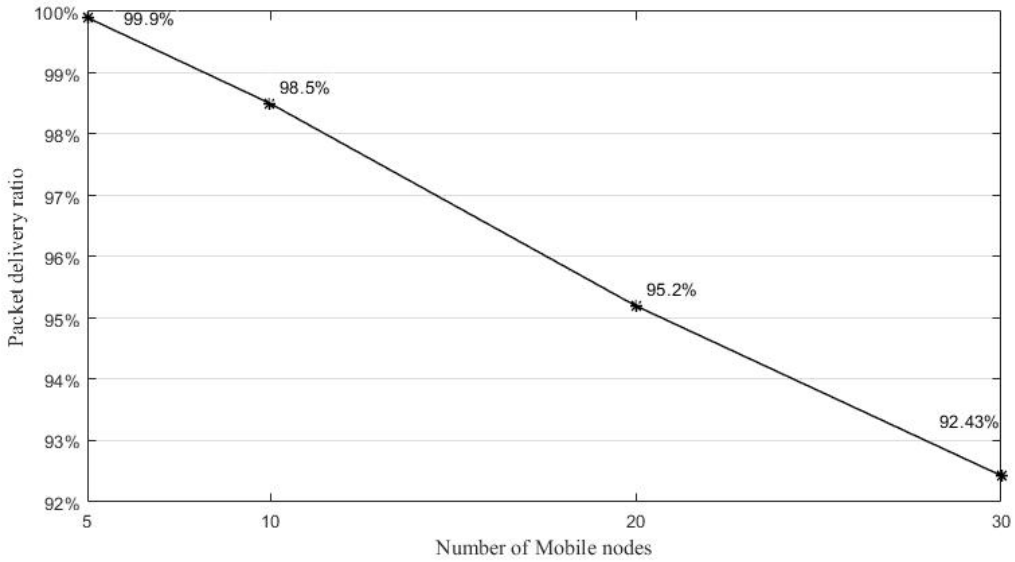


Figure 12 Packet delivery ratio



9 Performance analysis and comparison

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

9.1 Comparison of security and functional features

It is clearly evident from Table 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 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. It 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, our scheme achieves all the desirable security functionality features.

9.2 Comparison of computational costs and efficiency

Table 4 summarises the computational cost, efficiency and execution time in ms of the proposed scheme along with the other schemes namely Gope and Hwang scheme (2016), Wu

et al.'s scheme (2016) and Lee et al.'s scheme (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 the proposed scheme and the other schemes are tabulated in the Table 4.

Table 5 summarises the efficiency and execution time in ms of the proposed scheme and the schemes (Gope and Hwang, 2016; 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. The notations used in the Table 5 are: HF: Hash function, E/D: Encryption/Decryption, PM: Point Multiplication and ME: Modular exponentiation. Time complexities tabulated in Table 5 are calculated based on the time taken by the cryptographic operations t_h, t_m, t_s. 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 (Wu et al., 2018). Based on these time results, time complexities for the proposed scheme and the other schemes are calculated. Though the proposed scheme takes more time than the other schemes in the Table 5, it achieves better security compared to other schemes.

Table 3 Functionality comparison

Security requirements	*Proposed scheme*	*Gope and Hwang (2016)*	*Lee et al. (2017)*	*Wu et al. (2016)*
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	✓	✓	×	✓
Security against forgery attack	✓	✓	×	✓
User friendliness	✓	✓	×	✓

Table 4 Computational cost comparison

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

Table 5 Efficiency comparison

Phase	*Operation*	*Proposed scheme*	*Gope and Hwang (2016)*	*Lee et al. (2017)*	*Wu et al. (2016)*
Registration phase	HF	6	4	4	5
	E/D	0	0	0	0
	PM	1	0	0	0
	ME	1	0	0	0
Login and authentication phase	HF	18	11	26	26
	E/D	4	4	0	2
	PM	4	0	0	4
	ME	3	0	0	0

Table 5 Efficiency comparison (continued)

Phase	*Operation*	*Proposed scheme*	*Gope and Hwang (2016)*	*Lee et al. (2017)*	*Wu et al. (2016)*
Password change phase	HF	4	4	4	11
	E/D	0	1	3	0
Total no. of operations	HF	41	24	37	48
	E/D	4	5	3	2
	PM	5	0	0	4
	ME	4	0	0	0
	Execution time (ms)	1.66	0.13	0.18	1.35

9.3 Comparison of communication costs

Table 6 summarises about the communication overhead between the proposed scheme and other schemes, namely Gope and Hwang scheme (2016), Fan Wu et al.'s scheme (2016) and Lee et al. scheme (2017) for login and authentication phase. The experimental results shows that the SHA-1 hash function requires 160-bits (Eastlake 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.

9.4 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 R. and Shashidhara (2019, 2020) in terms of throughput, EED and PDR.

Table 6 Communication overhead

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

In Table 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.

Figure 13 compares the throughput of the proposed scheme with other schemes. Figure 14 compares the end to end delivery of the proposed scheme with other schemes. Figure 15 compares the packet delivery ratio of the proposed scheme with other schemes.

Table 7 Network scenarios

*1*Network scenarios (NS)*	*Proposed scheme*			*Scheme (Madhusudhan and Shashidhara, 2019)*			*Scheme (Madhusudhan and Shashidhara, 2020)*		
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

Figure 13 Throughput

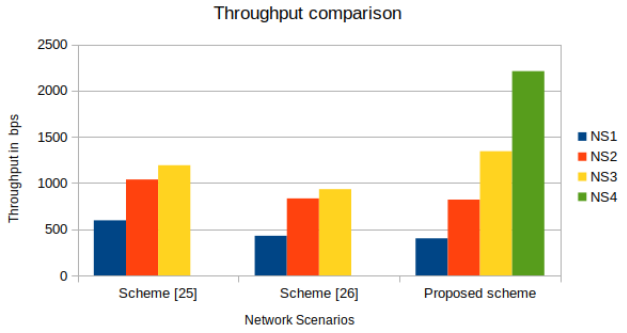


Figure 14 End to end delivery

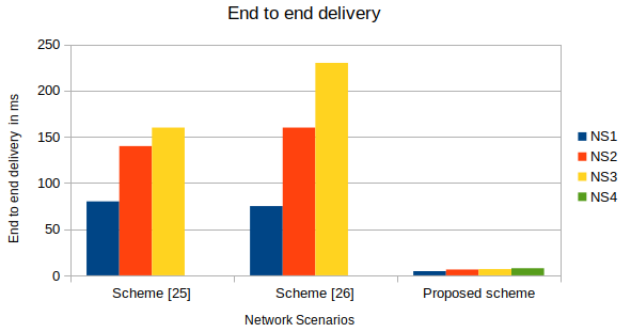
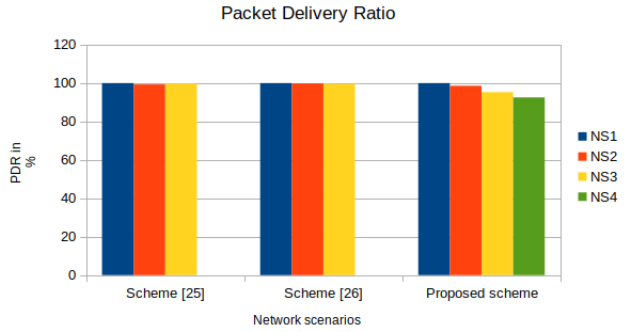


Figure 15 Packet delivery ratio



10 Conclusion

The proposed scheme designed for 5G 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 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.

References

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*, Vol. 6, pp.20673–20693.

Bellare, M., Pointcheval, D. and Rogaway, P. (2018) 'Authenticated key exchange secure against dictionary attacks', *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp.139–155.

Chang, C-C., Lee, C-Y. and Chiu, Y-C. (2009) 'Enhanced authentication scheme with anonymity for roaming service in global mobility networks', *Computer Communications*, Vol. 32, No. 4, pp.611–618.

Diffie, W. and Hellman, M. (1976) 'New directions in cryptography', *IEEE transactions on Information Theory*, Vol. 22, No. 6, pp.644–654.

Eastlake, D. and Jones, P. (2001) *Us Secure Hash Algorithm 1 (SHA1)*, Technical Report.

Fang, D., Qian, Y. and Hu, R.Q. (2017) 'Security for 5g mobile wireless networks', *IEEE Access*, Vol. 6, pp.4850–4874.

Glouche, Y., Genet, T., Heen, O. and Courtay, O. (2006) 'A security protocol animator tool for AVISPA', *ARTIST2 Workshop on Security Specification and Verification of Embedded Systems*, Pisa, pp.1–8.

Gope, P. and Hwang, T. (2016) '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*, Vol. 62 pp.1–8.

Gope, P. Islam, S.K.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*, Vol. 31, No. 2. Doi: 10.1002/dac.3461.

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*, Vol. 34, No. 3, pp.367–374.

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*, Vol. 94, No. 2, pp.860–864.

Karuppiah, M. and Saravanan, R. (2015) 'A secure authentication scheme with user anonymity for roaming service in global mobility networks', *Wireless Personal Communications*, Vol. 84, No. 3, pp.2055–2078.

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 authentication scheme for roaming service in global mobility networks', *Wireless Personal Communications*, Vol. 93, No. 2, pp.383–407.

Kim, J. and Kwak, J. (2013) 'Secure and efficient anonymous authentication scheme in global mobility networks', *Journal of Applied Mathematics*, pp.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*, Vol. 85, No. 12, pp.2899–2908.

Koblitz, N., Menezes, A. and Vanstone, S. (2000) 'The state of elliptic curve cryptography', *Designs, codes and cryptography*, Vol. 19, Nos. 2/3, pp.173–193.

Kocher, P., Jaffe, J. and Jun, B. (1998) *Cryptography Research*. Technical Report. Available online at: http://www.cryptography.com/dpa/technical

Kuo, W-C., Wei, H-J. and Cheng, J-C. (2014) 'An efficient and secure anonymous mobility network authentication scheme', *Journal of Information Security and Applications*, Vol. 19, No. 1, pp.18–24.

Lee, C.C., Hwang, M.S. and Liao, I.E. (2006) 'Security enhancement on a new authentication scheme with anonymity for wireless environments', *IEEE Transactions on Industrial Electronics*, Vol. 53, No. 5, pp.1683–1687.

Lee, C-C., Lai, Y-M., Chen, C-T. and Chen, S-D. (2017) 'Advanced secure anonymous authentication scheme for roaming service in global mobility networks', *Wireless Personal Communications*, Vol. 94, pp.1–16.

Li, C-T. and Lee, C-C. (2012) 'A novel user authentication and privacy preserving scheme with smart cards for wireless communications', *Mathematical and Computer Modelling*, Vol. 55, No. 1, pp.35–44.

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

Li, X., Sangaiah, A.K., Kumari, S., Wu, F., Shen, J. and Khan, M.K. (2017) 'An efficient authentication and key agreement scheme with user anonymity for roaming service in smart city', *Personal and Ubiquitous Computing*, Vol. 21, No. 5, pp.791–805.

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*, Vol. 9, No. 11, pp.1331–1339.

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*, pp.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*, Vol. 13, No. 1, pp.82–103.

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

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

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*, Vol. 31, No. 18. Available online at: https://doi.org/10.1002/dac.3814

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*, Vol. 51, No. 5, pp.541–552.

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*, Vol. 55, No. 1, pp.214–222.

Nohl, K., Evans, D., Starbug, S. and Plötz, H. (2008) 'Reverse-engineering a cryptographic RFID tag', *USENIX Security Symposium*, Vol. 28.

Von Oheimb, D. (2005) 'The high-level protocol specification language HLPSL developed in the EU project AVISPA', *Proceedings of the APPSEM 2005 Workshop*, pp.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*, Vol. 12, No. 4, pp.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, Report (2012)/4392012*.

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

Wu, CC-C., Lee, W-B. and Tsaur, W-J. et al (2008) 'A secure authentication scheme with anonymity for wireless communications', *IEEE Communications Letters*, Vol. 12, No. 10, pp.722–723.

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*, Vol. 9, No. 16, pp.3527–3542.

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 and Electrical Engineering*, Vol. 68, pp.107–118.

Xu, J. and Feng, D. (2009) 'Security flaws in authentication protocols with anonymity for wireless environments', *ETRI Journal*, Vol. 31, No. 4, pp.460–462.

Youn, T.Y., Park, Y.P. and Lim, J. (2009) 'Weaknesses in an anonymous authentication scheme for roaming service in global mobility networks', *IEEE Communications Letters*, Vol. 13, No. 7, pp.471–473.

Zhu, J. and Ma, J. (2004) 'A new authentication scheme with anonymity for wireless environments', *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 1, pp.231–235.