International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 5 (2018) pp. 2865-2871

Modified Privacy-Preserving Universal Authentication Protocol (MPriAuth) for Security of Mobile IP Networks

Abdurahem El Atman Igrair and Raghav Yadav

Department of Computer Science and Information Technology, Sam Higginbottom University of Agriculture, Technology and Sciences, Allahabad, India.

Abstract

An efficient universal authentication protocol is vital to preserve the users' privacy in mobile networks. Different privacy safeguarding authentication protocols was proposed lately. However the mass of them either have high communication expenses or lacks in privacy protection. In this given paper, propose a Modified Privacy Preserving Universal Authentication Protocol (MPriAuth) aimed at mobile IP networks. It is devised to authenticate the mobile users in foreign network whilst safeguarding the users' privacy. The proposed MPriAuth algorithm has three step; key generation, key sign and key verify. Group signature is utilized for key generation together with key verification. The proposed technique is simulated utilizing the NS3. The outcomes exhibit that the MpriAuth algorithm preserves the users' privacy without trading off the quality of service. Likewise the group signature sharing decreased the computation time; thus the communication cost is lessened.

Keywords: Privacy Preservation, Authentication, Mobile IP Networks

INTRODUCTION

The wireless communication turns into essentially on account of its mobility and instant access to services. The liberty to roam anyplace devoid of losing the network connectivity is made possible using the mobile networking protocol "Mobile IP" [1]. Mobile IP passes the IP datagram betwixt a Mobile Node (MN) and its corresponding node (CN) as the MN switches its attachment point on the Internet. Mobile IP stands appropriate for interconnecting heterogeneous mobile networks successfully giving worldwide mobility [2].

In MIP, a MN utilizes two IP addresses: home address as well as care-of addresses (CoA). The home address is static in addition utilized to recognize TCP connections. The CoA alters at every fresh point of attachment (PoA). MIP needs the presence of a network node recognized to be the home agent (HA) along with foreign agent (FA). At whatever point the MN advance, it enrolls its fresh CoA with its HA and the HA diverts the entire packets bound for the MN to the MN's CoA [3]. It empowers a MN to circulate without losing their transport-layer connectivity by utilizing resources in a foreign domain network.

However the mobile networks accompany certain inherent insecurities of the wireless medium. The wireless signals can be gotten by anybody inside its region. Absence of productive security privacy management system makes them defenseless against eavesdropping assault and exposure of exceptionally sensitive personal information [4] [5]. In wireless communications, the loss of privacy or confidentiality is dependably a possibility, which propels the need to devise measures to ensure privacy. The essential means used to ensure privacy in wireless frameworks is authentication protocol [6].

An authentication protocol permits mobile nodes (MNs) to wander across multiple access points (APs) while guaranteeing the safety of both communication parties. It permits access to roaming service presented by the FA with aid of the home specialist in mobile networks. After enlistment to the authentication server (AS), the MN can get to the network service from associated AP [7]. At the point when a MN leaving the current AP, handover authentication will be performed for identity authentication and also to secure the data being transmitted betwixt the MN and the AP, a shared session key will be set up. [8].

For secure wandering service, the foreign server must verify the roaming user, who initially bought in to the home server. Consequently, an authentication mechanism is a significant requirement for giving safe roaming services [9]. Be that as it may, the wireless networks' broadcasting nature and the constrained resources of mobile phones make designing a safe and effective roaming authentication protocol challenging [10]. Likewise how to secure user privacy in this sort of protocols still remains an open issue.

To make certain secure communication, the authentication protocol ought to contain the capacity to fulfill some security and function characteristics and withstand different assaults. The protocol should satisfy the accompanying security prerequisites [11].

a) Mutual authentication

To ensure only approved users could get to Internet services through MWNs, a privacy-preserving authentication protocol ought to give mutual authentication amongst AP and MN.

b) User anonymity

To make certain the user's privacy, a privacy-preserving authentication protocol ought to contain the capability to give user obscurity, that is, the adversary including the malignant access point can't separate MN's real identity through intercepted messages.

c) Non-traceability

To secure the user's location privacy, a privacy-preserving authentication protocol ought to encompass the capacity to

give non-traceability, that is, the adversary including the malignant access point can't follow MN's conduct.

d) Conditional privacy preservation

To chastise the user when he/she conveys some damage to MWNs, a privacy-preserving authentication protocol ought to encompass the capacity to give restrictive privacy preservation, i.e., just the AS can extract MN's real identity.

e) Session key establishment

To share private key for secure communication, a privacy-preserving authentication protocol ought to contain the capacity to give session key foundation, i.e., a session key is produced amongst MN and AP subsequent to executing the protocol.

f) Perfect forward secrecy

To make certain the safety of the session key, a privacy-preserving authentication protocol ought to encompasses the capability to give perfect forward secrecy, that is to say, the foe can't remove the session key created in past session even he/she gets both private keys of MN and AP.

g) Attack resistance

Owing to the open environment, the handover authentication protocol stands helpless to different assaults, for instance, the replay attack, the stolen verifier table attack, the modification attack the impersonation attack, along with the man-in-the-middle attack. To guarantee safe communication in MWNs, it is mandatory that a handover authentication protocol ought to encompasses the capacity to withstand those previously mentioned attacks.

A privacy-preserving universal authentication protocol (Priauth) aimed at wireless communications was introduced by Daojing et al. [12]. In this technique public-key operations are considered takes after: Elliptic Curve Digital Signature Algorithm (ECDSA) uses 1 Elliptic Curve Scalar Multiplication (ECSM) operation aimed at signing, moreover 1 Multi-ECSM operation aimed at verification; the Diffie-Hellman exchange uses 2 ECSM operations; in addition a public key encryption uses 2 ECSM operations. It gives solid user obscurity against the eavesdroppers and foreign servers, session key establishment. Most importantly, in Priauth, at the very starting itdelf the foreign server validates a user in the protocol execution. Hence Priauth can alleviate DoS attack taking place in foreign servers. However the home server is vulnerable to DoS attack because Priauth only needs the user along with the foreign server to be concerned in every protocol run.

The given paper is arranged this way. In the succeeding section, overview and analyzed the related work, as well talk about their security shortcomings. Section III depicts MPriAuth protocol thoroughly. The simulation outcomes along with the analysis of MPriAuth protocol is given in Section IV. At that point Section V deduces the given work.

RELATED WORKS

Xiaoyu et al. [13] displayed a SDN-enabled authentication handover along with privacy protection through sharing of client particular security context information amongst related access points. The SDN-enabled solution gives a reconfigurable network management platform, in addition simplifies authentication handover in accomplishing diminished latency. SDN-enabled authentication handover along with privacy protection scheme met the basic latency prerequisite, while keeping up the SDN flexibility, programmability, together with information offloading ability. However the framework is helpless against impersonation attack and also man in the middle attack owing to the frequent establishments of trust relationships.

Xu Yang et al. [14] displayed a trust along with privacy preserving handover authentication protocol aimed at wireless networks. It accomplished the user secrecy and untraceability and also trusts authentication amid handover authentication by utilizing the benefits of pseudo identity system along with elliptic curve cryptography. The security analysis and also performance assessment demonstrated that the protocol accomplished universality and robust security and an enhanced performance than other firmly related ones. But still it is susceptible to distributed denial of service attack.

Shin-Ming Cheng et al. [15] using group signature algorithms, introduced a distributed anonymous authentication protocol. By applying the MN and PoA as group members, the group signature algorithms gave identity verification specifically without nodes sharing insider facts in advance. This fundamentally lessened signaling overhead. By ways of group signature, the subjects of authentication are raised from nodes to groups to strengthen the security against interlopers, additionally to give user secrecy and also unlink ability against foreign domains. Hence, security and user privacy level are raised. Performance analysis demonstrated that the computational overhead is limited while keeping up user privacy. The weakness is that it can't anticipate the acting up nodes and keep the collusion attacks owing to the dearth of trust evaluation mechanism.

Debiao He et al. [16] exhibited an AHA protocol meant for MWNs to deal with issues existing in past AHA protocols. Contrasted with other AHA protocols, the enhanced AHA protocol had substantially less computation cost next to MN. A message authentication code or a digital signature is transported by the MN together with access point to guarantee the message' integrity. The alteration of message is detected by the AP accompanied by mobile nodes. Accordingly, the enhanced AHA protocol withstands the modification attack, impersonation attack together with man in the middle attack. Be that as it may, expanded security properties troubles the communication price vigorously. This protocol had higher communication cost if the security necessities are expanded.

Lai et al. [17] presented a conditional privacy-preserving authentication with access linkability aimed at roaming service. It provides multilevel privacy preservation aimed at the mobile networks. And creates authorized network operators or else service providers furthermore link the same user's entire access information devoid of revealing who the user is, what the current membership status of the user is, and the history of the user joining and revocation. Extensive analysis showed that this method resisted various security threats and as well provides more flexible furthermore elaborate privacy preservation including user tracking, anonymous user linking, joining, in addition revocation

function aimed at dynamic membership. In addition, performance evaluations demonstrated its efficiency concerning communication and also computation overhead. However this system fails to spot the internal attacks.

Centered upon the analysis, the formerly mentioned protocols [13]-[17] compromise the user privacy either to lessen communication cost or computation time. Therefore more balanced authentication protocol that meets the necessities of preserving privacy and furthermore diminish communication cost in inescapable.

PROPOSED METHODOLOGY

This given paper has proposed a Protocol MPriAuth. MPriAuth protocol is engaged to authenticate the mobile user in foreign network utilizing the group signature key. The HA generates this key and dispatches it to mobile user with location of mobile user in home agent (LocIP). Dissimilar to existing Priauth protocol that utilized ECDSA for check, MPriAuth protocol uses the group signature algorithm to guarantee secure and continuous communication betwixt network and the mobile user.

MPriAuth algorithm

MPriAuth algorithm begins with communication between HA and foreign agent. So as to trade the vital data between each accessible connection, master public keys for both with identification number was shared. MPriAuth protocol utilized the registration period of mobile user to enlist in home network. Verification stage to confirm HA along with foreign agent by mobile user to begin communication by utilization of secure authentication algorithm aimed at mobile IP networks against the other contribution techniques, for instance, MPriAuth and Priauth that utilized verify the mobile user in foreign agent just to establish connection.

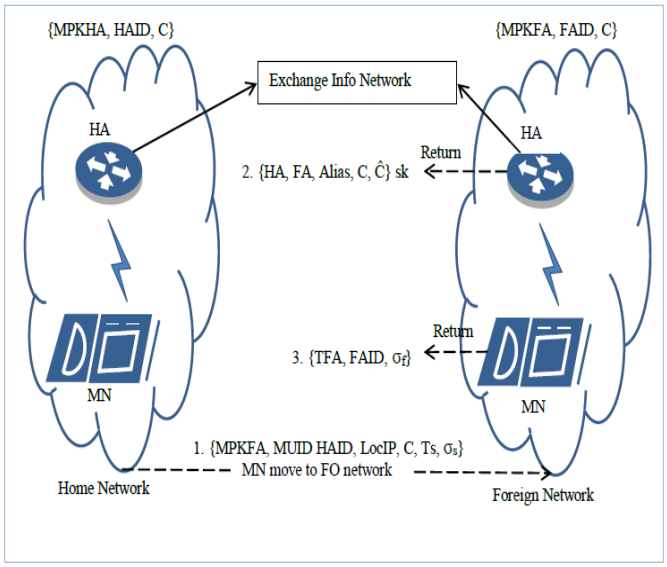

Figure 1: MPriAuth protocol for Mobile IP Networks

Steps involved in MPRIAUTH algorithm

The proposed MPriAuth algorithm has three parts in particular,

A. Key Generation
B. Key Sign
C. Key Verify

A. Key generation

The key generation commonly comprises of the accompanying segments: channel probing, quantization (and encoding), information reconciliation and privacy amplification. Amid channel probing, a similar statistic is utilized by the included transceivers to gather channel states. At that point, both transceivers independently implement a same quantization and also encoding procedure to their measurements so a bit sequence can be produced for every transceiver. Actually, these bit sequences are profoundly related going with numerous mismatches since channel measurement sequences of various transceivers have numerous errors. In this manner, the execution of information reconciliation is vital to correct these mismatches to make a shared bit sequence. By and large, some information may be spilled amid information reconciliation Therefore privacy amplification is applied to eradicate the consequences of leaked data and certification the randomness of the created shared secret key. In summary, we can locate that such key generation approaches are really data processing goes for extricating common patterns (shared bit sequence) from given data sets (channel measurements), albeit diverse statistics and algorithms are applied amid various key generation processes.

In the MPriAuth, key generation of group signature is finished by the home agent. The mobile user dispatches a request to HA by sending mobile user id together with location IP $\{MUid, LocIP\}$. Subsequent to getting the data, HA produces the group signature aimed at mobile user which contains $\alpha m_u \{\alpha, \beta, c, T_1, T_2 Mpkha, MUid, LocIP, HAid, ts\}$ likewise mobile user send $(Mpkha, MUid, C, HAid, ts, \alpha m_u)$ to the foreign agent. The communication betwixt mobile user and FA is given underneath.

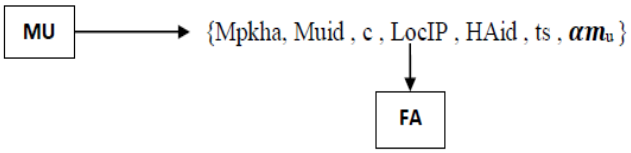

Figure 2: Communication between Mobile User and Foreign Agent

The accompanying notations are utilized in the key generation phase of the MPriAuth algorithm.

- $G1$ is a multiplicative cyclic group of prime order p;
- $G2$ is a multiplicative group of exponent p, whose order is some power of p that is a homomorphism from $G2$ onto $G1$.

- The challenge value $C \leftarrow H(gpk, M, S, T1, T2)$
- Select random number $\alpha, \beta, \delta \in G2$
- calculate helper values $T1 = g1 \oplus \alpha, T2 = g2 \oplus \beta$
- Compute support value $S = (T1 + T2)/(T1 \times T2)$
- calculate a challenge value $C \in \mathbb{Z}^*$ using $C \leftarrow H(gpk, M, S, T1, T2)$
- Output the signature $sign \leftarrow (\alpha, \beta, C, T1, T2)$

B. Key Sign

The FA obtains the message specified by mobile user in addition checks the HA with the assistance of $HAid$. The inputs of the signature algorithm are group public key $Gpk = (g1, g2, w)$, user private key $Gsk[i] = (Ai, Xi)$ together with a message $M \in \{0,1\}$. Foreign agent computes the group signature using $\alpha_{fa} = sign\{Gpk, Gsk[i], M\}$. figure 3 demonstrate the communication betwixt the FA and mobile user.

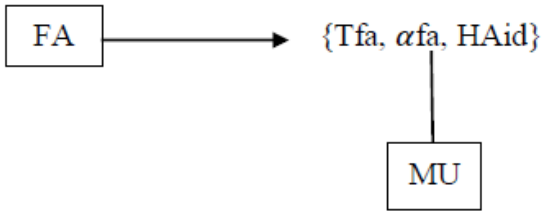

Figure 3: Communication between Foreign Agent and Mobile User

Key Signature Algorithm
Input : $MUid, LocIP, G1, G2, M, Gsk[i], Gpk$
Output : Signature αfa

Begin
Step 1. $\alpha \in G1, \beta \in G2$
Step 2. Calculate helper values $T1, T2$
Step 3. Calculate Support value S
If $(S == 0)$ then
Go to Step 1.
End if
Step 4. Calculate Challenge value C
Step 5. $\alpha fa \leftarrow (\alpha, \beta, C, T1, T2, MUid, LocIP)$
End

C. Key verify

Key verification verifies whether the signature is legitimate. To check σfa is a legit signature; the accompanying steps are taken after.

Re-derive $\hat{T}1, \hat{T}2$

Compute helper values, $\hat{T}1 = T1 \oplus \alpha$, $\hat{T}2 = T2 \oplus \beta$,
Compute support value $\hat{S} = (\hat{T}1 + \hat{T}2) / (\hat{T}1 \times \hat{T}2)$
Compute the encrypted challenge value $\hat{C} \leftarrow H(Gpk, M, \hat{S}, \hat{T}1, \hat{T}2)$
Check the challenge value $[C == \hat{C}]$. On the condition that it is similar acknowledge, dismiss if not.

The mobile user will confirm foreign agent by utilizing σfa signature check and extract the helper values $\hat{T}1, \hat{T}2$ and discover support value $\hat{S}$. Then calculates and dispatch encrypted challenge value $(\hat{C})$ to foreign agent with session key $sk = Ru.(\hat{C})$. Foreign agent fa receives the helper values and compares the challenge values. On the off chance that $[C == \hat{C}]_{at}$ that point fa returns 1 to the mobile user furthermore build up connection, else dismiss. The key verification algorithm is given beneath.

Key Verification Algorithm
Input : $Tfa, \alpha fa, HAid$
Output: Accept if the signature is True, Reject otherwise.

Begin
Step 1. Compute Helper values $\hat{T}1, \hat{T}2$
Step 2. Compute Support value $\hat{S}$
If $(s == 0 \&\& LocIP == IP)$ then
Output False and terminate.
End if
Step 3. Compute challenge $\hat{C}$
Choose a random number Ru
If $[C == \hat{C}]$ then
session key $sk = Ru.(\hat{C})$
$mi \leftarrow \{HA, Fa, Ru, C, \hat{C}, Sk\}$
Else
Reject
End if
End

RESULTS AND DISCUSSION

The MPriAuth algorithm was simulated and assessed utilizing the network simulation version 3 (NS3). It designed for the two chief diverse sorts of networks;

1) Varying MNs' mobility speed additionally it begins from (5m/s) to (25m/s),
2) Varying amount of attackers on the network begins form 1 attack to 9 attacks.

The quantity of MNs is set to 50 for the two cases. Figure 4 and 5 demonstrates the visualization snapshots. Figure 4 reveals the system model designed in which 50 roaming users are arbitrarily deployed under two servers those go about as a home server as well as foreign server when MNs are moving from home network to foreign network. The proposed methods is lightweight since just hash functions are embraced amid the entire method. Moreover, no confirmation procedure ought to be done at the user part, which diminishes the redundancy in authentication process.

There stands two end nodes associated by a gray colored link are two servers, foreign server and home server in the network. Figure 5 demonstrates the connectivity and detecting patterns in this network. As stated by Mobile IP Networks' property, every mobile hub is detecting its neighbor's mobile nodes for communication reason. Figure 6 demonstrates the showing on packet loss in red shading.

The outcome utilizes four major network performance pointers. Throughput is stated as the rate of effective data packets delivery over timeframe interim. Packet delivery ratio (PDR) stands as the proportion of ratio of actual packet delivered out of entire packets sent. Packet loss happen when no less than one data packet traveling across computer network neglect to achieve their goal. The end to end delays the packet is the duration it takes to achieve the goal relying upon location of particular pair of nodes.

The outcomes of MPriAuth are contrasted with existing Priauth strategy aimed at mobile IP network. To augment the network security together with QoS performance, MPriAuth is introduced. The MPriAuth algorithm gives authentication and also secure communication betwixt mobile nodes from home network to foreign network by secure channel.

Varying Mobility Scenario

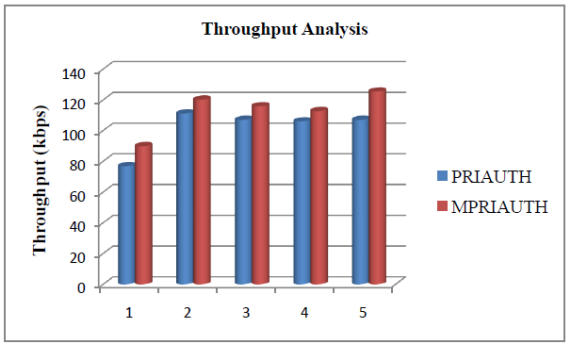

Figure 4: Average Throughput vs. Mobility Speed

In this given section, the throughput percentage is investigated matching to the mobility speed. Figure 4 displays the graphical variations of throughput regarding the difference in mobility speed from 5 to 25 m/s. The percentage throughput values equivalent to Priauth protocol start from 76.8 to 107.008 kbps respectively. Similarly, the percentage values equivalent to MPriAuth protocol are 89.9 to 125.432 kbps respectively. The comparative analysis between the existing Priauth with the proposed method MPriAuth reveals that the MPriAuth protocol offers 17.21 % improvement regarding Priauth protocol.

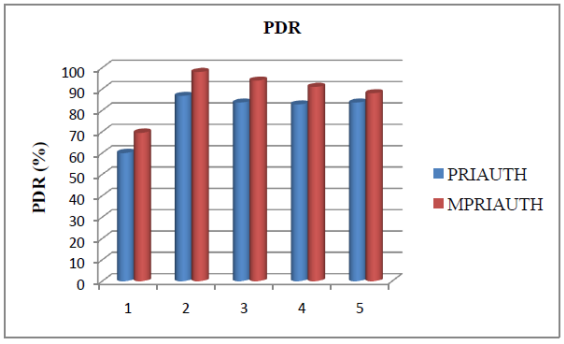

Figure 5: PDR vs. Mobility Speed

In this Figure 5 the percentage of PDR analysis equivalent to the number mobility speed is shown. The graphical variations shows for PDR regarding the variation in mobility speed from 5 to 25 m/s. The percentage PDR analysis values corresponding to Priauth protocol start offer from 60 to 83.6 % respectively. Similarly, the percentage values corresponding to MPriAuth protocol are offer 69.5 to 88% respectively. The comparative analysis between the existing method Priauth with the proposed method MPriAuth reveals that the MPriAuth protocol offers 12.90% improvement with reference to Priauth protocol.

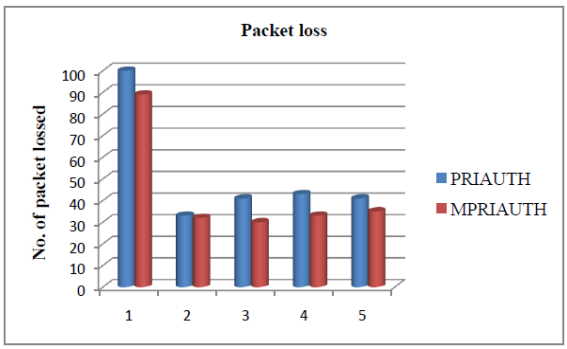

Figure 6: Loss Rate vs. Varying Mobility Speed

Figure 6 displays the packet loss ratio variations regarding the mobility speed from 5 to 25 m/s in addition to faulty nodes presences respectively. For minimum speed period (5 m/s), besides maximum speed (25 m/s), the maximum packet loss value of Priauth protocol is 100 packets for speed of 5 m/s along with minimum packet loss value is 33 packets for speed of 10 m/s. Similarly, the maximum packet loss for MPriAuth protocol is 85 packets intended for the speed of 5 m/s for and minimum packet loss is 30 packets in the speed of 15 m/s.

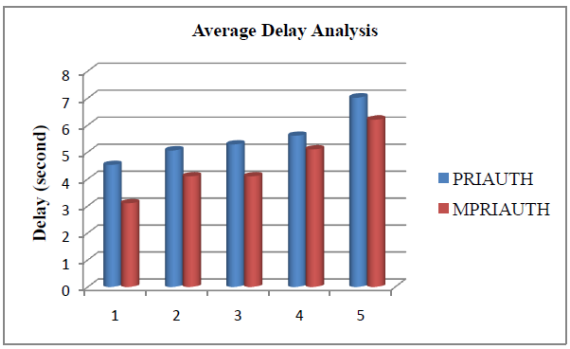

Figure 7: End to End Delay vs. Varying Mobility Speed

Figure 7 displays the end-to-end delay variations with reference to the faulty nodes presences respectively. For minimum mobility speed (5 m/s), the end-to-end delay value of Priauth protocol is 4.52 second and 7.02 second for maximum mobility speed of (25 m/s) for 50 faulty nodes. Similarly, the delay values for MPriAuth protocol are 3.1 second and 6.2 second for maximum mobility speed of (25 m/s).

Varying Number of Malicious Attackers

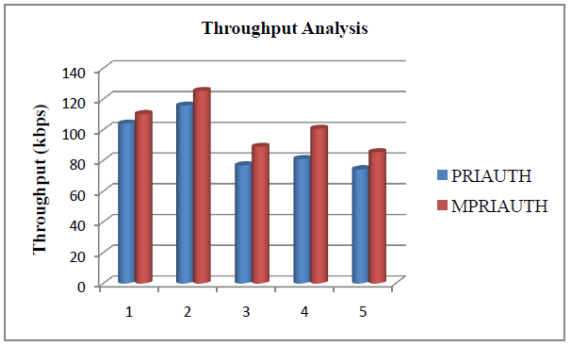

Figure 8: Analysis of Throughput with Varying Number of Attackers

In the given Figure 8 the throughput percentage is investigated equivalent to the number attackers. The graphical variations exhibit the throughput concerning the variation of attackers from 1 to 9 attacks. The percentage throughput values regarding to Priauth protocol start from 103.936 to 74.22 kbps respectively. Similarly, the percentage values corresponding to MPriAuth protocol are 110.2 to 85.432 kbps respectively. The comparative analysis between the existing Priauth method with the proposed MPriAuth protocol exhibits that the MPriAuth protocol offers 24.42 % improvement concerning Priauth protocol.

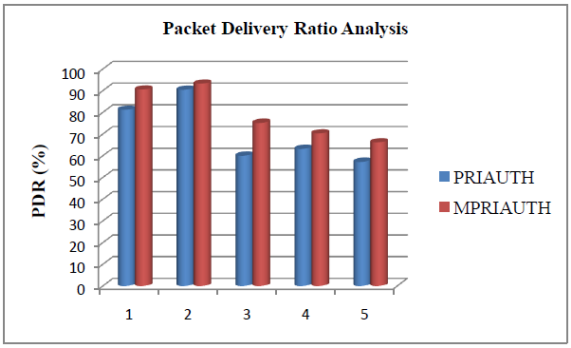

Figure 9: Analysis of PDR with Varying Number of Attackers

In the given Figure 9, the percentage of PDR equivalent to the quantity of attackers is shown. The graphical variations show for PDR with reference to the variation number of attackers from 1 to 9 attacks. The percentage PDR analysis values regarding to Priauth protocol start offer from 81.2 to 57.2 % respectively. Similarly, the percentage values corresponding to MPriAuth protocol are offer 90.5 to 66.2 % respectively. The comparative analysis between the existing Priauth protocol with the proposed MPriAuth exhibit that the MPriAuth protocol offers 25.33 % improvement regarding Priauth protocol.

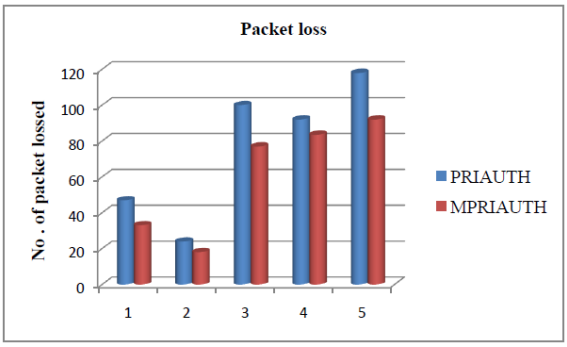

Figure 10: Analysis of packet loss with Varying Number of Attackers

Figure 10 demonstrates the packet loss ratio variations with reference to the number of attacks from 1 to 9 attacks and existence of faulty nodes respectively. For minimum attacks (1), and maximum speed (9), the maximum packet loss value of Priauth protocol is 118 packets for number of 9 attacks and minimum packet loss value is 18 packets for number of 3 attacks. Similarly, the maximum packet loss for MPriAuth protocol is 68 packets intended for the number of 9 attacks and minimum packet loss is 18 packets in the number of 3 attacks.

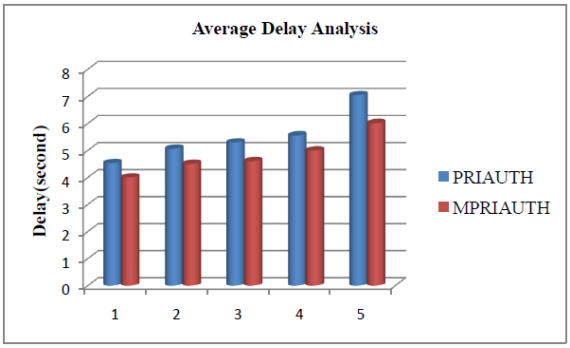

Figure 11: Analysis of average delay with Varying Number of Attackers

Figure 11 demonstrates the end-to-end delay variations with reference to the existence of faulty nodes respectively. For minimum number of attackers 1 attacks the end-to-end delay value of Priauth protocol is 4.53 second and 7.04 second for maximum number of 9 attacks for 50 faulty nodes. Similarly, the delay values for MPriAuth protocol are 4 seconds for minimum attack of 1 and 6.01 seconds for maximum number of 9 attacks.

CONCLUSION

In this given paper we examined the security prerequisites of Priauth intended for mobile networks and as well proposed a novel protocol to deal with the existing protocols' issues. The proposed MPriAuth strategy is simulated and tried utilizing two situations; differing MNs'mobility speed and fluctuating number of attackers in the network. PDR, throughput, packet loss ratio along with average delay are the parameters considered for the assessment. The widespread analysis

demonstrate that MPriAuth protocol opposes various security threats together with it offers more flexible furthermore elaborate privacy preservation, anonymous user authentication together with revocation function intended for mobile users. The evaluation of the performance reveals that the proposed protocol achieved universality with low communication cost.

REFERENCES

[1] Deng Yibing, Hu Wei, Li Minghui, Gao Feng, and Shen Junyi, “Research and Simulation on Application of the Mobile IP Network”, International Conference on Medical Physics and Biomedical Engineering, 2012.

[2] R. Wiangsripanawan, R. Safavi-Naini, and W. Susilo, “Location privacy in mobile IP In Networks”, Jointly held with the 2005 IEEE 7th Malaysia International Conference on Communication, 13th IEEE International Conference on Vol. 2, pp. 6-pp. IEEE, 2005.

[3] Khodor Hamandi, Imad Sarji, Ali Chehab, Imad H. Elhajj, and Ayman Kayssi, "Privacy enhanced and computationally efficient HSK-AKA LTE scheme", In Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on, pp. 929-934, IEEE, 2013.

[4] Dhasarathan Chandramohan, T. Vengattaraman, D. Rajaguru, and Ponnurangam Dhavachelvan, "A new privacy preserving technique for cloud service user endorsement using multi-agents", Journal of King Saud University-Computer and Information Sciences Vol. 28, No. 1, pp. 37-54, 2016.

[5] Victor Sucasas, Georgios Mantas, Firooz B. Saghezchi, Ayman Radwan, and Jonathan Rodriguez, "An autonomous privacy-preserving authentication scheme for intelligent transportation systems", Computers & Security Vol. 60, pp. 193-205, 2016.

[6] Shehzad Ashraf Chaudhry, Husnain Naqvi, Muhammad Sher, Mohammad Sabzinejad Farash, and Mahmood Ul Hassan, "An improved and provably secure privacy preserving authentication protocol for SIP", Peer-to-Peer Networking and Applications Vol. 10, No. 1, pp. 1-15, 2017.

[7] SuGil Choi, and Kwangjo Kim, "Authentication and payment protocol preserving location privacy in mobile IP." Global Telecommunications Conference, 2003. GLOBECOM'03, IEEE, Vol. 3. IEEE, 2003.

[8] Mohamed Amine Ferrag, Leandros Maglaras, Antonios Argyriou, Dimitrios Kosmanos, and Helge Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes", Journal of Network and Computer Applications 2017.

[9] Zaher Jabr Haddad, Sanaa Taha and Imane Aly Saroit, "Anonymous authentication and location privacy preserving schemes for LTE-A networks", Egyptian Informatics Journal 2017.

[10] Rui Chen and Dezhong Peng, "A novel NTRU-based handover authentication scheme for wireless networks", IEEE Communications Letters 2017.

[11] Elisa Bertino and Elena Ferrari, "Big data security and privacy", A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years, Springer International Publishing, pp. 425-439, 2018.

[12] Daojing He, Jiajun Bu, Sammy Chan, Chun Chen, and Mingjian Yin, “Privacy-Preserving Universal Authentication Protocol for Wireless Communications,” IEEE Transactions On Wireless Communications, Vol. 10, No. 2, pp. 431-436 2011.

[13] Xiaoyu Duan, and Xianbin Wang, "Authentication handover and privacy protection in 5G hetnets using software-defined networking", IEEE Communications Magazine Vol. 53, No. 4, pp. 28-35, 2015.

[14] Xu Yang, Yuexin Zhang, Joseph K. Liu, and Yali Zeng, "A trust and privacy preserving handover authentication protocol for wireless networks", In Trustcom/BigDataSE/I SPA, 2016 IEEE, pp. 138-143, IEEE, 2016.

[15] Shin-Ming Cheng, Cheng-Han Ho, Shannon Chen, and Shih-Hao Chang, "Distributed anonymous authentication in heterogeneous networks", In Wireless Communications and Mobile Computing Conference (IWCMC), 2014 International, pp. 505-510, IEEE, 2014.

[16] Debiao He, Ding Wang, Qi Xie, and Kefei Chen, "Anonymous handover authentication protocol for mobile wireless networks with conditional privacy preservation", Science China Information Sciences Vol. 60, No. 5, pp. 052104, 2017.

[17] Lai C, Li H, Liang X, Lu R, Zhang K, Shen X. CPAL: A conditional privacy-preserving authentication with access linkability for roaming service. IEEE Internet of Things Journal vol 1(1), pp. 46-57, 2014.