DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4264

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

AUTHENTICATION METHOD FOR SECURE COMMUNICATION IN MOBILE IP

Abdurahem El Atman Igrair
Department of Computer Science & information Technology
Sam Higginbottom University of Agriculture, Technology & Sciences Allahabad India.

Dr.RaghavYadav
Department of Computer Science & information Technology
Sam Higginbottom University of Agriculture, Technology & Sciences Allahabad India.

Abstract:The world is now growing in connectivity and communication like never before through the application of different mobility based devices. Mobile devices such as mobile phones, laptops etc. have become important and convenient to use. Mobile IP enhances the Internet Protocol (IP) by providing mobile hosts with the IP routing service. With Mobile IP, a host is able to move from an IP subnetwork to another and yet maintain its active connections and reachability with its constant IP address called the home address, security requirements in mobile ip authentication of all registration messages becomes important research challenge. The security of such networks is mainly achieved with use of security and privacy aware of authentication protocols. Additionally, the efficiency of such networks is mainly depends on use of authentication protocols in mobile ip . There are many authentication protocols already presented by various researchers with objectives of privacy preserving, authentication and secure communications. But most of protocols are failed to achieve both efficient user authentication schema and secure communication while achieving the quality of service (QoS) requirements of mobile ip . For roaming services in mobile networks, Priauth authentication protocol schema recent designed which is showing the efficient performance in terms of time and overhead parameters. For mobile ip , along with privacy preservation, secure communication method designing is also challenging task. Therefore in this research work, HPriauth (Hybrid Priauth) authentication protocol schema is designed and implemented which is based on recent Privacy-Preserving Universal Authentication Protocol (Priauth). HPriauth aimed to present not only efficient user authentication services but also secure routing communication in mobile ip in order to defend against any types of security threats in mobile ip . For secure communication we are proposed ECC cryptography technique.

Keywords: mobile Ip , PDR, Ecdsa, Ecdh, Wireless Networks, Quality of Service, Priauth, HPriauth, Loss Rate, Throughput.

I. INTRODUCTION

The current research area has seen an explosive growth in communications.Applications like on-line banking, personal digital assistants, mobile communication,Smartcards, etc. Have emphasized the need for security in resource constrainedEnvironments. Elliptic curve cryptography (ECC) serves as a perfect cryptographictool because of its short key sizes and security comparable to that of other standardpublic key algorithms. The authentication protocol must be able to keep up with the high degree of node mobility that often changes the network topology drastically and unpredictably. The combination of link-quality variation with the broadcasting nature of Wireless channels has revealed a direction in the research of wireless networking, namely, cooperative communication [6] [7].

The above paragraph is presenting the discussion on authentication and routing protocols behaviour. The intent is that, in this paper we are presenting the novel method for wireless networks privacy preserving, authentication and secure communication. Before discussing about proposed approach motivation, we are discussing below privacy preservation, authentication and secure communication needs for wireless networks [8].

The tiny mobile resources those are within range of current wireless network can able to transfer information or data at any time and at any place. Therefore, this is imposing the challenging problem of privacy, authentication of user and information security for wireless networks. Privacy in wireless communication is ensuring that the attacker cannot intercept the mobile user's communication data [1] [2]. The authentication process ensuring attacker cannot able to access the any services fraudulently of any mobile users. For seamless communications, mobile communication networks providing the roaming servicing by deploying roaming protocol so that user can get access of networks. For roaming scenario, basically three different parties considered such as home server S, roaming user R, as well as visiting foreign server F. User R is subscriber of server S. If user R is entered into the foreign network which is monitored by F, then roaming services allows R user to access the services those are subscribed via F. User R and F is having direct communication link, also same between S and F. But there is no direct communication link between user R and S. In order to prevent fraudulent services use, mechanism of authentication is required [3] [4] [12].

For designing the efficient privacy preserving mobile user authentication, there are different parameters which should be satisfied by this method. We have listed below are main requirements which needs to be satisfied by privacy preserving authentication method. A. Key establishment: in this requirement, foreign server and user can establish the random session key which is known to them. It is derived from the combination of foreign server and user. Basically, session key is not known by home server. B. User Anonymity: Apart from the home server as well as its subscribed user, no one can inform the identity of user including the foreign server. C. User Untraceablility: Apart from the home server and user, anyone cannot able to link to any future or past method including the foreign server for

similar user. D. Authentication of Server: foreign server identity is ensured by user. E. Subscription Validation: A foreign server is ensuring the home server of user identity. F. User Revocation Scheme Provision: by considering the related reasons, the process of user authentication should allow the foreign server in order to find whether or not roaming mobile user is revoked [12]. Therefore, for privacy preserving authentication methods, depending on basic interest of roaming users, it is necessary to keep users anonymous from the all eavesdroppers and the foreign server unless the identity information becomes critical which is known as user anonymity, the examples are special applications or some emergency situations. To achieve the privacy preservation and authentication in wireless networks, we studied different methodologies and from which Priauth is designed and implemented as MANET routing protocol to defend against different wireless attacks [12].

Apart from this privacy preservation and authentication, secure communication is another research challenge for wireless networks like MANET. Secure communication between the nodes was not addressed in Priauth method. Due to different types of security attacks, QoS performance of MANET is degrading as important data loss and leakage is impacted by security threats in MANET. In literature there are different methods introduced for MANET security attacks on different parameters and strategies, however such security methods having number of limitations [8]. This becomes the motivation for presenting the hybrid secure routing methodology in which both goals privacy preserving with authentication as well as secure network communication will be addressed. For privacy preserving and authentication we are using Priauth method which is contributed by Onion routing for secure communication in network. Onion Routing is a mechanism to provide private transmission over a public network. The source node sets up the core of an onion with a specific route message. During a way request phase, each send node adds an encrypted layer to the route request message. The proposed secure routing protocol is called as HPriauth (Hybrid Priauth). In section II, we are discussing about the related works on privacy preservation and authentication in wireless networks as well as secure communication methods. Section III, presenting the algorithm design and architecture for HPriauth routing protocol. Section IV, presenting the simulation results and discussions. Finally in section V, conclusion and future work discussed.

II. RELATED WORKS

2.1. Privacy Preservation and Authentication Methods for mobile ip

In [1], authors introduced the secure and light-weight authentication technique with the user anonymity to overcome the problems of previous methods. This method is also called as HZCB. At first, author discussed the security weaknesses of previous methods, and then proposed new technique to overcome them. From this paper, we studied that this method is simple to implement for mobile user since it only performs a symmetric encryption/decryption operation. Having this feature, it is more suitable for the low-power and resource-limited mobile devices. In addition, it requires four message exchanges between mobile user, foreign agent and home agent. Thus, this protocol enjoys both computation and communication efficiency as compared to the well-known authentication schemes. In special conditions author consider the authentication protocol when a user is located in his/her home network. Also, the session key will be used only once between the mobile user and the visited network. In addition to this, the security analysis demonstrates of this scheme enjoys important security attributes such as preventing the various kinds of attacks, single registration, user anonymity, no password/verifier table, and high efficiency in password authentication, etc. Moreover, one of the new features in our proposal is: it is secure in the case that the information stored in the smart card is disclosed but the user password of the smartcard owner is unknown to the attacker.

In [2], authors proposed the two new anonymous roaming protocols for wireless communication in which only the roaming users as well as the foreign network are involved in running protocol called YHWD. Both of the protocols are global and universal such way that both can directly be used as AKE protocols for the home network. In this secure two party roaming protocol, authors adopted the existing efficient method called Identity Based Signature (IBS) which is existentially unforgivable against the message attacks and adaptive selected ID attacks. Author used IBS method introduced by authors Zhu, Yang and Wong in reference number [6] as it is efficient as well as simple enough for resource constrained mobile devices. This technique needs the ECSM (Elliptic Curve Scalar Multiplication) functionality for generating the signature and one Multi-ECSM operation for verifying a signature, and the ECSM operation in the signing algorithm can further be pre-computed. In addition to this, author also introduced the revocation technique as well as billing method. A practical result of this method is showing the better performance for security against existing methods.

In [3], author proposed secure and lightweight user authentication protocol with anonymity for roaming service in the global mobility network (GLOMONET) called HCCBF. Author claimed that their approach is having more advantages as compared to related methods. Firstly, it uses low-cost functions such as one-way hash functions and exclusive-OR operations to achieve security goals. Having this feature, it is more suitable for battery-powered mobile devices. Secondly, it uses nonce instead of timestamps to avoid the clock synchronization problem. Therefore, an additional clock synchronization mechanism is not needed. Thirdly, it only requires four message exchanges between the user, foreign agent and home agent. Further, the security properties of this method are formally validated by a model checking tool called AVISPA. Author also demonstrate that this protocol enjoys important security attributes including prevention of various attacks, single registration, user anonymity, no password table, and high efficiency in password authentication. Security and performance analyses show that compared with other related authentication schemes, the proposed scheme is more secure and efficient.

In [4], author proposed the method of construction of anonymous as well as authenticated key exchange protocols for a *roaming* user and a visiting server in order to establish a random session key in such a way that the visiting server authenticates the user's home server without knowing exactly who the user is. This method is called as YWD. Network eaves dropper cannot find out the user's identity

either which is known as *user anonymity*. In addition, visited servers cannot track the roaming user's movements and whereabouts even they collude with each other this is known as *user Untraceablility*. This construction approach is generic and built upon provably secure two-party key establishment protocols. The advantage of this generic protocol construction include eliminating alias synchronization between the user and the home server, supporting joint key control, and not relying on any special security assumptions on the communication channel between the visiting server and the user's home server.

In [5], author proposed novel method for privacy-preserving universal authentication protocol which is named as Priauth. This protocol delivers the strong user anonymity against both foreign servers and eavesdroppers. Also providing the efficient session key establishment and achieves efficiency. In addition to this, this approach providing the efficient method to handle the user revocation problem at the same time strong user Untraceablility supporting. This method is considering the four different types of threats to the user authentication such as DoS attack, false mobile user attack, message env route attack and deposit case attack. There are two main contributions such as first is related to showing the weaknesses of present authentication methods in mobile wireless communications. The second is contribution is that they proposed the privacy-preserving universal authentication protocol called *Priauth*.

2.2. MOBILE WIRELESS NETWORK SECURITY METHODS

In [6], author Elhadi M. Shakshuki *et al.* EAACK is presented most recently to overcome the previous techniques discussed above. In this method author have proposed a novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. Practically this method was outperforming all above three methods. Delay performance is worst. For communication, this approach not used the efficient cryptography method.

In [7], author proposed TWOACK security method for MANET. With respect to the six weaknesses of the Watchdog scheme, many researchers proposed new approaches to solve these issues. TWOACK proposed by Liu *et al.* [2] is one of the most important approaches among them. The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network. However, many research studies are working in energy harvesting to deal with this problem.

In [8], author Marti *et al.* proposed a scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog serves as an ID for MANETs. Many following research studies and implementations have proved that the Watchdog scheme is efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than link. Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping.

In [9], Sheltami *et al.* proposed a new scheme called AACK based on TWOACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

In [10], Liu *et al.* proposed a 2ACK scheme for the detection of routing misbehavior in MANETs. In this scheme, two-hop acknowledgement packets are sent in the opposite direction of the routing path to indicate that the data packets have been successfully received. A parameter acknowledgment ratio, i.e., *R*ack, is also used to control the ratio of the received data packets for which the acknowledgment is required. This scheme belongs to the class of proactive schemes and, hence, produces additional routing overhead regardless of the existence of malicious nodes.

In [11], Jian-Ming Chang *et al.* proposed the recent technique for defending against collaborative malicious attacks by using CBDS approach on DSR protocol. Author proposed new mechanism (called the CBDS) for detecting malicious nodes in MANETs under gray/collaborative blackhole attacks. The practical simulation results revealed that the CBDS outperforms the DSR, 2ACK, and BFTR schemes, chosen as benchmark schemes, in terms of routing overhead and packet delivery ratio. This method is outperforming all existing techniques. The limitation of this method is that poor delay performance; also end to end data security is not considered which may be addressed using efficient cryptography technique only.

III. PROPOSED METHODOLOGY

Figure 1 is showing the simulation work flowchart and parameters evaluated for proposed Hpriauth and existing security authentication methods. HPriauth is designed by ECC cryptography technique which is compared with two existing privacy preserving authentication schema methods called Priauth, and YHWD. The performance of any routing protocol is mainly depends on four major parameters under the attacks such as throughput, packet delivery ratio (PDR), end to end delay and rate of packet loss. The novelty of HPriauth is that it providing efficient privacy preservation, efficient user authentication and most important efficient secure communication among mobile nodes.

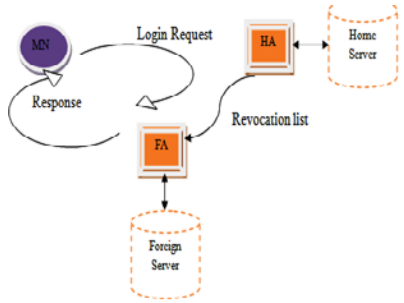

Figure 1: authentication system

Below main algorithms proposed for HPriauth authentication schemes protocol. Algorithm its secure authentication scheme for Registration process in mobile ip

Algorithm : Secure Authentication Schemes using ECC
Step1:ECDSA Digital signature algorithms are used to authenticate a digital content between FA & HA. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit
(integrity).

2.1. Key pair generation using ECDSA:
Let A be the signatory for a message M. Entity A performs the following steps togenerate a public and private key:
(1) Select a unique and integer, d, in the interval [1, n-1]
(2) Let Q = dg
(3) Sender Party1's private key is d (4) Sender Party1's public key is the combination
(E, g, n, Q)

2.2. Signature Generation Using ECDSA
Using Party1's private key, A generatesthe signature for message M using the following steps:
(1) Select a unique and unpredictable integer k in interval [1,n-1]
(2) Compute kg = (x1,y1), where x1 is an integer
(3) Compute r = x1 mod n; If r = 0, then go to step 1
(4) Compute h = H(M), where H is the SHA-512
(5) Compute s = k-1(h + dr)mod n; If s = 0, then go to step1
(6) Signature of A for message M is the integer pair (r, s)

2.3. Signature Verification Using ECDSA
The Party2 can verify the authenticity ofParty1's signature (r, s) for message M by performing the following:
(1) Obtain signatory Party1's public key (E, q, n, Q)
(2) Verify that values r and s are in the interval [1,n-1]
(3) Compute w = s-1 mod n.
(4) Compute h = H(M), where H is the same secure hash algorithm used by Party1.
(5) Compute u1 = hw mod n
(6) Compute u2 = rw mod n
(7) Compute u1g + u2Q = (x0,y0)
(8) Compute v = x0 mod n
(9) The signature for message M is verified only if v = r

Step 2: ECDH Secure key exchange algorithms
Are used to exchange our keys securely via a non secure channel between MU & FA .
FA will sent the public key and private key to MU. Mobile user will recive public and private key by ECDH.
MU calculates $S=d_AH_B$ (using her won private key and FA public key), FA calculates $S= d_BH_A$ (using his own private key and MU user public key).S is the same for both MU & FA

$$S=d_AH_B = d_A(d_BG)=d_B(d_AG) = d_BH_A$$

Step 3: ECIES: is an Integrated Encryption Scheme

Mobile user sent the keys in encrypted form by using ECIES for security. Key receives by FA form mobile user decrypted by FA and verify the authentication of the MU.

3.1. ECIES Encryption:
INPUT: Message m and public key OUTPUT: The ciphertext (U,c,r)
1. Choose k € R(1…….q-1)
2. U ← [k]G
3. T ← [k]Y
4. (k1||k2) ← KD(T,l)
5. Encrypt the message c ← Ek1(m)
6. Compute the MAC on the ciphertext r ← MACk2(c)
7. Output (U,c,r)

3.2. ECIES Decryption:
INPUT: Ciphertext (U,c,r) and a private key r. OUTPUT: The message m or an 'invalid
ciphetext' message.
1. T ← [x]U
2. (k1||k2) ← KD(T,l)
3. Decrypt the message m ← Dk(c).
4. if r ≠ MACk2(c) then output 'Invalid Ciphertext'
5. output m

IV. RESULTS AND DISCUSSION

The simulation of proposed methodology is done using NS3 software in which we have designed wireless networks with 50 mobile nodes and two servers (home and foreign) with two privacy preservingauthentication schemes and one hybrid method HPriauth.

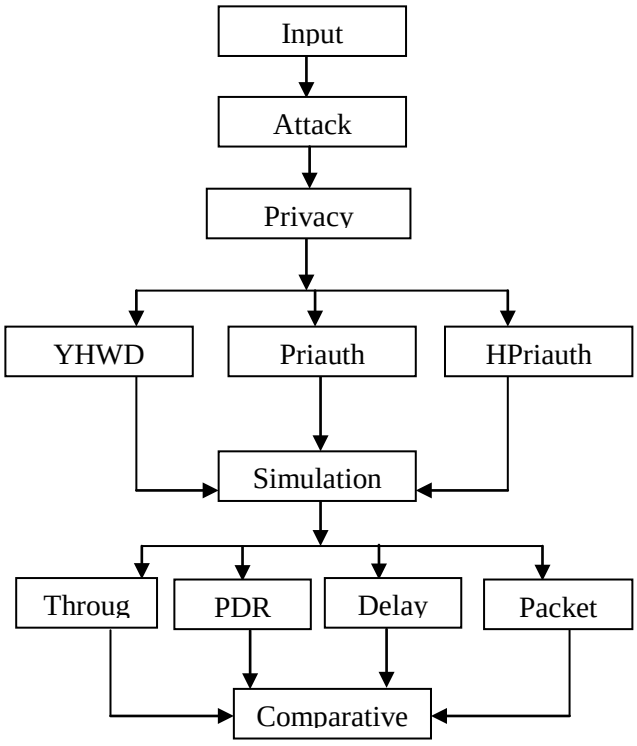

Figure 2: Proposed Methodology Architecture

4.1. Network scenario

Security authentication Protocols: YHWD, Priauth and HPriauth

Number of wireless nodes: 50

MAC: 802.11

Simulation Time: 30 Seconds

Mobility Speed: 5, 10, 15, 20, 25 (m/s)

Number of Attacks: 5 (Malicious users attacks)

4.2. Performance Metrics

1) Avg. Throughput

throughput=(seq number * segment size * 8) / active duration

2) Packet Delivery Ratio (PDR)

PDR= (number_of_received_packets/number_of_generated_packets) * 100

3) End to End Delay

dend-end= N[dtrans+dprop+dproc+dqueue]

where,
dend-end= end-to-end delay

dtrans= transmission delay

dprop= propagation delay

dproc= processing delay

dqueue= Queuing delay

N= number of links (Number of routers - 1)

4.3. Comparative Results

Figure 3 is showing the results measured for average throughput performance by varying mobility speed under the presence of 5 malicious attacks in network. The Priauth method is showing the promising improvement in throughput in each case. Further proposed HPriauth improving this performance against Priauth as security is provided while communications between mobile nodes. Therefore throughput is improving in HPriauth. Figure 4 and 5 is showing the PDR and packet loss rate respectively. Packet loss performance of HPriauth is very less; it means information loss due to attacks is prevented efficiently. In figure 5, the delay performance is showing, in which Priauth failed to minimize the delay as compared to existing methods. But by using our proposed HPriauth performance of delay is significantly minimized.

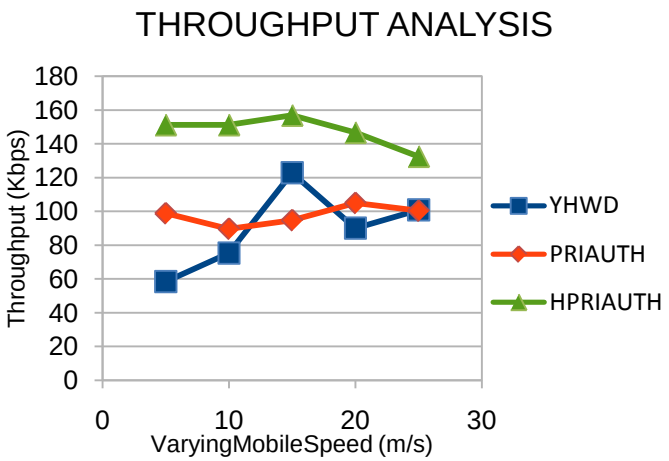

Figure 3: Average Throughput vs. Mobility Speed

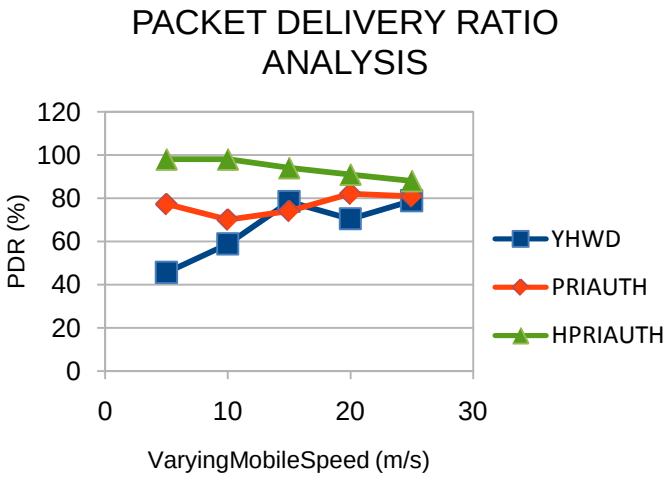

Figure 4**:** Packet Delivery Ratio vs. Mobility Speed

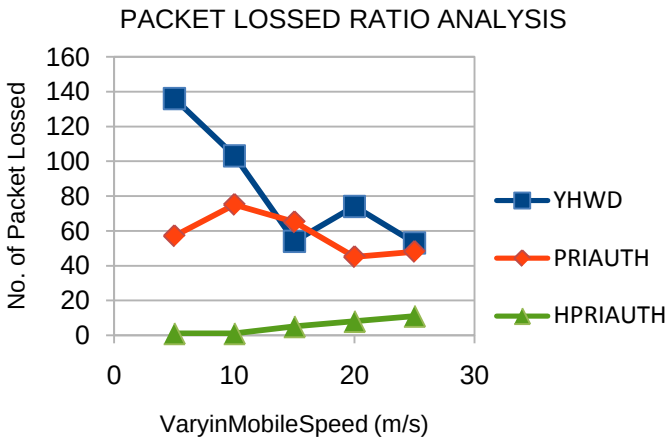

Figure 5: Loss Rate vs. Varying Mobility Speed

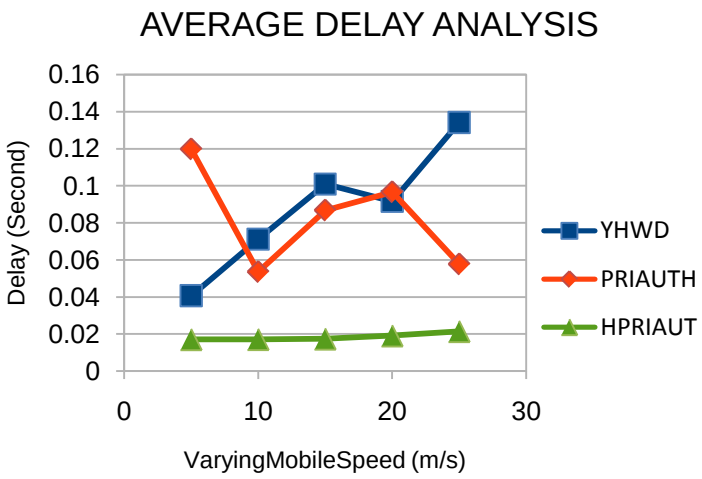

Figure 6: End to End Delay vs. Varying Mobility Speed

V. CONCLUSION AND FUTURE WORK

For infrastructure networks like mobile ip , there are two major security concerns such as privacy preservation with mobile user authentication as well as secure communication among mobile nodes. There are number of attacks such as DoS,Reply Attack , Passive Eavesdropping, malicious node attacks etc. In this paper we proposed hybrid authentication scheme protocol for mobile ip using Ecc algorithms , which is based on three methodologiesl. The authentication protocol is called HPriauth which designed and simulated using NS3. The network scenario considered for performance evaluation is varying mobility speed under the presence of malicious user attacks. HPriauth is showing the throughput improvement by 30 % as compared to Priauth method. The packet loss performance is improved 10 % approximately as compared to Priauth method. For future work, we suggest to work on different network conditions and networks.

REFERENCES

[1] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A strong user authentication scheme with smart cards for wireless communications," *ComputerCommun.*, 2010, doi: 10.1016/j.comcom.2010.02.031.

[2] G. Yang, Q. Huang, D. S. Wong, and X. Deng, "Universal authentication protocols for anonymous wireless communication ns," *IEEE Trans.WirelessCommun.*, vol. 9, no. 1, pp. 168-174, 2010.

[3] D. He and S. Chan, "Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks," Wireless Personal Commun., 2010, doi: 10.1007/s11277-010-0033-5

[4] G. Yang, D. S. Wong, and X. Deng, "Anonymous and authenticated key exchange for roaming networks," IEEE Trans. Wireless Commun., vol.6, no. 9, pp. 3461-3472, 2007.

[5] 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, FEBRUARY 2011.

[6] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013.

[7] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.

[9] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.

[10] R. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[11] Jian-Ming Chang, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", Published in: IEEE Systems Journal (Volume: 9, Issue: 1), 2014.

[12] Abdurahem El Atman Igrair, Dr. Raghav Yadav, "Review: Privacy Preserving Authentication (PPA) Protocols for Wireless Mobile Networks", Volume 6, Issue 5, May 2016, International Journal of Advanced Research in Computer Science and Software Engineering.