Journal of Engineering and Applied Sciences 12 (Special Issue 2): 6201-6207, 2017
ISSN: 1816-949X

Efficient Authentication Scheme and Secure Communication for Mobile IP Networks under Varying Mobility Speed

Abdurahem El Atman Igrair and RaghavYadav
Department of Computer Science and Information Technology,
Sam Higginbottom Institute of Agriculture, Technology and Sciences, Allahabad, India

Abstract: As increasing use of wireless networks like Mobile IP Networks (MINET) or Wireless Sensor Networks (WSNs) in day to day life its security requirements and privacy preserving requirements becomes important research challenge. The security of such networks is mainly achieved with use of security and privacy aware routing methods. Additionally, the efficiency of such networks is mainly depends on use of routing protocols. There are many routing methods introduced by researchers with objectives of privacy preserving, authentication and secure communications for MINETs. But most of methods are failed to achieve both efficient user authentication and secure communication while achieving the Quality of Service (QoS) requirements of mobile IP networks. For roaming services in mobile networks, Priauth protocol recent designed which is showing the efficient performance in terms of time and overhead parameters. For mobile wireless networks, along with privacy preservation, secure communication method designing is also challenging task. This study presents the novel HPriauth (Hybrid Priauth) routing method with goal of achieving multi-objectives like privacy preservation and secure data communication. For authentication and privacy preservation we designed roaming scenario based steps and for data security we designed onion routing based steps. This study is presenting both steps in HPriauth for MINET with its simulation analysis. From the simulation results, HPriauth is out performing all previous methods.

Key words: Secure routing, mobile IP, quality of service, Priauth, HPriauth, loss rate, throughput

INTRODUCTION

The group of self organizing mobile nodes which can be deployed without the need of any physical infrastructure is collectively known as wireless Mobile IP Networks (MINETs). The mobile nodes in MINETs are connective through the radio links independent of any network devices. In MINETs, every mobile device acts as both sender and router. Mobiles can send their data to destination nodes through the other mobiles nodes which are acts as routers to receive and forward data through the intermediate nodes (Abdelgadir *et al*., 2013). The mobile nodes in network are randomly moving in network. Hence, the first challenge of such networks is the designing flexible routing schemes which can efficiently finds the route within home networks or between home and foreign networks (Deng *et al*., 2002). It is must that routing scheme should come up with node a mobility problem that frequently changes the network topology unpredictably and drastically. Along with the dynamic and efficient routing scheme designing the link quality and security is another major research challenge in MINETs due to the open nature architecture. There is need to efficient authentication solutions while mobile nodes leaving home network to foreign network as well as their must be the secure data transmission between source to destination nodes. In this study, we are presenting the novel method for MINETs privacy preserving, authentication and secure communication.

In MINET, the mobile nodes under range of any wireless network can initiate the data transfer from any place at any time. This leads to the problem of user privacy and authentication problems as well as secure data communication problems. In MINETs, privacy ensures that malicious user not able to intercept the current communication of mobile users (He *et al*., 2010; Yang *et al*., 2010). The process of authentication ensures that malicious unable to access services of mobile users. In seamless networks, roaming services are used by MINETs via. roaming protocols in order to get the network access any time and any place. In roaming networks, there are three main components lie roaming user R, home server S and foreign server F (He and Chan, 2010). For mobile user R, home server is S. If R changes its

Corresponding Author: Abdurahem El Atman Igrair, Department of Computer Science and Information Technology, Sam Higginbottom Institute of Agriculture, Technology and Sciences, Allahabad, India

position and enters into the F then roaming protocol allows R to use the services of F. During this operations attacker may take access to the services of network F maliciously. Therefore, the technique of efficient authentication is required to prevent the use of services maliciously (Yang *et al*., 2007; Igrair and Yadav, 2016). The designing of efficient authentication technique for MINETs is impacted by the various constrains and parameters satisfaction. The core requirement of authentication schemes to satisfy are: key establishment, user anonymity, user untraceablility, authentication of server, subscription validation and user revocation (Igrair and Yadav, 2016). Hence based on the roaming user's main interest in privacy preserving and authentication schemes it is must to have mobile users anonymous from the foreign server as well as all eavesdroppers still the critical position of user identity information. This is called as user anonymity. To achieve the privacy preservation and authentication in wireless networks we studied different methodologies and Priauth is designed and implemented as MINET routing protocol to defend against different mobile IP attacks (Igrair and Yadav, 2016).

Apart from this privacy preservation and authentication, secure communication is another research challenge for MINETs. Secure communication between the nodes was not addressed in Priauth method. Due to different types of security attacks, QoS performance of MINET is degrading as important data loss and leakage is impacted by security threats in MINET. In literature there are different methods introduced for MINET security attacks on different parameters and strategies, however such security methods having number of limitations (Marti and Miglani, 2012). 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. We designed novel security steps based on onion routing terminology to achieve the secure data communication in roaming networks. 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.

Ease of use

Mobile IP networks: The mobile IP deliver the information exchange to and from the mobile devices like wireless communications and laptops. In MINET, mobile computer can change its current location to the foreign network and still able to access its home network. Figure 1 is showing the mobile IP topology.

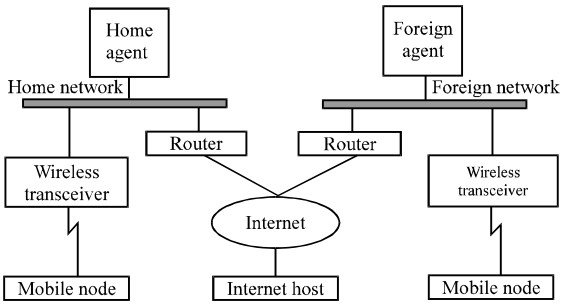

Fig. 1: Architecture of mobile IP communications (He *et al*., 2010)

Using mobile device home address, internet host transmit data to mobile node. The data is transmitted via normal IP functionality in case mobile node resides in home network; otherwise data collection is performed by home agent. Home agent transfer data to foreign agent if mobile device is in foreign network. The foreign agent transmits the data to intended mobile device. If mobile device is in foreign network, data collection is done by foreign agent and then forward data to internet host.

As showing in Fig. 1, there are three core components of MINET such as MN: Mobile Node, FA: Foreign Agent, HA: Home Agent. Next study, we are presenting the study over the different solutions of MINET security.

Privacy preservation and authentication methods: The novel approach was in presented by He *et al*. (2010) for light weight and secure authentication solution along with the user anonymity for MINETs. They designed this method to overcome the challenges or existing techniques. As there are four researchers included in design of this technique, it can be named as HZCB (initial letters of each author). The security problems of earlier methods had been discussed by them then designed HZCB solution. HZCB method seemed to easier for experimental analysis in MINETs as it is based on symmetric key cryptography functions. HZCB method is basically more suitable for limited resource mobile stations and lower energy devices. Additionally, HZCB solution required four different message exchanges among foreign agent, home agent and mobile node. Hence, experimentally this technique claimed communication and computation efficiency against the previous methods. They assumed the authentication scheme under the special network conditions when the mobile node is in within own home network. Use of session key was done only one time among the between visited network and mobile node. The security analysis conducted by researcher shown that HZCB method enjoyed the security

attributes importance like single registration, high authentication efficiency, different attacks prevention, etc. They added the one of feature in this scheme as this technique provided the security for stored information in smart card by not letting attacker to know the smartcard owner password.

Yang *et al.* (2010) another method designed for anonymous routing protocol in MINETs. They introduced the two anonymous schemes for mobile communications which was based on only two parties such as foreign network and roaming user. This method was proposed by four researchers hence collectively called as YHWD in this study. The methods presented in this study were universal as well as global so that both proposed methods are utilized as AKE method in home network. They used the already available technique IBS (Identity Based Signature) method in their proposed secure two party methods. IBS is inexcusable against the attacks like adaptive chosen ID attacks and message attacks. The IBS technique was referred and utilized from Abdelgadir *et al.* (2013) due to this efficiency and ease to use with mobile devices. The signature generation was done using the elliptic curve scalar multiplication approach. The signature verification was done using one Multi-ECSM functionality and pre-computation of ECSM function is used. Additionally, they proposed the method for revocation and billing. The experimental results of this method claimed the improved security performance.

The method for GLOMONET was designed by He and Chan (2010). Here researcher introduced mobile user authentication method with consideration of roaming service anonymity for the global mobility networks. This method is called as HCCBF. They had shown that HCCBF technique improving performance against the previous techniques of authentication through the practical works. In this approach, at first researcher designed the less cost functions like one way hash as well as exclusive OR functions in order to address the security problems. This features helped to minimize the consumption of energy of mobile nodes. Secondly, in this technique they utilized the nonce rather than timestamps to prevent the problem of clock synchronization. Hence, the extra task of using clock synchronization is not required with this technique. Finally, they used to four messages to exchange the information among the different components of MINET. They used AVISPA tool for the validation of security functionality of HCCBF technique. They demonstrated that HCCBC technique supports the security attributes importance like single registration, high authentication efficiency, different attacks prevention, etc. The practical results of this technique were shown that HCCBF achieved the efficiency in security.

Yang *et al.* (2007) novel technique designed for the anonymous user construction and authentication supported key exchange method for the networks like MINET in which frequent activities of roaming users happened. The authenticated supported key exchange was designed to mobile user and visiting network for establishing random session key in order to perform the visiting network authentication for home network of mobile user. There were three researchers contributed in design of this technique, hence named as YWD. In this method, network attackers failed to find the identity of mobile users it is called as user anonymity. Additionally, they designed method in such way that foreign network not able to track the activities of roaming mobile users and whereabouts even if they crossed each other in network. This feature is called as untraceability. Basically, this method was generic and designed based on secure two party methods of key establishment.

He *et al.* (2011), the most recent technique that under investigation of our work proposed. The modified technique for mobile user privacy preservation as well as global authentication was proposed. They called this method as Priauth. The novelty of this method was it delivered strong mobile user anonymity against the attackers and visiting networks. Additionally, this method was provided the optimized approach for session key establishment in MINETs. Priauth supported the functionality of handling the problem of user revocation efficiently as well as untraceablility.

Secure communication methods: Abdelgadir *et al.* (2013), Deng *et al.* (2002), Marti and Miglani (2012), the survey and introduction on mobile IP networks are presented with respect to security by defending against the different security threats. Apart from this, below are recent security methods proposed on wireless network security.

Sheltami *et al.* (2009) researcher designed the novel approach for wireless network security called as TWOACK. This method was based on AACK. The AACK is nothing but acknowledge based method. In TWOACK, there are two different methods combined such as TACK as well as Acknowledge (ACK). This technique was designed for wireless mobile ad hoc networks to prevent the malicious node attacks. Both TWOACK and AACK simulation results were shown that they can minimize the network overhead significantly while maintaining the throughput performance. However, both methods had the limitations of not detecting the malicious mobile users in the presence of forged acknowledgement data and false misbehaviour reports.

Balakrishnan (2007) researcher designed another acknowledgement based routing scheme for network security called 2ACK. With this method, 2 hop packets of acknowledgement were transmitted in reverse direction of routing path in order to claim that successful receipt of data packets. In this approach, researcher used the acknowledgement ratio parameter in order to control the received data packets ratio to which there is need to acknowledgement. Their method falls into the category proactive routing schemes. Therefore, this approach resulted into the extra routing overhead issues regardless of presence or absence of malicious users in network.

Chang *et al*. (2015) proposed the recent technique for defending against collaborative malicious attacks by using CBDS approach on DSR protocol. They designed the novel approach for network security called as CBDS. CBDS proposed to detect the malicious wireless users in mobile wireless networks for attacks like blackhole or grayhole attacks. Their experimental results claimed that performance of CBDS is outperforms the previous methods such as BFTR, 2ACK (Balakrishnan, 2007), etc., in terms of packet delivery rate and network overhead. The drawback of this technique was the worst performance of delay as compared to previous methods. Otherwise, this method was 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.

MATERIALS AND METHODS

Proposed: The system design of proposed approach is depicted in Fig. 2 with list of performance parameters evaluated for proposed HPriauth and existing security methods. HPriauth is designed as routing protocol which is compared with two existing privacy preserving methods called Priauth and YHWD. The performance of any routing protocol is mainly depends on four major parameters under the attacks like average throughput, E-2-E delay, PDR and number of data lost rate. The novelty of HPriauth is that it providing efficient privacy preservation, efficient user authentication and most important efficient secure communication among mobile nodes in MINET.

The study proposed for HPriauth protocol. The privacy preserving and authentication are designed as per the below system model showing in Fig. 3.

As showing in Fig. 3 MN is roaming user which is moving from home server (HA) to foreign server (FA) via. request response process in order to perform the privacy preservation and authentication.

Privacy preserving and authentication for mobile IP network

Input:

- N: Number of mobile IP network users
- T: Time interval
- G: Key generator

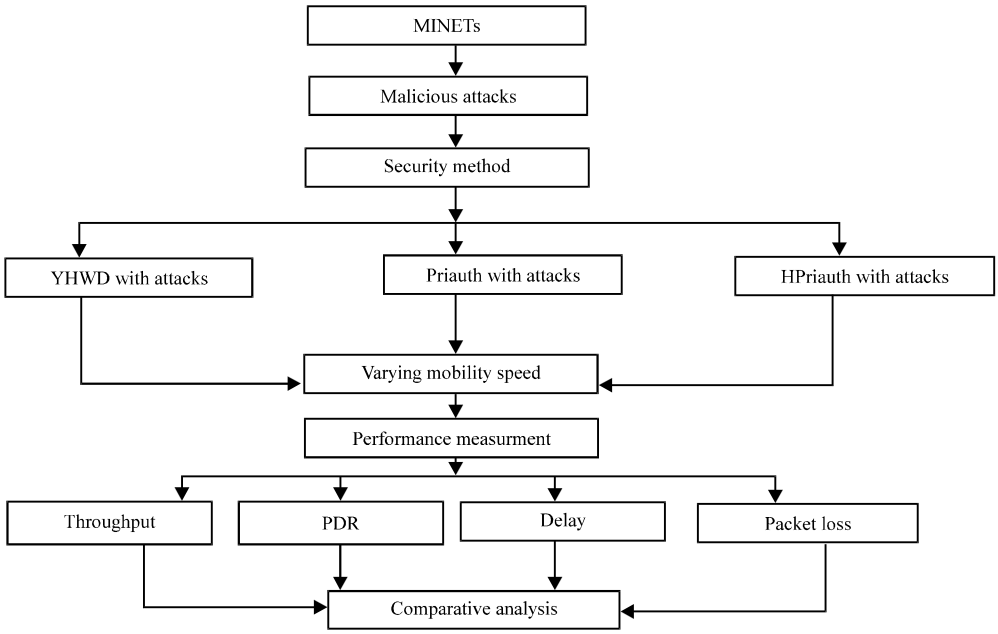

Fig. 2: Proposed methodology architecture (He *et al*., 2011)

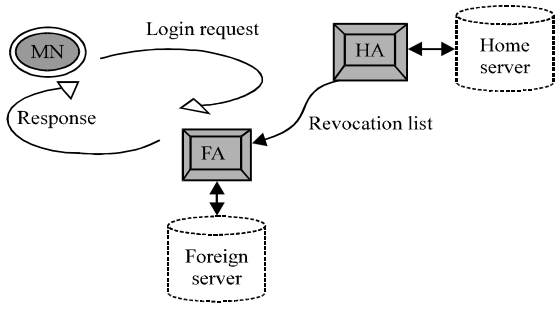

Fig. 3: System model for privacy preservation and authentication

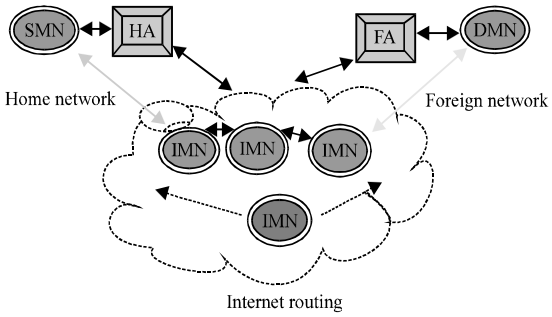

Fig. 4: Secure data transmission in mobile IP network (Sheltami *et al*., 2009)

Phase 1 (MN at home server)

Step 1: VLR-GS. Keygen (N, T): The random selection of generator g∈G and $\tilde{g} \in RG$ by group manager. Then choosing the h j∈RG for all j∈[1, T]. Selection of γ∈RZ*p and calculates w = gγ. It selects xi∈RZ p and computes Ai = g1/(γ+xi) for all i∈[I, N]. Group manager calculates the Bij = hxij for all i as well as j; mpk is (g, $\tilde{g}$, h1 ... hT, W), master public key. Secrete key of every subscriber is [i] is (Ai, xi). The revocation token at interval j of subscriber with secret key (Ai, xi) is [i] [j] = Bij.

Step 2 (VLR-GS. Sign (mpk, [i], k, M)): Select random number α, β, δ∈RZ*p. Compute T1 = Ai $\tilde{g}$ α, T2 = gα $\tilde{g}$ β, T3 = e (gxi, hj) δ and T4 = gδ. Compute V = SPK {(α, β, δ, xi, Ai): T1 = Ai $\tilde{g}$ α∧T_2 = gα $\tilde{g}$ β∧T_3 = e (gxi, hj) δ∧T4 = gδ∧e (Ai, wgxi) = e (g, g)} (M). Output the group signature σ = (T1, T2, T3, T4, V).

Step 3 (transmitting request to foreign server): After key generation and signature generation σ for foreign server FA. Ui (any roaming MN) firstly selects a random number Ru as well as temporary identity alias, generates signature σU = VLRGS. Sign (mpk_{HF}, [i], j, HF‖FA‖alias‖g^{Ru}‖ts). Then, sends {H, alias, g^{Ru}, ts} to FA. ts (timestamp) is added by Ui to counter replay attacks.

Phase 2 (MN signature at received foreign server)

Step 4 (FA verifying the received signature): VLR-GS Verify (mpk, j, RLj, σ, M); signature check: check that σ is valid or not. Revocation check: check that the signer is not revoked at interval j by checking T3/ = e (T4, Bij) for all Bij∈RLj. FA chooses a random number Rv. Computes σ FA = ECDSA. (SkV, mV) where mV = HF‖FA‖alias ‖g^{Ru}‖g^{Rv}. FA sends {FA, g^{Rv}, σV} to HA. FA computes the session key SK = ( ). Erase Rv from its memory.

Phase 3 (FA response sends back to MN)

Step 5 (upon receiving {FA, Rgv, σV} at MN): MN verifies σ FA by using ECDSA. Ver (pkv, mv, σV). If verification returns 1, MN generates sessions key SK = ( ). Erase Ru from the memory. MN generates (HA‖FA‖alias‖g^{Ru}‖g^{Rv}); sends to FA.

Phase 4 (Authentication at FA)

Step 6 (FA Authenticating MN): FA decrypts message received from MN and then verifies it. If the message is valid, FA concludes that MN has established a session key. Else FA rejects the connection.

Secure onion routing in MINET is designed to achieve the MN privacy and authentication in mobile IP networks. In order to prevent the black hole attacks in MINET we designed the second steps mentioned below. Figure 4 is showing the working architecture for this steps and then actual steps of discussed there.

As showing in Fig. 4, SMN is source mobile node which is in its home network whereas DMN is destination mobile node which is in foreign network. SMN is transmitting the data to DMN through the intermediate MNs (IMN). IMN in black color is indicating the attacker node in network. As per the system model designed in Fig. 5 is described.

Secure onion routing in MINET

Input:

- N: Number of mobile IP network users
- T: Time interval
- G: Key generator

Step 1 (privacy preservation and authentication): SMN sends request to FA; FA verify the request from SMN; FA response to request back to SMN; FA authenticate the validation of SMN for data transmission.

Step 2 (at SMN in home server): PKI generation done by broadcasting source node ID. Extract the public key, private key and session key. Insert all three current keys into the routing table.

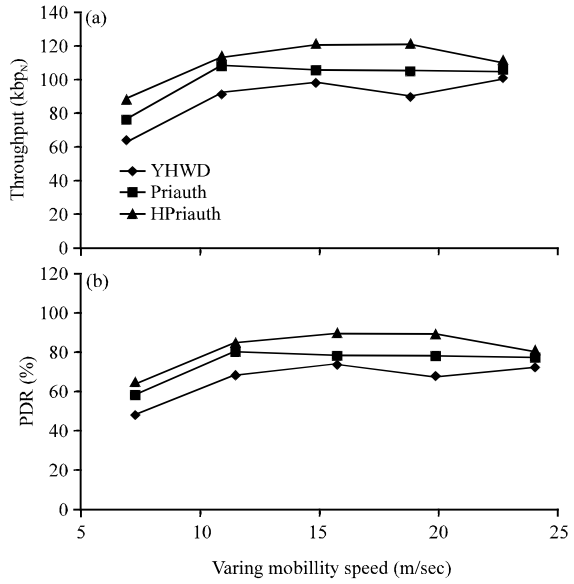

Fig. 5: a) Throughput analysis and b) PDR analysis

Step 3 (at SMN in home server): Extract the current routing information; get the current session key; generate the new session key and update the routing table entries; broadcast RREQ packet; apply the key encryption onion at intermediate nodes and destination node; signing by source node with its group private key; broadcasting finally the authenticated RREQ; set the status "P" and update the routing table entry for current path with this status.

Step 4 (at IMN): Verify the received packet with group private key; if packet verification is successful then extract all details from the received packet else marked current received packet is from malicious node and drops it. Transfer the received packet further by following below steps of onion routing. If the Nsq exists in the table but with an old timestamp it has been processed before and will be ignored, else current rreq is new and it will be proceed further. Apply decryption operation if its destination node, else forward it to next hope by performing the encryption operation by using the keys generated. Signing the source node with its group private key. Set the status "P" and updated routing table entry with current route

Step 5 (at DMN in foreign server): Verify the received packet with group private key. If packet verification is successful then extract all details from the received packet else marked current received packet is from malicious node and drops it. Decrypt and recover the packet data at DMN.

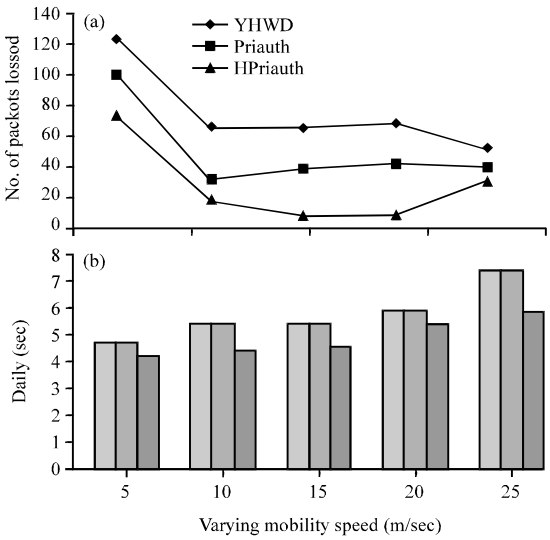

Fig. 6: End to end delay vs. varying mobility spee; a) Packet loss analysis and b) Delay analysis

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 three privacy preserving schemes and one hybrid method HPriauth.

Network scenario: Security routing protocols: YHWD, Priauth and Hpriauth. Number of wireless nodes: 50 MAC: 802.11. Simulation time: 30 sec. Mobility speed: 5, 10, 15, 20, 25 (m/sec). Number of attacks: 5 (Malicious users attacks). Avg. throughput: throughput = (seq. number×segment size ×8) active duration. Packet Delivery Ratio (PDR) = (number_of_received_packets/number_of_generated_packets)×100; end to end delay = L [T+P+Pc+Q] where T = transmission delay, P = propagation delay, Pc = processing delay, Q = Queuing delay, L = number of links (number of routers -1).

Comparative results: Figure 5a 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 5b and 6a 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 Fig. 6b, 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.

CONCLUSION

For mobile IP networks, 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, blackhole, grayhole, selfish node, malicious node attacks, etc. In this study, we proposed hybrid security routing protocol for MINET which is based on two methodologies such as Priauth and secure onion routing. The proposed routing 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.

SUGGESTION

For future work, we suggest to work on different network conditions and networks.

REFERENCES

Abdelgadir, O.A., A.B.A. Nabi and A.G.E. Abdalla, 2013. Security overview on mobile IP networks. Intl. J. Sci. Res., 4: 1328-1337.

Balakrishnan, R., 2007. An acknowledgement based approach for the detection of routing misbehavior in MANETs. IEEE. Trans. Mob. Comput., 6: 536-550.

Chang, J.M., P.C. Tsou, I. Woungang, H.C. Chao and C.F. Lai, 2015. Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. IEEE Syst. J., 9: 65-75.

Deng, R.H., J. Zhou and F. Bao, 2002. Defending against redirect attacks in mobile IP. Proceedings of the 9th ACM Conference on Computer and Communications Security, November 18-22, 2002, ACM, Washington, USA., ISBN:1-58113-612-9, pp: 59-67.

He, D. and S. Chan, 2010. Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks. Wirel. Pers. Commun., 61: 465-476.

He, D., J. Bu, S. Chan, C. Chen and M. Yin, 2011. Privacy-preserving universal authentication protocol for wireless communications. IEEE Trans. Wireless Commun., 10: 431-436.

He, D., M. Ma, Y. Zhang, C. Chen and J. Bu, 2010. A strong user authentication scheme with smart cards for wireless communications. Comput. Commun., 34: 367-374.

Igrair, A.E.A. and R. Yadav, 2016. Review: Privacy Preserving Authentication (PPA) protocols for wireless mobile networks. Intl. J. Adv. Res. Comput. Sci. Software Eng., 6: 1-6.

Marti, S. and S. Miglani, 2012. Analysis of mobile IP protocols security. Intl. J. Comput. Appl., 46: 1-9.

Sheltami, T., A. Al-Roubaiey, E. Shakshuki and A. Mahmoud, 2009. Video transmission enhancement in presence of misbehaving nodes in MANETs. Int. J. Multimedia Syst., 15: 273-282.

Yang, G., D.S. Wong and X. Deng, 2007. Anonymous and authenticated key exchange for roaming networks. IEEE. Trans. Wirel. Commun., 6: 3461-3472.

Yang, G., Q. Huang, D.S. Wong and X. Deng, 2010. Universal authentication protocols for anonymous wireless communications. IEEE. Trans.Wirel. Commun., 9: 168-174.