Hybrid Privacy-Preserving Authentication Protocol for Secure Communication under Malicious Attacks in Mobile IP

Abdurahem El Atman Igrair and RaghavYadav

Department of Computer Science & information Technology
Sam Higginbottom Institute of Agriculture, Technology & Sciences Allahabad India.'
Department of Computer Sciences & Information Technology
Sam Higginbottom Institute of Agriculture, Technology & Sciences Allahabad India.'

Abstract
Use of wireless network like mobile communications, mobile ad-hoc networks is now days very common and increasing worldwide. Due to open nature of such networks, there is the possibility of different types of attacks on a network such as malicious nodes, blackhole nodes, selfish nodes, DoS attacks, etc. Hence it is vital to have security mechanism for wireless networks. In this paper, our scope is limited to Mobile Ad Hoc Networks with mobile Ip (MIPMANET). The requirements for secure data communication, as well as privacy preserving, are significant research problem for MIPMANET. In this paper, we are presenting the novel routing protocol design called HPriauth (Hybrid Privacy-Preserving Universal Authentication) to achieve efficient, secure data communication and user privacy preservation under different types of security threats. There number of methods presented individually either for secure data communication or user privacy perseveration. HPriauth is based on existing Priauth protocol which is proposed for privacy preserving and authentication without actual evaluation. In this paper, we addressed the problem of Quality of Service (QoS) requirements while providing the data security and privacy preservation under malicious attackers. The data protection method is designed based on onion routing terminologies. The simulation results are showing the proposed HPriauth routing protocol having best QoS performance under a different number of malicious attacks as compared to existing routing protocols.

Keywords
Secure Routing, Mobile Ip, Wireless Networks, Quality of Service, Priauth, HPriauth, Loss Rate, Malicious Attack

1. Introduction

Wireless Ad hoc network consists of self-organizing devices and can be deployed without infrastructure. Mobile IP for Mobile Ad hoc Networks (MIPMANETs) can be Provide internet access by using Mobile IP with foreign agent and reverse tunneling . Each node acts as a host as well as a router and forwards each other's packets to enable the communication between nodes not directly connected by wireless links [1]. A central challenge in the design of ad hoc networks is the development of dynamic routing protocols that can efficiently find routes between the communicating nodes. In this paper, we are presenting the novel method for wireless networks privacy preserving, authentication, and secure communication as security is major research problem for MIPMANETs. To achieve the privacy preservation and authentication in wireless networks, we studied different methodologies and from which Preauth is designed and implemented as MIPMANET routing protocol to defend against different wireless attack. Apart from this privacy preservation and authentication, secure communication is another research challenge for wireless networks like Mobile Ip . Secure communication between the nodes was not addressed in Priauth method [2] [3]. Due to different types of security attacks, QoS performance of MANET is degrading as security threats in MANET impact significant data loss and leakage. In literature there are various methods introduced for MIPMANET security attacks on different parameters and strategies, however such security methods having some limitations. 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 preservation and authentication the methods proposed in [1]-[5]. The review of privacy preserving methods is deeply discussed in [12] by us. For secure data communication methods proposed in [6]-[11]. We studied this method and observer this performance with limitations for our research motivation.

The design of HPriauth routing protocol is proposed with algorithms in this paper. The practical implementation and evaluation of proposed approach are done by using the NS3 simulator. The networks are designed by considering the varying number of malicious nodes attacks in the network to check the performance of proposed method. In section II, the malicious node attack model is presented which we used for evaluation of proposed and existing security methods. In section III, we are performing the algorithm designed for HPriuath and other security methods. In section IV, the simulation configurations and results achieved are presented. In section V, the conclusion is discussed.

Manuscript received April 5, 2026
Manuscript revised April 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.4.9

2. Malecious Attack Model

The malicious attack is also called as blackhole attack. In this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listens to the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a reply consisting of a highly short route. If the malicious reply reaches the initiating node before the response from the actual node, a fake route gets created [6]. Once the malicious device has been able to insert itself between the communicating nodes, it can do anything with the packets passing between them. It can drop the packets between them to perform a denial-of-service attack, or use its place, on the route as the first step in a man-in-the-middle attack [7]. As shown in Figure 1 below, source node 1 broadcasts an RREQ message to discover a route for sending packets to destination node 3. An RREQ broadcast from node one is received by neighboring nodes 2, 4 and 5. However, malicious node 5 sends an RREP message immediately without even having a route to destination node 3. The RREP message sent by the malicious attacker node is the first message reaches to the source node.When the node of origin receive the message sent by the malicious attacker node, updates its routing table for the new route to the intended destination node and then also discards any RREP message from other neighboring nodes even from an actual destination node [8]. When the Source node gets the route, it sends the data packets immediately from the path which is provided by the malicious attacker node. Nevertheless, a Black hole node drops all data packets rather than forwarding them on [9].

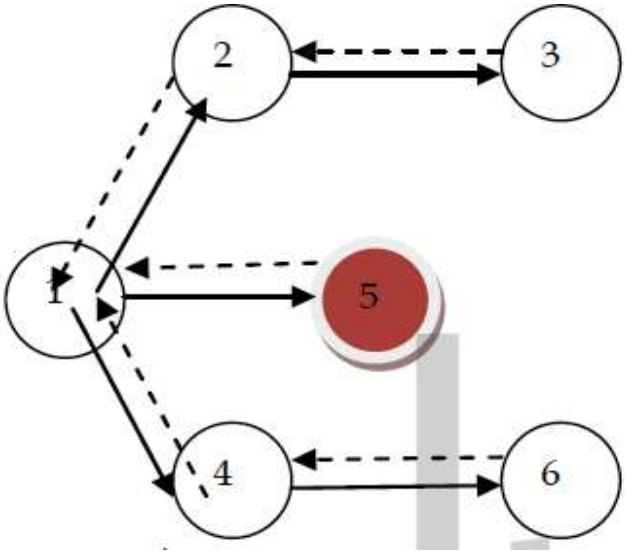

Fig.1. Example of Malicious Node Attack

When a node breaches any of the security principles and is therefore under any attack. Such nodes exhibit one or more of the following behavior:

- Packet Drop- Simply consumes or drops the packet and does not forward it.
- Battery Drained- A malicious node can waste the battery by performing additional operations.
- Buffer Overflow- A node under attack can fill the buffer with fake updates so that official updates cannot be stored further.
- Bandwidth Consumption- Whenever a malicious node consumes the bandwidth so that no other legitimate node can use it.
- Malicious Node Entering- A malicious node can enter the network without authentication [10].
- Stale Packets- This means to inject stale packets into the network to create confusion in the system.
- Delay- Any malicious node can purposely delay the packet forward to it.
- Link Break- This can result in restricting the two legitimate nodes from communicating if the malicious node is between them.
- Message Tampering- A malicious node can tamper the content of the packets.
- Denying from Sending Message- Any malicious node may deny from sending messages to other legitimate nodes.
- Fake Routing- Whether there exists a path between nodes or not, a malicious node can send fake routes to the legitimate nodes to get the packets or to disturb the operations [11].
- Node Not Available- An intruder can isolate the node from taking part in any transaction so as to create delays when the source node chooses another alternative path.
- Stealing Information- Information like the content, location, the sequence number can be stolen by the malicious node to use it further for the attack.
- Session Capturing- When two legitimate nodes communicate; a malicious node can capture their session so as to take some meaningful information.
- Others- There are other ways also in which a node behaves in a malicious manner.
- The usual and the malicious behavior of a node can be easily understood by the algorithm below.

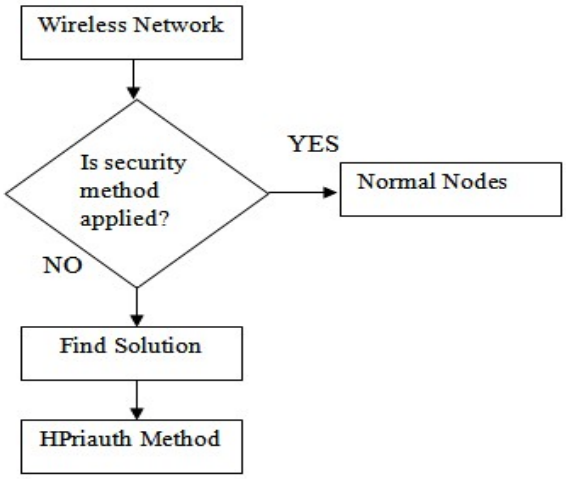

Fig.2. Defined Algorithm for Normal & Malicious Behavior of a Node

3. Proposed Methodology

In this paper, we are designing and presenting new efficient HPriauth routing protocol. Below discussing the algorithm designs, figure 3 is showing the system flowchart used for simulation work.HPriauth is designed as routing protocol which is compared with existing privacy-preserving methods called Priauth and YHWD. The performance of any routing protocol mainly depends on four major parameters under the attacks such as throughput, packet delivery ratio (PDR), an end to end delay and rate of packet loss. The novelty of HPriauth is that it is providing efficient privacy preservation, efficient user authentication and most important effective secure communication among mobile nodes.

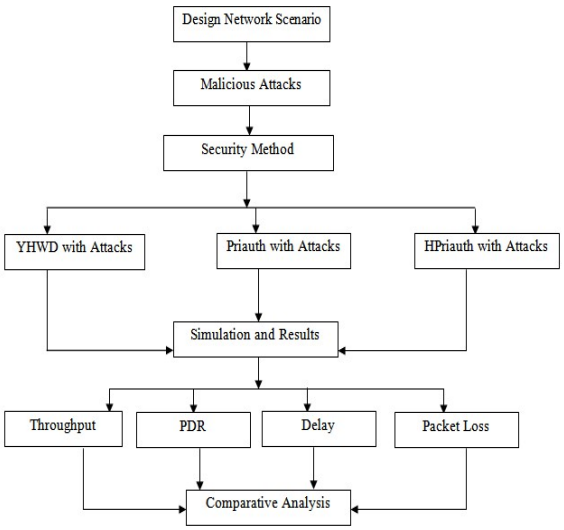

Fig.3. System Flowchart

Below two are main algorithms proposed for HPriauth protocol. Algorithm 1 is for privacy preservation and authentication. Algorithm 2 is for secure routing in MANET. The algorithm of privacy preserving and authentication are designed as per the below system model showing in figure 4.

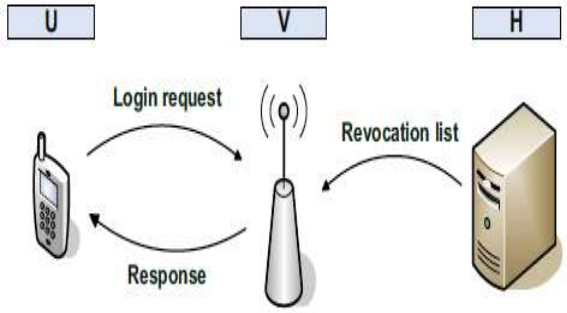

Fig.4. System Model for Privacy Preservation and Authentication Algorithm (Algorithm 1)

Algorithm 1: Privacy Preserving and Authentication

Step 1: VLR-GS. Keygen (,)

1.1. The group manager randomly selects a generator ∈ and ˜∈. Additionally, it selects ℎ∈ for all ∈ [1,].

1.2. Then it selects ∈ℤ ∗ and computes = . Subsequently, it selects ∈ℤ ∗ and computes = 1/(+) for all ∈ [1,].

1.3. After that, it computes = ℎ for all and . The master public key *mpk* is (, ˜, ℎ1, . . ., ℎ,). Each subscriber's secret key [] is (,).

1.4. The revocation token at an interval of subscriber with the secret key (,) is [][] = .

Step 2: VLR-GS. Sign (, [], ,)

2.1. Select random number , , ∈ℤ ∗.

2.2. Compute 1 = ˜, 2 = ˜, 3 = (, ℎ) , and 4 = .

2.3 Compute = {(, , , ,): 1 = ˜∧2 = ˜∧3 = (, ℎ) ∧4 = ∧ (,) = (,)} ().

2.4. Output the group signature = (1, 2, 3, 4,).

Step 3: VLR-GS. Verify (, , , ,)

3.1. Signature check. Check that σ is valid, by checking the V.

3.2. Revocation check. Check that the signer is not revoked at the interval , by checking 3≠ (4,) for all ∈.

Step 4: Stop

Algorithm 2: Secure Onion Routing

Step 1: Generate the PKI.

Step 2: PKI generation done by broadcasting source node ID.

Step 3: Extract the Public Key, Private Key and Session Key.

Step 4: Insert all three current keys into the routing table.

Step 5: At Source Node

Step 5.1: Extract the current routing information

Step 5.2: Get the current session key

Step 5.3: Generate the new session key and update the routing table entries

Step 5.4: Broadcast RREQ Packet

Step 5.5: Apply the Key encryption onion at intermediate nodes and destination node

Step 5.6: Signing by source node with its private group key

Step 5.7: Broadcasting finally the authenticated RREQ

Step 5.8: Set the status 'P' and update the routing table entry for current path with this status

Step 6: At Intermediate Node

Step 6.1: Verify the received packet with private group key

Step 6.2: If package verification is successful then extract all details from the received packet else marked current received packet is from the malicious node and drops it.

Step 6.3: Transfer the received packet further by below steps of onion routing

Step 6.4: 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 proceed further.

Step 6.5: Apply Decryption operation if its destination node, else forward it to next hope by performing the encryption operation by using the keys generated

Step 6.6: Signing the Source node with its private group key

Step 6.7: Set the status 'P' and updated routing table entry with current route

Step 7: At Destination node

Step 8: Step 6 are repeated to get the original data at the original destination node.

Step 9: Stop

4. Results and Discussion

The simulation of proposed methodology is done using the NS3 software in which we have designed wireless networks with 50 mobile nodes and two servers (home and foreign) with varying number of malicious attackers in the network. HPriauth is compared against YHWD and Priauth method in results.

A. Network scenario

Security Routing Protocols: YHWD, Priauth, and HPriauth

Number of wireless nodes: 50

MAC: 802.11

Simulation Time: 30 Seconds

Mobility Speed: 5 (m/s)

Number of Attacks: 1, 3, 5, 7, 9

Results Measurement

Throughput vs. Varying Number of Attacks

Loss Ratio vs. Varying Number of Attacks

Overhead vs. Varying Number of Attacks

Delay (Time) vs. Varying Number of Attacks

B. Performance Metrics

1) Avg. Throughput

Throughput= (seq number * segment size * 8) / active duration (1)

2) Packet Delivery Ratio (PDR)

PDR= (number_of_received_packets/number_of_generated_packets) * 100 (2)

3) End to End Delay

end-to-end= N[dtrans+dprop+dproc+dqueue] (3)

where,
end-to-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)

C. Comparative Results

Below comparative graphs for different performance metrics showing the results achieved from the extensive simulation work.

Average Throughput vs. Number of Attackers:

Throughput performance metrics plays an important role in deciding the efficiency of a routing protocol in MANET. Higher the throughput, better the routing protocol. As showing in the graph of figure 5, proposed HPriauth method has more throughputs as compared to existing methods

under varying number of malicious attackers. It is showing that as the attackers increasing, throughput performance is dropping.

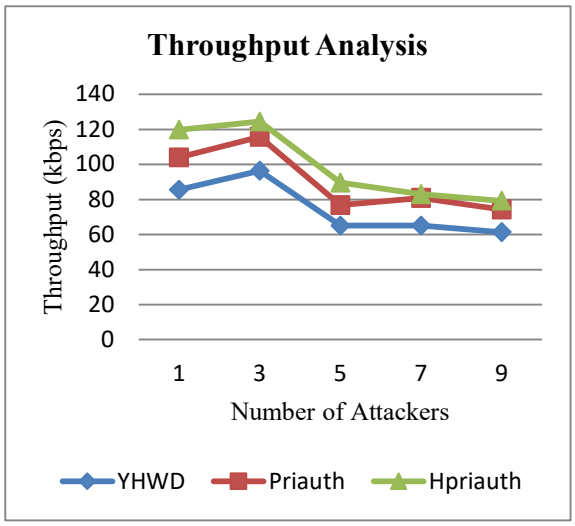

Fig.5. Throughput Performance Analysis with Varying Number of Malicious Attackers

Packet Delivery Ratio vs. Number of Attackers

Packet delivery ratio is nothing but some successfully delivered packets from the source node to destination node under home server and foreign server scenario. Figure 6 is showing proposed method achieving more throughput performance in the presence of a number of attackers in the network. This claims that HPriauth is delivering efficient security against malicious attack.

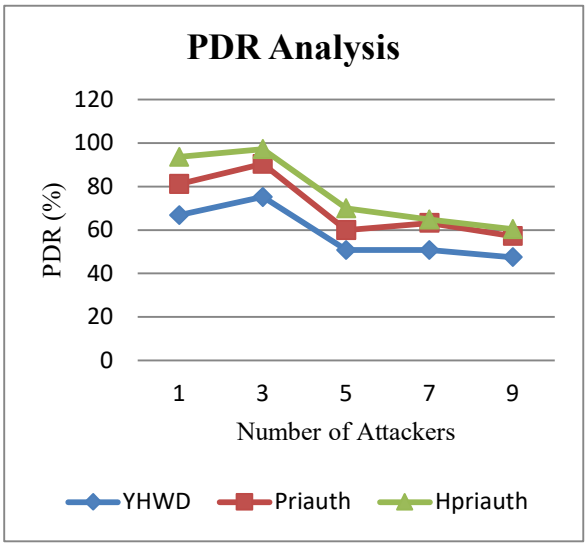

Fig.6. PDR Performance Analysis with Varying Number of Malicious Attackers

Loss Rate vs. Number of Attackers

Malicious attacks mainly resulted into information leakage means packets dropped in MIPMANET. Hence the efficiency of security methods is mainly based on loss rate performance. The more efficient method is having less number of packets drop. Figure 7 is showing the comparative analysis of loss rate for all three simulated security methods. It is clearly showing that as the number of attacker's increases, packet drops increasing. In such case, proposed HPriauth is achieving less packet drop performance as compared to existing methods.

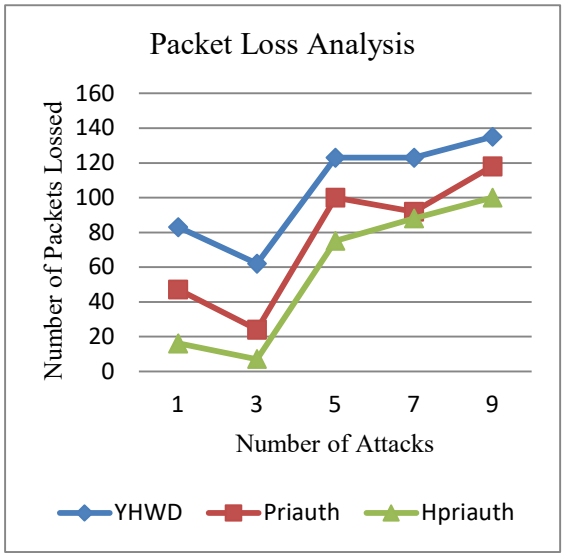

Fig.7. Loss Rate performance Analysis with Varying Number of Malicious Attackers

End to End Delay Vs. Number of Attackers

Figure 8 is showing the end to end delay performance. HPriauth is showing better delay performance against YHWD and HPriauth.

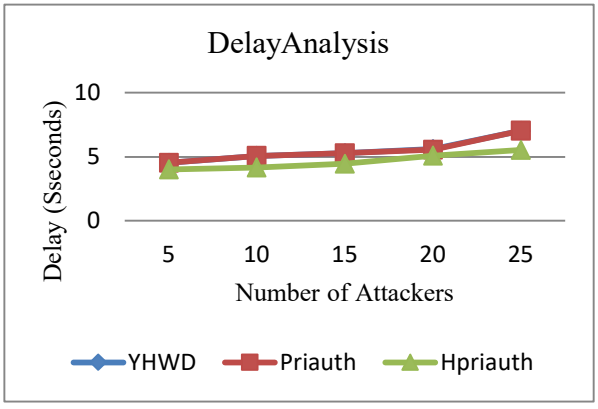

Fig.8 Delay performance Analysis with Varying Number of Malicious Attackers

5. Conclusion and Future Work

For wireless networks like mobile ad hoc network with 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 some attacks such as DoS, blackhole, grayhole, selfish node, malicious node attacks, etc. In this paper, we proposed hybrid security routing protocol for mobile Ip 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. Malicious node attack model is discussed in this paper. The network scenarios are based on varying number of malicious nodes in the network. The simulation results are showing that proposed HPriauth is showing better QoS performance as compared to existing methods under a different number of attackers. For future work, we suggest working on various network conditions and systems.

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 communications,” *IEEE Trans.WirelessCommun.*, vol. 9, no. 1, pp. 168-174, 2010.

[3] [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 misbehavior 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 misbehavior 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 of misbehaving 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.