Securing Mobile Ad Hoc Network using Double Hash Authentication technique

V.Mukundan ,
Assistant Professor,
Department of ECE,
V.S.B college of Engineering,

Dr.A.Rajaram ,
Associate Professor,
Department of ECE,
Karpagam College of Engineering,

S.Gopinath
Assistant Professor,
Department of ECE,
Karpagam Institute of Technology,

Abstract - **Mobile Ad hoc Network (MANET) is an infrastructure less network where routing protocols play a major role. Because of the features like unreliability of wireless link between nodes, dynamic topology, limited battery power, lack of centralized control and others, the mobile ad hoc networks are more vulnerable to suffer from malicious behavior, security threats and attacks. The prevention methods like firewalls, authentication and cryptography techniques alone are not able to provide the security. Therefore Intrusion Detection System (IDS) is required for MANETs. An effort has been made to overcome the problems of overhearing technique by incorporating Double Hash Authentication Technique (DHT) in to the routing protocol. Here, DSR has been modified so that discovered route will not have nodes with less remaining power. Nodes with sufficient transmission power will be taken into consideration for packet transmission at the time of route discovery.**

Index Terms - Double Hash Authentication Technique (DHT), Dynamic Source Routing, Intrusion Detection System (IDS).

I.INTRODUCTION

Rapid development in wireless communication systems leads to tremendous need of independent mobile users. To name a few disaster relief efforts, emergency rescue operatios, battlefield military operations etc. Users of such network is termed as Mobile Ad-hoc Network (MANET). The characteristics of these networks are dynamic topology, autonomous, bandwidth constraint and Energy constraint. Autonomous and decentralized characteristics of mobile nodes which can enter or leave the network at any time makes MANET unpredictable.

These nodes are systems of devices which can be Mobile phone or laptop. Each node can act as a host or router or both. All the activities in the network such as data transmission are performed either individually or collectively. MANET can be connected to the internet also. When one node desires to communicate with another that is out of transmission range, intermediate nodes are used to relay messages. This is the major advantage of wireless network over wired network.

Security in MANET is a very important issue for the basic functionality of network. MANET is vulnerable to various threats because of its open medium, dynamic topology and lack of centralised management. A node during its transmission process may tend to drop the packet or may not forward it as the node may be overloaded, selfish, malicious or broken. Hence Intrusion Detection System is needed.

The rest of the paper is organized as follows : Section 2 gives the literature survey . The proposed method with algorithm is explained in section 3. Simulation results are carried out in section 4. Conclusions are given in section 5.

II.RELATED WORK

S.Marti, T.Guili, and K.Lai,M.Baker [6] proposed a technique Watchdog and Pathrater built on Dynamic Source Routing Protocol (DSR) that has become the basis for many researches. Now most of the IDSs are based on this technique. Watchdog identifies the misbehaving node in the path while the Pathrater rates the path based on the watchdog results. Watchdog does this by listening to its neighboring node in promiscuous mode. If the next node does not forward the packet then it may be a malicious node. Counting of the transmit failure activities is done. If the counter exceeds a threshold the node is declared malicious and avoided by the Pathrater. This method also has the disadvantage of dropping data packets upto threshold level. If the threshold level is 20%, then a node dropping packets before this level are not termed malicious. This technique performs well but it fails in case there is ambiguous collision, receiver collision, limited transmission power, false misbehavior reporting, collusion and partial dropping. Moreover if a malicious node is present in more than one path, then the performance of this method greatly reduces.

Core, a Collaborative Reputation mechanism proposed by P.Michiardi and R.Molva [7], also uses a Watchdog mechanism. The reputation table is used which keeps track of reputation values of other nodes in the network. Since a misbehaving node can accuse a good node, only positive rating factors can be distributed in Core. Since there is no incentive for a node to maliciously spread negative information about other nodes, simple denial of service attacks are prevented.

In [11],A.Hassawa,., H.Hassanein,M. Zulker proposed an intrusion detection and response system called Routeguard. This technique uses the two techniques that were proposed by Marti et al., Watchdog and Pathrater, are combined to classify each neighbor node as: fresh, member, unstable, suspect, or malicious. However, when the malicious nodes are misbehaving for 50% to 60% of the time there is a slight drop in Routeguard's performance.

Nasser and Chen [4] proposed an Enhanced Intrusion Detection system for discovering malicious nodes in the network called Exwatchdog. Exwatchdog extends the Watchdog . They focus on one of the weaknesses of the Watchdog technique,namely the false misbehaving problem where a malicious node falsely reports other nodes as misbehaving while in fact it is the real intruder. However, there may exist a true misbehaving node is in the all available paths from source to destination then it is impossible to confirm and check the number of packets with the destination.

Roubaiey and T. Sheltami [8] proposed a mechanism named: Adaptive Acknowledgment (AACK) that was an attempt to remove two significant problems: thelimited transmission power and receiver collision. The AACK mechanism may not work well on long paths that will take a significant time for the end to end acknowledgments. This limitation will give the misbehaving nodes more time for dropping more packets.Also AACK still suffers from the partial dropping attacks (gray hole attacks).All the previous solutions used Watchdog as the base for their techniques. Whereas, the Three phase solution, replaces Watchdog and solves all the problems of it.

Three phase technique for intrusion detection[2] Proposed by K.V.Arya, P.Vashistha and V.Gupta replaces watchdog and overcomes its problems namely ambiguous collision, Receiver collision, False misbehaviour, Less Transmission power, Collusion and Partial Dropping. However the authentication technique used here makes an assumption that the node has to take certificates from its entire neighbour which is difficult if the number of nodes is high. This assumption may not be practical in every case that the nodes get certified from all the neighbours.

III. PROPOSED SCHEME

The Double Hash Authentication technique for intrusion detection in MANET which mainly consists of the route discovery through modified DSR, authentication using Double Hash technique and packet transmission after authentication is successful.

A. Discovery Of Route Using Modified DSR

To discover the route from the source node to the destination node, a route request (RREQ) is broadcasted to all the nodes in the neighbourhood. Each node upon receiving the Route Request, retransmits the request appending its address, its current power and its queue length (buffered packets that are needed to be processed) only if it has not already forwarded a copy of the RREQ. Queue length will be taken so that source node can decide whether this node will be having sufficient battery to participate in the packet transmission. The destination node returns a reply for each route request it received. Nodes with the sufficient power will be considered by the source node. The energy contained in any node is estimated as follows

$$\text{Power} = E_c\text{-}(Q_i\text{*Energy}) \qquad (1)$$

Where E_c represents the current energy and no. of packets in the buffer of node under consideration are represented by Q_i. In this paper we have considered decay in energy with time is very less and can be ignored. For successful transmission of the packetfrom source through the selected node, the estimated power should follow the relationship given in (2).

$$\text{Power}>(\text{Num}_p)\text{*Energy} \qquad (2)$$

Where Num_p is the number of packets the source wants to send to the destination.

If an intermediate node is unable to deliver the packet to the next hop, then node returns a ROUTE ERROR to source, stating that the link is currently broken. Source Node then removes this broken link from its cache. For sending such a retransmission or other packets to this same destination, if source node has another route to destination in its route cache, it can send the packet using the new route immediately after the authentication. Otherwise, it has to perform a new route discovery for this destination.

Any malicious node may reply to the request from the source by claiming to have the shortest path to the destination. To overcome this problem, source node does not initiate the data transfer process immediately after the routes are established. Instead it waits for the authenticated reply from the destination.

B. *Authentication Using Double Hash Technique*

The Fast and Efficient Hash function is adopted to authenticate routing information instead of digital signatures. Under the reasonable assumption that no two compromised nodes are colluding and are within two hops of each other. In this double Hash authentication one of which is used to authenticate the received routing packets and other is used to prevent the current nodes modifying the routing information themselves. If some compromised node modified the routing information, its neighbouring nodes can detect the misbehaviour immediately. In an initial phase each node makes use of the management of local node group to distribute the common secret with its two hop node group.

Distribution of common secret key

In this technique each node needs to distribute a common secret by its two-hop node group. This secret key is kept secret against its one-hop node group. Each node has a pair of private and public keys. The source node generates random key Ks and encrypts it with the public key of the nodes within two- hop. On receiving the encrypted key each node decrypts it with the corresponding private key and gets the common secret key Ks. Due to the mobility, ad hoc network can result in the change of the local node groups and the distribution of the common secrets should be adjusted timely. When some new nodes join in two hop node group, the source node needs to distribute Ks to those new nodes and if some nodes within two-hop becomes the member of its one-hop node group(due to roaming) the source needs refreshing and redistribution of Ks.

C. DOUBLE HASH ALGORITHM

The Public one way hash function H(.) is used to authenticate the RREQ twice, so the routing packets includes not only the RREQ but also two hash values(H1,H2), where H2 is used to check whether the received routing packet has been modified and H1 is used to prevent the current node modifying the packet.

The algorithm can be explained as follows:

1. Generate RREQ from source node RREQ={S,L,H,R}
   S- Source Identity
   L- sequence number (RREQ)
   R- Routing information
   H- Hop count.
2. Source multicasts{S, L+1, H, R, H1, 0} to its multicasts group.
3. Any intermediate node within this group can verify the authenticity of packet. H2=0(from source node); H1 = H(S\L+1\H\R\K) K- Secret key shared by two-hop node and source.
4. Before forwarding the packet increment the hop count by 1 and copy H1 to H2 and calculate the new H1.i.e. H1=H(S\L+1\H+1\R\Ki); H2=H(S\L+1\H\R\K) where Ki is common secret key between intermediate node and two hop node.
5. Forward the Routing packet to its Multicast group.
6. On Receiving {S\L+1\H+1\R\H1\H2} nodes within the group can use {S, L+1, H+1, R} and public hash function to calculate H(S\L+1\H\R\K).
7. Compare this value with H2 and validate whether routing packet is modified by intermediate node.
8. If intermediate node wants to modify the packet it has to forge the H2 value before forwarding the packet.

The same concept is applied for RREP from destination to source.
After successful authentication, packet transmission takes place.

IV. RESULTS AND DISCUSSION

The analysis of the work is carried out in the NS2 simulator under LINUX platform for analyzing the performance of Double Hash Authentication technique. The the important parameters chosen for the NS2 simulation. The following table 4.1 shows the important parameters chosen for the NS2 simulation.

Table 4.1 Simulation setup

Number of nodes	80
Square area	700 x 700 m^2
MAC type	MAC 802.11
Routing protocol	DSR
Packet size	512 bytes
Movement Model	Random waypoint
Traffic type	CBR(UDP)
Maximum speed	15 m/s
Pause time	3 s
Simulation time	900 s

A. Performance Metrics

Packet delivery ratio

Packet delivery ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by the source (i.e. CBR source).

Routing Overhead

The routing overhead describes how many routing packets for route discovery and route maintenance needed to be sent in order to propagate the CBR packets

Throughput

Throughput refers to the number of packets transmitted per unit time.

Network life time

It refers to the lifetime of the network.

End to End delay per packet

The total delay experienced by a packet that successfully reached the destination node.

B. Packet Delivery Ratio

Packet Delivery Ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by the source or it is the ratio of data packets delivered to the destinations and data packets originated by the sources. The greater the packet delivery ratio is, the more reliable the network.

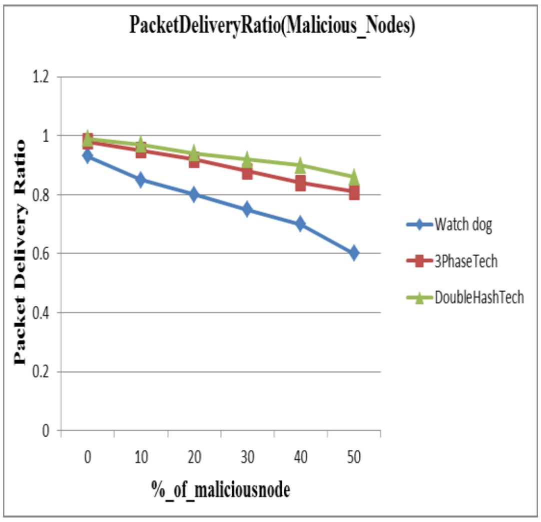


Figure 4.1 Comparison of Packet Delivery Ratio

In the figure 4.1, comparison of Packet Delivery Ratio for Watch dog, Three Phase Tech and Double Hash Authentication is shown where X axis represents percentage of malicious nodes and Y axis represents PDR (%). As the number of malicious nodes increases, packet delivery ratio decreases. Double hash authentication technique has better PDR than the existing watch dog and three phase technique.

C. Routing Overhead

The routing overhead describes how many routing packets for route discovery and route maintenance needed to be sent in order to propagate the CBR packets.

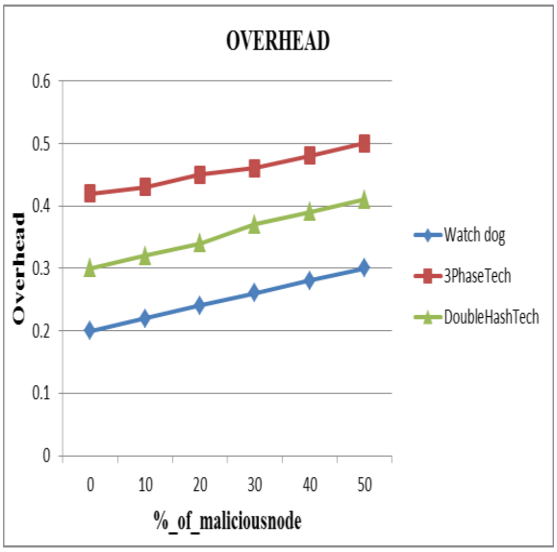


Figure 4.2 Comparison of Routing Overhead

In the figure 4.2, comparison of Routing Overhead for Watch dog, Three Phase Tech and Double Hash Authentication is shown where X axis represents percentage of malicious nodes and Y axis represents routing overhead. As the number of malicious nodes increases, routing overhead also increases. There is a considerable overhead in three phase technique when compared to watch dog and double hash authentication technique. Overhead increase in three phase and DHT is because of the authentication technique.

D. Throughput

Throughput refers to the number of packets transmitted per unit time.

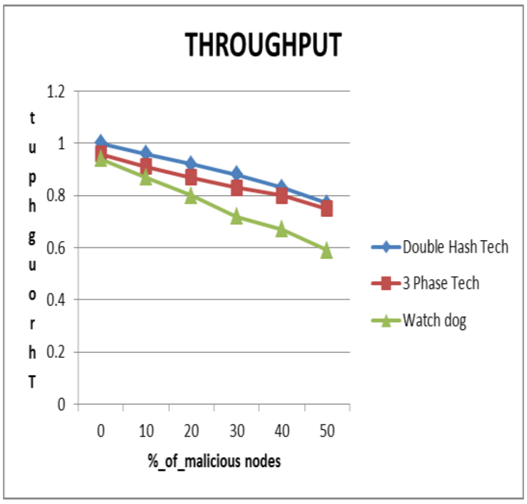


Figure 4.3 Comparison of Throughput

Figure 4.3 shows the comparison of throughput for Watch dog, Three Phase Tech and Double Hash Authentication technique. Throughput of the network decreases with the increase in malicious node. Double Hash Aunthentication technique maintains better throughput than the other two methods.

E. Network Life Time

It refers to the lifetime of the network.

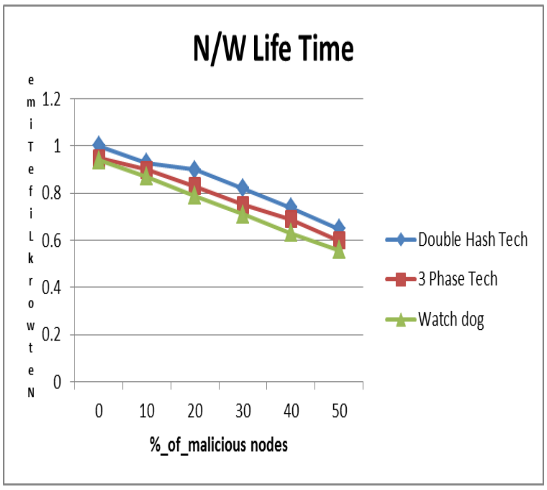


Figure 4.4 Comparison of Network Life Time

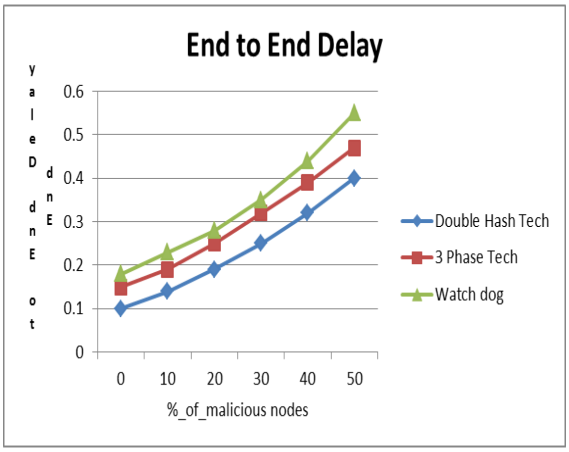
Figure 4.4 shows the comparison of Network life time for Watch dog, Three Phase Tech and Double Hash Authentication technique. Double Hash Aunthentication technique have better Network life time than the three phase and watchdog methods.

F. End to End Delay Per Packet

The total delay experienced by a packet that successfully reached the destination node.

Figure 4.5 Comparison of End to End Delay

Figure 4.5 shows the comparison of End-to-End delay for Watch dog, Three Phase Tech and Double Hash Authentication technique. From this result, it is clear that DHT algorithm achieves a considerable reduction of End-to-End delay per packet.



V.CONCLUSION

The Double Hash Authentication technique (DHT) scheme for securing the Mobile Ad-hoc Network is proposed and implemented. DHT achieves better PDR, throughput , network life time and end to end delay than the watch dog and three phase technique. Moreover DHT shows a decreased routing overhead when compared with the three phase technique. DHT detect malicious and selfish nodes and mitigate their impact by avoiding them in later transmissions. It removes the concept of threshold which allows a malicious node to drop a certain number of packets. The results show that security of MANET has been greatly improved when compared with the existing watch dog and three phase technique. The future work is to incorporate the DHT into other routing protocols and their performance can be compared.

REFERENCES

1. S. Varadhaganapathy, A.M. Natarajan and S.N. Sivanandam,(2011): “Authentication Based and Optimized Routing Technique in Mobile Ad hoc Networks”, Journal of Computer Science.

2. K V Arya, Prerna Vashistha and Vaibhav Gupta,(2011) “Three Phase Technique for Intrusion Detection in Mobile Ad Hoc Network”, Digital Information and Communication, Part I, CCIS 166, pp. 675-684

3. S. Buchegger and Boudec, (2002)“Performance Analysis of the CONFI- DANT Protocol Cooperation Of Nodes-Fairness in Dynamic Ad-hoc Networks”, In: Proc. IEEE/ACM Symp. Mobile Ad Hoc Networking and Computing

4. N.Chen and Nasser, (2007)” Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad- hoc Networks”,In:IEEE International conference on Communication

5. J.Deng, K. Balakrishnan and P.K Varshney, (2005) ”TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks”, In: IEEE Wireless Comm. and Conf.

6. S Marti, T.Giuli, K. Lai and M.Baker, (2000)” Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”, In: Sixth Annual International Conference on Mobile Computing and Networking.

7. P.Michiardi and R.Molva, (2002)” Collaborative security architecture for black hole attack prevention in mobile ad-hoc networks”,. In: Proc. IEEE/ACM Symp. Mobile Ad Hoc Networking and Computing.

8. A.Roubaiey, E.Shakshuki, T.Sheltami, A.Mahmoud and H.Mouftah,(2010) ”AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement” .In:IEEE International Conference on Advanced Information Networking and Applications.

9. Dyanamic Source Routing Protocol, http://en.wikipedia.org/wiki/DynamicSourceRouting

10. RSA, http://en.wikipedia.org/wiki/RSA

11. Hassawa,A., Hassanein ,H., Zulker,M., : Routeguard : An intrusion detection and Response System for Mobile Adhoc Networks. In : Wireless And Mobile Computing, Networking and Computing (2002)

12. Johnson DB, Maltz DA. Dynamic source routing in ad hoc wireless networks. Kluwer Academic Publishers; 1996. p. 153–81.

13. S Ouni, J Bokri and Kamoun Farouk,(2009): “DSR based routing algorithm with delay guarantee for ad hoc networks”. Journal of Networks. pp 359– 69.

14.B Gassend, GE Suh , D Clarke, M Dijk and S Devadas,(2003): Caches and hash trees for efficient memory integrity verification. In: Proceedings of the IEEE ninth international symposium on high-performance computer architecture; pp 295–306.

AUTHORS PROFILE

V.Mukundan received the **B.E**. degree in electronics and communication engineering from Pavendar Bharathidasan College of Engineering and Technology , Trichy, Anna University, Chennai, India, in 2005.He obtained **M.E**. in electronics and communication engineering (Communication Systems) in Anna University of technology, Coimbatore, India, in 2012.He is currently working as Assistant Professor, ECE Department in V.S.B college of Engineering, Coimbatore, India. His research interest focus on Mobile Ad hoc networks ,wireless communication (WiFi,WiMax),Sensor Networks ,Neural Networks , Communication networks and Digial electronics .

Dr.A. Rajaram received the **B.E.** degree in electronics and communication engineering from the Govt., college of Technology, Coimbatore, Anna University, Chennai, India, in 2006, the **M.E.** degree in electronics and communication engineering (Applied Electronics) from the Govt., college of Technology, Anna University, Chennai, India, in 2008 and he received the **Ph.D.** degree in electronics and communication engineering from the Anna University of Technology, Coimbatore, India in March 2011. He is currently working as a Associate Professor, ECE Department in Karpagam College of Engineering, Coimbaotre, India. His research interests include mobile adhoc networks, wireless communication networks **(WiFi, WiMax HighSlot GSM),** novel **VLSI NOC** Design approaches to address issues such as low-power, cross-talk, hardware acceleration, Design issues includes **OFDM MIMO** and noise Suppression in **MAI** Systems, **ASIC** design, Control systems, Fuzzy logic and Networks, **AI**, Sensor Networks.

S.Gopinath received the **B.E.** degree in electronics and communication engineering from the Govt. College of Engineering, Salem, Anna University, Chennai, India, in 2007.He earned **M.E.** year in electronics and communication engineering (Communication Systems) in Anna University of technology, Coimbatore, India, during june 2011. He is currently pursuing Ph.D in Anna University, Chennai. He is currently working as Assistant Professor, ECE Department in Karpagam Institute of Technology, Coimbaotre, India. His research interest includes wireless communication (**WiFi,WiMax**), Mobile Ad hoc networks ,Sensor Networks ,Neural Networks and fuzzy logic, Communication networks.