International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 01 | Jan-2016 www.irjet.net p-ISSN: 2395-0072

SECURING AODV ROUTING PROTOCOL IN MANET TO DETECT WORMHOLE ATTACK USING NMAC AND HBKS TECHNIQUE

NEHA KULKARNI[1] VINOD. S. WADNE[2]

[1] Student, Department of Computer Engineering, Imperial College of Engineering & Research, Pune, India
[2]Asst. Prof. , Department of Computer Engineering, Imperial College of Engineering & Research, Pune, India

---

Abstract - ***In MANET (mobile ad hoc wireless network) communication is much more challenging task due to its characteristics like infrastructure less architecture, wireless and distributed cooperation of task, dynamic topology, lack of association, lack of resource utilization , power limitation and physical existing of node. In MANET, attacks can be classified into different categories: routing attacks and data forwarding attacks. The main aim of attack to disrupt functioning of network by updating routing updates. data forwarding attacks are done modification or dropping of data packet. In paper work, a secure method is proposed for ad hoc on-demand distance vector (AODV) routing protocol. The proposed method used the authenticate and secure technique to secure the routing message in AODV and efficiently prevent wormhole. The key pre- distribution technique is used in this method. by using this method .the overhead can be minimize due to sharing the keys. In this paper, the selection of keys is depend upon the of hop count value in control packet.***

Key Words: *Mobile ad hoc network (MANET), Routing attack, AODV, NMAC, Authentication.*

1.Introduction

A Mobile ad hoc network (MANET) is a wireless network of wireless mobile nodes that can be setup anywhere MANET differs from other networks or wired networks as there is no centralized architecture ,Security of Routing Message is an important issue in MANET In MANET, mainly two types of messages are in network , Routing messages are used for the route sense, route establishment and route maintenance. Routing messages are processed by intermediate nodes during their processing. Different types of attacks are found by the malicious node like routing table updation, and check poisoning of packet The work to secure AODV protocol uses asymmetric key cryptography technique. The previous technique are requires more processing time ,more battery consumption and large memory .so key pre-distribution method proposed using hash message authentication code . Aim of the paper is to introduce a secure version of S-AODV routing protocol. The proposed method used the nested authentication technique (NMAC) to secure the packet, modifying routing information. And Key pre- distribution technique used to overcome the overhead. that is based on key pre- distribution concept using hash message authentication code. The method can be easily implemented and requires a little bit CPU processing capacity and battery power.

1.1 Wormhole Attack

A hidden security attack, called the wormhole attack, in this attack, a malicious node catch packets from one point or one node in the network and send them to another. The packet receive with same or with a lesser number of hops with respect to the transmitted packets over node routes. it is used by malicious nodes to disrupt the normal function of ad hoc routing protocols. Wormhole can be form in-band channel where malicious node m1 capture the received route request packet to another node m2 using encapsulation property even no. of node can vary between two malicious nodes, the nodes following m2 nodes séance that there is no node between m1 and m2. Second, out-of-band where two malicious nodes m1 and m2 create a physical channel.

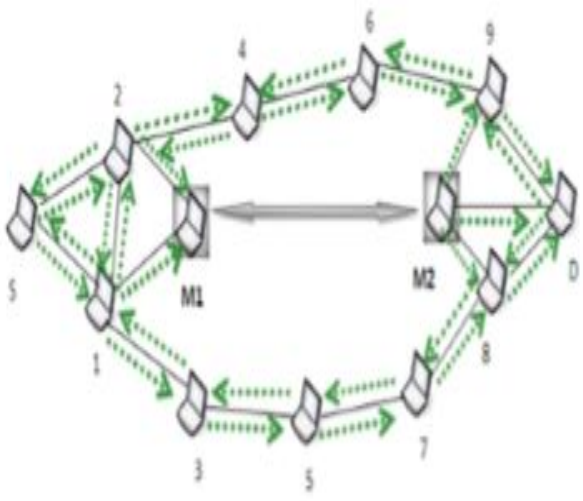


Fig. 1: Worm hole attack

2. RELATED WORK

proposed technique are related misbehaving of .The attack has mainly two characteristics: first one, the misbehave node depending to the information that it has shortest with the intention of dropping the packets. The proposed technique is focused on the malicious nodes and tries to prevent doing wormhole attack on the network by preventing other nodes from the current routing paths and select the alternative path by the route discovery for the same[1]. The method is based on AODV routing

protocol and uses shared key technology.. The hop count is mutable field as intermediate nodes increment/decrement the hop count while forwarding the RREQ. The rest such as sequence number or IP address are non mutable fields as they remain unchanged. prevents a member node from removing IP address of intermediate node from intermediate node list, the receiver node can verify the hop count field in RREQ or RREP message using the intermediate node list. In the proposed method, only the destination node is permitted to initiate route reply message therefore the delay involved in the route discovery process increases as the size of the network increases. Moreover with increased in network size[2][11][16]. proposed a method to detect wormhole attacks in mobile ad hoc networks (MANET). The concept method is to develop shortest path when Route Request (RREQ) send from node 1 to another and find malicious nodes. The proposed method follows different steps, , routes aggregation (RTT), round-trip time, routes redundancy. [4][12] this method gives efficient result to detect a wormhole attack using modified wormhole detection. In MAODV, to detect wormhole attacks a concept in the network by collecting both numbers of hop count [5][15] valuated the performance of on demand routing protocols i.e AODV (Ad hoc on demand distance vector routing) and DSR (dynamic source routing) with and without wormhole attack. It maintains the routes as long as required by the source. It uses sequence number to show that route is new. By using sequence number it make sure that route is loop free. When a node has to send data to the another node and route is not available then it broadcast a RREQ (route request) message, nodes receiving this RREQ message checks that they are the destination node to which source node want to send data [6][14] They investigates a recently proposed Advanced Encryption Standard (AES)-based routing algorithm.[8] proposed wormhole detection Mechanism that overcome Two fake neighbors with a wormhole tunnel in between has longer RTT, compared to the RTT with true neighbors. [9] [10].

3. MOTIVATION

security is an important. We need to consider a better mechanism for higher security and network performance while designing of secure routing protocol. The proposed method based on hash message authentication and hop count base key selection , message authentication and intermediate nodes authentication. We compare proposed method with SAODV protocol. In MANET, the internal attacks are typically more curious , since malicious node already belongs to the network. To prevent internal attacks, we need to create the unique identity of each node. Our scheme provides an efficient way to verify the message integrity, message authentication. The receiver node authenticate message and intermediate nodes using the shared secret key. the receiver node can verify the hop count field in RREQ or RREP message using the intermediate node list. In proposed method, The limitation of this method is that, ARAN uses asymmetric cryptography mechanism which causes higher overhead.

4. THE PROPOSED METHOD

4.1 Architecture of S-AODV routing protocol

S-AODV protocol in MANET is proposed. The proposed solution method secure AODV again the attack by using symmetric key based method authentication and key distribution technique provide better performance than the existing method. In this proposed method MD is calculated before broadcasting In NAMC two keys are required which are selected according to the key table which are dependent in to hop count field. At the starting node the value of the hop count field is zero so K0 is used as the first key while next key from key table (i.e 1) is used as second key. To check the integrity of the packet at the each node first get the hop count value and calculate the hash function then append it to the message .then send the secure AODV message .now on the other node If new and old MD are matched then it proceed the messages. Otherwise block it . Then value of hop count is increment automatically . After then calculate the digest with new hop count value and add it to the message. Same procedure is followed at the end i.e receiver

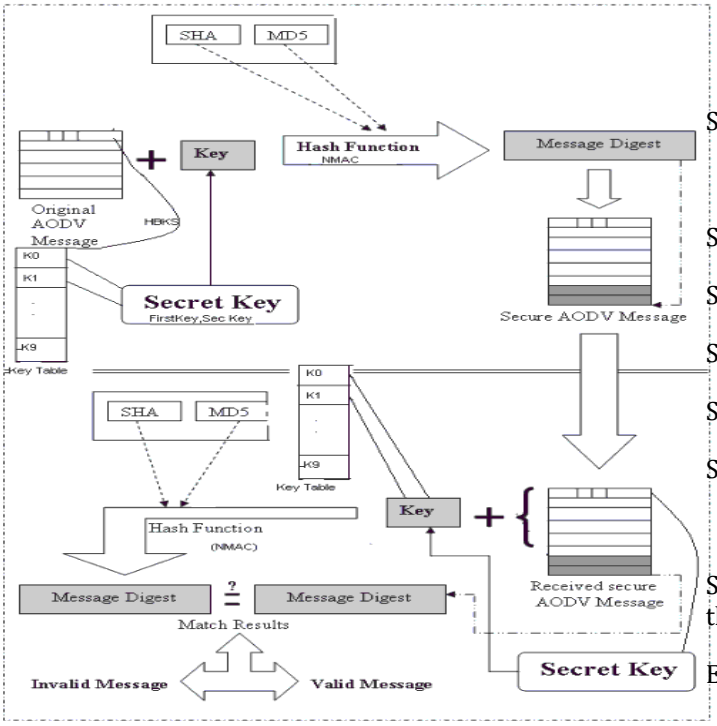


Fig .2 : Architecture of Secure AODV

4.2 Algorithm

We use the NMAC for node to node authentication. When the malicious nodes change the hop count value in the control packet. it would be detected by authorized node. In NAMC requirement of two keys are needed which are selected according to hop count value in the control packet . At the sender the value of the hop count is zero so *K*0 is used as the first key while next key(K1) from table is used as second key. At the each intermediate node check the integrity of the message. And compare old one with new . If new and old MD are not matched then it discards messages. If both are same it means the message is correct Then the value of hop count is increment by one. After this it generate the new MD with new hop count value and appended with the Packet . Same procedure is followed The proposed method is described by the ALGORITHM 1 to 3

1. **Message generation at sender:**

Step 1 : create pkt

Step 2: select (hop value from pkt);

Step 3: now select first key =K(HP mod no of key)

Step 4: second key =K(next value)mod no of key)

Step 5: calculate hash function

H(P)=hash(p||K first);

H('P)=hash(H(p)||K second);

Step 7: send(p||H'(p));

2. **Message generation at receive**

Step 1 : create packet

Step 2: select (hop value from packet);

Step 3: now select first key =K(HP mod no of key)

Step 4: second key =K(next value)mod no of key)

Step 5: calculate hash function

H(P)=hash(p||K first);

Step 6: if msg send from the sender = msg receive from the sender then packet is accepted;

Else packet is rejected(drop p);

3. **Integrity Check At Intermediate Node**

If p is accepted then increment HP value

i.e now keys is

K first=(K first+1)mod n;

K second=(K second +1)mod n;

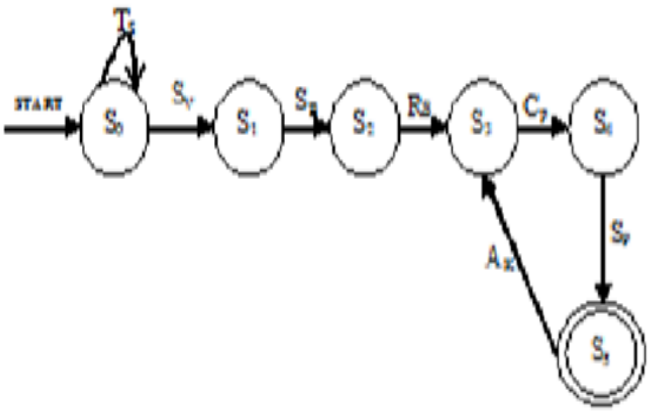
5. MATHEMATICAL MODEL USING DETERMINISTIC FINITE AUTOMATA

The State Transition Diagram in Fig contains:
M = (Q,Σ,δ,q0,F) where

Q = {S0,S1,S2,S3,S4,S5},

Σ = { TS,SV ,SP,RS,CP ,SP ,AK}, Where,

TS = time to send packet from source



SV = Sensed to establish path

SR = Send request

RS = Route establishment

SP = Send Data Packet

AK =Acknowledgement

q0 = S0, F = {S5}, and

δ is b define by the following state transition table:

TABLE I
STATE TRANSITION TABLE

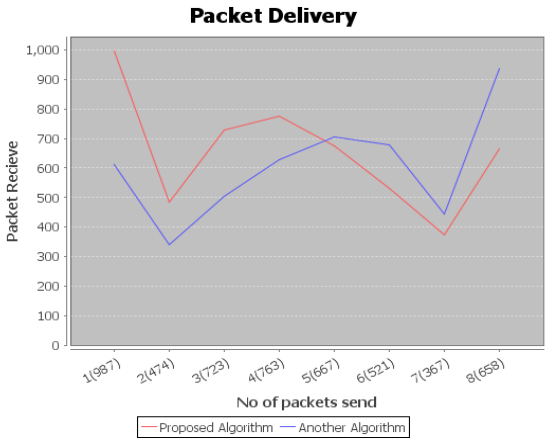
δ	T_S	S_V	S_B	C_H	C_P	S_P	A_K
S_0	S_0	S_1	Φ	Φ	Φ	Φ	Φ
S_1	Φ	Φ	S_2	Φ	Φ	Φ	Φ
S_2	Φ	Φ	Φ	S_3	Φ	Φ	Φ
S_3	Φ	Φ	Φ	Φ	S_4	Φ	Φ
S_4	Φ	Φ	Φ	Φ	Φ	S_5	Φ
S_5	Φ	Φ	Φ	Φ	Φ	Φ	S_3

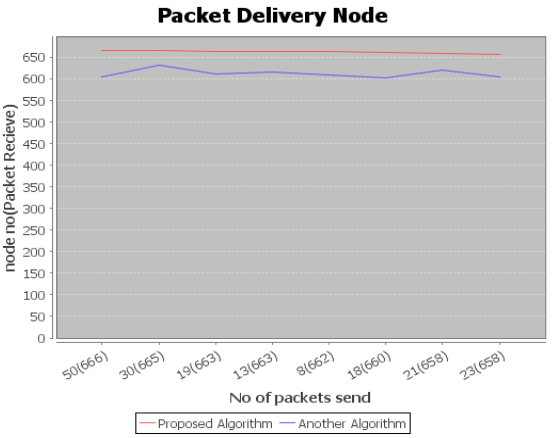
6. PERFORMANCE EVALUATION

6.1 Runtime Analysis

A) Packet Delivery Ratio :

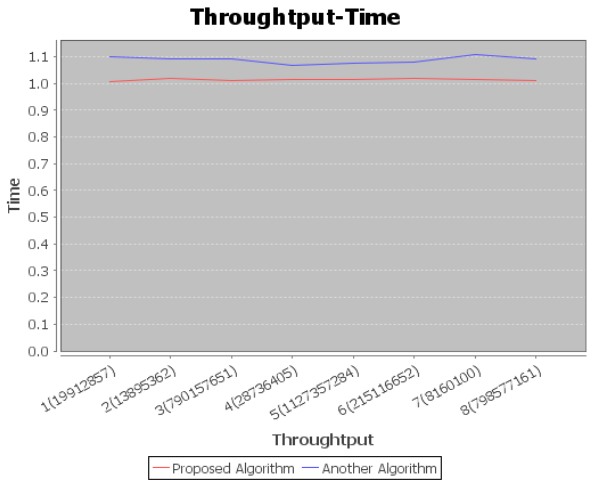
Packet Delivery Ratio = Total Packets Received / Total Packets Sent.

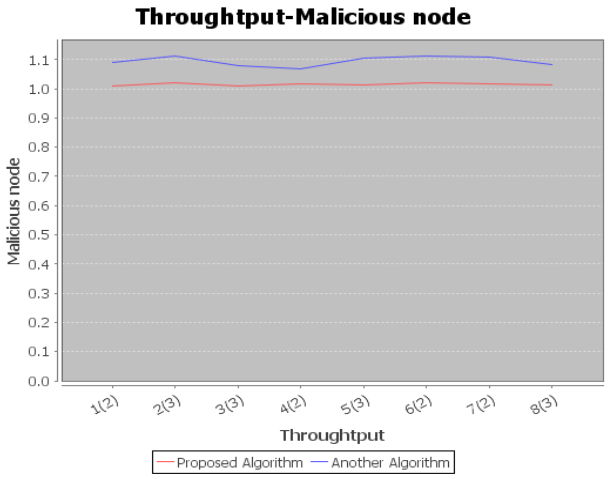




B) Throughput

It is the average rate of successful delivery of message over a network . And measured in bits per seconds or bps.





6.2 Comparison with other protocols

S-AODV protocol can trace the out-band and in-band wormhole attack. .DELPHI protocol receives route reply for all the requests at the sender so it uses more resources in the network. Both protocols DELPHI and MAODV does not need any hardware support and synchronization. both can easily detect wormhole attack . WHOP uses hound packet after discovery process of route so, it requires extra time for wormhole detection.

TABLE II. Comparison of S-AODV with other protocols

Protocol	Based on	Remark	In-band/out of band
WHOP	AODV	Required extra processing time due to use of hound packet	Detect
DELPHI	AODV	Extra resources needed because destination node replies all nodes	Detect
AODV	AODV	No burden	Detect

7. CONCLUSIONS

The proposed solution or method i.e secure AODV to find out wormhole attack by using symmetric key based method authentication and run time key distribution technique provide better performance than the previously used method. The proposed technique or method much more secure against the wormhole attacks by using symmetric key based message authentication and run time key pre distribution technique .

REFERENCES

[1] Syed Atiya Begum, L.Mohan, B.Ranjitha, " Techniques for Resilience of Denial of Service Attacks in Mobile Ad Hoc Networks", Proceedings published by International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 – 071X National Conference on Research Trends in Computer Science and Technology – 2012.

[2] Abderrahmane Baadache, Ali Belmehdi, "Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks", Elsevier Journal of Network and Computer Applications,Volume 35, Issue 3 (Special Issue on Trusted Computing and Communications), May 2012, Pages 1130–1139.

[3] Woungang, "Detecting blackhole attacks on DSR-ImadAad, Jean-Pierre Hubaux, "Impact of Denial of Service Attacks on Ad Hoc Networks", IEEE/ACM Transactions on Networking, VOL. 16, NO. 4, AUGUST 2008.

[4] Xie, Liang, "Message Dropping Attacks in Overlay Networks: Attack Detection and Attacker Identification" IEEE Securecomm and Workshops, 28 Aug. to 01-Sept. 2006.

[5] AymanHelweh-Hannan, "Avoiding Misbehaving Nodes in Mobile Ad- Hoc Environments: Towards Improved QoS Routing", 2nd IEEE International Conference on Distributed Frameworks for Multimedia Applications, 2006.

[6] L. Abusalah, A. Khokhar, and M. Guizani, A survey of secure mobile ad hoc routing protocols, IEEE Communications Surveys and Tutorials, vol. 10, no. 4, pp. 78-93, 2008.

[7] S. Kalwar, Introduction to reactive protocol, IEEE Potentials, vol. 29, no. 2, pp. 34-35, 2010.

[8] J. -H. Song, V. W. Wong, and V. C. Leung, Efficient on-demand routing for mobile ad hoc wireless access networks, IEEE Transactions on Selected Areas in Communications, vol. 22, no. 7, pp. 1374-1383, 2004.

[9] M. G. Zapata and N. Asokan, Securing ad hoc routing protocols, in Proc. of the 1st ACM Workshop on Wireless Security, pp. 1- 10, 2002.

[10] based mobile ad hoc networks", International Conference on Computer, Information and Telecommunication Systems (CITS), 14-16 May 2012.

[11] George Adam, Vaggelis Kapoulas, Christos Bouras, Georgios Kioumourtzis, Apostolos Gkamas, Nikos Tavoularis "Performance Evaluation of Routing Protocols for multimedia transmission over Mobile Ad hoc Networks", IEEE International Conference on Wireless and Mobile Networking Conference (WMNC), 2011

[12] S.Prahmkaew, "Traffic Policing over Various Ad Hoc Networks and Inter-Vehicular Communications", 5th IEEE International Conference on Embedded and Multimedia Computing (EMC), 11-13 Aug. 2010.

[13] B. B. Jayasingh, B. Swathi, "A Novel Metric For Detection of Jellyfish Reorder Attack on Ad Hoc Network", BVICAM'S International Journal of Information Technology (BIJIT) Vol. 2 No. 1, ISSN 0973 – 5658 Year – 2010.

[14] S.A. Hussain; A. Ali ; M. Hassan Raza, "Persistent packet reordering attack in TCP based Ad hoc wireless networks", IEEE International Conference on Information and Emerging Technologies (ICIET), 2010.