ISSN 2348 – 9928
IJAICT Volume 6, Issue 3, March 2019 Doi:01.0401/ijaict.2015.05.09 Published on 05 (3) 2019

AN ENHANCEMENT TOWARDS THE SECURITY OF AODV ROUTING PROTOCOL IN MANET

Mr. P. Krishna Subba Rao *Ms. K. Sindhu* *Ms. E. Sirisha* *Mr. A. Ajay Kumar*

Department Of Computer Science and Engineering,
GVP College of Engineering,
Visakhapatnam, India

Abstract*—Mobile Ad-hoc Network (MANET) is an infrastructure less network of mobile nodes. Because of the increased number of budget friendly, modest and more powerful devices MANET became a fastest growing network. As it does not have a centralized administration mechanism and the network is open shared medium any node can enter or leave the network at any time. This is the main vulnerability in MANET which leads to many security attacks. The previous approaches for the security of MANET couldn't completely prevent the problem. Many researchers had developed many algorithms, but none of them made a decent trade off between the security and performance. In this paper, we enhance the AODV protocol to minimize the attacks and hence the error packets. The proposed method uses NMAC(nested message authentication code) along with the sequence number of the node to minimize the attacks. In this method we detect sinkhole attack and minimize the rate of error packets by observing the highest sequence number. This paper shows performance metrics as the average packets sent, packets lost and the overall error rate.

Keywords*— Nested Message Authentication Code; Hop Count Based Key Selection; Sinkhole attack Introduction.

I. INTRODUCTION

MANET is the new emerging technology, which enables users to communicate without any physical infrastructure, regardless of their geographical location, that's why it is sometimes referred to as an ―infrastructure less network. The increase of cheaper, smaller and more powerful devices makes MANET a fastest growing network. An ad-hoc network is self-organizing and adaptive. It is defined as a category of wireless networks[2] and is competent of operating without the support of any infrastructure.

As MANET is a decentralized network, the network is vulnerable to many attacks[3][4] like black hole attack, DOS, sinkhole attack etc. In the previous methods attacks like black hole were precluded but still the system is vulnerable to sinkhole attack. This paper describes about sink hole attack and the steps to forbid the attack to minimize the error rate.

Sinkhole is one of the severe representative attack in MANET under which AODV is needed to be evaluated. AODV is a reactive protocol that is the network is silent until a connection is needed. Sinkhole attack tries to attract the data to itself from all neighboring nodes. It generates fake routing information by advertising highest sequence number. Hence the attacker node actively participates in the network. By notifying the highest sequence number the remaining nodes in the network start sending packets towards the malicious node.

Ease of Use

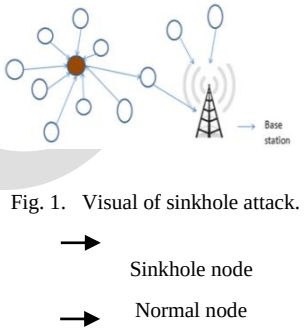


Fig. 1. Visual of sinkhole attack.

In this paper, we are going to detect the sinkhole attack and prevent it to some extent by identifying the node that advertising highest sequence number and reduce the error rate. The detailed method of preventing sinkhole will be discussed in section IV.

II. LITERATURE REVIEW

Sanzgiri et al. [6] developed authenticated routing for AD-HOC networks (ARAN). This method uses the public-key based cryptographic mechanism to secure the AODV against most possible attacks in MANET. ARAN secure the AODV against various attacks such as modifying routing information, impersonation attacks etc. The limitation of this method is that, ARAN uses asymmetric cryptography based mechanism which cause higher overhead due to use of public Key Cryptographic techniques which primarily require more processing power, large memory and hence, more battery power but the devices used in MANET have limited processing power, memory and battery power. The second drawback of this method is that the length of the control packet is large which cause higher overhead in route

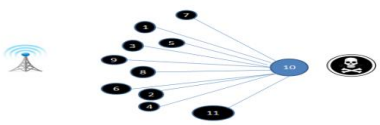
ISSN 2348 – 9928
Doi:01.0401/ijaict.2015.05.09 Published on 05 (3) 2019

discovery and maintenance phase of the protocol. Also ARAN uses the trusted third party which is very difficult to maintain as the nature of nodes in MANET is mobile that may lead to a single point of failure. Secure AODV is another protocol to secure the AODV developed by Zapata and Asokan [7]. This method uses the digital signature and one way hash function to secure the AODV and provide security against the various possible routing attacks in MANET but it also has the similar limitations as those in ARAN. secure routing protocol developed by Zhou et al. [9] protects against the internal attack called Byzantine Attacks for MANETs in Adversarial Environments. It was successful to remove some of the limitation of previous method because it uses shared secrete key based authentication mechanism for end to end authentication of the messages and established the secure route between source to destination. The drawback of this method is that it uses the RSA cryptography technique and hence, requires lots of processing power.

Preeti Sachan and Pabitra Mohankhilar[8] proposed "Securing AODV Routing protocol in MANET based On the cryptographic Authentication Mechanism. This method provides security for routing packets. It prevents attacks such as black holes, impersonation and modifying routing information. To achieve this, hashed Message Authentication Code(HMAC) is used that provides fast message verification. This method minimizes the time delay and network routing load involved in computation and verification of security fields during route discovery. This method uses a pair wise secret key. Establishing secret key between any two nodes is an expensive operation. K.V.Arya et al.[1] developed a secured version of AODV to prevent routing attacks in MANET's. This method uses key pre-distribution to reduce the overheads caused by distributing and sharing keys at run time. A technique called Hop Count Based Key Selection(HBKS) is used in this method for authentication. Though this method prevented few attacks still the network is vulnerable to some routing attacks.

III. PROBLEMS ON SINKHOLE ATTACK

Sinkhole attack is a service attack that prevents the base station from obtaining complete and correct information. In sinkhole attack a compromised node tries to attract the data to it from all neighboring nodes by broadcasting a bogus route request. The attacker node then can modify or drop the packets.



Sink hole problem.

The sinkhole node selects the source destination node. It observes the source node sequence number carefully and generates bogus route request with selected source destination and higher sequence number than observed source sequence number. It then broadcasts the bogus route request. Sinkhole node causes severe problems in the network. It increases network overhead, decreases networks life time by boosting energy consumption; and finally destroy the network[5].

IV. PROPOSED METHOD

In this method an enhanced version of AODV is developed to authenticate the nodes and the attacker node is detected to reduce the error rate. The attacker node is detected by the use of sequence number. In this the keys are pre-distributed to minimize the overhead and Nested Message Authentication Code(NMAC) is used to provide authentication. The keys are selected from the key table according to the hop count value of the node. This technique is known as Hop Count Based Key Selection(HBKS).This method is more secure because attacker cannot perform malicious activity because of NMAC where different key is selected from the key table based on the hop count value that is difficult to identify by the attacker consequently making the cryptanalysis complex.

To detect the sinkhole node the node with highest sequence number is observed and prevented. The sinkhole drops/modify the packets going through that node. It advertises highest sequence number and attracts the data to it from the other nodes.

This attack convinces neighboring nodes through broadcasting fake route information and let them know itself on the way to specific nodes. In this way it tries to attempt to draw all network traffic to itself. To detect the node that exhibits highest sequence number, the node that forwards packet to other neighboring node first checks the sequence number of previous route request and current route request. If the sequence number between these two have a lot of variance then the node is malicious. Otherwise the node is authenticated and the packets are sent through that node. The active node also checks if the neighboring node is malicious or not by sending a fake packet with highest sequence number. If the other node that received this request accepts it then it is a malicious node, if not it is an authenticated node.

I. ALGORITHM

Step1: A packet is generated. The source node starts route discovery and requests for a route to transfer the packet.

Step2: Route Requests are stored in a Route Request (RR) table.

Step3: Source sequence number of the current route

ISSN 2348 – 9928
Doi:01.0401/ijaict.2015.05.09 Published on 05 (3) 2019

request is selected. Source sequence number of the previous route request from the table is checked.

Step4: Sequence number difference = Source sequence number of current route request - Source sequence number of previous route request.

Step5: If source sequence number of current route request >>> source sequence number of previous route request, then the node is malicious and the node will be discarded.

Step6: Else, the hop count value of the node is taken and the keys are taken from the key table according to the hop count value
(i) Key1: k(HP mod n)
(ii) Key2: k(HP+1) mod n

Step7: Now NMAC is called that is, hashing is done twice.
(1) H(P) = Hash(P||key1)
(2) H'(P) = Hash(H(P)||Key2)

Step8: The original AODV packet and the hashed packet is sent to the destination.

Step9: End

V. RESULTS

TABLE I. *EXTRACTED VALUES FROM SIMULATOR TRACE FILE*

Iteration	Total Packets	ACK Packets	REQ Packets	ERR Packets	Packet Loss
1	422980	284861	129920	8199	1.938389522
2	421980	286861	126920	8199	1.94298308
3	422980	286850	127785	8345	1.97290652
4	422980	285341	129654	7985	1.887796113
5	422980	283607	130562	8811	2.083077214
6	422980	286891	128984	7105	1.679748451
7	422980	288349	124546	10085	2.384273488
8	422980	293025	120505	9450	2.234148187
9	422980	285890	128940	8150	1.92680505
10	422980	286642	127842	8496	2.008605608
11	422980	293839	121296	7845	1.854697622
12	422980	285424	128546	9010	2.130124356
13	422980	284614	130856	7510	1.775497659
14	422980	287372	128125	7483	1.769114379
15	422980	290976	125145	6859	1.621589673
16	422980	287293	126845	8842	2.090406166
17	422980	294662	120125	8193	1.936971015
18	422980	289638	125480	7862	1.858716724
19	422980	286046	128652	8282	1.958012199
20	422980	293423	121458	8099	1.914747742

The simulations were performed using widely used simulator tool(NS2) version 2.35 for simulation using the trace file. In this method we showed the experimental results for acknowledged, received packets and overall packet loss. It is found that Node 7 has received (attracted) maximum number of packets (17660). Also it is noted that same node 7 has the maximum number of dropped packets (1050). Hence it is concluded that node 7 is the malicious node.

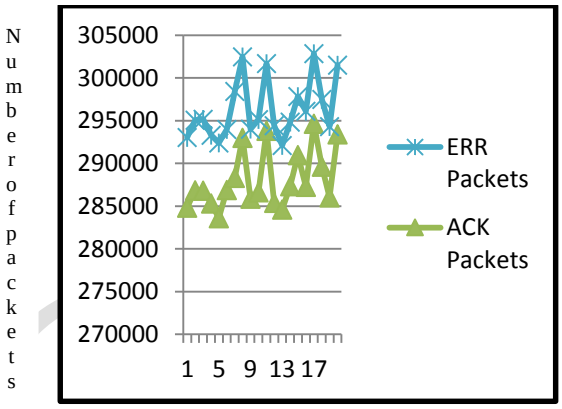


Fig. 2. ***Total acknowledged Vs Received packets.***

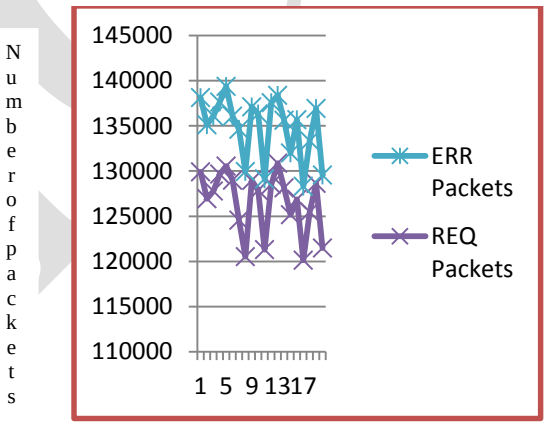


Fig. 3. ***Total Requested Vs Error packets.***

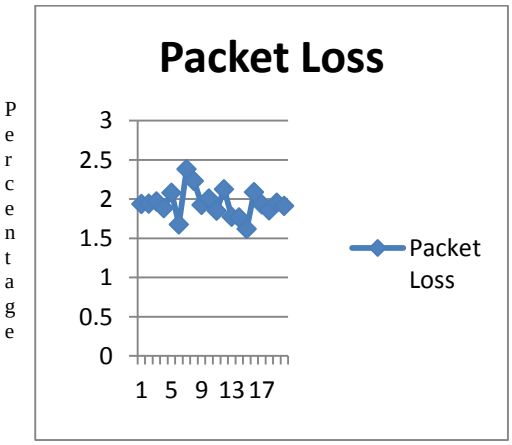


Fig. 4. ***Packet loss.***

ISSN 2348 – 9928
Doi:01.0401/ijaict.2015.05.09 Published on 05 (3) 2019

TABLE II. *VALUES EXTRACTED FOR INDIVIDUAL NODES*

Node Numbers	Received packets	Dropped packets
0	12549	740
1	6452	214
2	12525	648
3	14086	792
4	13149	822
5	12700	916
6	14711	761
7	17660	1050
8	11021	534
9	17255	786
10	10778	690
11	15174	891
12	12912	890
13	16215	714
14	9186	415
15	11401	594
16	11520	741
17	5641	166
18	13230	757

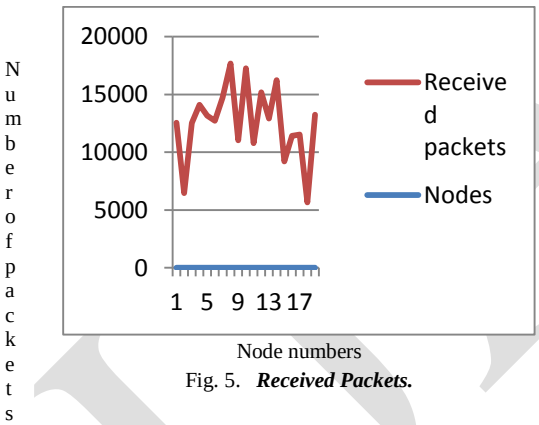


Fig. 5. ***Received Packets.***

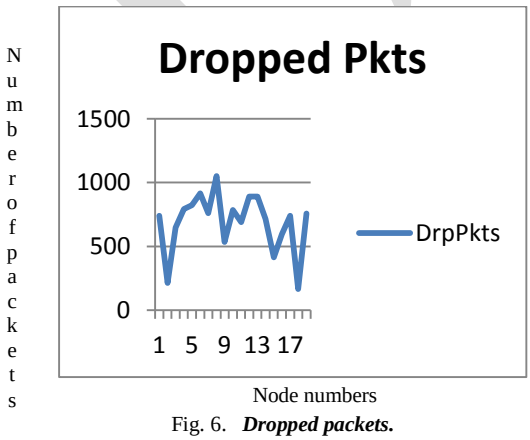


Fig. 6. ***Dropped packets.***

VI. CONCLUSION

In this paper an enhanced version of AODV routing protocol in MANET is introduced for detection of Sink hole attacks using NMAC and by detecting the node with highest sequence number. The proposed method detects sinkhole attack and minimizes the error rate. The simulation results showed that the proposed method gives better performance. This work may also be extended by checking the performance of proposed method in the presence of wide variety of MANET routing attacks.

References

[1] K.V.Arya,Shyam singh Rajput, "Securing AODV Routing Protocol In MANET using NMAC with HBKS Technique",International conference on signal processing and integrated networks(SPIN) 2014.

[2] Y. Zhang and B. -H. Soong, "Performance of mobile networks with wireless channel unreliability and resource inefficiency," IEEE Transactions on Communications, vol. 5, no. 5, pp. 990-995, 2006.

[3] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," IEEE Wireless Communications, vol. 14, no. 5, pp. 85-91, 2007.

[4] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "DOS attacks in mobile ad hoc networks: A survey," in Proc. of the 2nd IEEE International Conference on Advanced Computing and Communication Technologies, pp. 535-541, 2012.

[5] Benjamin J. Culpepper, H.Chris Tseng," Sinkhole Intrusion Indicators in DSR MANET", First International Conferenc on broadband networks IEEE 2004.

[6] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A secure routing protocol for ad hoc networks," in Proc. of the 10th IEEE International Conference on Network Protocols, pp. 78-87, 2002.

[7] 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.

[8] M. Yu, M. Zhou, and W. Su, "A secure routing protocol against byzantine attacks for MANETs in adversarial environments," IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 449-461, 2009.

[9] P. Sachan and P. M. Khilar, "Securing AODV routing protocol in MANET based on cryptographic authentication mechanism," International Journal of Network Security and Its Applications (IJNSA), vol. 3, no. 5, 2011.

[10] Rajeshwar L.Balla, Venugopal Kotoju,"Sinkhole Attack detection and prevention in MANET & Improving the Performance of AODV Protocol",An international journal of advanced computer tchnology,2(7),July-2013.