A Protected Adhoc Routing In Manets Against Blackhole Attack

P. Aruna[1], Dr. Puja S. Prasad[2] , Dr. D. Baswaraj[3]
[1]Department of CSE, CMR Institute of Technology, arunapadamati@gmail.com
[2]Department of CSE, CMR Institute of Technology, puja.s.prasad@gmail.com
[3]Department of CSE, CMR Institute of Technology, braj.d.1668@gmail.com

Abstract— MANET is a group of mobile nodes communicate through a wireless medium without the needs of any fixed infrastructure such as an access point or mobile base station. In such a network every node is transfer data to forwarding packets to its neighboring nodes. Some nodes may not participate in forwarding the packets for reduction its resources. In this paper we propose a novel secured routing protocol to mitigate a blackhole attack by modifying existing AODV protocol with secured authentication technique to discovery blackhole attack by preventing the address forgery. Existing AODV routing protocol is modified to detect and prevent the black hole attack. The experiment results show that our proposed algorithm secure the AODV against black hole attack in MANETs.

Keywords—Blackhole; MANET; AODV; Security; PKI.

I. INTRODUCTION

MOBILE ad hoc networks (MANETs) represent complex distributed systems that consist of wireless mobile nodes that can dynamically and freely self-organize into arbitrary and temporary ad hoc network topologies. This allows people and devices to seamlessly internetwork in areas where no pre-existing communication infrastructure exists, for example disaster recovery environments. The unique characteristics of MANETs, such as dynamic topology and resource constraint devices, pose a number of nontrivial challenges for efficient and lightweight security protocols design. Due to the lack of centralized identity management in MANETs and the requirement of a unique, distinct, and persistent identity per node for their security protocols to be viable, Blackhole attacks pose a serious threat to such networks.

MANET technology is used to immediately provide secure access between multiple mobile nodes without the need for a preset communications infrastructure achieving a multichip architecture. These networks are identified by two basic principles: routing and auto- configuration. While there is already quite a lot of established work undertaken on routing and consequently those related to secure routing , there is still a room for continuous improvements on those which are still under construction, notably those related to auto- configuration and in particular, those in connection with secure MANET auto -configuration.

MANETs are unsecure from various attacks. Attack can cause decrease of network traffic and modification of control message fields or forwarding routing messages. Main goal of Attacks:
a) Enhance latency of particular packets.
b) Reduce overall network performance.
c) Split down a particular link or node.
d) Divert packets will affect the link bandwidth
.

A Link layer attacks The MANETs is and multi-hop peer-to-peer network architecture. In particular,one-hop connectivity among nodes is maintained by the link layer protocols and the network layer protocols extend the connectivity to other nodes in the network. Attacks may goal the link layer by disrupting the cooperation of the layer's protocol these attacks are misbehavior attacks, selfish attacks in data link layer attacks each node operates as both host and router to further packets for other nodes. Every node forwards every packet. But some of the nodes may act as the selfish nodes. These nodes use this network and its services but they do not cooperate with other nodes. the CPU power, battery and also bandwidth does not consume any energy for retransmitting the data of other nodes and they reserve them only for themselves.The characteristics of selfish nodes as follows:

1. ***Routing process is not participating:*** selfish node is not forwarding the routing messages. Route Request and Reply packets are modifies by changing TTL value to smallest possible value.

2. ***Send hello messages are not reply:*** A selfish node may not respond to hello messages, hence other nodes may not be able to detect its presence when they need it.
3. ***Intentionally delay the RREQ packet: A*** selfish node may delay the RREQ packet up to some extent.. It will avoid the routing paths.
4. ***Dropping of data packet:*** A selfish nodes participate in routing messages. And not forward data

II. RELATED WORK

IDENTIFICATION OF SELFISH NODES:

To detect selfish nodes in MANETs by using existing methods are reputation based method, credit based method, acknowledgement based systems, collaborative based methods etc.

Reputation based method : The reputation value in the case of a selfish node is the indication to the other nodes about the perception about the cooperation of a node. The network will collectively detect the selfish and suspicious nodes then the declaration will propagated to the entire network and the selfish node will be eliminated from the network. If the reputation value of a node is low then the node is considered to be selfish by other node. If the reputation value is high then the node is cooperative.

A. Credit Based Schemes: In order to perform networking functions will provide incentives to nodes. This kind of strategy stimulates nodes increase the cooperation among the nodes by utilizing the concept of virtual credit or electronic currency or similar payment schemes. There are two models for implementing the credit based schemes 1) The Packet Purse Model 2) The Packet Trace Model.

B. Acknowledgement Based Schemes: The acknowledgement based schemes will use the acknowledgement packet to ensure the packet is forwarded by the node. If the node does not receive the acknowledgement from a node, that means that node not forwarding the data packet. Based on the acknowledgement it detects the selfish nodes.

SECURITY METHODS OF PROVIDING NEIGHBOURING NODES

To providing security to the neighbor nodes in MANETs by existing methods are (1) ARAN secure routing protocol, (2) ARIADNE secure protocol, (3) SEAD protocol, (4) SAODV protocol.

ARAN: is an on-demand secure routing protocol. It detects and protects against authentication, message integrity and non-repudiation. It uses asymmetric key cryptography. ARAN requires trusted certification server, the certificate accommodates the IP address of the node, its public key and a time-stamp of when the certificate was created and a time at which the certificate expires along with the signature by certification authority. But the disadvantages of ARAN are it uses the central authority (Certification Authority) and it can't protect against attack.

ARIADNE: A secure on demand routing protocol for ad-hoc network (ARIADNE) is based on DSR routing protocol, it uses highly efficient symmetric cryptography. It providing point-to-point authentication of a routing packets using a message authentication code (MAC) and a shared key between the two parties. For broadcasting RREQ packets it uses TESLA broadcast authentication protocol. TESLA keys are distributed to the participating nodes via an online key distribution center AODV by providing security features like integrity, authentication and non-repudiation.

SEAD: is a proactive routing protocol and is based on destination sequenced distance vector routing (DSDV). SEAD deals with attackers that modify routing information broadcast during the update phase of the routing information. SEAD makes use of efficient one-way hash chains rather than relying on expensive asymmetric cryptography operations. SEAD does not cope with attacks.

Secure Ad Hoc On-Demand Distance Vector (SAODV): routing, it is an extension of AODV protocol. The Secure AODV scheme is based on the assumption that each node possesses certified public keys of all network nodes. SAODV can be used to protect the route discovery mechanism repudiation.

III. PROPOSED WORK

Every node in a network receives a public key infrastructure from trusted third party by securely using RSA algorithm. Black hole attack initiates the malicious activity by giving false route reply message. Fig.1 shows the RREP packet format for the proposed protocol. In order to get integrity of route replay message, destination node needs to replay the route reply by using proposed algorithm.

Algorithm

1. Destination get the RREQ packets from different node
2. Node selects a best route based on metric less hop count, and prepare the route replay packet
3. Node adds the route replay packet with its secrete key got from the PKI.

$$(RREP)\ XOR\ (Secrete\ Key)$$

4. Node calculate the message digest using the digest algorithm according to PKI instruction (In our method it is MD5)
   $H(RREP\ XOR\ Secrete\ Key)$
5. Node append the calculated digest information with original route replay packet
6. RREP unicast towards the source node
7. Source node remove the $H(RREP\ XOR\ Secrete\ Key)$ from the RREP packet and adds the secrete key got from the PKI and perform the following task
   $(RREP)\ XOR\ (Secrete\ Key)$
   $H(RREP\ XOR\ Secrete\ Key)$

Fig.1: RREP Packet format

To overcome many steps in Existing System, to decrease high storage cost and make it more secure we use a private key exchange method to reduce black attack , I introduced a new method by checking the private key and accept the packet, then the source send the packet to the destination node .
in this method when a node wants to send a packet from source i used to assign a key for every node, and also finding the neighborhood no node. Afterhoosing the destination node then check the key of relay node and the RSS value of neighbor node, by checking these values we are able to identify the black node if the node is not black then the packet will be delivered.

Algorithm : Secured Routing against Blackhole

Step 1: Mobile Adhoc Network is constructed with 'n' number of nodes.

Step 2: Assign Private key and public key for all nodes

Step 3: Nodes are aware of their direct neighbors. The one-hop neighbors of all the mobile nodes are identified

Step 4: For a sender node 'S', relay node is selected, by checking the distance to the destination node 'D'.

Step 5: Sender Node 'S' checks for next hop node and forwarding node.

Step 6: Assign threshold for UB−THRESHOLD=7

Step 7: Read the RSS while sending data packets from source node

addNewRss (Address, rss, time−recv)

BEGIN SUB:
Step 8: IF: Address is not in the Table THEN
Step 9: IF: rss >= UB−THRESHOLD, then: Add−to−Malicious−list(Address)
Step 10:Bcast−Detection−Update(Address) ELSE: Add−to−Table(Address)
Step 11:END−IF

END SUB:
Step 12: Check private key and accept packet

Step 13: The source Send packets to destination node

IV. EXPERIMENTAL RESULTS

To evaluate performance of our secured aodv technique, we are present simulation environment setting in the results as shown below

Simulation parameter	*Value*
Simulator	*NS-2(v.2.35)*
No of nodes	*33*
Packect size	*50 bytes*
Traffic type	*CBR*
Simulation time	*50 s*
Recevier energy	*0.0395kj*
Transmitter energy	*0.066 kj*
Initial energy	*10 kj*

Table 1 Simulation Parameter Setup

In this section we are analyzing our proposed work with the presence of malicious node in a routing path with varying number of nodes from 10 to 30 with respect to throughput packet loss and delay.

Performance comparison of proposed work is discussed in figure 2 to 5, it is clearly indicates that our proposed work mitigate the malicious attack from routing path and enhance the throughput with less delay and considerable overhead. In below section we are comparing our work with existing monitoring based proposed work to mitigate the black hole in mobile ad hoc networks , the comparison results are shown in below figures 2 to 5.

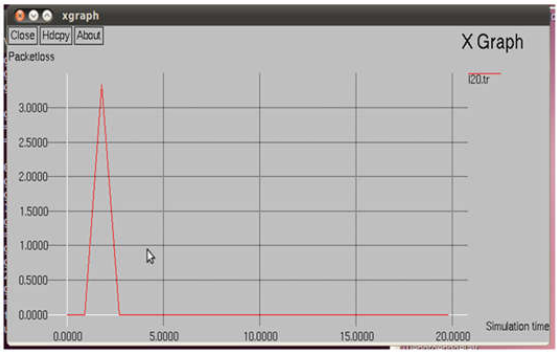

Fig.2: Delay Proposed Work

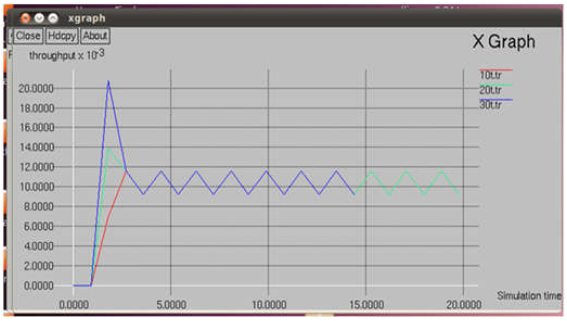

Fig.3: Throughput Analysis

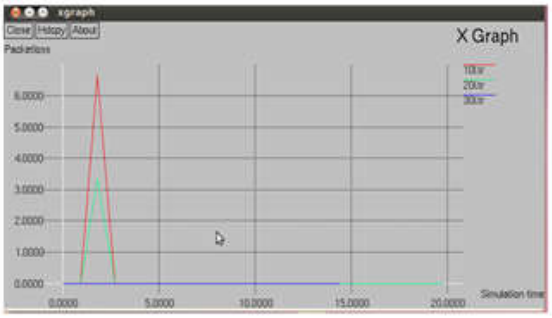

Fig.4: Packet Loss Analysis

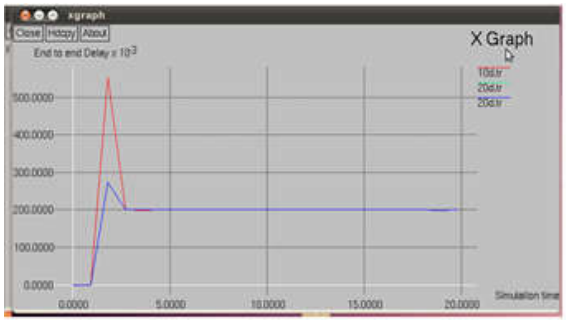

Fig.4: End-to-End Delay Analysis

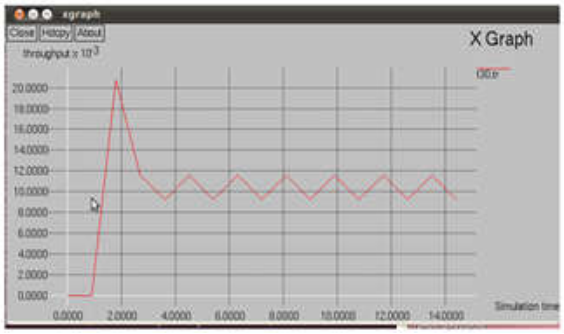

Fig.5: Throughput Analysis of Proposed work

V. CONCLUSION

In this paper, a PKI based algorithm for "mitigating black hole attack in AODV protocol" has been proposed, which is used to provide security to the MANETs. This algorithm prevent the black hole attack at initial stage. The main goal of SKA is not only to mitigate black hole attack but also to increase the throughput thereby reducing the packet loss due to black hole node.

If any node drops a packet our algorithm checks for the packet drop reasons first before declaring it as a black hole node, thereby preventing a trusted node from becoming a black hole node.

The main goal of SKA is not only to mitigate black hole attack but also to increase the throughput thereby reducing the packet loss due to black hole node. In future, we can work on Co-operative Black hole attack detection & prevention by using Cryptographic techniques.

REFERENCES

[1] Siddiqua, Ayesha, Kotari Sridevi, and Arshad Ahmad Khan Mohammed. "Preventing black hole attacks in MANETs using secure knowledge algorithm." Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on. IEEE, 2015.

[2] Bhandare, A. S., and S. B. Patil. "Securing MANET against Co-operative Black Hole Attack and Its Performance Analysis-A Case Study." Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on. IEEE, 2015.

[3] Dorri, Ali, and Hamed Nikdel. "A new approach for detecting and eliminating cooperative black hole nodes in MANET." Information and Knowledge Technology (IKT), 2015 7th Conference on. IEEE, 2015.

[4] Wahane, Gayatri, Ashok M. Kanthe, and Dina Simunic. "Detection of cooperative black hole attack using crosschecking with truelink in MANET." Computational Intelligence and and Networking Technologies (ICCCNT), 2013 Fourth International Conference on. IEEE, 2013.

[5]. Payal N. Raj, Prashant B. Swadas ?DPRAODV: A Dyanamic Learning System against Blackhole Attack in Aodv Based Manet? IJCSI International Journal of Computer Science Issues, Vol. 2, pp 54-59 2009.

[6] Rutvij H. Jhaveri , Sankita J. Patel. (2012). DoS Attacks in Mobile Ad-hoc Networks: A Survey. 2012 Second International Conference on Advanced Computing & Communication Technologies. 2 (2), p535-540.

[7] Rachh, A.V., Shukla, Y.V. and Rohit, T.R., 2014. A Novel Approach for Detection of Blackhole Attacks. *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN*, pp.2278-0661.

[8]. Rajaram, A. and Palaniswami, S., 2010. Malicious node detection system for mobile ad hoc networks. *International Journal of Computer Science and Information Technologies*, *1*(2), pp.77-85.

[9]. Hu, Y.C.P.A., 2002. Johnson D& A SEAD; Secure Efficient Distance Vector Routing for Mobile W ireless Ad Hoc Net—works1, A. In *Proc of the 4th IEEE Workshop on Mobile Com—puting Systems and Applications [-q. 2002.3-13. I-3] Yi S. Naldurg P, Kravets RA Security Aware Routing Pro—toeol for Wireless/\ d Hoc Networks* (pp. 15-149). Proc of the 6th W orld Muhi—Conference on Systemics. Cybernetics and In—formatlcs1, C].

[10]. Hu, Y.C., Johnson, D.B. and Perrig, A., 2003. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad hoc networks*, *1*(1), pp.175-192.

[11]. Castelluccia, C. and Montenegro, G., 2002. Protecting AODV against Impersonation attacks. *ACM SIGMOBILE Mobile Computing and Communications Review*, *6*(3), pp.108-109.