SECURE AODV AGAINST CONTROL PACKET DROPPING ATTACK

Ms. Deepa Athawale
Department of Computer Engineering, Terna Engineering College Nerul, Navi Mumbai
Email: deepaathawale@gmail.com
Dr. Lata Ragha
Department of Computer Engineering, Terna Engineering College Nerul, Navi Mumbai
Email: lata.ragha@gmail.com

Abstract— **The mobile ad hoc networks (MANET) are collection of autonomous nodes that communicate by forming a multi-hop radio network. Ad hoc networks are more vulnerable toward a security attacks like DoS (Denial of service), which is a kind of packet dropping attack. Packet dropping attacks are of three types i.e., control packet dropping, selective dropping or collaborative packet dropping. Most of the current proposed methods worked on data packet dropping, but these solutions are not directly applicable to control packets. Dropping control packets may be advantageous for selfish nodes and malicious ones as well.**

We propose a solution to protect control packet dropping in reactive routing protocols. Our proposal provides a general solution to monitor, detect, and isolate control packet droppers in Ad hoc network. The solution handles both directed and broadcast control packets. For monitoring we use the two-hop ACK approach for directed control packets and time based approach for broadcast control packets. For detection and judgment a redemption strategy will be used and for isolation a reputation-based approach is used.

***Keywords*—Packet drops attack, AODV, MANETs, Malicious node, and routing protocols**.

I. Introduction

A MANET is a collection of wireless hosts that can be rapidly deployed as a multi-hop packet radio network without the aid of any established infrastructure or centralized administrator MANETs are vulnerable to various types of attacks like Packet Dropping Attack where malicious node intentionally drops the packets they receive. The packet dropping attack can be any one of the following way given below.

- Dropping Control Packets
- Selectively Dropping Packets
- Group of nodes collaboratively drop packets

The inherent nature of MANET is susceptible to different kinds of attacks. One of them is DoS (Denial of service) attack, its main aim is to increase the packet loss, delay, more usage of bandwidth and decrease the throughput [3]. Secure routing in MANET is a topic that attracts more and more attention amongst researchers. In this manuscript we deal with securing routing protocols of mobile ad hoc networks (MANETs) against packet dropping misbehavior more specifically. Most current proposals focus on data packets and not on dropping control packets it may be beneficial for selfish nodes and malicious ones as well. For example, simply by dropping RREQ (Route Request) packets a selfish node could exclude itself from routes and thereby avoid receiving data packets to forward. Similarly, a malicious could drop RERR (Route Error) packets to keep the use of failed routes, potentially resulting in a denial of service. We propose a solution to protect control packets against reactive source routing protocols.

II. RELATED WORKS

Flooding Attack Aware Secure AODV

A control packet flooding is a DoS attack in which malicious nodes takes advantage of either route discovery process or to maintain a local connectivity between the nodes. In the route discovery process either it floods the RREQ or RREP packets. So overflow of the routing table in the intermediate node is the effect of this malicious activity. Hello flood is one of the active attacks call as the packet dropping attack. If the malicious node floods the hello packet unnecessarily, neighbors of the malicious node cannot receive other packets. In general, it results in congestion, exhaustion of battery power, wastages of bandwidth and degrades the throughput.

Secure AODV (SAODV) is similar to AODV but it uses cryptographic mechanisms for providing a security in a reactive routing protocol it deals with DOS attacks specifically for flooding attack. A security extension of the AODV protocol, based on public key cryptography in which SAODV routing messages are digitally signed to guarantee their integrity and authenticity. Therefore, a node that generates a routing message signs it with its private key and the nodes that receive this message verify the signature using the sender's public key. This method is pertained to the presence of only one kind attack that is flooding attack. Presence of more than one kind of attacker may affect the performance of the network

A. A Security-Aware Routing Protocol for Wireless Ad Hoc Networks

Many secure routing protocols have been recently proposed for MANET. They aim at preventing the establishment of falsified routes and control packet dropping attacks. SAR (A Security-Aware Routing Protocol) is a general proposal that can be implemented with a reactive routing protocol [5]. It defines the trust degree that should be associated with each node, and ensures that a node is prevented from handling a RREQ (Route Request) unless it provides the required level. This way, data packets and the control packets will be sent only through trusted nodes, with respect to the defined level. SAODV is an implementation of SAR on AODV. One of the difficulties of this approach is the definition of the trust level. Further, assuming that nodes showing the required trust level are genuine is not always correct.

B. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks

The watchdog is the first solution dealing with the packet dropping problem. Its principle is that each node in the source route monitors its successor using the promiscuous mode. For this purpose, a source routing protocol should be used. This basic solution has the advantage of not requiring any overhead as long as nodes behave well, and it could be applied both to data and control packets [6]. Nevertheless, it is inappropriate when using the power control technique, employed by some new power aware routing protocols. Moreover, it does not deal with the isolation step. When a misbehaving node is detected, packets will be sent around it, but no measures will be taken against it, which does not prevent nodes from misbehaving.

C. An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs

Liu et al, proposed a two hop acknowledgement scheme to prove that wireless node has actually forwarded packets to next hop, receiver sends acknowledgement in reverse direction for multiple hops to achieve the goal. But well behaved nodes can become a part of malicious link and may result in losing good routes in network.

This scheme is based on 2ACK packet that is assigned a fixed route of two hops in the opposite direction of the received data traffic's route. In this scheme, each packet's sender maintains the following parameters; (i) list of identifiers of data packets that have been sent out but have not been acknowledged yet, (ii) a counter of the forwarded data packets, (iii) and a counter of the missed packets. According to the value of the acknowledgement ratio (Rack), only a fraction of data packets will be acknowledged in order to reduce the incurred overhead. This technique overcomes some weaknesses of the Watchdog/pathrater such as: ambiguous collisions, receiver collision and power control transmission [7].

III. METHODOLOGIES ADAPTED

In MANET, routing protocols are classified as reactive, proactive and hybrid. The proposed method uses reactive routing protocol, specifically extension of AODV for security purpose. The reactive routing protocols consist of series of actions from either the source to the destination nodes or intermediate node who knows a route to the destination. The reactive routing protocol consists of two different phases such as route discovery and data transmission [4]. For example, route discovery process includes sequence of actions like (1) The source node delivers an initial Route Request; (2) Each node (except for the source node and the node that has a route to the destination) in the forward path receives a Route Request from the previous node and forwards it; (3) The replying node receives the Route Request and replies with a Route Reply message; 4) An intermediate node in the reverse path receives a Route Reply message and forwards it. Secure AODV (SAODV) is similar to AODV but it uses cryptographic mechanisms for providing a security in a reactive routing protocol

SAODV includes a kind of delegation feature that allows intermediate nodes to reply to RREQ messages. This is called the double signature. When a node A generates a RREQ message, in addition to the regular signature, it can include a second signature, which is computed on a fictitious RREP message. Intermediate nodes can store this second signature in their routing table, along with other routing information related to node A. If one of these nodes then receives a RREQ towards node A, it can reply on behalf of A with a RREP message, similarly to what happens with regular AODV. To do so, the Intermediate node generates the RREP message, includes the signature of node A that it previously cached and signs the message with its own private key.

IV. PROPOSED SYSTEM

A general solution to monitor, detect, and isolate control packet droppers is proposed here that deal with both directed and broadcast packets (control packets). For the monitoring we propose different approaches. Regarding the directed packets the two-hop ACK approach is used as the number of these packets is too low compared to data ones. The two-hop ACK is not applicable to broadcast packets, as it becomes too much costly with this kind of packets [7]. Therefore, we propose a promiscuous based solution to monitor broadcast control packets. Finally, we propose a redemption strategy for judgment and a reputation based approach for isolation, applicable to directed packets as well as broadcast ones. However, the optimal values of thresholds used in judgment and isolation may change according to the kind of packets. The below figure 1 shows the block diagram representation of proposed system.

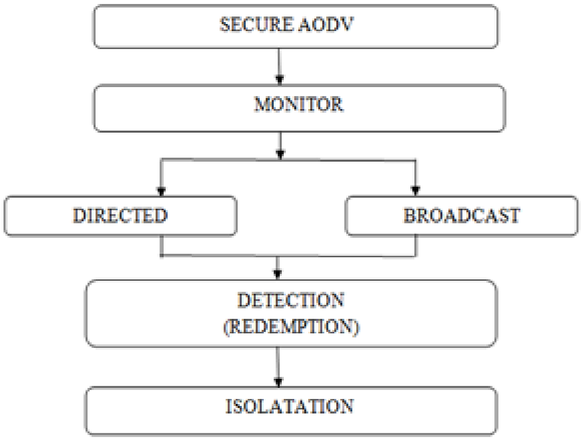

Figure 1 Block Diagram Representation

A. Monitor

1) Directed Packets [RREP, RERR] use two-hop ACK.

The approach uses to monitor the forwarding of directed routing control packets (RREP, RERR) is implemented with a reactive routing protocol. Each node A monitors its successor B in the source route and checks whether it later forwards to C each packet it provides, such that C is B's successor in the source route and A could be either the source or any intermediate node. This process is repeated on each of the hops until reaching the final destination. Here we use a special kind of feedbacks called two-hop ACK [8] that travel two hops.

Node C acknowledges packets sent from A by sending this latter via B a two-hop ACK. To ensure authentication of two-hop ACK packets an asymmetric cryptography-based strategy is used. Node A generates a random number and encrypts it with C's public key (PK), then appends it in the packet's header. When C receives the packet it retrieves the number, decrypts it using its secret key (SK), encrypts it using A's PK, and puts it in a two-hop ACK it sends back to A via B. In the first hop (C, B) the ACK is not transmitted in a separate packet, but piggybacked to the ordinary MAC ACK. This inclusion and employment of the MAC ACK reduces the number of two-hop ACK packets as much as half compared with a separate transmission on each hop. When A receives the ACK it decrypts the random number and checks whether it matches with the one it has generated, in order to validate B's forwarding regarding the appropriate packet. However, if B does not forward the packet A will not receive the two-hop ACK, and it will be able to detect this dropping after a timeout. This strategy requires key distribution mechanisms enabling a security association between each pair of nodes.

2) Broadcast Packets [RREQ]

For RREQ packets each node monitors every RREQ it forwards from the source. The monitoring starts from the reception of the RREQ or its launch if the node is the source and ends after a timeout from its retransmission. For each RREQ, the transmitter monitors all its neighbors. It should either receive (or overhear) the RREQ or a RREP from every neighbor, except the node from which it received the RREQ if the node is not the source. If no one of these packets is received from a neighbor B, then the monitor notices a packet dropping for B. When a node observes that another node B drops more than the configured threshold number of packets it judges B as misbehaving, and tries to isolate the node.

B. Redemption

To get over false detections of packets that may occur due to nodes mobility and channel conditions, we propose a redemption strategy for both kinds of packets. The aim is to allow a well-behaving node improving its reputation and tolerance threshold after it has been observed to drop packets due to mobility or collisions. This can be achieved by decreasing the number of packets considered dropped each time it is perceived to correctly forward packets

After judging a node as misbehaving, the detector attempts to isolate it. Isolating a misbehaving node means:

1) Do not route packets through it, to avoid losing them, and ii) Do not forward packets for it, to punish it.

Node A that judges some other node B as misbehaving should not punish it unilaterally, but must ensure that this will be done by all nodes [9]. This is because when A unilaterally punishes B; the others could consider A as misbehaving when they realize that it does not forward packets for B. To isolate a detected node the proposed method uses a testimony-based protocol [10].

V. RESULTS AND DISCUSSION

A. Packet Delivery Ratio

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the source.

It can be defined as:

PDR=∑ Number of packet receive / ∑ Number of packet send

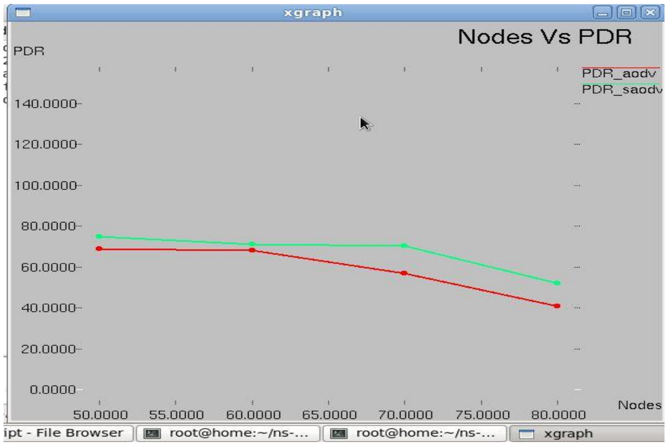

Figure 2 PDR graph of ADOV and SAODV

Figure 2. shows the impact of network density on packet delivery ratio. SAODV protocol increases the packet delivery ratio by 10% to 30% compare to conventional AODV protocol. In SAODV protocol, source node and intermediate node both verify signature before updating their routing table. A malicious node can impersonate a destination node but cannot generate signature of destination node. Similarly in proposed method, malicious node does not know the secret key shared between destination node and others node. The source node or intermediate node discards RREP packets coming from malicious node and hence does not establish route through malicious node. Therefore in proposed method the packet delivery ratio increases by almost 20% to 30% when the numbers of nodes increases with Dos attacker nodes

B. Control overhead

The number of RTR packets generated by source nodes. Figure 3 shows control overhead graph.

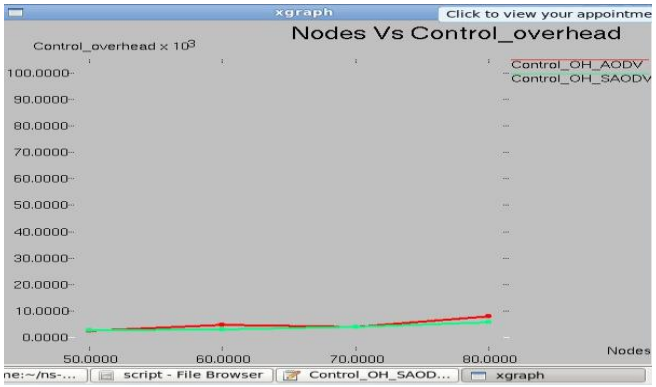

Figure 3 Control overhead graph of AODV and SAODV

C. End-to-End Delay

End-to-end Delay is the average time taken by a first control packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the packets that successfully delivered to destinations that counted.

End to End delay=∑ (arrive time – send time) / ∑ Number of connections.
The figure 4 shows end to end delay graph between AODV and SAODV.

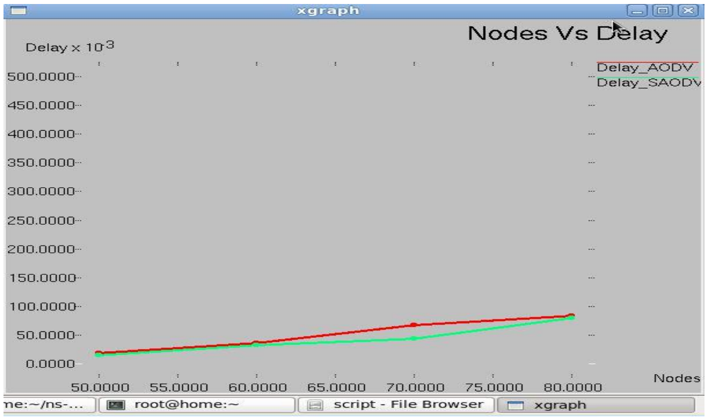

Figure 4 Delay graph of ADOV and SAODV

D. Throughput

Throughput is a measure of successful delivery of packets in a given interval of time. The graph between Throughput Vs number of mobile nodes is shown in figure 5. It depicts that as the number of nodes increases, throughput decreases, the proposed protocol SAODV increases throughput as compare to AODV by 30%.

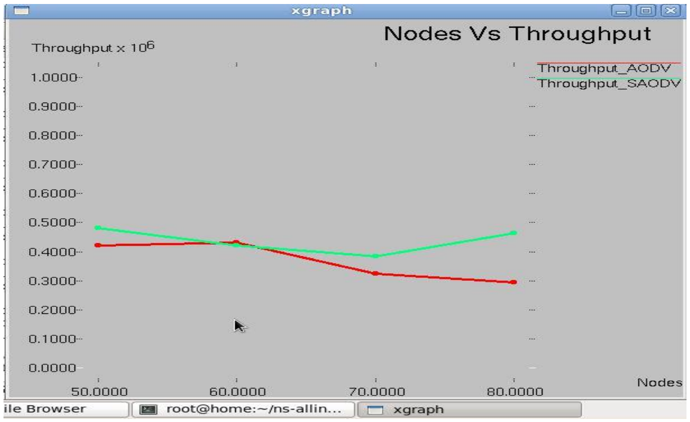

Figure 5 Throughput graph of AODV and SAODV

VI. CONCLUSIONS

Due to the inherent nature MANET is susceptible to various kinds of attacks. One of them is DoS (Denial of service) attack, who increases the packet loss, delay, more usage of bandwidth and decrease the throughput. Secure routing in MANET is a topic that attracts more and more attention amongst researchers.

Due to broadcasting of RREQ, RREP packets infinite times by the Dos attacker nodes (malicious node) other participated nodes are unable to handle other packets which are received by them. Due to the flooding of RREQ, the intermediate cannot concentrate on other activities like forwarding. In a similar manner the flooding of either control or data

Packets affect the network operation in general it result in congestion exhaustion of battery power, wastage of bandwidth and degrades the throughput.

Our proposed solution is a general solution to monitor, detect, and isolate control packet droppers. That deals with both directed and broadcast control packets. For monitoring directed control packets we use two-hop ACK approach and for broadcast control packets we use time based solution. We use a redemption strategy for judgment and a reputation based approach for isolation applicable to directed packets as well as broadcast ones. We use packet delivery ratio, control overhead, throughput and end to end delay as one of the performance metric for evaluation.

The proposed protocol increases packet delivery ratio and throughput by 10 to 30% and decreases the delay as compared to AODV protocol.

REFERENCES

[1] Soufiene djahel, farid na¨ıt-abdesselam, and zonghua zhang "mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges" ieee communications surveys & tutorials, vol. 13, no. 4, fourth quarter 2011.

[2] Bhalaji .N & Dr. Shanmugam "A Reliable Routing Against Selective Packet Drop Attack in DSR Based MANET', Journal of Software 2009.

[3] Djamel Djenouri , et al.(2007),'On Securing MANET Routing Protocol Against Control Packet Dropping', Pervasive Services, IEEE International Conference on July
2007 ,Pp: 100 - 108.

[4] Madhavi, S. and K. Duraiswamy Flooding attack aware secure AODV in Journal of Computer Science, Feb 2013 9 pp: 105-113.

[5] S. Yi, P. Naldurg, and R. Kravets." Security-aware ad hoc routing for wireless networks". In The ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC01), Long Beach, CA, October 2001.

[6] S.Marti,T.Giuli,k.Lai,and M.baker,"Mitigating routing misbehaviour in mobile ad hoc networks",proceedings of international conference on mobile computing and networking, ACM 1-58113-197-6/00 AUG 2000.

[7] Kejun Liu, Jing Deng, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs", Mobile Computing IEEE Transactions on Vol. 6, May 2007 pp- 536 - 550.

[8] K. Balakrishnan, D. Jing and V. K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad hoc Networks," in Proc. of Wireless Communications and Networking Conference (WCNC'05), vol. 4, March 2005, pp. 2137- 2142.

[9] K.Vijaya "Secure 2Ack Routing Protocol In Mobile Ad Hoc Networks," TENCON 2008, IEEE Region 10 Conference, November 2008, pp. 1-7.

[10] D. Djenouri and N. Badache. "Testimony-based isolation: New approach to overcome packet dropping attack in manet. In The 7th Postgraduate Symposium on Convergrnce (PgNet'06), John Moors University, Liverpool, UK, June 2006, pp 114-119.

[11] Ashok M. Kanthe, Dina Simunic, Ramjee Prasad "The Impact of Packet Drop Attack and Solution on Overall Performance of AODV in Mobile Ad–hoc Networks" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2249-8958, Volume-2, Issue-2, December 2012

[12] P. Swetha1, Vinod Bhupathi2 "Unmasking of packet drop attack in manet" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) ISSN: 2278-6856 Volume 2, Issue 6, December 2013.

[13] G. Acs, L. Buttyan, and I. Vajda. "Provably secure on-demand source routing in mobile ad hoc networks". IEEE Transactions on Mobile Computing, 5(11):1533- 1546, 2006

[14]P. Michiardi and R. Molva. "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks". In The 6th IFIP Communication and Multimedia Security Conference, Portoroz, Slovenia, September 2002.

[15] D. Djenouri and N. Badache. "A novel approach for selfish nodes detection in manets: Proposal and petri nets based modeling". In The 8th IEEE International Conference on Telecommunications (ConTel'05), pp 569-574, Zagreb, Croatia, June 2005.