Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security Enhancement in AODV Protocol in MANET

Arunima Saini
Student CSE Department, Kurukshetra University
Kurukshetra, Haryana, India

Abstract- Today secure communication is the primary aspect while communicating in the networks. Internet has become the primary medium for communication which is used by number of different users across the network. Black hole attacks have become a major problem to wireless systems such as MANETs. MANET is a wireless ad-hoc network that allows collaboration in real time. In the proposed work it is shown that the proposed technique of blackhole nodes detection works better than the existing AODV technique and the results are recorded against two parameters- packets received and PDR (Packet Delivery Ratio %). This technique can be deployed to large networks (more than 8 nodes) as part of the future work.

Keywords: – Blackhole attack, MANET, Misbehaving Nodes, AODV, RIP, PDR

I. INTRODUCTION

Mobile Ad hoc Networks (MANET) are the extension of the wireless networks [1] and are self-configuring and infrastructure-less. A Fixed Infrastructure Wireless network provides communication among wireless nodes not directly through the Access Point (AP). The access points also works as a bridge. In the mobile ad hoc networks, the routing protocols play a major role in order to route the data from one mobile node to another mobile node. In such mobile networks, routing protocols are vulnerable to various kinds of security attacks such as blackhole node attacks.

The routing protocols of MANET are unprotected and hence resulted into the network with the malicious mobile nodes in the network. These malicious nodes in the network basically act as attackers in the network. One such attack on mobile ad hoc network is called blackhole attack. The mobile ad hoc network means MANET is nothing but the temporary network in which the mobile nodes collected independently on other mobile nodes in the same wireless network. The mobile nodes in these networks are moving arbitrarily all over the complete network. MANET networks are basically building temporary wireless networks and they are not requiring any kind of infrastructure for deploying as well as centralized administration. The communication among these mobile nodes depends on the kind of routing mechanism used called multihop routing protocols. These routing protocols are having the functionality of forwarding the data packets from sender mobile number to the intended recipient. Every mobile node in the mobile network is operating as the both forwarding node means routing operations and host node. Thus in other words we can say that, routing protocols for the mobile ad hoc network are introduced for building the communication routes as well as wireless communication network.

A. Characteristics

1. In Wireless communication mobile nodes act as both hosts and routers.
2. There's no need of infrastructure and decentralized network.

B. Wireless Network Types

[1] In wireless networks, the infrastructure is not fixed and the nodes move freely for the purpose of communication and routing inside the network. These kinds of networks don't have routers and the wireless nodes act like routers.

A mobile Ad hoc network consists of mobile nodes that use wireless transmission for communication. In MANETs, the mobile nodes can move from one place to another and the motion of the mobile nodes may be random or periodical. The setup of these networks is very easy because these networks don't have a fixed infrastructure or a fixed topology. The setup time of the network is also very less and the routers can move freely anywhere in the network.

Mobile ad hoc networks (MANET) are widely used where there is little or no infrastructure available. A larger group of mobile devices may be formed by a number of people and later on they may split into smaller groups and so on. This property of dynamically changing network topology of MANETs makes it vulnerable for a wide range of attacks.

C. The Routing Protocols

There are several routing protocols and important of them are AODV, TORA, and DSDV etc. However, most of these MANET secure routing protocols do not provide a complete solution for all the attacks on MANET. Their assumption is that any node participating in the MANET is not selfish and it will cooperate to support different network functionalities which is not true all the times. ARAN – (Authenticated routing protocol) [2] is a solution which is a secure protocol.

1) The AODV Protocol: The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is a protocol for dynamic link conditions. In an Ad-hoc network, every node maintains a routing table, which contains information about the

various routes to a destination. The node checks with its routing table first if there is any entry for the route to the destination. If yes, then it uses that route to send the packets to the destination. If a route is not available, then the node initiates a route discovery process. A RREQ (Route REQuest) packet is broadcasted by the node in the network. The nodes which receive RREQ packets, first check if they are the destination node for that packet and if so then they send back an RREP (Route Reply) packet. If they are not the destination then the routing table is checked again to determine if there is any route to the destination. If not, the nodes relay the RREQ packet by broadcasting it to its neighbors.

Type	J	R	G	D	U	Reserved	Hop count
RREQ ID							
Destination IP Address							
Destination Sequence Number							
Originator IP Address							
Originator Sequence Number							

Fig. 1 RREQ Packet

Type	R	A	Reserved	Prefix size	Hop Count
Destination IP Address					
Destination Sequence Number					
Originator IP Address					
Life Time					

Fig. 2 RREP Packet

Type	N	Reserved	Dest Count
Unreachable Destination IP Address (1)			
Unreachable Destination Sequence Number (1)			
Additional Unreachable Destination IP Addresses (if needed)			
Additional Unreachable Destination Sequence Numbers (if needed)			

Fig. 3 RERR Packet

2. DSR Protocol Dynamic Source Routing: DSR is one of the protocols developed for routing in mobile ad-hoc networks. The working is as follows: The nodes send a ROUTE REQUEST message; nodes that receive this message put themselves into the source route and forward this message to their neighbors, unless they receive the same request before. If a receiving node has a route to the destination, it does not forward the request, and instead sends a REPLY message containing the full source route. It may send the reply along the source route in reverse order or issue a ROUTE REQUEST including the route to get back to the source, if the former is not possible because of the asymmetric links. ROUTE REPLY messages can be triggered by ROUTE REQUEST messages or are gratuitous. After receiving one or several routes, the source selects the best (by default the shortest), stores it, and sends messages along that path. The better the route metrics (number of hops, delay, bandwidth, or other criteria) and the sooner the REPLY arrives at the source, the higher the preference given to the route and the longer it will stay in the cache. When a ROUTE REPLY arrives very quickly after a ROUTE REQUEST has been sent out, this is an indication of a short path.

D. Blackhole Attack

A blackhole attack is a type of denial-of-service attack in which a router discards the packets which are meant to be relayed rather.

[3] When the packets reach this malicious node, they merely disappear, as a matter of fact, they are said to have been disappeared into a blackhole in universe. In fact, the blackhole node impersonates the destination node by sending a spoofed route reply packet to the source node that have initiated the route discovery, hence deprive the packets from the source node. A blackhole node has two properties. First, the node takes advantage of the ad hoc routing protocol, such as AODV or DSR and advertises itself as having a valid route to the destination node. Second, the node consumes the intercepted packets. This type of attack is dangerous and may cause immense harm to the network.

In the following figure 4, imagine a blackhole node B1. When node 1 broadcasts RREQ packets to the nodes 2 and 4, B1 receives it. Node B1 being a blackhole node, does not check with its routing table for the requested route to destination 5. And hence it immediately sends back an RREP packet, claiming a route to the destination node. Node 1 receives the RREP packet from B1 ahead of RREP from other nodes. Node 1 assumes that the route through node B is the shortest route and sends packets to the destination nodes through it. When the node 1 sends data to B it drops out all the data and behaves like a blackhole node.

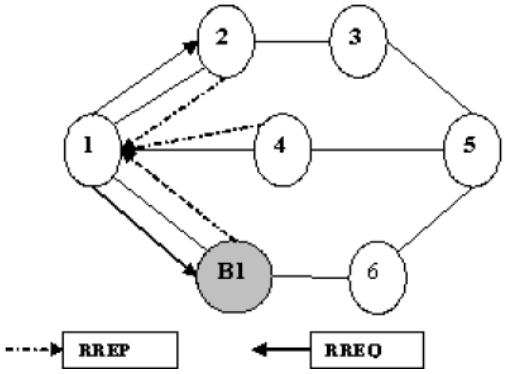

Fig. 4 Blackhole attack scenario

E. Misbehaving Nodes in MANET

Any form of disobeying the protocol specification to obtain the given goal at the expense of honest participants. A node may misbehave in order to save its resources like process time and energy. A misbehaving node will continue to perform any type of misbehavior till it gains sufficient benefits from the network [7]. Fig 5 shows the packet forwarding in a network with regular nodes and in the presence of misbehaving nodes. Misbehaving nodes can be usually classified as selfish nodes and malicious nodes. Selfish nodes are those nodes which misbehave to save their resources like power whereas malicious nodes disturb the network operations by their malicious activities. These misbehaving nodes may participate in the route discovery and route maintenance phases [5] and transmit control packets which can benefit it. However they refuse to forward data packets. Malicious nodes, on the other hand, will participate actively in both route discovery and maintenance phases and transmit the control packets since they need a path to send the data packets so that they can alter or drop those packets.

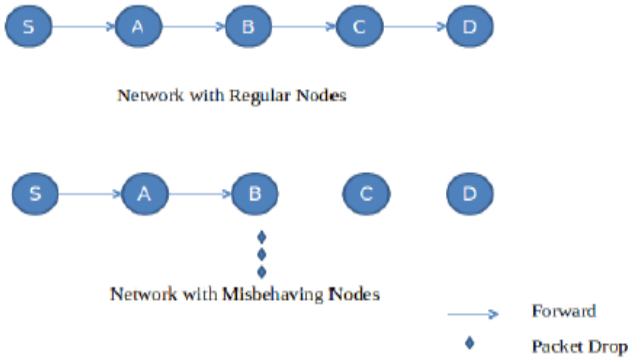

Fig. 5 Network with regular noded VS misbehaving node

II. RELATED WORK

Neelam Khemariya et al. [1]. In this research paper a secure efficient algorithm for the detection of the Black hole attack is described. This algorithm firstly identifies the black hole node in the given Mobile Ad hoc Network and then removes the entries for that node from the routing table. The algorithm is implemented in a popular reactive routing protocol, called AODV (Ad hoc On demand Distance Vector Routing). The beauty of the proposed algorithm is that it works in both the cases when there is no communication (i.e., a node is idle) and when a node is communicating (node is not idle).

R. Sudha et al. [2]. In this paper, a reputation-based scheme to be combined with one of the secure routing MANET protocols, ARAN, to make it detect and defend against selfish nodes and their misbehavior has been explained and the problem associated with it is studied and a solution to overcome it is shown. An explanation of the different phases of this scheme and analysis of the various forms of selfish attacks that this scheme defends against are studied. Temporal table is more efficient and more secure than ARAN secure routing protocol in defending against both malicious and authenticated selfish nodes.

Isaac Woungang et al. [3]. In this paper, we proposed the DBA-DSR scheme, a feasible DSR-based solution to mitigate blackhole attacks in MANETs. Simulation results showed that (1) the original DSR heavily suffers from blackhole attack in terms of network throughput and packet delivery ratio, (2) the proposed DBADSR scheme performs better than the DSR scheme in terms of network throughput rate and minimum packet loss percentage. In future, we plan to extend the proposed DBA-DSR scheme so that it can handle the case of cooperative blackhole attacks in MANETs as well.

Prashant Dewan et al. [4]. The reputation of the nodes, based on their previous relaying history, can not only be used to increase the throughput of an ad hoc network, but also to motivate nodes to cooperate. The reputation scheme improves the throughput to 65% with 40% malicious nodes, in a network where the nodes are static. The cost of this improvement is the increased number of route requests. The throughput can be further improved at the cost of extra messages, by making the nodes exchange their reputation databases using cryptographic protocols for ascertaining the credibility of the source of information and the correctness of the reputation information obtained. Quantitative models for calculating threshold values R will increase the usability of the proposed approach.

V. Giri Babu et al. [5]. In this paper we illustrated the problem of selfish replica allocation in MANETs. Our SCF+ procedure is based on the SCF technique [5]. Our work is motivated by the observation that the existing SCF technique may suffer from poor system performance, because it loses the original distance information between nodes when building the SCF tree. To cope with this limitation, we measure the degree of selfishness by considering both node distance and selfish behavior in an integrated manner. In addition, we propose a novel node levelling technique that utilizes the memory space of all connected nodes, including selfish nodes as well. In our proposed strategy, nodes prefer to allocate replicas to near, non-selfish nodes, even though faraway nodes are not necessarily selfish. An important consequence of this strategy is that risky and faraway nodes, which are likely to disconnect frequently, are effectively measured. Through a simulation, we confirm the efficacy of our strategy in terms of data accessibility, query delay, and communication cost. We are currently working on the impact of data updates and different moving patterns on our scheme. We also plan to improve the current levelling technique by considering the frequency of disconnections and/or the weighted ratio of total number of items and average of shared memory space.

Abdul Fatau et al. [6]. This paper presented a scheme that utilizes a mesh structure and alternate paths. This scheme AODVPlus can be incorporated into any ad hoc on-demand unicast routing protocol to improve reliable packet delivery in the face of node movements and route breaks. The mesh network generates multiple alternate routes without any extra overhead. Alternate routes are utilized only when data packets cannot be delivered through the primary route. Unlike in earlier works where local route repairs were not considered as important [10] for performance comparison of ad-hoc routing protocols, its importance is highlighted in this work. To improve the AODV performance there is the need for fast locally corrective mechanisms which avoid the traditional route error broadcast to trigger fresh route discovery in the event of link failure and other congestion related situations. This paper has proposed improvements using a mechanism which provides robustness to mobility and local congestion control in AODV.

Latha Tamilselvan et al. [7]. In this paper the routing security issues of MANETs, are discussed. One type of attack, the black

hole attack, which can easily be deployed against the MANET is described and a feasible solution for it in the AODV protocol is proposed. The solution is simulated using the Global Mobile Simulator and is found to achieve the required security with minimal delay & overhead.

III. PROPOSED WORK AND RESULTS

Blackhole attack is a dangerous active attack on the Mobile Ad hoc Networks. A black hole attack is performed by either a single node or combination of nodes. This attacker node is also called selfish node. In this research paper, I have proposed a blackhole detection and prevention scheme which efficiently detects and prevents the blackhole attacks in the network. The main objectives of this proposed work are to develop a scheme to detect and prevent black hole node in MANET and comparison of proposed detection technique with others. The proposed scheme works as, the source node requests one of the backbone nodes for a restricted IP address whenever the node wants to make a transmission. After confirmation of RIP (Restricted IP Address), the source node sends dummy packets to all the intermediate nodes and packet loss is checked, if it is greater than the threshold value then the node is added to the blacklist. The proposed scheme is able to detect the blackhole nodes and prevents the packet dropping in the network. The number of packets received and the Packet Delivery Ratio have been calculated to measure the efficiency of the proposed scheme.

A. Simulation Results

The following table compares the proposed scheme results with the AODV approach.

The network nodes have been simulated and following 2 parameters have been calculated-

1. Packets Received (Proposed scheme vs. AODV scheme) - The number of packets received every five seconds has been calculated and compared in both the proposed scheme and the AODV scheme.
2. PDR (Packet Delivery Ratio %) - This parameter gives the percentage of packets delivered in the proposed scheme and the AODV scheme with the passage of time.

I have analyzed the network against these two parameters. The number of packets delivered has been noted down e.g. the simulation starts at 5 seconds. It can be seen that the number of packets delivered in the proposed scheme at 5 seconds is 83 while it is 54 in AODV. It can be also seen that there is no packet drop in this scheme and hence, the proposed scheme outperforms the AODV scheme. The same process has been repeated for the packets delivered at 10, 15, 20 and 25 seconds which is shown in the below table.

Table I. Calculation of PDR from existing AODV

Simulation Time (sec)	Total Packets	Packets Received (AODV)	Packets dropped in AODV	PDR (Packet Delivery Ratio %)	Packets Received (Modified AODV)
4.99	83	54	29	34.93975904	83
9.95	161	100	61	37.88819876	161
14.95	268	158	110	41.04477612	268
19.95	354	191	163	46.04519774	354
24.95	436	227	209	47.93577982	436

B. Simulation Graphs

The simulation Graphs have been plotted against two network parameters which are Packets received and Packet Delivery Ratio. The two are shown below-

1. *Packets Received*- The packets received per unit time has been calculated. The graph has been plotted for the packets received every 5 seconds. Blue bars in the graph show the packets received in the old AODV scheme. Red bars show the packets received in the proposed scheme.
   It can be clearly seen that the proposed schemes receives more than approx 50% packets as compared to AODV scheme.

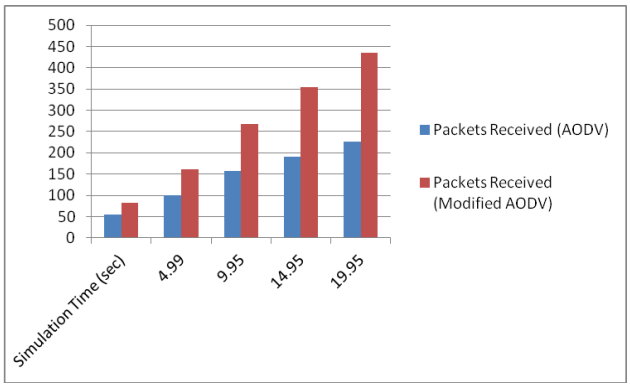

Fig. 6 Comparison of packets received in proposed and existing AODV technique

2. *PDR (Packet Delivery Ratio %)* - This parameter gives the percentage of packets delivered in the proposed scheme and the AODV scheme with the passage of time.
   The graph has been plotted showing the PDR in old AODV scheme. The PDR ranges from 35% to 48% in old AODV scheme whereas in the proposed scheme, the PDR achieved is 100%.

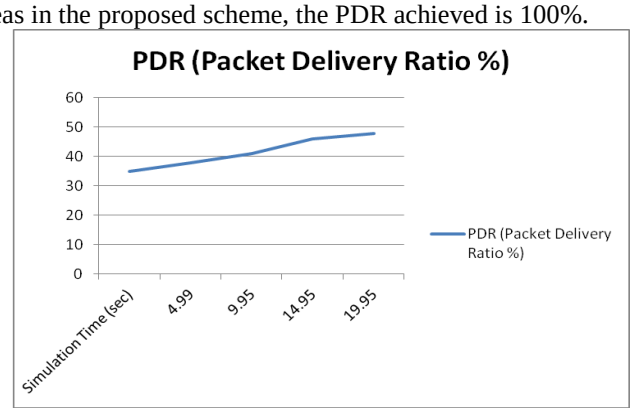

Fig. 7 Graph showing PDR of existing AODV

IV. CONCLUSION AND FUTURE WORK

A blackhole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. When the packet reaches this malicious node, the node discards that instead of relaying and hence the packet never reaches to the intended node. In this paper, comparison of the proposed detection technique with the existing AODV technique is performed. The parameters on which the results have been compared are packets received per second, packets dropped per second and PDR (Packet Delivery Ratio). The results show that the proposed technique of detecting the blackhole nodes performs better than the existing AODV technique. As part of the future work, this technique can be extended to large networks and can be measured against more performance parameters such as throughput and delay.

REFERENCES

[1] Neelam Khemariya and Ajay Khuntetha, "*An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs"* International Journal of Computer Applications (0975 – 8887) Volume 66– No.18, March 2013

[2] R. Sudha and Dr. D. Sivakumar, "*A Temporal table Authenticated Routing Protocol for Adhoc Networks"* 978-1-4577-1894-6/11/$26.00©2011 IEEE

[3] Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi, and Mohammad S. Obaidat , "*Detecting Blackhole Attacks on DS based Mobile Ad Hoc Networks"* 978-1-4673-1550-0/12/$31.00 ©2012 IEEE

[4] Prashant Dewan, Partha Dasgupta and Amiya Bhattacharya *On Using Reputations in Ad hoc Networks to Counter Malicious Nodes* Proceedings of the Tenth International Conference on Parallel and Distributed Systems (ICPADS'04) 1521-9097/04 $ 20.00 IEEE

[5] Abdul-Fatau Adam, "*Performance enhancement of AODV over DSR on demand routing protocols - aspect of packet salvaging in ADOV"* 978-1-4244-6252-0/11/$26.00 ©2011 IEEE

[6] V. Giri Babu and T. Sreenivasulu, "*Detection of Selfish Node and Replica Allocation Over MANETs"* International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 9, September 2013

[7] R. Gomathi, Sony Jose and J. Govindarajan, "*A Survey on Detection Schemes of Misbehaving Nodes in MANETs"* International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 9, September 2013

[8] Latha Tamilselvan, Dr. V Sankaranarayanan, "*Prevention of Blackhole Attack in MANET"* The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007) 0-7695-2842-2/07 $25.00 © 2007

