© 2018 IJSRST | Volume 4 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

AODV Routing Protocol to Defence Against Packet Dropping Gray Hole Attack In MANET

M. Jeevamaheswari*, R. Anandha Jothi, V. Palanisamy
Department of Computer Applications, Alagappa University, Karaikudi, Tamil Nadu, India

ABSTRACT

A Mobile Ad Hoc Network (MANET) is self-organizing multi-hop network. In general MANET is characterized by the open wireless medium and open to anyone. Due to the unique characteristics such as dynamic network topology, limited bandwidth, limited battery power and infrastructure less network environment, MANET is lacking in centralized authorization and highly vulnerable to malicious gray-hole attacks. Thus the security is a critical problem when implementing MANET. Every node in MANET is vulnerable and the good performance of the network is depends on nodes or participate path from the source to a given destination. It is very tedious to sense some attacker nodes when it becomes a part of network. Ad-hoc on-demand distance vector (AODV) protocol is a popular reactive routing protocol but exposed to well-known packet dropping attack, where a malicious node purposely drops some packets without forwarding them to destination. In this paper, we discuss the security mechanisms, namely Data routing information (DRI), and cross-checking operations to defend against packet dropping attack in MANET.

Keywords : AODV, DRI, Packet Dropping, Routing

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a collection of well-defined mobile nodes. In this network is an infrastructure less network because such network does not have any fixed infrastructure. The mobile nodes are dynamically change the topology and paths between themselves to transfer the data packets from one node to another node and it is self-organizing network, Each and every mobile nodes are acts as a host and router .when Request (REQ)/Replay (REP) information from/to in the network and route determining and preserving routes other nodes in network.

MANET is a wireless nature to make some susceptible to the security attacks. The network layer is severely affected by the security attack especially on gray-hole attack which comes belong to the security attack. such kind of network has various applications like Military , Battle fields, disaster recovery ,earthquakes, and setup virtual class & conference rooms for educational applications multi –user games, robotics pets for entertainment applications, remote weathers for sensors, earth activities for sensor network emergency relief scenario etc. Naturally the MANET has dynamically changed their behavior, in this nature easily vulnerable for extensive kind of attack. The Individualities of MANET pose together challenges and opportunities in attaining security goals. We proposed a technique to define multiple gray-hole nodes cooperative as group. In this studied work was tiny modify the AODV routing protocol and its Data Routing Information (DRI) Table in addition to the stored and present routing table.

The rest of this paper is planned as follows. In Section 2, studied some related work, Section 3, explained gray hole attack and its functionalities. Section 3, implementation of MAODV and AB-DRI table with

verification process further we present a new methodology to prevent a cooperative gray hole attack. Finally, in Section 4, we conclude and discuss future work.

II. RELATED WORK

Various researchers are estimated and implemented some solutions but the most important Aids were the trust based security. Security is a big challenging in MANET. Lot of researchers recommended various techniques and modifies the existing protocols and some researchers suggested new protocols. Hence, the overall network performance is degraded by various attacks. In this study we take well known packet dropper attack like gray hole attack.

Jayadeep sen et al. [1] studied to discover the gray-hole attack by choosing different path to the ultimate source node and to prevent hazardous attack based on alarm message techniques for avoid malicious nodes. During the packet forwarding stage some nodes are behaved irregular, it is very critical to determine and prevent in during the communication. This method was improved the security mechanism and reliability for detecting vulnerable nodes by proactively linking neighbor nodes of malevolent gray-hole node. M. Jaydip sen,et al. [1]. Proposed algorithm for detect and protect beside the network. In this studied attack which may be launched combined by a set of vulnerable nodes.in this proposed mechanism to find the gray-hole malicious node used by threshold cryptography and finally to improve the high detection rate, low False Positive Rate (FPR) and control overhead.

Sukla Banerjee et al. [2] studied the mechanism of detection and prevention of gray-hole attack in MANET. This method was improving the time consuming algorithm and the total amount of traffic was taken then apply the time into small blocks. S. Banerjee et al. [2] proposed prelude and postlude messaging methods. Before starting transaction the source node sends prelude information to the destination for aware. The flow of traffics is monitored by its neighbors. After finishing the transmission, the destination sends postlude message for covering the number of packets received [2]. Suppose the data loss is beyond the limit, high off the process of finding and eliminating all vulnerable nodes through collective response from observing node and the network.

M. Ahmed et al. [3] Studied to find the gray-hole node based on the mechanism of ID techniques with voting attribute to found the malicious node and generate difference between original and malicious node.

III. GRAY HOLE ATTACK

Grayhole attack is one of the route misbehaviour attacks. Black hole attack is an extension of grayhole attack. Such kind of attack drops some data packets this grayhole node act like a genuine node and go to contribute into full communication. The malicious grayhole attacker node participate two different phases [4]. At the first phase route discovery process the node advertises itself having right path to the destination. In the second phase update the source route cache and routing table as shortest route. Subsequently, source node continuously consider malicious node as next hope node and onward packet to same. The attacker node arrests all the received packets however drop on random basis. The whole phenomena make toughness beside.

The functionalities of the grayhole node are each incoming UDP packets are dropped partially with random collection process. This kind of attacker node can change character from genuine to sinkhole. Since it performance as an normal node change over to malicious node it develop also typical to identify the State whether it us original or malicious node

A. Gray-hole Functionalities on AODV

Generally MANET functionalities depends on routing protocols in this work we combined with ad-hoc on demand distance vector (AODV) routing protocol. The major advantage of AODV routing protocol each and every node should be maintain routing table, next hop and destination information[5]. The stored information is used to determine the route from source to destination. In addition, each and every node in a network to verify the routing table to know whether the route is exist or not. During this protocol communication, the packets are forwarded to next hop node and then destination.

The exploits of the malicious gray-hole attacker node on AODV protocol apprises the source routing table as shortest path in next nearest neighbor[6]. The aim of the malicious node is, to update the false information on routing table and distract all the packets to the malicious node rather than original route. During the implementation stage the gray-hole attack whenever malevolent node dropped the disturbed packets with a definite probability [7,8]. Packet selection process depends on probabilistic method. In some situation, malicious node alters the behaviors quickly. Therefore, the attacker node transfer and drop packets alternatively. Generally, such kind of nodes is very hard to find out in the network path because of this nature. Figure 1 depicts the gray-hole node functionalities.

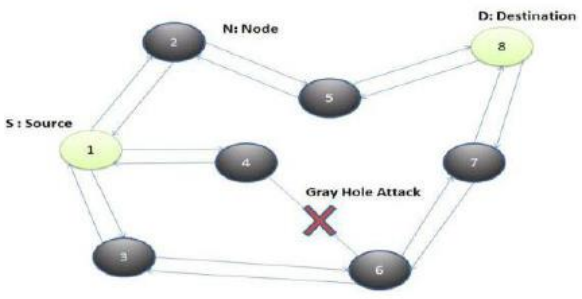

Figure 1. Gray-hole node sample on network

B. Problem investigation of AODV Routing Protocol

The AODV routing protocol is specially designed for improve the performance of the mobile network but not guarantee for security. Naturally the wireless medium is an open access to all in this nature is very easy for external attackers to interrupt the legitimate traffic. The proactive AODV Routing protocol does not integrate any other mechanism to discover and avoid communication from misbehaviours affect. In this proposed study is to detect the malicious gray-hole attacker node. Accordingly, this work combined with Data Routing Information Table (DRI) which is applied on AODV routing protocol for enhance the protection of network. The major aim of this work depends on (Association based –Data Routing Information) AB-DRI is to choosing the best and secure route further the verification mechanism is used for improve the routing security. The proposed studied techniques to detect the malicious gray-hole node.

C. AB-DRI implementation

The process of route discovery phase, the source node wants to send a route request to destination and its neighbour nodes [9]. Each node sends route replay and combined with two bit of addition information [9] to the source node. In this proposed work each node should be maintain additional AB-DRI table, in bit " 1" is denoted by true at the same time bit "0" denoted by false. The bit "from" is designates where any data packets routed from the nodes in node field. The bit "through" signifies for routing data packets through the node in the node field. The next field is a status bit. Which is updated based on the two bit entries in the AB-DRI table. Example of route maintenance for node 5 is depicts in fig.2 .The threshold value and detail of node5 shown in table 1.

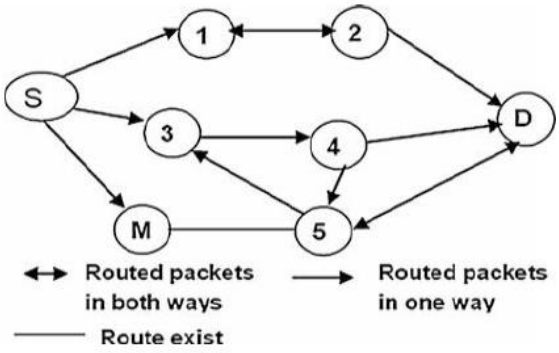

Figure 2. Sample network with gray-hole attack

Table 1. ab-dri table for sample network

Node Address	Starting From	Through	Status	Value of Threshold	Level of Trust
4	1	0	K	0.4-0.6	Medium
M	0	0	UN	0.0-0.3	Very Low
D	1	1	C	0.7-1.0	High
3	0	1	W	Inhibition mode	Low

The above mentioned Figure 2 and Table 1 show the sample network and its routing table respectively. The trust or association values are computed for each and every connected node which sends route request and response. To determine the status of all nodes and its neighbour by the trust estimation function along with fixed threshold. As shown in Figure 2 the following terms are denoted for each node.

Notation:

- Source node denoted as –S
- Destination denoted as –D
- Malicious node denoted as – M
- N1 to N5 is considered as the neighbouring node in a sample network.
- The relationship among node D and N5 has Companion relationship
- The relationship between N5 and N4 has known relationship.

The unknown relationship between in node N5 and M, node N5 and N3 set as a wait mode and it has medium trust level. Those functionalities are shown in table 1.

To detect the malicious grayhole node, each node should be maintaining an association table. The trust table is store the detail of association status for each node and its neighbour. Node 4 status bit was updated as "K" because the node route utilized at one time. Node "D" has 1, 1 entry, because node 5 has routed data packets from and through node D and the entry 0, 0 for node "M" because node 5 have not routed from and through. The status bit was updated as "UN" on the node "M". The node 5 has not routed the data packet from node 3 but at the same time Node 5 has routed through on node 3. The status bit was updated as "W" in node field 3 because it may have not got some chance to routed data packets from it or it may be new node to the network. Finally the node 3 updates the status as inhibition- mode operation.

I. ssociation Calculation Techniques

The trust value depends upon the value of association status. The following parameters are used to calculate the trust values [10, 11].

TV = tan h (A1+A2+ACK)

Where, TV= Trust Value

$$A1=\frac{\text{No .of packets forwarded successfully by neighbour node}}{\text{Total no .of packets to be forwarded by neighbour node}}$$

$$A2=\frac{\text{No.of packets received from neighbour node but originated from other node}}{\text{Total no.on packets received from that node}}$$

When the denominator is not equal to zero and (A1<1) then it can achieved selective packet drop attack. The Acknowledgement bit (ACK 0 or 1) when the destination node receives the data packet from the source. Then the nodes in that path are assigned 1 else 0 based on the TV. Trust values are assigned by the following equation. The relationships are characterized as.

1. A (node y → node z) = Companion, if T ≥ TC (the threshold trust level for a known node to become a companion of its neighbor is denoted by TC).
2. A (node y → node z) = Known, if TK ≤ T < TC A (node y → node z) = Unknown, if 0< T >TK (The threshold trust level for an unknown node to become a known to its neighbor is represented by TK).

The connections of these nodes are unequal, node y, z have not trusted, Hence the node z,y has trusted vice versa. In adhoc network, the participating nodes should be recognized its nearest neighbourhood companion done with a certain period of time by measuring their trust levels [12,13]. Certain companions nodes may be shortly turn malicious and non-cooperative due to node attractive. Finally to detect this kind of node during the data transfer cloud invokes the trust assessor for a particular interval of time and then re-establishes the level of trust. Suppose the trust value is not fulfilled, the companion node is degraded to recognize their packets and not send. The penalties for the node pay not being cooperative. Nevertheless, the node goes out to be a regretful offender that is no longer as a malicious node and then it has act as normal node for certain period, further to re-integration in to the network is passible the companion nodes threshold trust level is satisfied. In this situation, the troubled node will have to work its way up to increase its level of trust to the threshold set for a friend.

IV. VERIFICATION PROCESS

The studied method based on the nodes trust level. During the data transmission process, thru the nodes, which data packets are routed earlier by source node are recognized to be reliable [14, 15]. The proposed method was shown in figure 3.

The verification process of Intermediary Node (IN) is send the Route Replay (RREP) information gives to Next Hop Node (NHN) and updates its AB-DRI table. After received the RREP information from the IN, whether the source node checks its private AB-DRI table for verify the status bit and its IN worthy level. If the NHN status bit is “C” its indicate trustworthy; if not, the NHN is unreliable. If the NHN is reliable, the source conform the IN node is a malicious node. Suppose the status bit of IN is “UN” that node is a malicious node. If the status entry is “W” the route is not selected for routing however it sent to inhibition mode for future use. If the IN is malicious, then the source node recognize all other malicious node in the reverse path from IN to the node which has created RREP as vulnerable nodes. When a nearest adjacent node is friend node, the information transformation is completed rapidly[16,17,18]. This eliminates the overhead is raising the trust estimation among the friend node. The designed protocol will join to the AODV if all the nodes in the network are companions.

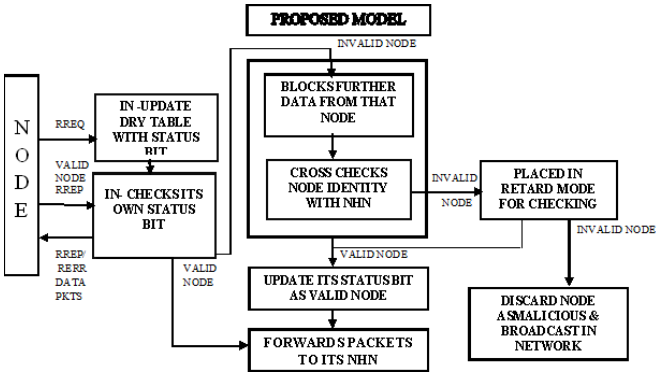

Figure 3. Schematic Block Diagram of Proposed Method

A. Algorithm for detecting Gray-Hole Attacker Node

Notations:

SN: Source Node, IN: Intermediate Node,

TN: Target Node,

NHN: Next Hop Node Reliable Node: The node through which the SN has routed data

FP: Further packet, FRq: Further request FRp: Further reply

Step 1: Source Node (SN) broadcasts RREQ

Step 2: SN receive RREP

Step 3: IF (RREP is from Friend node)

{// not verified the AB-DRI table// Routed data packets (That path is considered as secure path)}

Step 4: ELSE

DO

{SN stopped FP from IN

Send FRq and ID of IN to NHN

Receive FRp,

NHN of current NHN AB-DRI entry with Status bit for NHN next hop, AB-DRI entry with status bit for current NHN

IF (RREP is from Known node)

{//Check its AB-DRI appended trust value and choose// Routed data packets (the route is a secure route)}

If (NHN is a reliable node)

{Check IN is a packet dropping or not using status bit of AB-DRI entry & inhibition mode operation.

If (IN is not a malicious node) then Accept data packets from the source node

ELSE

{

IF (RREP from Unknown node)

{//Insecure Route//

IN is a malicious node

All nodes in the network broadcast the node as malicious}}

Else {

Current IN = NHN}

} While (IN is NOT a Companion node) college

B. Methodology of evaluation

The studied work was verified using NS-2(V-2.35) networking simulator. The simulator Provide faithful simulation results and various network protocols. The layers physical and data link layer. The proposed studied work was utilized IEEE 802.11 algorithm. The simulation setup used wireless channel combined with two ray ground radio propagation model. AODV routing protocol used the network layer. In addition, the UDP was used by transport layer. Tested and transmitted packets are continuous bit rate (CBR), and the packet size is 512 bytes. Transmission packet rate is 0.2 Mbps. The territory area is 800m X 800m per number of nodes changing from maximum to minimum of 100 to 10 respectively with select the maximum speed up to from 10 to 70 m/s. each and every data points are signifies and average of ten times. The similar connection patterns and mobile models id used in simulations to preserve the uniformity through the protocols. Table 2 depicts the simulation parameters.

Table 2. Simulation Parameters

Parameter	Value
Simulator	Ns-2(ver.2.33)
Simulation Time	100 s
Number of nodes	10 to 80
Routing Protocol	AODV
Traffic Model	CBR

Pause time	2 s
Mobility	10 - 70 m/s
Terrain area	1000m X 1000m
Transmission Range	250m
No. of malicious node	5

Table 3. Packet Delivery Ratio Of Aodv And Ab-Aodv With Attack

Number of Nodes	Packet Delivery Ratio (PDR in %)	
	AODV	MAODV
10	42	42
25	43	70
50	43	75
75	38	78
100	35	60

The PDR is organized beside the number of nodes connected in the network as shown in table 3. The maximum delivery ratio is attained among the link 50 to 75. Nevertheless, the Packet delivery ratio decreases when the maximum connection is established. Generally, the packet dropping attack is seriously affected on the original AODV. The maximum PDR is achieved by the MAODV compared with AODV.

V. CONCLUSION

In this proposed work studied on AODV routing protocol against packet dropping attack has been studied effectively. The MAODV protocol has been detect the way of packet dropping nodes in MANET and thus forwarding a secure route from source to destination nodes and then avoiding the malicious nodes. The studied experimental results have been verified using with ns-2 and compared with the AODV and AB-DRI security approach. We planned work on future for packet dropping attack with various routing protocols for security in MANET and ns-2 simulations are used.

VI. REFERENCES

[1]. Wei, L. Xiang, B. Yuebin and G. Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks", Second International Conference on Communications and Networking in China, pp. 366-370, August 2007.

[2]. P. Agrawal, R. K. Ghosh and Sajal K. Das, "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks", 2nd international conference on Ubiquitous information management and communication, pp.310-314, 2008.

[3]. S. Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", World Congress on Engineering and Computer Science, pp. 337-342 October 2008.

[4]. R. Anandha Jothi, V. Palanisamy" Various Attacks and Countermeasures in Mobile Ad Hoc Networks: A Survey" International Journal of Engineering Research & Technology (IJERT) RACMS-2014 Conference Proceedings.

[5]. R. Anandha Jothi, V. Palanisamy, "Trust Based Association Estimation Technique on AODV Protocol against Packet Droppers in MANET", International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.55 (2015).

[6]. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-demand Distance Vector (AODV) Routing," IETF RFC3561, July 2003.

[7]. A. M. P. M. (2009). Trust Based Secure Routing in AODV Routing Protocol. Information Sciences, 0-5.

[8]. Choi, Kim, Lee and Jung. WAP: Attack Prevention Algorithm in Mobile Ad Hoc Networks. IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, June 2008 250.

[9]. Jaydip Sen, M.Girish Chandra, Harihara S.G. "A Mechanism For Detection Of Gray Hole Attack

in Mobile Ad Hoc Networks" published in IEEE Journal in 2007.

[10]. Parineet D. Shukla, Ashok M. Kanthe, Dina Simunic "An Analytical Approach for etection of Gray Hole Attack in Mobile Ad-hoc Network (MANET)" published in IEEE 2014.

[11]. G.Usha and Dr.S.Bose "Impact of Gray Hole Attack on Adhoc networks" published in IEEE Journal 2014.

[12]. M. Zeshan, S.A. Khan, et al., Adding security against packet dropping attack in mobile ad hoc networks, in Proceedings of ACM International Seminar on Future Information Technology and Management Engineering (FITME, 2008).

[13]. J. Sen, G. Chandra, P. Balamuralidhar, et al., A distributed protocol for detection of packet dropping attack in mobile ad hoc networks, in Proceedings of IEEE International conference on Telecommunication (2007).

[14]. S. Djahel, F. Nait-abdesselam, Z. Zhan, Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges, in IEEE Communications Survey and Tutorials (IEEE,2010).