I. J. Computer Network and Information Security, **2016, 5, 55-62**
Published Online May 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2016.05.08

Addressing Packet Forwarding Misbehavior with Two Phase Security Scheme for AODV-based MANETs

Ankit D. Patel
Dept. of Computer Engineering & Information Technology, SVM Institute of Technology, Bharuch-392001, India
E-mail: ankitpatel.bharuch@gmail.com

Rutvij H. Jhaveri
Dept. of Computer Engineering, SVM Institute of Technology, Bharuch-392001, India
E-mail: rhj_svmit@yahoo.com

Abstract—One of the important issues related to MANETs is the security. Grayhole attack is one of the most prominent attacks on the network layer of MANET which tends to degrade the network performance by performing selective packet dropping. In this paper, we propose a security mechanism that tends to mitigate the Grayhole attack during the route discovery time as well as during data transmission time. We modify AODV protocol such that it can avoid Grayhole attacker node from participating in the data transmission route, and if the attacker node somehow enters the route, it can be detected through the promiscuous mode monitoring.

Index Terms—MANET, AODV, dual security, Grayhole attack, promiscuous mode monitoring.

I. Introduction

MANET is an ad-hoc network in which all the nodes come together and communicate to each other without the need for any centralized infrastructure [1]. The communication between the mobile nodes is facilitated via wireless multihop links [2].Moreover MANETs posses dynamic topology: every node is free to enter and leave the network and move anywhere within the network. [1]. As MANET is bound with such characteristics, it finds its use in variety of applications such as military communication by soldiers, emergency management schemes etc [3].

As there is no centralized entity, each node in the MANET acts as a router [1]. If the sender and the receiver appear to be in the communication range of each other, then only they can communicate with each other directly otherwise they have to communicate with each via the intermediate nodes between them [4]. Thus the routing work in the mobile ad-hoc network is accomplished by the nodes taking part in the route between the source and the destination.

Due to the inherent characteristics of MANET, it faces many issues. The most important issue of concern is the security [3]. MANETs are prone to variety of security attacks [5]. The major threat towards the mobile ad-hoc network is the Denial of Service attack. Denial of Service attacks fall under the category of the active attacks and they tend to degrade the performance of the network by sending false messages [4]. The important attacks that fall under the category of the Denial of Service attack are the Blackhole and the Grayhole attacks [1]. In this paper we present a solution for the detection of these attacks during the route discovery phase as well as during the data transmission phase: hence providing the security during the two phases of network operation.

Our solution for the mitigation of the Grayhole attack consists of two stages: 1) The Route Discovery Phase detection stage and 2) The Data Transmission Phase Detection stage. If the attacker node misbehaves maliciously during the route discovery stage by sending fake destination sequence number, then our solution will detect it. And If the attacker node behaves genuinely during the route discovery stage and once after getting place in the route starts acting maliciously by dropping data packets and not forwarding them, then also such an attacker would be detected in the data transmission phase mechanism.

The remainder of the paper is organized as follows: Section 2 describes the routing process in MANET. Section 3 describes the operation of the Grayhole attack. Then in Section 4 we discuss the related work. Section 5 presents the detailed description of out proposed method. Then in Section 6 we present the result analysis based on the simulation results obtained. Then finally in Section 7 we present the Conclusion of the work.

II. Routing in Manet

The main objective of the routing protocol in MANET is to establish an optimal path between the source and the destination which can facilitate smooth communication between them [6]. In MANET, the routing protocols are classified as table driven or on-demand routing protocols [7]. Table driven protocols are known proactive protocols [4]. In proactive protocols, the routes are established in advance to the requirement of the route between the source and the destination. Proactive protocols involve

the continuous updating of the routing information in the routing table. Examples of proactive protocols are DSDV, OLSR etc. Proactive protocols require a large amount of bandwidth due to high amount of information [4]. On-demand Routing protocols are known as reactive routing protocols [6]. These protocols are initiated by the source and the routes are created only when they are needed by the source [7]. These protocols do not maintain the routes in advance. In fact they establish the path when it is required. Reactive routing protocols consume less bandwidth but they require high route discovery time and the packet flooding can give rise to congestion in the network [4]. Examples of On-demand routing protocols are DSR, AODV [4],[6],[7]. In this paper we primarily focus on the mitigation of the Grayhole attack in the AODV routing protocol.

In AODV routing protocol, nodes forming the MANET do not rely on any active paths nor do they periodically exchange any routing information [8]. AODV protocol is the mixture of the DSDV and the DSR routing protocols [9]. In AODV, when the source node wants to communicate with the destination, the source node broadcasts the Route Request (RREQ) packet in the network [10]. Upon receiving the RREQ packet, the intermediate node will reply with the Route Reply (RREP) packet if it has a route to the destination or else it will again broadcast the RREQ packet further. The RREQ packet is broadcasted further till it reaches the destination. When the destination node receives the RREQ packet, it generates the RREP packet and unicast it through the particular path until it reaches the source. When the source node receives the RREP it establishes the route and forward the data packets through that route towards the destination.

There are three types of control messages in AODV which are discussed below [8].

A. Route Request Message (RREQ)

Whenever the source node wants to communication with the destination node, it initiates the route discovery procedure by broadcasting the RREQ packet to its neighbors in the network [8]. The neighboring node will reply with the RREP packet if it is the destination or if it has a route towards the destination otherwise it will forward the packet further to its neighbors [1]. This process continues until the RREQ packet reaches the destination.

B. Route Reply Message (RREP)

RREP packet is generated whenever the destination receives the route request or whenever any intermediate node has a fresh enough route towards the destination. This RREP packet is traversed in the reverse direction towards the source [8]. Whenever source node receives the RREP packet, the source node may start forwarding the data packets through the route just established [1].

C. Route Error Message (RERR)

When the node detects a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is down [8].

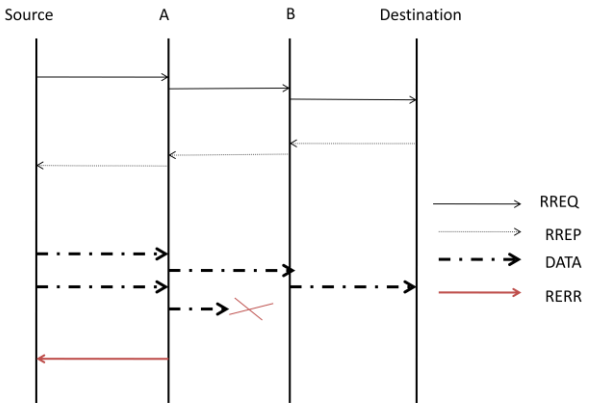

Fig.1. Working of AODV Protocol

As shown in Fig. 1, Source node wants to transmit data to destination node. So it initiates the route discovery procedure by sending RREQ packet to its neighbour A. Node A forwards the RREQ packet further to node B and node B forwards the RREQ packet to the destination. The Destination node then sends the RREP packet in the reverse direction towards the source. Once the source node receives the RREP packets, it transmits the data packets. Anytime the link damage is observed, the node generates the RERR packet and sends to the source. The source after receiving the RERR packet reinitiates the route discovery procedure.

AODV protocol makes the use of sequence numbers to indicate the freshness of the route. The destination sequence number is an integer value that depicts how fresh the route is [11]. This sequence number value is updated when the node generates the RREQ or the RREP packet [1]. Higher is the value of the sequence number, higher is the freshness of the route.

III. GRAYHOLE ATTACK

Grayhole attack is an extension of Blackhole attack [4]. In Grayhole Attack, the attacker may behave as a normal legitimate node during some time duration and may drop the packets during some duration [1]. Thus the Grayhole attacker can act as a slow poison which can degrade the network performance [12].

There are three types of Grayhole attack possible [4]. In the first approach, the Grayhole attacker nodes forwards the packets that are sent by certain nodes and it drops the packets that are sent by other nodes. In the second approach, the attacker node behave as normal legitimate node for a particular time duration and later for some other time duration it may behave as a malicious node and drop the packets. In the third approach, the Grayhole attack acquires the properties of both the method approaches i.e. it forwards the packets of certain nodes and also acts normally for particular time duration.

Fig. 2 shows the network scenario where S is the Source node and D is the destination and M is the malicious Grayhole node. At time slot T1, the Grayhole

node behaves as an original legitimate node. The Grayhole node M forwards all the packets during this time slot.

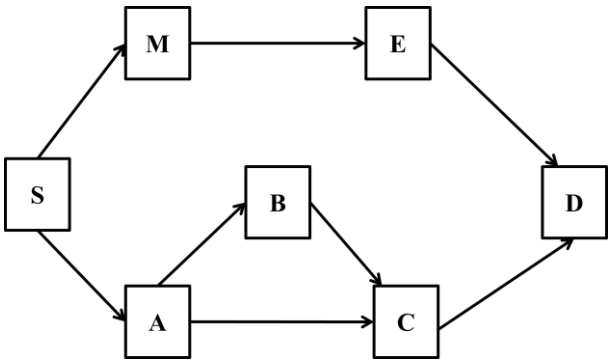

Fig.2. Grayhole Attack at Time Slot T1

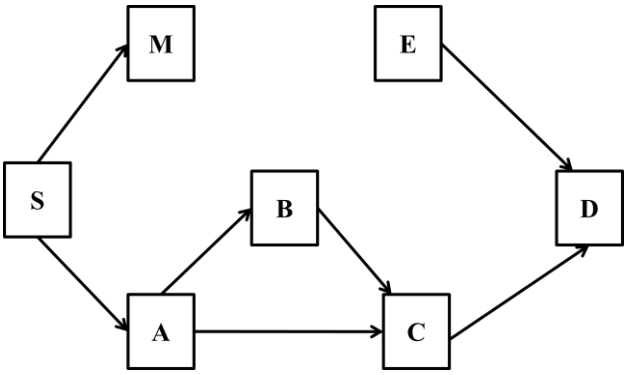

Fig.3. Grayhole Attack at Time Slot T2

Fig. 3 shows the operation of the same network as in Fig. 2 for time slot T2. For this time slot, the malicious Grayhole node M starts acting maliciously and it does not forward the packets and drops them.

Thus due to this unexpected behavior of the Grayhole attacker, it is very difficult to detect such node [1]. Thus the Grayhole node acts like a slow poison in the network because the probability at which the Grayhole node changes its behaviour is highly uncertain [12]. Thus such an attack can degrade the network performance to a high limit.

IV. Related Work

The following research works have been surveyed to discover their limitations and derive the proposed scheme.

Rutvij et. al in [2][3] proposed a solution which makes use of the calculation of the peak value for the selection of the route during the route discovery process. In this process, the node receiving the RREP packet calculates the peak value based on certain parameters. If the destination sequence number in the RREP packet exceeds the peak value, then that RREP is considered as DO_NOT_CONSIDER RREP. This DO_NOT_CONSIDER RREP is then forwarded in the reverse direction towards the source. The Source on receiving the DO_NOT_CONSIDER RREP ignores that RREP and hence the malicious node is prevented from getting into the route. This approach works fine during the route discovery time, but if the attacker node behaves normally during the route discovery time and behaves maliciously during data transmission, then this approach fails to detect it.

Ankit et. al in [13] proposed a method which detects the attacker node during route discovery phase as well as during the data transmission phase. In this method, the node receiving the RREP packet computes the threshold value and if the destination sequence number exceeds the threshold value, then that RREP is not considered. During the data transmission phase, the node sending or forwarding the packets monitors the neighbouring node in the promiscuous mode. In the promiscuous mode, the node computes the difference between the packets forwarded and received. If the difference exceeds the threshold value then the neighbouring node is considered to be the malicious node and an ALARM packet is transferred in the network revealing the identity of the malicious node in the network.

Rutvij in [14] proposed the approach of peak value calculation same as in [2][3]. In this method if the destination sequence number in the RREP packet extends the peak value, then that RREP is not marked as DO_NOT_CONSIDER and the node receiving that RREP is simply ignored. Thus there is no need to send the DO_NOT_CONSIDER RREP to the source. This method also has the limitation of detecting attacker node behaving maliciously only during the data transmission phase.

Gundeep et. al in [15] proposed the method of detecting the Grayhole nodes by making the use of Extended Data Routing Information (EDRI) tables. In this method every nodes keeps an EDRI table which keeps the history regarding the number of packets sent and received by the neighboring nodes. The nodes in the MANET compare the EDRI entry of its neighboring node and the EDRI entry of the neighbor of the neighbouring node in the route. If both the entries do not match then the neighbouring node is considered to be malicious node. This approach induces the increase in the delay and the routing overhead.

Ankit et. al in [16] proposed advancement in the method proposed in [15]. This method makes the use of I-EDRI tables. I-EDRI table contains the decimal count of the number of packets received and sent to the neighbouring node whereas the EDRI entry contains the binary count which does not indicate multiple data packet transfer. This method also faces the limitation of the increased delay and routing overhead.

Payal et. al in [17] proposed DPRAODV method to mitigate the Blackhole attack. In this method, the node receiving the RREP packets compares the destination sequence number in the RREP packet with the threshold value. The threshold value is updated dynamically using different parameters. This approach faces increase in the average end to end delay and normalized routing overhead.

Nital et. al in [11] proposed a method in which the source node after receiving the RREP packet waits for a

particular time interval and all the RREP's received in that time interval are stored in a table at that node. The sources after storing all the RREP's analyzes them and the RREP's having very high sequence number are ignored by the source node. This approach increases the delay and it also follows heuristic approach in the selection of the time interval for the source node to wait.

Chen et. al in [18] proposed an approach which comprised of three algorithms: Creating Proof, Check-Up Algorithm and Diagnosis algorithm,. The node sending the packet computes the hash function on that packet. The node receiving the packet computes the hash value again and if they match then there is no issue, otherwise there is a malicious node present. This method results in the increase in the average end to end delay because the node spends some time in computing the hash value for each packet sent and received.

Sukla et. al in [19] proposed the approach which takes into account the prelude and postlude messages. The source node before sending the data divides the data into blocks. The source node sends the prelude message to the destination before sending the blocks of data. After receiving the prelude message the destination node maintains a timer and counts the number of the data blocks received. After timeout interval, the destination node sends the postlude message which contains the number of blocks received. If the count match then there is no attacker node otherwise a malicious node is present. The pr-elude and the postlude messages increase the delay and the routing overhead.

Disha et. al in [20] proposed the Course Based Detection Method. In this approach, every node monitors the neighbouring node. Every node maintains a buffer. The node sending the packet keeps the copy of the packet in the buffer and then it overhears the neighbouring node, When the neighbouring node forwards the packet, the than packet is deleted from the buffer. Source node then calculates the overhear rate and if it exceeds the threshold then the neighbouring node is the malicious node. This approach needs some extra space for buffer and computations require time.

Jaydip et. al in [21] proposed a method of Grayhole detection which makes the use of DRI table and a probe packet. This approach makes the use of the local as well as co-operative detection of the Grayhole Attack. In this approach every node maintains a DRI table and stores the history about the packets transmitted to the neighbors in the form of binary numbers. Whenever IN node wants to initiates the detection procedure, it appoints the CN node which is the trusted node. The IN nodes broadcasts the RREQ packet to its neighbouring node and requests for a node to CN node. It then sends the probe packet to the CN node for enquiring about which node has sent the RREQ packet. If CN's node reply is affirmative then there is no attacker else an attacker node is present in the route.

V. Proposed Work

Our approach focuses on the detection of the Grayhole attacker node during the Route discovery Phase as well as during the Data Transmission Phase as shown in [13]. Hence we tend to provide a solution which tends to detect the misbehaving malicious node.

A. Route Discovery Phase

In AODV, the selection of a route largely depends upon the sequence number of the received RREP packet [22]. Therefore, our approach during the Route Discovery Phase focuses on the destination sequence number in the RREP packet. When a node in the network receives the RREP packet, it calculates a Threshold value. The Threshold value is calculated on the basis of the three parameters: Routing Table Sequence number, Number of RREQ's received and the number of RREP's received.

$$TH = RQ_{COUNT} + RP_{COUNT} + RT_{SNO} \quad (1)$$

where

TH represents the Threshold Value.

RQ_{COUNT} Represents count of the RREQ packets
RP_{COUNT} Represents count of the RREP packets
RT_{SNO} Represents the sequence number of the node in the routing table

When the intermediate node receives the RREP packet, it computes the threshold value as calculated in (1). If the destination sequence number in the RREP packet is greater than the calculated threshold value, then the intermediate node does not consider that RREP and simply ignores that packet. Hence the RREP having the destination sequence number greater than the Threshold value is sent by the malicious node. Hence that RREP is ignored and is not considered for the route formation. Hence the Grayhole node acting maliciously during the Route Discovery time can be avoided from getting into the route.

B. Data Transmission Phase

Suppose the Grayhole attacker node behaves normally during the route discovery time i.e. the Grayhole node does not send a high destination sequence number in the RREP packet. If such attacker node becomes the part of the route then it may drop the data packets. In such situations, only route discovery mechanism will not work: hence we need to switch over to the data transmission security mechanisms.

In our approach during the data transmission phase every node will monitor the neighbouring node in the route in the promiscuous mode. Every node will maintain the count of the number of packets forwarded to the neighbouring node in the route as shown in (2).

$$FR_{COUNT} = \sum_{k=0}^{n} D_K \quad (2)$$

Where

FR_{COUNT} is the count of data packets forwarded
D represents the Data Packets.

Similarly the monitoring node will receive the packets forwarded by the neighbouring node to its neighbouring node as shown in (3).

$$RR_{COUNT} = \sum_{k=0}^{n} RD_K \quad (3)$$

Where

RR_{COUNT} is the count of data packets received in promiscuous mode.

D is the data packets in promiscuous mode.

Now the monitoring node will calculate the difference between the numbers of the packets forwarded and received and if the difference between the two exceeds the threshold value then the neighbouring node can be considered as the malicious node. The threshold value in our approach is kept 5%.

Once the monitoring node detects the malicious node, then it adds the ID of the malicious node to the Blacklist and it stops transmitting the data to the neighbouring node which results in the new route discovery process.

In Future, when the neighbouring node receives the RREP packet, it checks the ID of the node sending the RREP packet in the Blacklist. If the entry in the Blacklist is found, then that RREP packet is discarded by the monitoring node. Hence in this way the malicious node is avoided from coming into the route.

C. Algorithm

Node receiving the RREQ Packet

Step 1: Node receives the RREQ Packet.
Step 2: Increment the RREQ count for the source entry in the routing table.
Step 3: Generate the RREP or broadcast the RREQ further.

Node receiving the RREP Packet

Step 1: Receive the RREP packet.
Step 2: If (RREP_NODE_ID present in Blacklist) Ignore the RREP.
Step 3: Increment the RREP count for the destination entry in the routing table.
Step 4: Calculate the threshold value as follows:

$$TH = RQ_{COUNT} + RP_{COUNT} + RT_{SNO}$$

Step 5: If(Destination_Seq_no > Threshold)

Ignore the RREP packet
Else
Forward the RREP packet

Step 6: Follow Steps 1 to 4 when any RREP packet arrives.

Node Transmitting the Data

Step 1: All nodes in the route enter in the promiscuous mode and monitor their neighbours.
Step 2: Node receives the data packet and then increments the FR_COUNT and then forward the data packet.
Step 3: The node forwarding the data packet monitors its neighbouring node.
Step 4: If neighbouring node forwards the packet Increment the RR_COUNT;
Step 5: After fixed time intervals compute % difference

$$\%Diff = ((FR_{COUNT} - RR_{COUNT})/FR\_COUNT) * 100$$

Step 6: If (% Diff > 5)

Begin
Abort the data transmission.
Neighbouring node is malicious node.
Add the neighbouring node in the blacklist
Reinitiate the route discovery process and avoiding the nodes present in blacklist from coming in the route.
End If

VI. Simulation Results

We carried out our simulations in NS-2 (ver. 2.34) simulator in the Ubuntu environment.

A. Experimental Setup

The simulations are carried out by implementing two protocols. We implemented GRAYHOLEAODV protocol to implement the Grayhole attack and we implemented THAODV to mitigate the Grayhole attack. The experimental parameters are listed in the below table.

Table 1. Experimental Parameters.

Parameter	Value
Terrain Area	800 m x 600 m
Simulation Time	200 seconds
MAC	802.11
Application Traffic	CBR (UDP)
Routing Protocols	AODV
Transmission Range	250 m
Pause Time	2 seconds
Number of Nodes	10 to 50
Number of Sources	1 to 5
Number of Attackers	1 to 5

B. Result Analysis

PACKET DELIVERY RATIO

Packet Delivery Ratio (PDR) is defined as ratio between the numbers of packets received by destination to the number of packets originated from source [14]. The Grayhole attack mainly focuses on reducing the Packet Delivery Ratio by dropping the packets. We evaluate the Packet Delivery Ratio (PDR) by varying the network size

from 10 nodes to 50 nodes and keeping the mobility speed of 30 m/s and by having 1 source in the network. From the Fig.4, we can conclude that the performance of the AODV protocol in the presence of the Grayhole attack is very low as compared to the performance of the standard AODV protocol. Moreover with the increase in the number of nodes, the PDR slightly decreases. While on the other hand, as shown in Fig. 4, TH.AODV (Threshold AODV) produces the results similar to that of the standard AODV in the presence of the Grayhole attacker node. Thus TH.AODV produces the Packet Delivery Ratio (PDR) which is almost similar to the PDR produced by the standard AODV protocol without any attack.

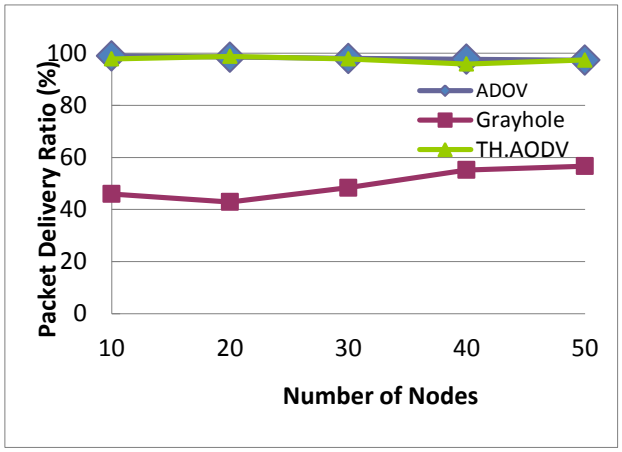

Fig.4. Effect of Network size on Packet Delivery Ratio

AVERAGE END-TO-END DELAY

The difference in the time it takes for a sent packet to reach the destination. It includes all the delays, in the source and each intermediate host, caused by the routing discovery, queuing at the interface queue etc [17]. We now evaluate the Average End to End delay by varying the network size from 10 nodes to 50 nodes having the mobility speed of 30 m/s and the number of sources are equal to 1. The delay would be caused due to the calculation of the threshold value and the calculation of the percentage difference between the number of packets sent and the number of packets received in the promiscuous mode. The results for the average end to end delay are represented in Fig. 5.

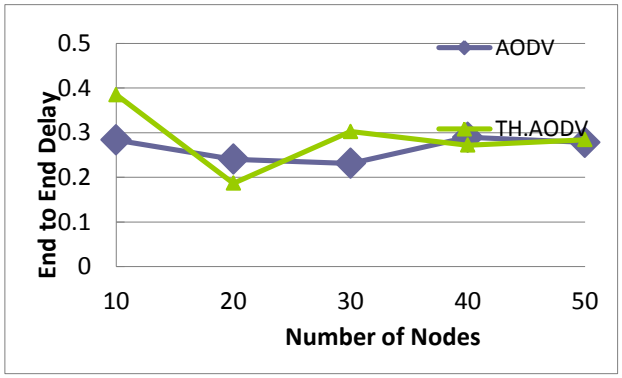

Fig.5. Effect of Network Size on Average End-to-End Delay

As shown in fig 5, we can conclude that the delay of the TH.AODV (Threshold AODV) is little bit high as compared to the standard AODV but this slight increment can be neglected with getting the benefits of the Packet Delivery Ratio similar to that of the Standard AODV. The average end-to-end delay can be considered in the acceptable range of the standard AODV protocol.

ROUTING OVERHEAD

This is the ratio of routing-related transmissions (RREQ, RREP, RERR etc) to data transmissions in a simulation. A transmission is one node either sending or forwarding a packet. Either way, the routing load per unit data successfully delivered to the destination.

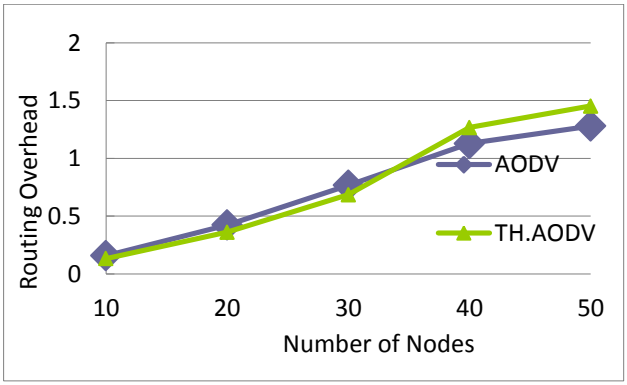

Fig.6. Effect of Network Size on Routing Overhead

From fig 6, we can conclude that the routing overhead in the TH.AODV protocol produces almost the same results as that of the standard AODV protocol. The routing overhead in our approach increases when the network size exceeds 40 nodes compared to the standard AODV protocol.

PACKET DELIVERY RATIO UNDER MULTIPLE MALICIOUS NODES

Here we calculate the Packet Delivery Ratio of the network having multiple attacker nodes.

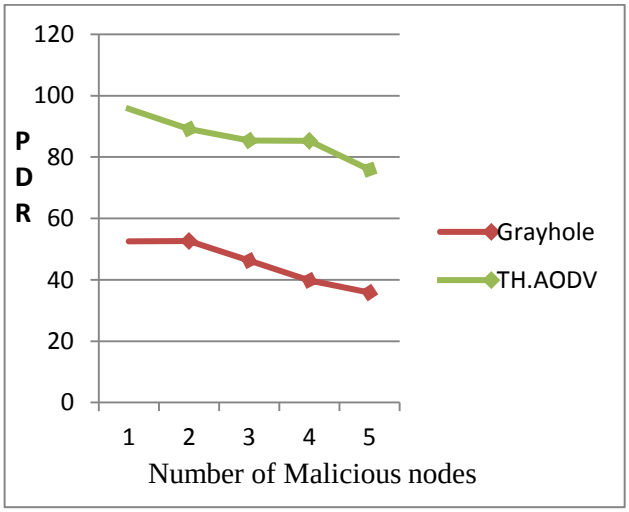

Fig.7. Effect of number of malicious nodes on Packet Delivery Ratio

Fig. 7 shows the graph of the Packet Delivery Ratio v/s the number of malicious node with the mobility speed of 30m/s and 10 nodes network. The graph shows that the packet delivery ratio under the Grayhole attack is in the range of 35 to 55 %. Whereas on the other hand, the Packet Delivery Ratio of our solution TH.AODV under Grayhole attack falls in the range of 75 to 95 %. Thus our approach gives the better performance against the Grayhole attack. The graph shows that as the number of malicious nodes increases, the packet delivery ratio tends to decrease a little bit.

VII. Conclusion And Future Scope

In our work, we have described the operation of the Grayhole attack. We have also discussed the harms that would be caused by the Grayhole attack in MANET. Our proposed approach tends to provide the security during the route discovery phase as well as during the data transmission phase. Thus the attacker misbehaving at any of the phase gets detected by our approach. The results obtained are in the acceptable range of the AODV protocol.

The future scope includes the calculation of the threshold value dynamically during the data transmission.

References

[1] Ankit D. Patel, Kartik Chawda, "Blackhole and Grayhole Attacks in MANET", Interna-tional Conference on Information Communication & Embedded Systems (ICICES 2014), IEEE, 2014.

[2] Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala, "Improving Route Discovery for AODV to prevent Blackhole and Grayhole Attacks in MANETs.", INFOCOMP, Version 11, No. 1, p. 01-02, March 2012.

[3] Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala, "A novel approach for Grayhole and Blackhole Attack in Mobile Adhoc Networks.", Second International Conference on Advanced Computing & Communication Technologies, IEEE, 2012.

[4] Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala, "DoS attacks in Mobile Adhoc Networks: A Survey", Second International Conference on Advanced Computing & communication Technologies, IEEE, 2012.

[5] Ankit D. Patel, "Denial of Service attacks in MANET", National Conference on Emerging Vistas of Technology (NCEVT-13), PIET, May 2013.

[6] Preetam Suman, Dhananjay Bisen, Poonam Tomar, Vikas Sejwar, Rajesh Shukla, "Comparative study of Routing Protocols for Mobile Ad-Hoc Networks", November 2009.

[7] Su Mon Bo, Hannan Xiao, Aderemi Adereti, James A. Malcolm and Bruce Christianson, "A Performance Comparison of Wireless Ad Hoc Network Routing Protocols under Security Attack", Third International Symposium on Information Assurance and Security, IEEE 2007.

[8] Charles E. Perkins, Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector Routing".

[9] Vahid Nazari Talooki, Koorush Ziarati, "Performance Comparison of Routing Protocols For Mobile Ad Hoc Networks", IEEE, 2006.

[10] Thomas Clausen, "Comparative Study of Routing Protocols for Mobile Ad-hoc Networks", Unité de recherche INRIA Rocquencourt Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le ChesnayCedex (France).

[11] Nital Mistry, Devesh C. Jinwala and MukeshZaveri, "Improving AODV Protocol against Blackhole Attacks", International Multiconference of Engineers and Computer Scientists 2010, vol. 2, March 2010.

[12] Meenakshi Patel, Sanjay Sharma, "Detection of Malicious Attack in MANET A Behavioral Approach", 3rd IEEE International Advance Computing Conference (IACC), IEEE, 2013.

[13] Ankit D. Patel, Kartik Chawda, "Dual Security against Grayhole attack in MANET", Advances in Intelligent Systems and Computing, Springer, 2014.

[14] Rutvij H. Jhaveri, "MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs ", Third International Conference on Advanced Computing & Communication Technologies, IEEE, 2013.

[15] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agarwal, "Detection and Removal of Co-operative Blackhole and Grayhole attacks in MANET's ", International Conference on System Engineering and Technology, IEEE, 2012.

[16] Ankit D. Patel, Rutvij Jhaveri, Shaishav Shah, "I-EDRI scheme to mitigate Grayhole attack in MANET", Advances in Intelligent Systems and Computing, Springer, 2014.

[17] Payal N. Raj and Prashant B. Swadas "DPRAODV: A Dynamic Learning System against Blackhole attack in AODV based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[18] Chen Wei, Long Xiang, Bai Yubein, Gao Xiaopeng, " A new solution for resisting Grayhole Attack in Mobile Adhoc Networks.", IEEE, 2007.

[19] Sukla Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", Proceedings of the World Congress on Engineering and Computer Science 2008, WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[20] Disha G. Kariya, Atul B. Kathole, Sapna R. Heda, "Detecting Black and Gray Hole Attacks in Mobile Ad-hoc Network Using an Adaptive Method,", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 1, January 2012.

[21] Jaydip Sen, M. Girish Chandra, Harihara S.G. , Harish Reddy, P. Balamuralidhar, " A mechanism for Detection of Grayhole Attack in Mobile Adhoc Networks.", IEEE, 2007.

[22] Rutvij H. Jhaveri, Narendra M. Patel, "Mobile Ad-hoc Networking with AODV: A Review", International Journal of Next-Generation Computing, 6(3):165-191, November 2015.

Authors' Profiles

Ankit D. Patel is working as an Assistant Professor in Computer Engineering and Information Technology Department in SVM Institute of Technology, Bharuch, India, affiliated to Gujarat Technology University. He has completed his Master's degree in Computer Engineering from Parul Institute of Engineering and Technology, Vadodara. He has completed his Bachelor of Engineering in Information Technology from Sarvajanik college of Engineering and Technology, Surat.

He serves as a program committee member/reviewer in renowned International conferences. He authored several papers published by prominent publishers such as IEEE, Springer. He is a life member of ISTE. His research interests include mobile ad-hoc networks and information security.

Rutvij H. Jhaveri is a Ph.D. scholar in the Department of Computer Engineering, CSPIT, CHARUSAT University, Changa, India. He has completed his Master's degree in Computer Engineering from Saradar Vallabhbhai National Institute of Technology, Surat and Bachelor of Engineering from Birla Vishvakarma Mahavidyalaya, V.V.Nagar in India. Since 2002, he is working as an Assistant Professor in SVM Institute of Technology, Bharuch, India affiliated to Gujarat Technological University.

He serves as a reviewer in high quality journals such as Wireless Networks (Springer), Computer Journal (Oxford), Journal of Internet Technology and other reputed journal. He also serves as a program committee member/reviewer in renowned International conferences. He is an editorial board member in OMICS journal(s). He authored several papers/book-chapter(s) published by prominent publishers such as Springer, Elsevier, IET, IEEE and Perpetual Innovation. Some of these articles are published in renowned international journals such as Wireless Networks (Springer), International Journal of Next-Generation Computing and INFOCOMP Journal of Computer Science. He is also a member of various technical organizations such as ISTE, IDES, IACSIT, ICST and others. His papers have received 335+ peer citations as of January, 2016. His research interests include issues and challenges in wireless ad-hoc networks and information security.

How to cite this paper: Ankit D. Patel, Rutvij H. Jhaveri,"Addressing Packet Forwarding Misbehavior with Two Phase Security Scheme for AODV-based MANETs", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.5, pp.55-62, 2016.DOI: 10.5815/ijcnis.2016.05.08

