Volume-4, Issue-5, May Special Issue-2015 • ISSN No 2277 - 8160

Research Paper Engineering

Mitigation of Grayhole Attacks in MANET using Baiting Process and Reverse Tracing Mechanism

I.J.Jenifhar Jolla KCG College of Technology, Chennai, TN, India

R.Dhanalakshmi KCG College of Technology, Chennai, TN, India

ABSTRACT

Securingnetwork is efficient in order to avoid attackers from violating the network performance and reliability. One such vulnerable network is MANET. Mobile Adhoc Network (MANET) is a self configurable and infrastructure less network with no centralized administration. Hence, MANET is vulnerable to routing attacks such as blackhole, flooding,grayhole,DDos, wormhole etc. There are two important phases that are carried out to detect and prevent the grayhole attacks in MANET. Initially in the baiting process, the source node broadcasts the bait request RREQ' to attract the malicious grayhole nodes to reply and thereby the reverse tracing mechanism is started to detect and prevent the grayhole nodes in the network. Finally, the alarm packets are sent by the source node to all other nodes in the network and prevent the blacklisted malicious nodes from communicating with the legitimate nodes. The whole process is incorporated with the Dynamic Source Routing (DSR) protocol and holds the features of proactive defense architecture. The simulation is implemented in NS2 simulator and the results are provided in terms of throughput, routing traffic, packet delivery ratio and delay.

KEYWORDS : MANET, DSR, Grayhole Attack, Baiting Process, Reverse Tracing Mechanism.

I. INTRODUCTION

A Mobile Adhoc Network (MANET) is a self configurable network. As there is no centralized administration, the nodes tend to join or leave the network any time. As all the nodes in the network are self-configuring, MANET is extremely vulnerable to routing attacks like blackhole, wormhole, flooding, DDos attacks, etc. Each node in the MANET acts as a router as well as a host.MANET has enormous advantage in military and civilian applications.

Many research works has been carried out focusing on the security of MANET. The baiting process and reverse tracing mechanism are the two recently used mechanisms [6] to detect and prevent the cooperative blackhole attacks. In this paper, these two mechanisms play a vital role in preventing the grayhole attacks in MANET.

Grayhole Attack[1] [12] [14] is basically an extension of blackhole attack. The important features of grayhole attack are,
(a) Initially, the grayhole node (see Fig. 1(a)) acts as a legitimate node and forwards the destined packets to the destination.
(b) Later, the legitimate node become malicious (see Fig. 1(b)) and selectively drops the destined packets without forwarding it to the destination. Hence this type of attack named as reactive attack i.e., acting as legitimate node in the beginning and becoming malicious later on. The special feature of grayhole node is, it forwards the packets from some nodes and drops the packets of some other nodes.

In this paper, the main focus is on detecting and preventing grayhole attacks in MANET using baiting process and reverse tracing mechanism.

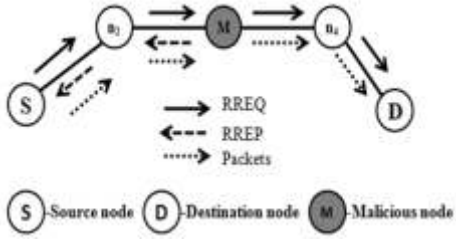

Fig. 1(a) Legitimate Grayhole Node

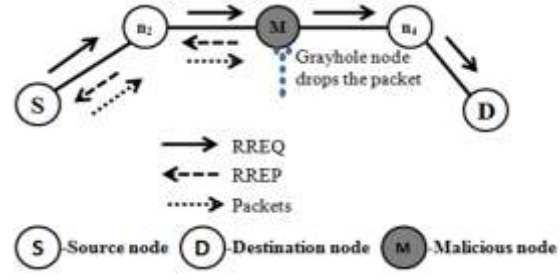

Fig. 1(b) Grayhole Attack

II. RELATED WORKS

Many researchers proposed different security solutions in detecting and preventing grayhole attacks in MANET.Jaydip Sen and et al.,[5]proposed a defensive mechanism based on AODV routing protocol to detect and prevent the collaborative grayhole attacks. This mechanism uses the distributed algorithm involving neighbor nodes of grayhole nodes and their detection involves a consensus algorithm on threshold cryptography basis.

Gundeep Singh Bindra and et al.,[3] proposed an Extended Data Routing Information (EDRI) Table in addition to routing table at each node to detect the blackhole and grayhole attacks in MANET. The Routing Table maintains a history of the nodes malicious behavior in order to predict the presence of grayhole attacks.

Gao Xiaopeng and Chen Wei [2] uses DSR protocol, proposed aggregate signature algorithm and network model. An aggregate signature algorithm is used to trace the packet dropping nodes using three algorithms such as, the creating proof algorithm, the checkup algorithm and the diagnosis algorithm. These algorithms are used to create proof, check the routing nodes and locate the malicious nodes respectively.

Rutvij H. Jhaveri and Narendra M. Patel [10] proposed a Sequence Number based Bait Detection Scheme (SNBDS) which is used to separate the malicious nodes during route discovery. The approach is based on AODV protocol.Using the receive RREP packet's destination sequence number and its corresponding routing table, the SNBDS approach prevents the grayhole attacks.

The extension of BDSR scheme is CBDS (Cooperative Bait Detection Scheme). CBDS [9] is a DSR-based technique used for identifying mali-

cious nodes in MANET. CBDS uses proactive detection in the initial stage and the reactive detection at the later stage. The bait node for the bait RREQ' is selected as one hop neighbor from the source. If any node other than this neighbor replies to RREQ then it is assumed that the malicious nodes are present in that routing path. Then the reverse tracing mechanism is used to identify the malicious nodes and they are blacklisted.The simulation results are provided showing that CBDS outperforms DSR and 2ACK protocol.

III. BAITING PROCESS AND REVERSE TRACING MECHANISM

The baiting scheme [9] starts with the neighbor selection process which identifies all the neighbor nodes in the network. The baiting process is to select a bait node in order to attract the malicious nodes in the route to reply that is followed by the reverse tracing mechanism which detects and prevents grayhole attacks in the network. After the detection of grayhole attacks, the source node sends the alarm packets to all the nodes in the network and prevents them from communicating with the other legitimate nodes. The whole approach is incorporated with the DSR protocol.

.

DSR (DYNAMIC SOURCE ROUTING) [1], [2] and [5] is an on-demand source routing protocol that the source node adds the routing information up to the destination node to the packets header. DSR has two basic mechanisms such as route discovery and route maintenance. During the route discovery a route is set up on-demand. The route maintenance monitors the established connection during the communication between nodes.

A Neighbor Selection method:

The source node randomly identifies each neighbor node in the network and the distance from one node to all other nodes in the network is calculated effectively. All the nodes are identified with in one hop and two hop distances. For MANET, the identification of neighbor nodes within the network is vital as the network has no centralized administration and it involves the system of nodes joining and leaving the network at any time.

B. Baiting Process

The important part in detecting the grayhole nodes is baiting process. This process is effectively carried out to attract all malicious nodes and thereby preventing them by reverse tracing mechanism.

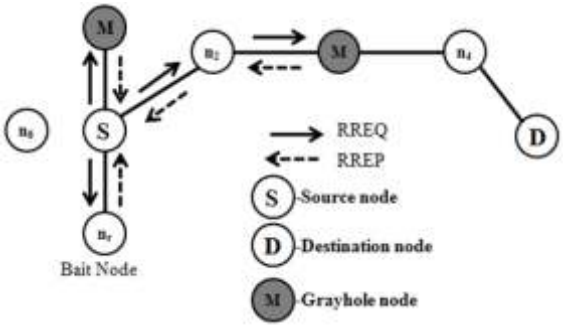

Fig. 2.Baiting Process for Grayhole Attack

Bait node selection:

1. First the source node randomly chooses a neighbor node nr as a bait node using neighbor selection algorithm.

2. Once the bait address is selected, the source node broadcast the bait RREQ'. In the packet filed of bait RREQ, the target address will be the bait node address in order to attract all the malicious nodes in the network.

3. If n_r (bait node) and other nodes reply RREP to the bait request RREQ', then there are malicious nodes exist in the routing path and therefore reverse tracing mechanism is started to trace and detect the malicious nodes.

C. Reverse Tracing Mechanism

The reverse tracing mechanism[9] is used to prevent the grayhole nodes from communicating with other legitimate nodes. On receiving bait RREQ' then the grayhole node **M** reply with a false RREP along with the address list **P= {n_1,n_2, M, n_4, nr}.** Each intermediate node on receiving the false RREP would separate the **P** list by its destination addressof the RREP in the IP field and obtain the address list Aiand perform a set difference **A'i = P – Ai** and reply with **A'i** to the source node.

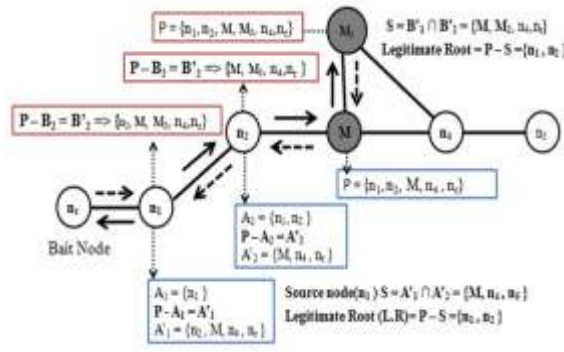

Fig. 3.Reverse Tracing Mechanism for Grayhole Attack

Each node's **A'i** is sent to source node for intersection. When the source node **S** intersects each node's **A'i**,then route to grayhole node **($S = A'_1 \cap A'_2 = \{M, n_4, n_r\}$)** is obtained. Now, on separating the list, the node which sends the fake reply RREP' for the bait request RREQ' is found. i.e, the grayhole node M started the route reply.

By performing set difference **($L.R = P - S = \{n_1, n_2\}$),** the legitimate nodes in the MANET are obtained. Thus the malicious grayhole is blacklisted. Likewise all the malicious nodes in the network are baited and detected and then blacklisted. The same process is continued for the malicious grayhole node M_2.

D. Alerting the MANET

Once the reverse tracing mechanism detects the grayhole nodes in the network, the source node prevent the communication of grayhole nodes with the other legitimate nodes by sending the alarm packet to the entire network.

The alarm packet has the grayhole list that is detected by reverse tracing mechanism.

IV. PERFORMANCE EVALUATION

A. Simulation

The simulation is being implemented in NS2(Network Simulator). There are 33 nodes in theenvironment. The simulation parameters are provided in the TABLE 1.

On bait selection,the nodesin the MANET reply to the source node. This shows that there are grayhole nodes present in the route reply which are traced using reverse tracing mechanism. The whole operation of baiting process and reverse tracing mechanism is shown in Fig. 6.

Parameters	Value
Application traffic	CBR
Transmission rate	4packets/s
Radio range	250m
Protocol	DSR
Pause time	10secs
Maximum speed	10m/s
Simulation time	200s
Number of nodes	33
Area	1100*1000
Malicious nodes	5
Threshold	Dynamic

TABLE 1
SIMULATION PARAMETERS

A. Performance metrics

A dynamic threshold algorithm is designed with the initial threshold of 90% that controls the simulation time when the packet delivery ratio falls below the same threshold value. The dynamic threshold algorithm is depicted in TABLE 2.

The baiting process and reverse tracing mechanism is incorporated with DSR protocol. The simulation result shows a higher packet delivery ratio.

TABLE 2
DYNAMIC THRESHOLD ALGORITHM

```
set threshold 0.9
proc Dynamic {threshold} {
        global ns null5
        set T1 0
        set T2 0
        set npr [$null5 npkts_]
        set PDR [expr ($npr/10)*100]
        if {$PDR<$threshold} {
                set T1 [$null5 lastPktTime_]
                $ns at [$ns now] "InitialProactiveDefense"
        }
        set npr [$null5 npkts_]
        set PDR [expr ($npr/10)*100]
        if {$PDR<$threshold} {
                set T2 [$null5 lastPktTime_]
                set threshold [expr $threshold+0.01]
        } else {
                if {$threshold>0.85} {
                        set threshold [expr $threshold-0.01]
                }
        }
        if {$val(stop)<20.0} {
                return $threshold
                Dynamic($threshold)
        } else {
                return 0.9
        }}
```

In the presence of 20% of malicious grayhole nodes in the network, the packet delivery ratio shows a better increment of 94%.

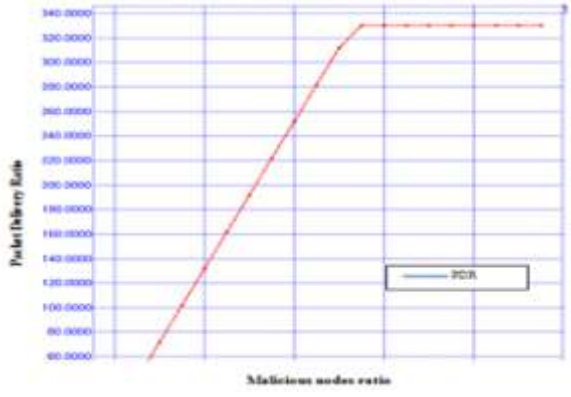

Fig. 4.Packet Delivery Ratio of Baiting and Reverse Tracing Mechanism

However, there is no 100% achievement of packet delivery ratio. The results are captured in Fig.4.

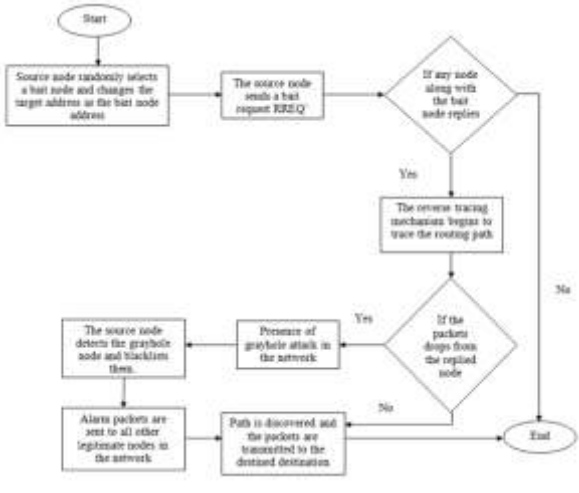

Fig. 5.Operation of Baiting and Reverse Tracing Mechanism

The whole operation of baiting process and reverse tracing mechanism is illustrated in Fig. 5. The source node randomly selects a neighbor node as a bait node and uses it's address as the destination address and entice the malicious grayhole nodes to reply RREP' by broadcasting bait RREQ'. When the nodes reply

RREP' for the bait request, the reverse tracing mechanism is started to detect and prevent the grayhole nodes. By then the malicious grayhole nodes are blacklisted and the alarm packets are sent by the source node to the entire network to avoid the legitimate nodes from communicating with the grayhole nodes.

TABLE 3
PERFORMANCE EVALUATION

Routing Protocols/ Schemes	Percentage of Malicious Nodes	Packet Delivery Ratio	Routing Overhead	Throughput
Baiting and Reverse Tracing Mechanism under DSR protocol	10%	96.5%	48.10%	98%
	20%	94%	58%	95%
	30%	89%	65.7%	93%
	40%	81.5%	72.4%	81.57%

In the presence of grayhole attacks in MANET, the packet delivery ratio decreases when the number of grayhole nodes increases. In the presence of 40% of malicious grayhole nodes, the packet delivery ratio decreases from 94% to 81%. And the routing overhead increases from 58% to 72% in the presence of40% of grayhole nodes. The overall percentage of baiting and reverse tracing process in detecting the grayhole attack is illustrated in the terms ofperformance metrics such as packet delivery ratio, routing overhead and throughput in TABLE 3.

Routing Overhead increases when the percentage of malicious node increases. In the presence of 20% of grayhole nodes, the routing overhead increases with 58%. The results are captured in Fig. 6. The well known routing protocol Adhoc On-demand Distance Vector protocol [15] provides extra routing overhead when the number of packets transmitted is increased.

Fig. 6.Routing Overhead of Baiting Process and Reverse Tracing Mechanism

End-to-End delay is defined as the average time taken for a packet to be transmitted from the source to the destination

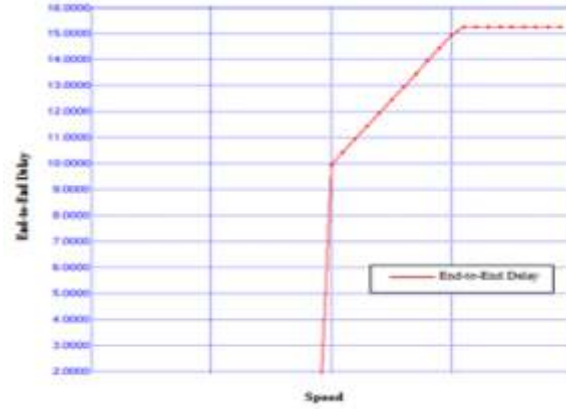

Fig. 7.End-to-End Delay of Baiting Process and Reverse Tracing Mechanism.

The end-to-end delay of baiting and reverse tracing mechanism under DSR protocol experiences a slight increase. This shows that when the speed increases then the delay increases. The results are captured in Fig. 7.

The throughput of baiting and reverse tracing process under DSR protocol increases with 95%. The results are captured in Fig. 8.If the baiting and reverse tracing mechanism avoids the inference of malicious nodes in the network, then the baiting and reverse tracing approach can achieve high-

est throughput.

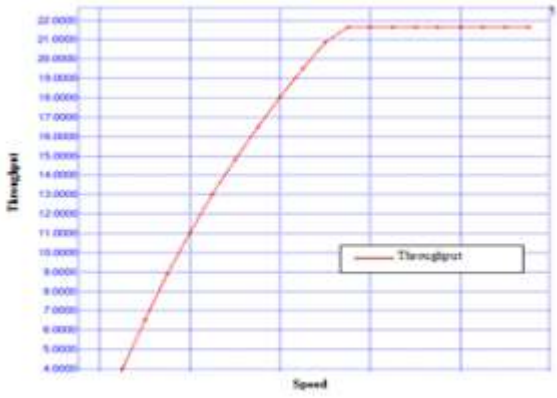

Fig. 8.Throughput of Baiting Process and Reverse Tracing Mechanism

V. CONCLUSION

The baiting scheme starts with the neighbor selection process which calculates the distance from one node to all other nodes in order to identify the neighbor nodes in the network. The detection and prevention of grayhole attack is effectively carried out using baiting process and reverse tracing mechanism. Once the grayhole nodes are blacklisted, the alarm packets from source node to all other nodes are transmitted to avoid grayhole nodes from communicating with the other legitimate nodes. The simulation results are provided showing that baiting process and reverse tracing mechanism is effective in detecting and preventing grayhole attacks. The simulation result provides better packet delivery ratio and throughput.

REFERENCES

[1] BounpadithKannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato, Tohoku University Abbas Jamalipour, "A Survey of Routing Attacks In Mobile Adhoc Networks", University of Sydney, IEEE WIRELESS COMMUNICATIONS,2007. | [2] Gao Xiaopeng andChen Wei "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", International Conference on Network and Parallel Computing, DOI 10.1109/NPC.2007.88,IEEE,2007. | [3] Gundeep Singh Bindra, Ashish Kapoor , Ashish Narang, Arjun Agrawal "Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs", 2012 International Conference on System Engineering and Technology, 978-1-4673-2376-5IEEE, 2012.| [4] Isaac Woungang, Sanjay Kumar Dhurandher, RajenderDheerajPeddi, Mohammad S. Obaidat, "Detecting blackhole attacks on DSR- based mobile ad hoc networks", 978-1-4673-1550- 0/12, IEEE 2012 .| [5] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar "A Mechanism for Detection of Gray Hole Attack inMobile Ad Hoc Networks", 1-4244-09837, ICICS, IEEE, 2007.| [6] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao, Jiann-Liang Chen, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", IEEE Systems Journal, 2014.| [7] K.Liu, D. Pramod, Varshney K., and Balakrishnan K., "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550,May 2007.| [8] Marti S., Giuli T. J., K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," inProc. 6th Annu. Intl. Conf. MobiCom, 2000, pp. 255–265.| [9] Po-Chun TSOU, Jian-Ming CHANG, Yi-Hsuan LIN, Han- Chieh CHAO, Jiann-Liang CHEN, "Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs", ICACT, February 2011 .| [10] Rutvij H. Jhaveri, Narendra M. Patel "A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks, DOI 10.1007/s11276-015-0945-9, Springer.| [11] Usha and Bose "Comparing The Impact Of Black Hole And Gray Hole Attacks In Mobile Adhoc Networks", Journal of Computer Science 2012, 8 (11), 1788-1802,ISSN 1549-3636, Science Publications,2012.| [12] Vishnu K. and A. J Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," Int. J. Comput. Appl.,vol. 1, no. 22, pp. 28–32, 2010.| [13] Weerasinghe H. and H. Fu, "Preventing cooperative blackhole attacks inmobile ad hoc networks: Simulation implementation and evaluation," in Proc. IEEE ICC, 2007, pp. 362–367.| [14] Wang W., Bhargava B., and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," in Proc. 28th IEEE Int. Symp. Reliable Distrib. Syst., New Delhi, India, Sep. 2009.