DETECTION AND REMOVAL OF BLACK HOLE ATTACK IN MOBILE AD-HOC NETWORKS USING COOPERATIVE BAIT DETECTION METHOD SCHEME

Sathya M, Priyadharshini M

Abstract—In Mobile Ad-Hoc Network (MANET) due to dynamic topology the nodes are free to move in and out of the network at any point of time. MANET is widely used in military based applications due to their infrastructure less property. Ad-hoc network are vulnerable to various types of attacks such as eavesdropping, denial of service, etc. Protecting the network from malicious attacks such as black hole attack, grey-hole attack which is very demanding in case of reactive routing protocols. This paper mainly focuses on designing Ad-hoc On Demand based routing (AODV) to protect the network from black hole/grey-hole attack by using Cooperative Bait Detection method Scheme. CBDS method implements a reverse tracing technique to track the malicious nodes in the Network.

Keywords—Ad-hoc On Demand based routing (AODV), Black hole attack, Cooperative Bait Detection method Scheme, grey-hole attack, malicious attack.

1 INTRODUCTION

MANET is a type of Ad-hoc network which consists of mobile routers connected by wireless links. Here nodes communicate with each other using multi-hop links. Since mobile nodes are not controlled by any controlling entity, they have unrestricted mobility and connectivity than normal nodes. Each node not only acts as host but also act as a router [1]. Due to this dynamic nature, MANET suffers from various security issues than the conventional networks. Presence of malicious nodes in the network may lead to same performance degradation [2]. Some of the other security threats are wormhole attack, rushing attack and so on.

In black hole attack the nodes which are malicious broadcasts that it has the shortest path to the destination in order to gain all the messages. The malicious nodes attracts all the packets by using forged Route Reply Packet (RREP) which is a fake shortest route to the destination and drops all the packets instead of forwarding it to the destination.

In grey-hole attack the nodes are initially recognised as malicious, they may become malicious at any point of time. This attack instead of dropping all the packets it selectively drops some packets or drop only the packets that passes through them. This paper is focused on removal of black hole attacks in the MANET using AODV routing protocol.

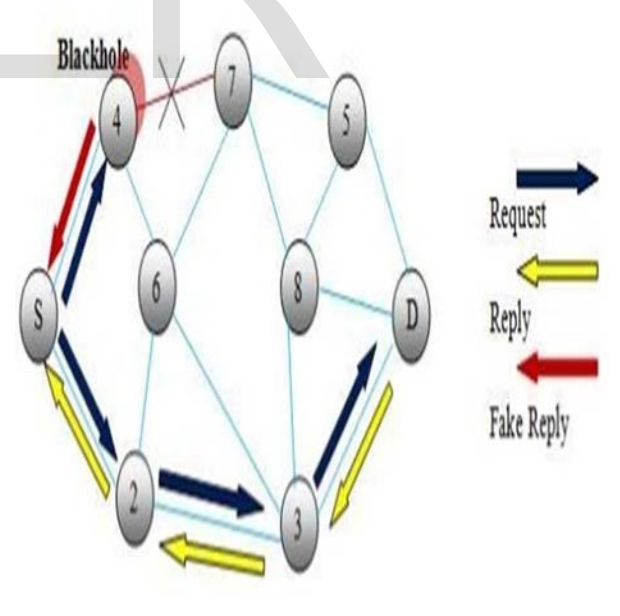

Fig. 1. Black hole attack

AODV is an On Demand routing protocol which has two phases as Route discovery and Route error [3]. If the source desires to communicate with destination to send the packet, it checks the existing routing table

- *Sathya M is currently pursuing masters degree program in Sri Krishna College of Engineering &Technology ,in Coimbatore,India, E-mail:14mg018@skcet.ac.in*
- *Priyadharshini M is currently working as Assistant Professor in the department of CSE, Sri Krishna College of Engineering &Technology,Coimbatore,India E-mail:priyadharshinim@skcet.ac.in*

whether it has a fresh route to the destination or not. If fresh route for destination is available then it uses the same route to send packets to destination. Otherwise source node broadcasts Route Request (RREQ) packet through the network i.e., the Route discovery phase is initiated. RREQ is forwarded by the intermediate nodes to all its neighbours. If the intermediate node has a fresh route to destination then it sends Route Reply (RREP) packet to the destination. The data packets are sent from source to the destination.

CDBS scheme is used to detect the malicious node which launches black hole / grey-hole attacks. In this scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a false reply RREP message and malicious nodes exact location in the network are detected using a reverse tracing technique.

2 RELATED WORK

In MANET the Ad-hoc routing protocol is classified into two major categories as Reactive routing protocol, Proactive routing protocol and Hybrid routing protocol. Reactive routing protocol [5]-[7], initiated only when the destination node identifies significant drop in the packet delivery ratio. DSR, AODV uses this type of routing protocol. Proactive protocol [8]-[11] constantly monitors the nearby nodes to detect the malicious nodes. If malicious nodes doesn't exists, overhead for detection is constantly created and resources used for detection is a waste. Only advantage of this routing is that it helps in avoiding the malicious attack at the initial stage itself. DSDV, OLSR uses this type of routing protocol. Hybrid routing protocol is the combination of both reactive and proactive routing protocol. Zonal Routing Protocol (ZRP) uses hybrid routing protocol.

In [3], AODV protocol is slightly modified to detect and remove the black hole/grey-hole attack in MANET. It uses new table Cmg_RREP_Tab, a timer MOS_WAIT_TIME and a variable Mali_node to the data structures in the default AODV protocol. In this method, the source node after receiving first RREP control message waits for MOS_WAIT_TIME. All the RREP messages are stored in the Cmg_RREP_Tab table. Source node analyses all the RREP messages and discards the RREP which has very high destination sequence number. After selecting RREP from Cmg_RREP_Tab table, other RREPs are flushed out to maintain freshness.

In [4], Data Routing Information table (DRI) and Cross check methods are applied to detect cooperative black hole attack. DRI table is generated for each node which contains two fields from and through. From contains information from which node data is routed. Through contains information through which node the data is routed.

In [5], this method some nodes which are trustworthy in terms of powerful battery and range are chosen as Back Bone Nodes (BBN). Each BBN generates numbers that are unique for that host. When source node desires to communicate with the destination, it request nearest BBN for Restricted Ip (RIP). BBN on receiving the RIP sends one of the unused IP address which is selected randomly from the pool of unused IP address. Source node sends RREQ for both the destination and RIP simultaneously.

If the source node gets RREP only from the destination node and not from the RIP, then the network is free from both the grey-hole and black hole attacks. Source node (SN) can use that IP for further transmissions. If SN receives RREP from RIP then black hole detection is initiated. SN alerts the neighbouring nodes to enter into promiscuous mode so that they listen not only to the packet destined to them, but also to the packet destined to the specified Destination node. SN sends a few dummy data packets to the destination, while the neighbouring nodes start monitoring the packet flow. These neighbouring nodes further transmit the monitor message to the next hop of the dummy data packet & so on. At a point when the monitoring nodes finds out that the dummy data packet loss is way more than the normal expected loss in a network, it informs the SN about this particular Intermediate Node(IN).

CBDS scheme can applied in Dynamic Source Routing (DSR) to detect and remove the malicious attack launched by black hole/grey-hole attack in Ad-hoc Networks.

3 PROPOSED APPROACH

In CBDS the source node selects an adjacent node as bait destination address to bait malicious nodes to send a reply RREP message. Malicious nodes are detected and prevented from participating in the routing operation, using a reverse tracing technique. When malicious node is detected it is moved to malicious list and alerts the other nodes so that it is not used for further communication. When a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again.

3.1 Initial Bait Step

To identify whether malicious nodes exists in the network, source node say n_r selects the adjacent node as bait destination. If malicious node exists it sends RREP messages once it gets the RREQ'. If other nodes sends RREP message in addition to n_r node, then this indicates that malicious node exists in the network. The revers tracing step is initiated. If only the n_r node had sent the reply RREP, it means that there is no other malicious node present in the network.

3.2 Reverse Tracing Step

If a malicious node has received the RREQ', it will reply with a false RREP. When a malicious node, for example, *nm*, replies with a false RREP, an address list $P = \{n1, \ldots nk, \ldots nm, \ldots \mathrm{nr}\}$ is recorded in the RREP. If node *nk* receives the RREP, it will separate the *P* list by the destination address $n1$ of the RREP in the IP field and get the address list $Kk = \{n1, \ldots nk\}$, where Kk represents the route information from source node $n1$ to destination node nk. Then, node nk will determine the differences between the address list $P = \{n1, \ldots nk, \ldots nm, \ldots nr\}$ recorded in the RREP and $Kk = \{n1, \ldots nk\}$

$$k'_k = p - p_k = \{n_{k+1,......}n_m, \ldots . n_r\} \qquad (1)$$

The source node S union all the k list and stores them at S.

$$S = k'_1 \cap k'_2 \cap k'_3 \cap k'_k \qquad (2)$$

Temporary set T stores the difference of the P and S.

$$T=P-S. \qquad (3)$$

In order to confirm that malicious exist in set S, source node sends test packets in that route and sends recheck message to second node towards the last node in set T. the node has enter into promiscuous mode so that it listens to which node the last node in T sent the packets to and sends the result back to the source node. Then the source node stores that node in black hole list and informs all nodes in the network to terminate the communication with that node by broadcasting alarm packets. if the last node drop the packets instead of diverting them ,then the source node stores it directly in the black hole list.

3.3 Shifted to Reactive Defense Phase

When the route is established and if at the destination it is found that the packet delivery ratio significantly falls to the threshold, the detection scheme would be triggered again to detect for continuous maintenance and real-time reaction efficiency. The threshold is a varying value in the range [85%, 95%] can be adjusted according to the current network efficiency. The initial threshold value is set to 90%. If the time of packet delivery ratio is less than the threshold then detection scheme will be triggered.

4 PERFORMANCE EVALUATION

4.1 Performance Metrics

4.1.1 Packet Delivery Ratio

This is defined as the ratio of the number of packets received at the destination and the number of packets sent by the source. Here, pktdi is the number of packets received by the destination node in the ith application, and pktsi is the number of packets sent by the source node in the ith application. The average packet delivery ratio of the application traffic n, which is denoted by PDR, is obtained as

$$\mathrm{PDR} = \frac{1}{n}\sum_{i=1}^{n}\frac{\mathrm{pktd_i}}{\mathrm{pkts_i}} \qquad (4)$$

4.1.2 Routing Overhead

This metric represents the ratio of the amount of routing-related control packet transmissions to the amount of data transmissions. Here, *cpki* is the number of control packets transmitted in the ith application traffic, and *pkti* is the number of data packets transmitted in the ith application traffic. The average routing overhead of the application traffic n, which is denoted by RO, is obtained as

$$RO = \frac{1}{n}\sum_{i=1}^{n}\frac{cpk_i}{pkt_i} \qquad (5)$$

4.1.3 Average End-to-End Delay

This is defined as the average time taken for a packet to be transmitted from the source to the destination. The total delay of packets received by the destination node is *di*, and the number of packets received by the destination node is *pktdi*. The average end-to-end delay of the application traffic n,

which is denoted by E, is obtained a

$$E = \frac{1}{n}\sum_{i=1}^{n}\frac{d_i}{pktd_i} \qquad (6)$$

4.1.4 Throughput

This is defined as the total amount of data (*bi*) that the destination receives them from the source divided by the time (*ti*) it takes for the destination to get the final packet. The throughput is the number of bits transmitted per second.

TABLE 1

SIMULATION PARAMETER

Parameter	Value
Number of nodes	50
Transmission range	250m
Transmission rate	4 packets/s
Packet size	512 bytes
Application traffic	10 CBR
Area	700m*700m
Threshold	Dynamic threshold
Mac	IEEE 802.11
Channel data rate	11Mbps

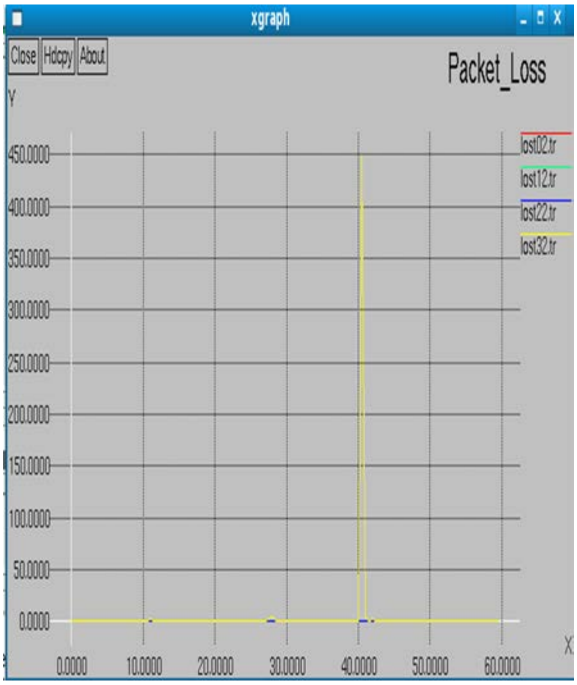

Fig. 2. Packet delivery ratio

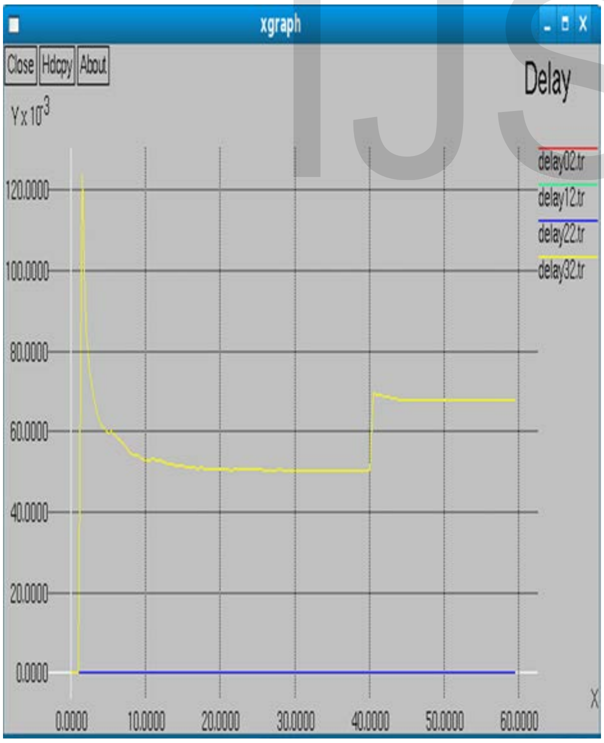

Fig. 3. Average Delay

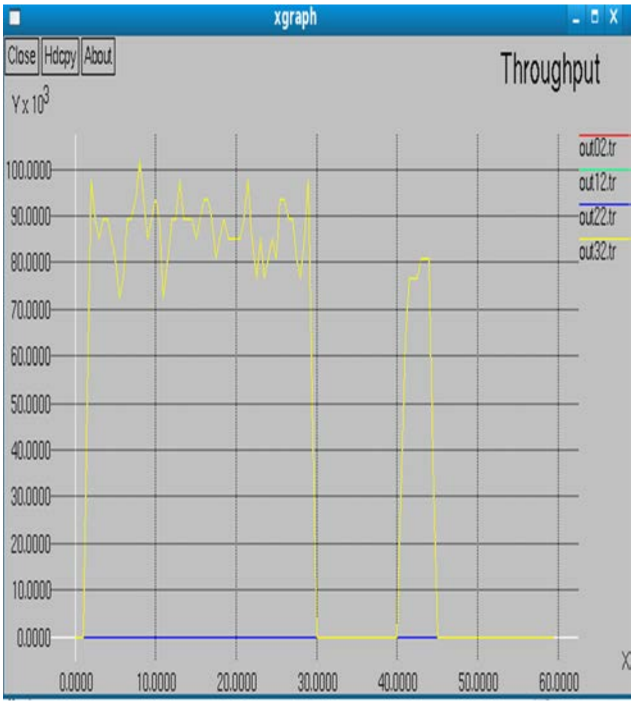

Fig. 4. Throughput

5 CONCLUSION

In this paper new scheme called CBDS is proposed to detect and remove black hole/grey-hole attack efficiently. In the future CBDS scheme can be applied to some other attacks such as Wormhole attack/rushing attack and its performance can be stimulated.

REFERENCES

[1] P.C.tsou, et.al ,"CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture," in Proc. 2nd Intl. cconf. Wireless Commun.,VITAE, chennai,India,Feb.28 Mar., 03,2011.

[2] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", *Member, IEEE* SYSTEMS JOURNAL, VOL. 9, NO. 1, MARCH 2015

[3] K. Vishnu 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

[4] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks", in *Proc. Int. Conf. Wireless Netw.*, Jun. 2003, pp. 570–575

[5] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", proceedings of the International Multi Conference of Engineers and Computer Scientists 2010 Vol II, IMECS 210

[6] M. Mohanapriya, Ilango Krishnamurthi,"Modified DSR protocol for detection and removal of selective black hole attack in MANET" Elsevier Ltd, June 2013

[7] H.Weerasinghe and H.Fu, “Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation,” in Proc.IEEE ICC,2007,pp.362-367.

[8] Y. Xue and K.Nahrstedt, “providing fault ad hoc routing service in adversarial environments,” Wireless Pers.Commun., vol. 29, pp. 367-388,2004.

[9] W.Kozma and L.Lazos, “REAct: resource-efficient accountability for nodes misbhaviour in ad hoc networks based on random audits”, 2009,pp.103-110.

[10] http://www.ijetae.com/files/Volume4Issue8/IJETAE_0814_26.pdf

[11] http://arxiv.org/ftp/arxiv/papers/1111/1111.4090.pdf