Detection and Removal of Black or Grayhole Attacks in Fully Connected MANET

[1]Soumya T V, [2] C R Arjunkumar
[1] Final Year Student, ME Communication Systems, [2.]Assistant Professor
EASA College of Engineering & Technology, Navakkarai-641115

***Abstract* - Mobile adhoc network (MANET) is a self -configuring, infrastructureless network of mobile devices connected wirelessly. The basic requirement for the formulation of communication among nodes is that, they should cooperate with each other. The routes between the nodes in the network are set up using routing protocols in MANET. The routing protocols are highly sensitive to many kinds of security attacks such as black hole and gray hole attacks. In the presence of malicious node, this requirement may lead to serious security concerns such as corruption in the routing process. In this paper we propose a cooperative bait detection scheme to detect and remove black or grayhole attacks.**

Index Terms: Cooperative bait detection scheme (CBDS), collaborative black hole attacks, detection mechanism, dynamic source routing (DSR), gray hole attacks, mobile ad hoc network (MANET).

I .INTRODUCTION

MANET is a type of network which consists of mobile routers connected by wireless links. Here nodes communicate with each other by using multi-hop links. MANETs have no fixed infrastructure. Due to this nature MANETs have been broadly used for several important applications such as personal area networking, military environments and emergency operations. Mobile routers are connected by wireless links in MANET. Self organizing, multi-hopping, mobility, scalability, security, energy conservation etc are the characteristics of MANET. Mobile adhoc networks consist of a network of mobile devices and these are free to move independently in any direction, therefore its links changes to other devices over and over again.
Each node in MANET can act as both host and router. While forwarding and receiving data packets, nodes should cooperate with each other to form a wireless local area network. Due to the mobility of the nodes the topology of the network varies promptly and is unpredictable over the time. In MANET, each node can interact with the help of its neighboring node which is in its radio range. Due to the uses of wireless communication in a MANET, the transmitted messages are tapped simply by the attacker. Various types of attacks appear in a MANET, such as black hole or grey hole. In black hole attack, any malicious node can attack the packet, falsely replies for the route requests such as not having any active route to that specified destination and losses all the retrieving packet. Black hole attack is shown in the figure 1.

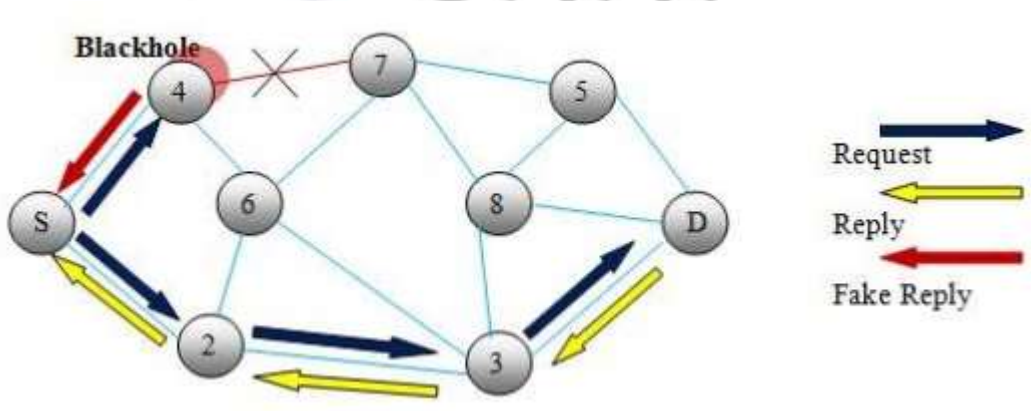

Fig. 1 Black hole attack

In grayhole attack, the nodes are initially identified as malicious; they may be malicious at any point of time. This attack selectively drops some packets or drops only the packet which passes through it instead of dropping all the packets .Grayhole attack is the variation of black hole attack. Several malicious nodes can cooperate with each other and acts like a group, which is the collaborative black hole. Many detecting methods may fail and causes more harm to the entire network in these type of attack.

In this paper a method based on dynamic source routing technique is used for detecting and removing the malicious nodes launched by black or grayhole attacks. This method is called cooperative Bait detection scheme.

II. PROPOSED SYSTEM

This paper proposes a method called the cooperative bait detection scheme (CBDS), which targets detection and prevention of malicious nodes launched by grayhole/collaborative black hole attacks in MANETs. Source node randomly selects nearby node with which it has to coordinate. Address of the neighboring node is set as the bait destination address and using this address baits malicious nodes to send RREP reply and recognize the malicious nodes by the reverse tracing method and subsequently prevent their attacks. In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to start the detection mechanism again. Here CBDS method combines the advantage of proactive detection in the initial step and the superiority of reactive response at the subsequent steps which reduces the resource wastage. The source node receives the RREP message then DSR can identify all the addresses of nodes in the selected routing path from the source to destination. The source node cannot identify which of the intermediate node has routing information to the destination node and reply RREP. It may result the source node to send its packets through the fake shortest path selected by the malicious node, which may lead to a black hole attack and it will results the packet loss. To solve this problem, the function of HELLO message is added to the CBDS to help each node to identify the adjacent nodes within one hop. This function helps in sending the bait address to entrap the malicious nodes and to utilize the reverse tracing program of the CBDS to detect real addresses of malicious nodes. The original RREQ packets and baiting RREQ packets are similar but the destination address of the bait RREQ packet is the bait address.

A. SYSTEM ARCHITECTURE

To solve the issue of collaborative black-hole attacks by designing AODV routing as DSR-based routing mechanism, it is called CBDS (Cooperative Bait Detection Scheme). It incorporates the advantages of both proactive and reactive defence architectures. In my approach, the source node selects an adjacent node with which to establish cooperation, the address of this node is used as bait destination address to deceive malicious nodes to send a RREP reply message Malicious nodes are therefore detected and prevented against routing operation, using a reverse tracing technique.

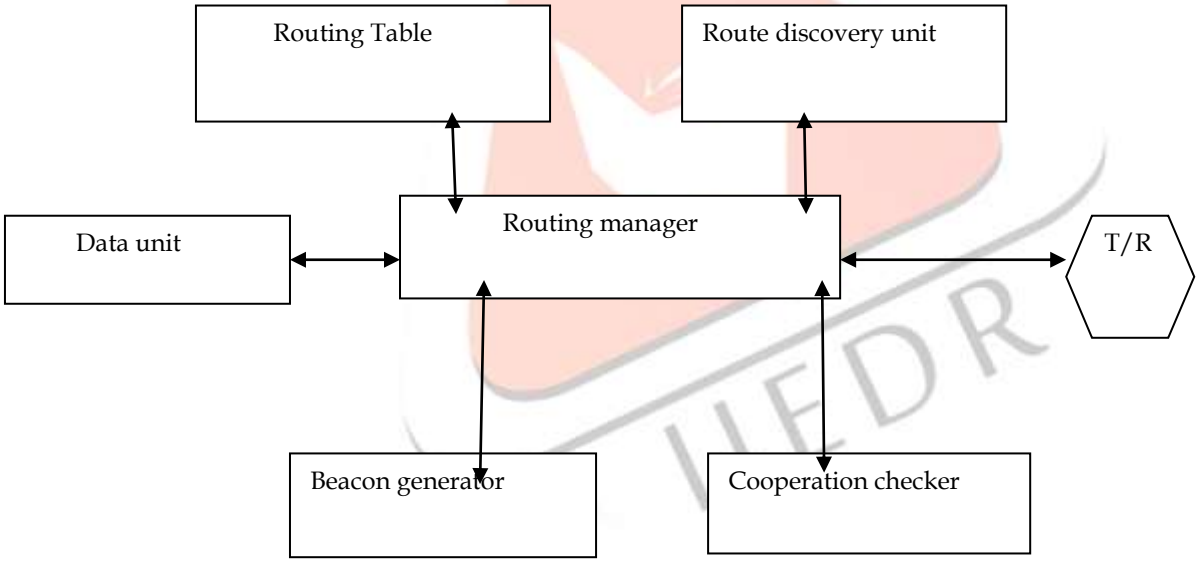

Fig.2. System architecture

Figure 2 shows the system architecture, in this module the beacon generator generates the periodic packet, it can be read by any neighbor node, and the beacon life is only for one hop. The neighbor management unit is to store the neighbor information into routing table when it receives the beacon packet from the neighbor. In Cooperation checker a timer is used to keep the time expire and intimates to generate the packet. If the time is got expire the neighbor node information will be deleted from the table.

III. SYSTEM REQUIREMENTS

Operating System: Ubuntu 10
Tool needed: Network Simulator 2
Packages needed: ns-allinone-2.35
Languages: TCL (Tool Command Language), C++

Network simulator is an object oriented discrete event simulator targeted at network researching .It provides substantial support for routing and multicast traffic

IV. SIMULATIONS AND RESULTS

Network simulator 2 is used to simulate the CBDS scheme. Figure 3 shows packet delivery ratio of DSR &CBDS at different thresholds. It is observed that higher packet delivery ratio compared with DSR. Packet delivery ratio is defined as the ratio of the number of packets received at the destination and the numbers of packets send by the source. Here consider only two performance parameters of CBDS

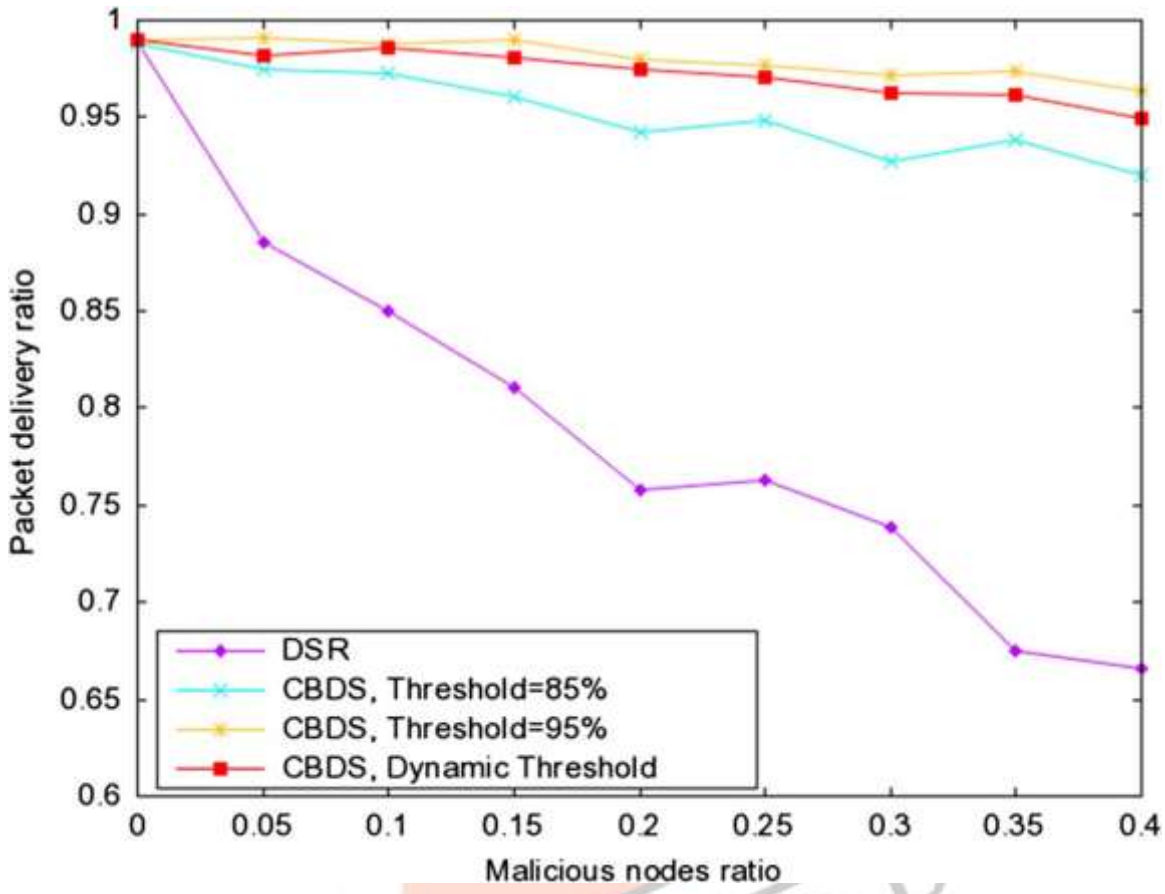

Fig.3. Packet delivery ratio of DSR &CBDS at different thresholds

Figure 4. Shows routing overhead of DSR &CBDS. Routing overhead is defined as the ratio of the amount of routing-related control packet transmissions to the amount of data transmissions. It is observed that DSR is produced lowest routing overhead compared with the CBDS when the number of malicious node increases. This is attributed to the fact that DSR has no intrinsic security mechanism or defensive mechanism. In fact, the routing overhead produced by the CBDS at different thresholds is a little bit higher than the routing overhead produced by DSR. This is due to the fact that the CBDS would first send bait packets in its initial bait phase and then it turns into a reactive defensive phase

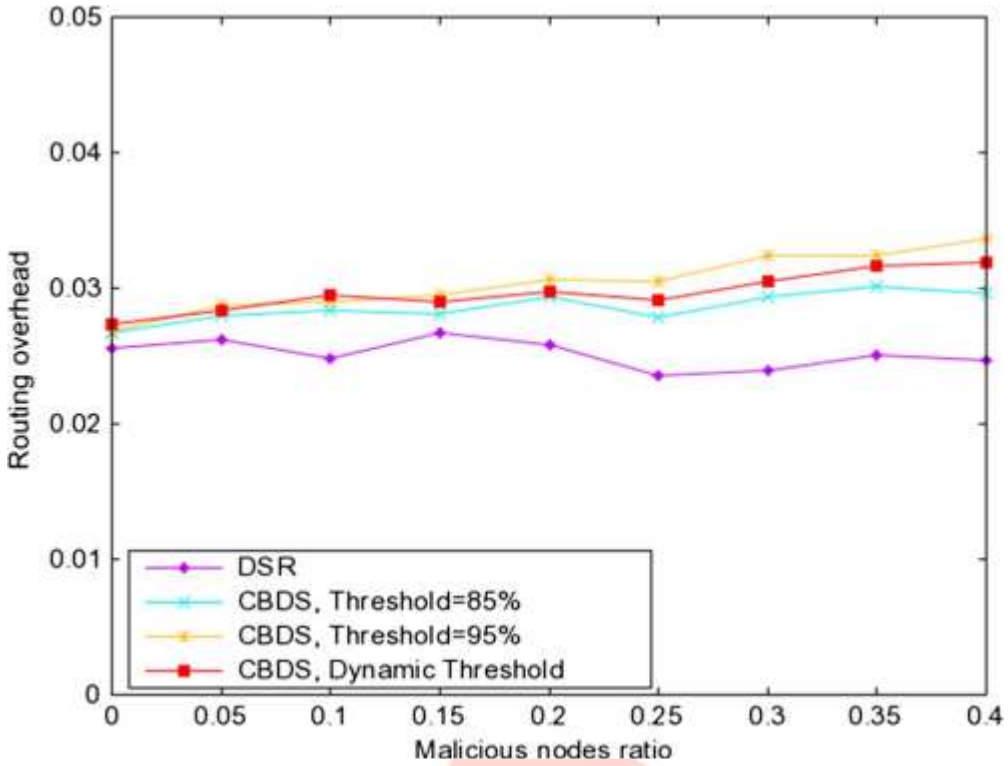

Fig. 4 packet delivery ratio of DSR &CBDS at different thresholds

V. CONCLUSION

Researchers proposed variety of solutions for many kinds of security issues in MANETs. In this approach, we have proposed a new mechanism called the CBDS (cooperative bait detection scheme) for detecting/preventing malicious nodes launched by gray/collaborative blackhole attacks in MANET. The address of an adjacent node is set as the bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Unlike previous works, the merit of CBDS lies in the fact that it integrates the advantages of both proactive and reactive defense architectures to achieve the aforesaid goal.

VI. REFERENCES

[1] P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defence architecture," in Proc. 2nd Intl. Conf. Wireless Commun., VITAE, Chenai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.
[2] C. Chang, Y.Wang, and H. Chao, "An efficient Mesh-based core multicast routing protocol on MANETs," J. Internet Technol., vol. 8, no. 2, pp. 229– 239, Apr. 2007.
[3] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," Mobile Comput., pp. 153–181, 1996.
[4] 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.
[5] 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.
[6] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "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.
[7] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," IEEE Commun. Mag., vol. 40, no. 10, Oct.2002.
[8] 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.
[9] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," Wireless Pers.Commun., vol. 29, pp. 367– 388, 2004..
[10] I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, "TBONE: A mobile-backbone protocol for ad hoc wireless networks," in Proc. IEEE Aerosp. Conf., 2002, vol. 6, pp. 2727–2740.
[11] A. Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1, 2010.