EXPLORATIONS ON ENGINEERING LETTERS (EEL)
VOLUME 1, ISSUE 1 (2016):PP.41-45
SANA ACADEMIC PRESS

Detecting Malicious Nodes in MANETs under Grayhole/Collaborative Blackhole Attacks

T.MarySanthaPriya[1], S.Vasantha[2], R. Latha[3]
[1]*Research Scholar, St.Peter's University, Chennai.*
[2]*Asst.Prof. & Head., Dept. of Computer Applications, St.Peter's University, Chennai*
[3]*Prof. & Head., Dept. of Computer Applications, St.Peter's University, Chennai*
marysanthapriya@gmail.com

Abstract-- *Preventing attacks in MANETs using DSR routing in terms of packets delivery ratio and routing overhead. In a widespread availability of mobile devices many security issues may causes. In this paper it hands the grayhole/collaborative blackhole, Blackhole attacks attract all packets by the way of fake Route Reply (RREP) then discard the packet without forwarding them to destination. To resolve these two issues we are going to use DSR mechanism which belongs to CBDS (Cooperative bait detection scheme) that effectively detects the malicious node that attempts to launch grayhole/collaborative black hole attacks. Dynamic Source Routing technique involves two mail process route discovery and route maintenance.DSR does not have mechanism of detection at early stage. so that CBDS lies to integrates the proactive and reactive to achieve goal at initial stage. In the presensence of malicious attack CBDS operates the DSR,2ACK .Best-effort fault-tolerant routing(BFTR)protocols in terms of delivering packet ratio and metrics.*

Keywords: *Cooperative bait detection scheme (CBDS), collaborative bait, collaborative blackhole , detection mechanism, dynamic source routing (DSR), grayhole , malicious node, mobile ad hoc network (MANET).*

I. INTRODUCTION

Because of Sparse Availability of mobile devices,mobile ad hoc networks (MANETs) have been heavily used for various task such as applications in military crisis operations and emergency alerts and response activities. In preliminary stage due to their infrastructure lack of resources. In MANET a single node not only works but also acts as a router. When receiving data, nodes are need to forward the data packets with each other. At this stage creating a wireless local area network(LAN).with this unique feature also come with major drawback in a security point of view. Regarding the application impose some open source on the security of the network topology, routing and collision.some of the presence and collaboration of malicious nodes in the network may disrupt the routing process, leading to a malfunctioning of the network operations. car. A mechanism [so-called cooperative bait detection scheme (CBDS)] is presented that effectively detects the respective malicious nodes that attempt to launch grayhole/collaborative black hole attacks. In my paper the address of an nearby node is used as bait destination node to an address malicious node to sent a message RREP reply and malicious nodes are recused using a reverse tracing method. Any recused malicious node is held in a blackhole list so that all nodes should participate to the routing of the message alerted to stop communicating with their neighbour node list. Unlike an existing system, the range of CBDS lies in the facts that it combining both proactive and reactive defence architecture to achieve the

above technology. In the pre-existing detection method takes the advancements of the characteristics on both proactive and reactive methods to implements a DSR based on routing algorithm which is able to detect attacks in MANETs blackhole. Many of the research people investigated this issues of malicious node recuse in MANETs.Major solutions deal with the detection of a single malicious node or number of resources in terms of time and costing the blackhole attacks in MANET.

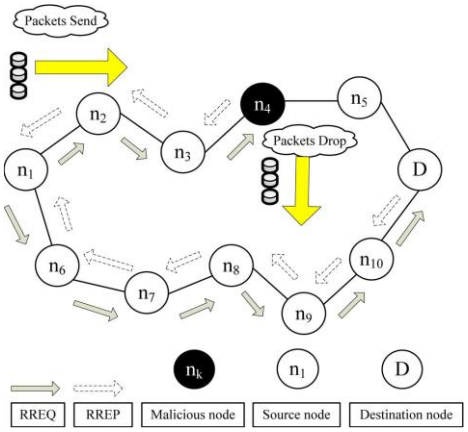

Fig.1 Black hole attack–node *n*4 drops all the data packets

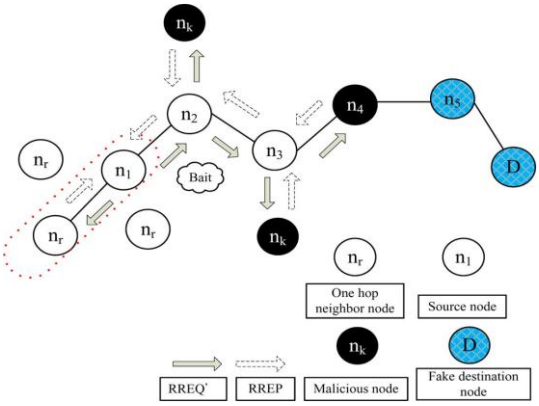

Fig.2 Random selection of a cooperative bait address.

II. MATERIAL AND METHODS

The CBDS scheme comprises three steps: 1) the initial bait step; 2) the initial reverse tracing step; and 3) the shifted to reactive defense.

A. Initial Bait Step

The goal of the bait phase is to entice a malicious node to send a reply RREP by sending the bait RREQ_ that it has used to advertise itself as having the shortest path to the node that detains the packets that were converted.

B. Initial Reverse Tracing Step

The reverse tracing program is used to detect the behaviours of malicious nodes through the route reply to the RREQ_ message. If a malicious node has received the RREQ_, it will reply with a false RREP. Accordingly, the reverse tracing operation will be conducted for nodes receiving the RREP, with the goal to deduce the dubious path information and the temporarily trusted zone in the route.

C. Shifted to Reactive Defence Phase

After the above initial proactive defense (steps A and B), the DSR route discovery process is activated. 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.

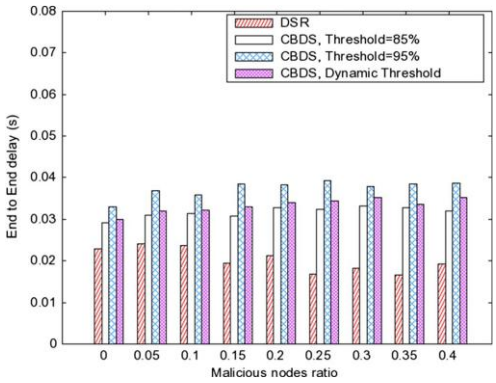

Fig.3 End-to-end delay of DSR and the CBDS for different thresholds**.**

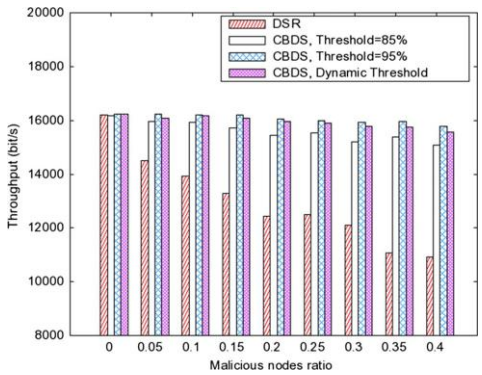

Fig.4 Throughput of DSR and the CBDS for different thresholds.

Fig.3 It can be observed that the CBDS incurs a little bit more end-to-end delay compared with that DSR.CBDS necessitated more time to bait and detect malicious nodes. Fig.4 It can also be observed that DSR heavily suffers the most from malicious node attacks compared with CBDS.

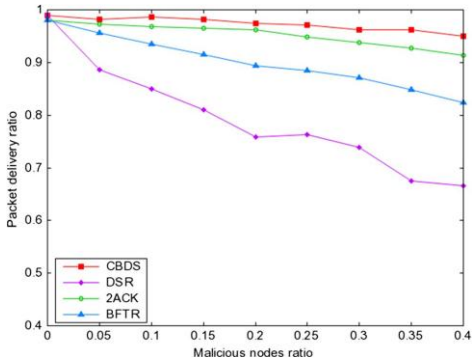

Fig.5 Effect of malicious nodes on the packet delivery ratio

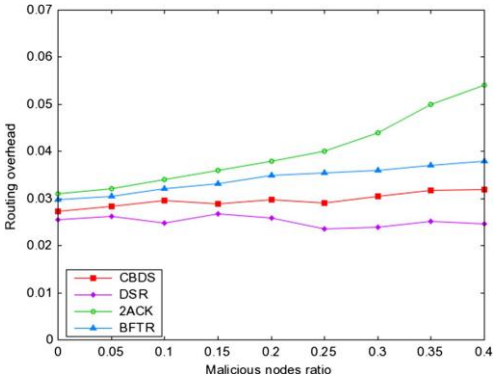

Fig.6. Effect of malicious nodes on the routing overhead

Fig.5 It can also be observed that DSR heavily suffers from increasing blackhole attacks since it does not have any detection and protection mechanism to prevent blackhole attacks. Fig.6 It can be observed that when percentage of malicious nodes increases, DSR produces the lowest routing overhead compared with all other schemes including the CBDS

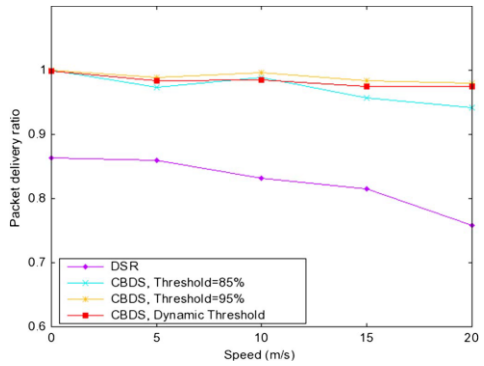

Fig.7 Packet delivery ratio for different threshold, under varying node speed

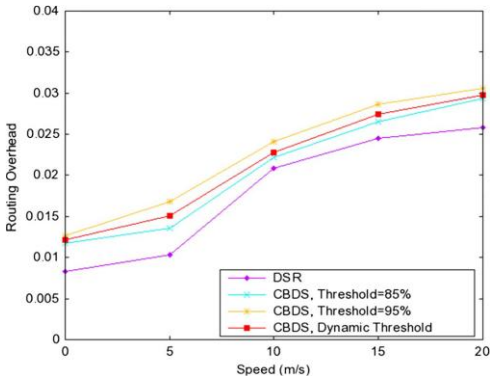

Fig.8 Routing overhead for different thresholds, under varying node speed

Fig.7 It can also be observed that the packet delivery ratio of DSR and the CBDS for different thresholds slightly decreases when the node's speed increases. The CBDS yields a higher packet delivery ratio compared with DSR. Finally, the CBDS can detect malicious nodes successfully while keeping the packet delivery ratio above 90%. Fig.8 It can be observed that the routing overhead of DSR and the CBDS for different thresholds increases when the node's speed increases. Moreover, the CBDS can still detect malicious nodes successfully while keeping a routing overhead a little higher than that of DSR. It can be observed that the throughput of DSR and the CBDS for different thresholds slightly decreases when the node's speed increases. The CBDS yields the highest throughput compared with DSR in all cases. It can be observed that the average end-to-end delay incurred by the CBDS is higher than that incurred by DSR in all cases. This is attributed to the fact that the CBDS requires more time to detect and trace the malicious nodes, which is not the case for DSR since the latter has no intrinsic malicious node detection mechanism.

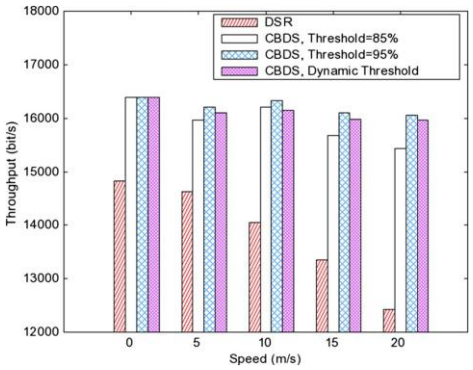

Fig.9 Throughput for different thresholds, under varying node speed

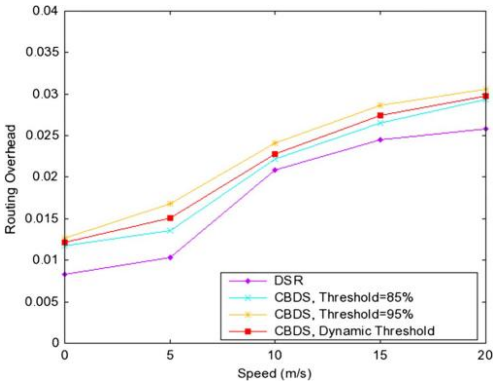

Fig.10 End-to-End delay for different thersholds,under varying node speed

III DISCUSSION

In this scenario, the maximum speed of nodes is varied from 0 to 20 m/s, and the percentage of malicious nodes is fixed to 20%. In First step the packet delivery ratio of the CBDS and DSR differ in their threshold values. The value is set to 85%,95% and dynamically changes to that packet delivery ratio.it is also

diagnosed that the packet delivery ratio of CBDS and DSR has been decreases and increases slightly depends on the node. At final stage CBDS can detect malicious nodes without fail and keeping the ratio over a 90%. Next step routing overhead of CBDS and DSR values. As to set 85%, 95% randomly results can be a routing overhead of DSR and CBDS of Different threshold values. In Fig. 8, it can be observed that the routing overhead of DSR and the CBDS for different thresholds increases when the node's speed increases. Moreover, the CBDS can still detect malicious nodes successfully while keeping a routing overhead a little higher than that of DSR. Third, Here we go through CBDS and DSR for different thresholds. The threshold value is set to 85%, 95%, and the Randomly changes, respectively. The results are shown in Fig.9.It can be observed that the throughput of DSR and the CBDS for different thresholds slightly decreases when the node's speed increases. The CBDS yields the highest throughput compared with DSR in all cases. It is also found that the CBDS can still keep the highest throughput while avoiding interference with malicious nodes. Finally we use end-to-end delay of the CBDS and DSR for different threshold values such as 85%, 95%. The results are shown in Fig.10.It can be observed that the average end-to-end delay incurred by the CBDS is higher than that incurred by DSR in all cases. This is attributed to the fact that the CBDS requires more time to detect and trace the malicious nodes, which is not the case for DSR since the latter has no intrinsic malicious node detection mechanism.

IV. CONCLUSION

A new mechanism which is called CBDS for detecting malicious nodes in MANETs belongs to grayhole/collaborative blackhole attacks. The simulation results revealed that the CBDS outcome over the DSR, 2ACK, and BFTR schemes, chosen as benchmark schemes, in terms of routing overhead and packet delivery ratio. As we intend to 1) investigate the feasibility of adjusting our CBDS approach to address other types of collaborative attacks on MANETs and to 2) investigate the integration of the CBDS with other well-known message security schemes in order to construct a comprehensive secure routing framework to protect MANETs against miscreants.

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 forMANET based on hybrid defense 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 efficientMesh-based core multicastrouting protocol onMANETs," *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] 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.
[5] 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.
[6] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in *Proc. 6th Annu. Intl. Conf. MobiCom*, 2000, pp. 255–265.
[7] 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.