COMPARATIVE PERFORMANCE ANALYSIS OF CBDA AND DSR ROUTING PROTOCOL AGAINST COLLABORATIVE ATTACKS BY MALICIOUS NODES IN MANET

R. Nivetha*, E. Gnanamanoharan
* PG student Department of Electrical Engineering, Annamalai University, Tamil Nadu, India
Asst professor Department of Electrical Engineering, Annamalai University, Tamil Nadu, India

DOI: 10.5281/zenodo.58277

KEYWORDS: Cooperative bait detection, gray hole, black hole, Malicious node, MANET

ABSTRACT

In mobile ad hoc-hoc Networks (MANETs), the important concern is the security as well as establishment of verbal exchange amongst nodes is that nodes have got to work at the side of each different. Averting or sensing malicious nodes initiation grayhole or collaborative black hole attacks is the fundamental undertaking. Cooperative bait detection approach mixes the benefits of each proactive and reactive defense manners. Right here it makes use of the method of transposition for implementing safety and the CBDA procedure outfits a reverse tracing procedure to aid achieve the certain goal. The demo in the existence of malicious-node assaults, the CBDA beats the DSR, chosen as performance metrics in terms of throughput, delay and energy. Within the transposition method we use the key which is the ascii worth of the personality which is encrypted at sender aspect and decrypted at receiver.

INTRODUCTION

The term MANET (Mobile Ad hoc Network) refers to a multihop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time, without using any kind of fixed wired infrastructure. MANET is actually self-organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. Otherwise, a stand for “Mobile Ad Hoc Network” A MANET is a type of ad hoc network that can change locations and configure itself on the fly[1]. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.

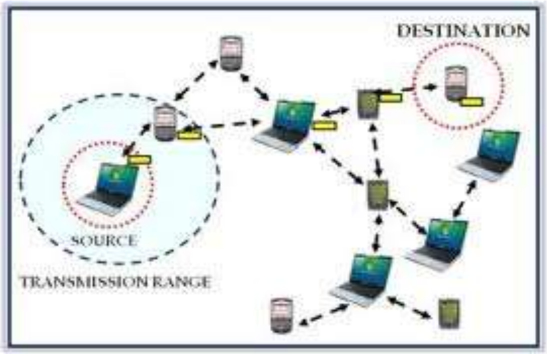

Fig.1 Structure of MANET

The purpose of the MANET working group is to standardize IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies with increased dynamics due to node motion and other factors[2]. Approaches are intended to be relatively lightweight in nature, suitable for multiple hardware and wireless environments, and address scenarios where MANETs are deployed at the edges of an IP infrastructure. Hybrid mesh infrastructures (e.g., a mixture of fixed and mobile routers) should also be supported by MANET specifications and management features. Using mature components from previous work on experimental reactive and proactive protocols, the WG will develop two Standards track routing protocol specifications:

- Reactive MANET Protocol(RMP)
- Proactive MANET Protocol(PMP)
- Hybrid routing Protocol

If significant commonality between RMRP and PMRP protocol modules is observed, the WG may decide to go with a converged approach. Both IPv4 and IPv6 will be supported. Routing security requirements and issues will also be addressed[3].

Mobile ad hoc network (MANET) falls within the class of wi-fi ad hoc network, and is a self-configuring network. Each and every device is allowed to move freely in any course, and accordingly will adjust its link with different devices ordinarily. Each and every node need to ahead traffic which is not involving its own use, and hence be each a router and a receiver. This option additionally comes with a extreme concern from the protection point of view. Obviously, the above-stated applications impose some extreme constraints on the security of the network topology, routing, and information site visitors[4]. For instance, the presence and collaboration of malicious nodes in the community may disrupt the routing approach, main to a misguided of the network operations. The protection of MANETs deals with prevention and detection ways to battle man or woman misbehaving nodes. With admire to the effectiveness of these ways becomes weak when more than one malicious nodes conspire together to initiate a collaborative assault, which can outcome to more shocking damages to the community.

PROPOSED METHODOLOGY

It is proposed to develop a new improved Comparative Performance Analysis of CBDA and DSR Routing Protocol against Collaborative Attacks by Malicious Nodes in MANET with a view to increase the lifetime of the network and to reduce the energy consumption. The performance metrics for proposed scheme evaluated through Network Simulator 2(NS2) platform.

In this paper, a mechanism [so-called cooperative bait detection scheme (CBDS)] is presented that effectively detects the malicious nodes that attempt to launch gray hole /collaborative black hole attacks. In our scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a black hole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list. Unlike previous works, the merit of CBDS lies in the fact that it integrates the proactive and reactive defense architectures to achieve the aforementioned goal.

MALICIOUS NODES WITH A FIXED MOBILITY

It should be noticed that the CBDS offers the possibility to obtain the dubious path information of malicious nodes as well as that of trusted nodes; thereby, it can identify the trusted zone by simply looking at the malicious nodes reply to every RREP. In addition, the CBDS is capable of observing whether a malicious node would drop the packets or not. As a result, the proportion of dropped packets is disregarded, and malicious nodes launching a grayhole attack would be detected by the CBDS the same way as those launching blackhole attacks are detected. It can be observed that when the number of malicious nodes increases, DSR produces the lowest routing overhead compared with the CBDS. This is attributed to the fact that DSR has no intrinsic security method or defensive mechanism. In fact, the routing overhead produced by the CBDS for different thresholds is a little bit higher than that produced by DSR; this might be due to the fact that the CBDS would first send bait packets in its initial bait phase and then turn into a reactive defensive phase afterward.

Advantages

- 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 trigger the detection mechanism again.
- This function assists in sending the bait address to entice the malicious nodes and to utilize the reverse tracing program of the CBDS to detect the exact addresses of malicious nodes.

FLOW DIAGRAM OF PROPOSED SYSTEM

The following flow diagram in Figure 2 clearly shows the working principle of the proposed approach

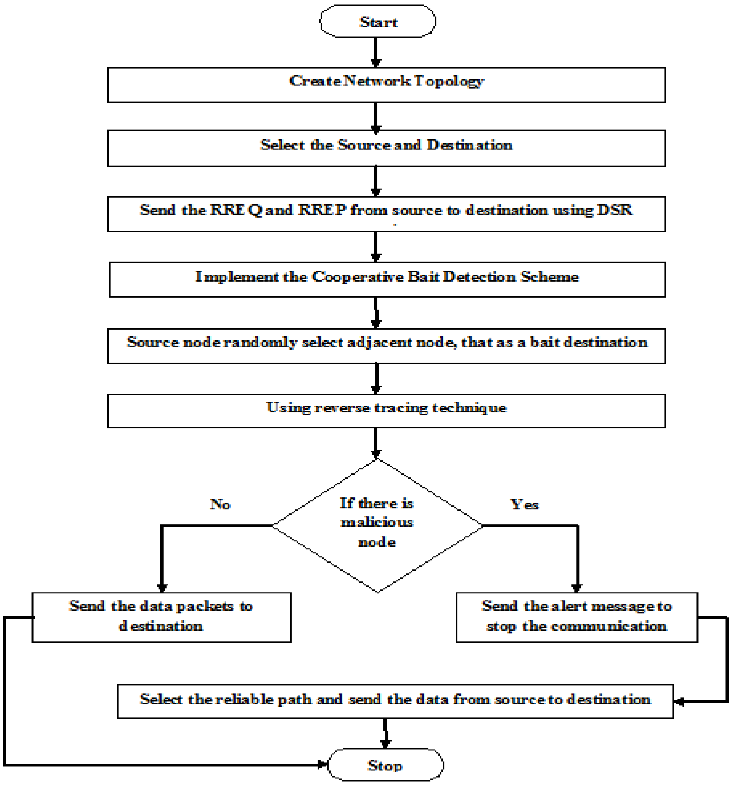
Start
Create Network Topology
Select the Source and Destination
Send the RREQ and RREP from source to destination using DSR
Implement the Cooperative Bait Detection Scheme
Source node randomly select adjacent node, that as a bait destination
Using reverse tracing technique
No
If there is malicious node
Yes
Send the data packets to destination
Send the alert message to stop the communication
Select the reliable path and send the data from source to destination
Stop

Fig. 2 Flow Diagram of Proposed Approach

SIMULATION RESULTS

In this project we are using 50 nodes. Node 0 is the source node and 1 is the destination node. The source node the sending the route request to the destination node.

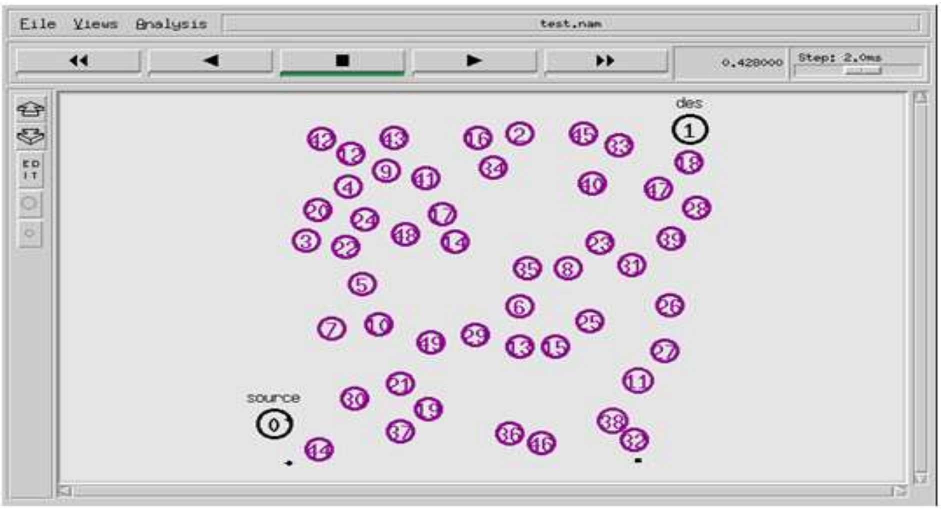

Fig. 3 Source To Destination Data Transmission

Node 7,13,14,34 are the malicious nodes. The source node 0 does not choose these nodes for sending or broadcast the message to the destination node 20.

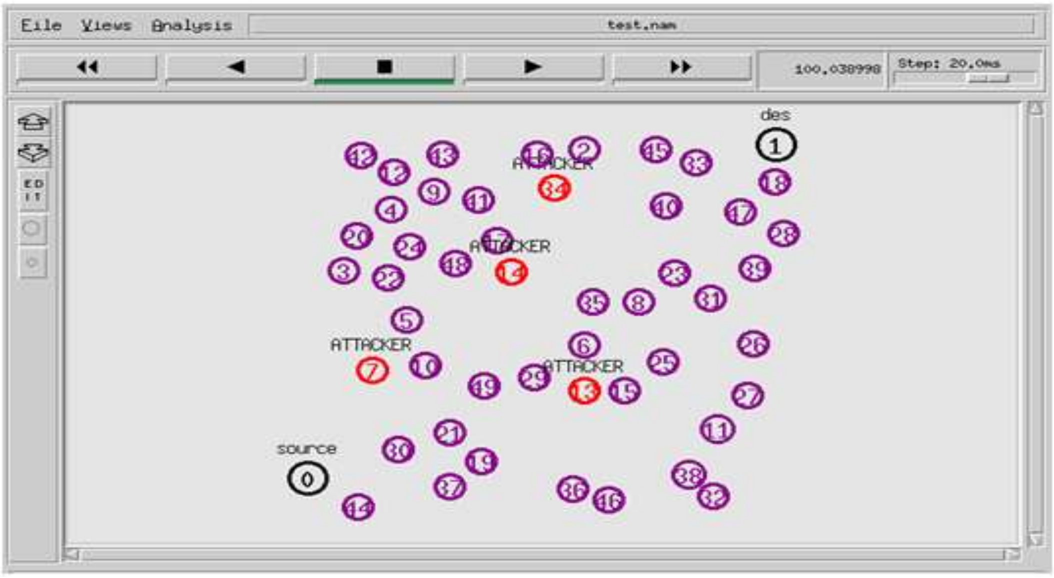

Fig. 4 Attacks Detections

In this characteristic curve, x-axis is the time (ms) and y-axis is the delay. The DSR drastically suffers from blackhole attacks, when the percentage of time increase. This is attributed to the fact that DSR has no secure method for detecting / preventing blackhole attacks. Our CBDA delay is reduced. The graph shows an exponential growth in average delay as more nodes are introduced and transmit data within our network over time

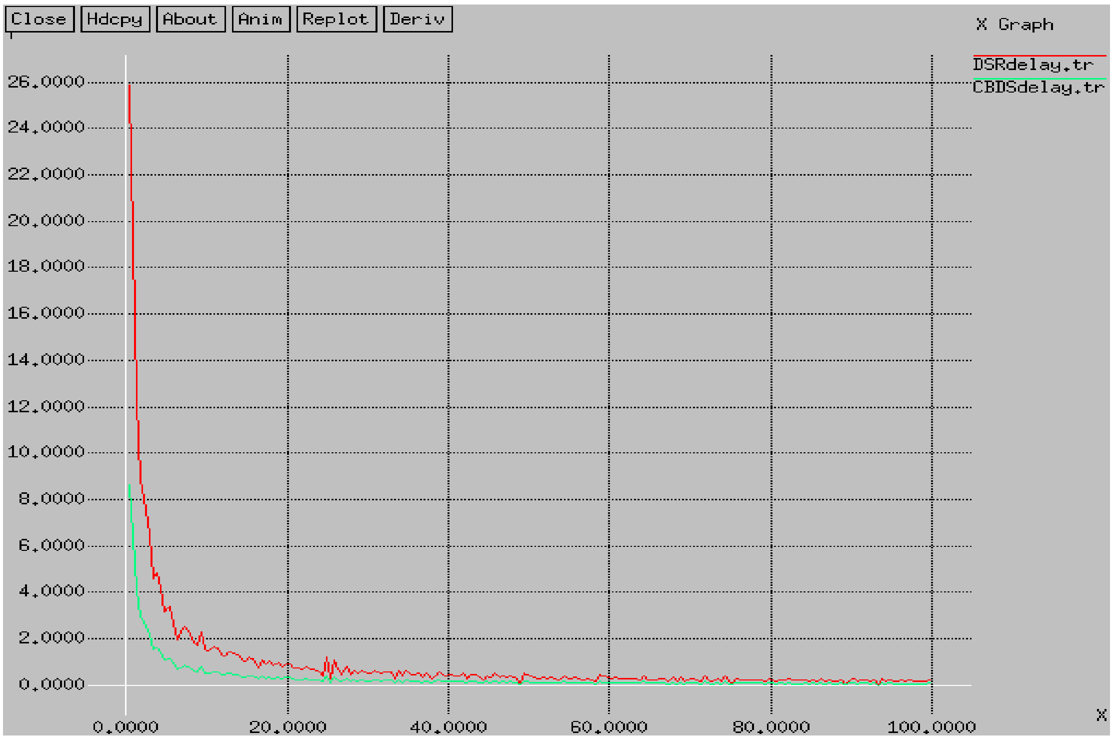

Fig. 5 Delay

In this characteristics curve, X-axis is the time (ms) and y-axis is the energy. When the number of time increases, DSR energy is increased. This is attributed to the fact that DSR has no intrinsic security method. Finally, the characteristic curve of CBDA energy is lower than the DSR energy and it remains constant.

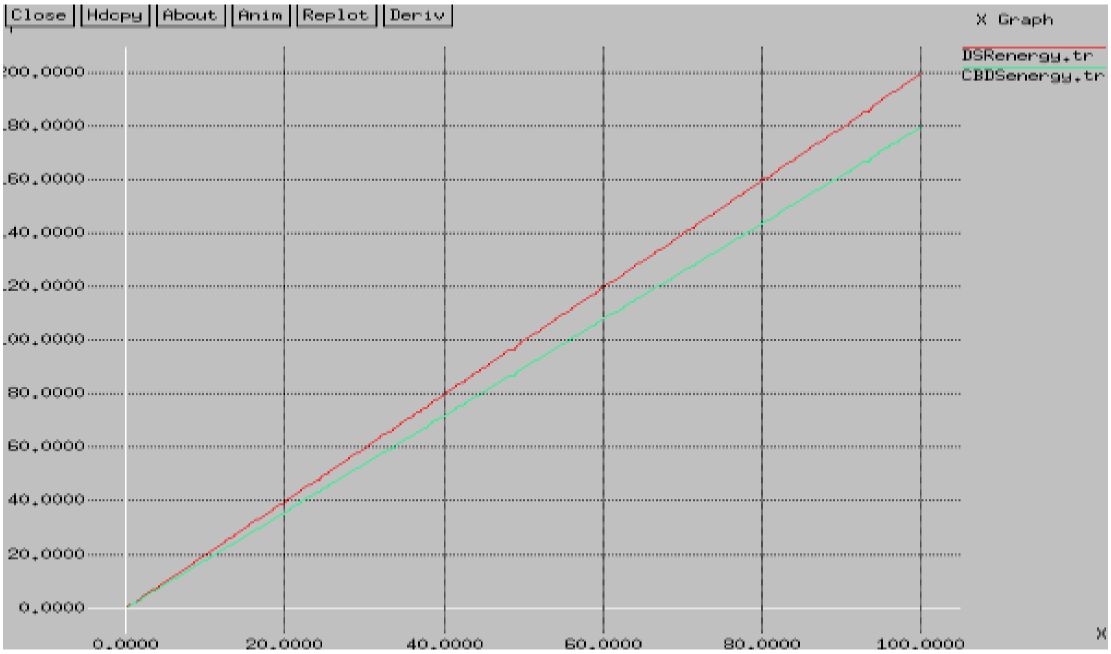

Fig. 6 Energy

In this characteristic curve, x-axis is the time (ms) and y-axis is the Throughput. Here the CBDS throughput is increased when compare to DSR throughput. The simulation begins and mobile node 0 starts transmitting data at 10.0s. As expected, the entire available bandwidth is provided to mobile node 0 resulting in high performance of this node...

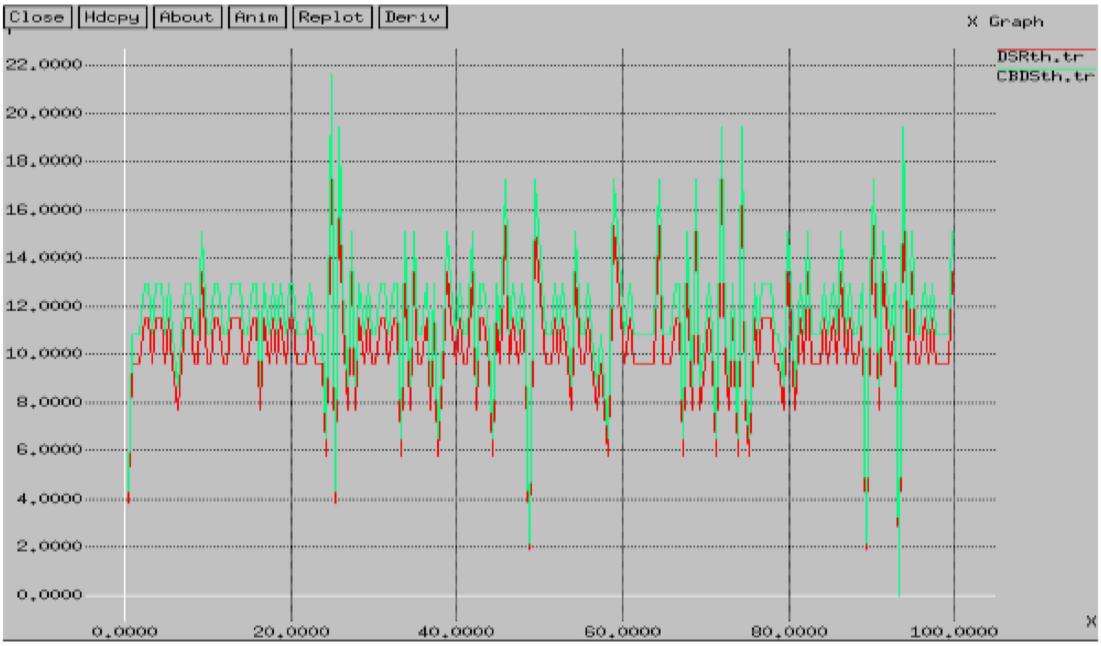

Fig. 7 Throughput

CONCLUSION

As the transposition protection model is applied to the co-operative bait detection approach the information is distributed in a secured manner and the packet delivery ratio can be expanded and the loss of knowledge packets is lowered. Enhancement can be completed with distinct types of Ad-Hoc routing protocols. Here, the CBDA and DSR routing protocol against collaborative attacks by malicious nodes in MANET. From the experimental result it shows that delay and energy consumption is less and throughput is high compared to conventional methods.

ACKNOWLEDGMENT

The authors thank the authorities of Annamalai University for providing the necessary facilities in order to accomplish this piece of work.

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 defense architecture,” *in Proc. 2nd Intl. Conf. Wireless Communication*., VITAE, chennai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.
2. S. Corson and J. Macker, RFC 2501," Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", *International Journal of Computer Application*s ,Jan. 1999. (Last retrieved March 18, 2013).
3. C. Chang, Y.Wang, and H. Chao, “An efficient Mesh-based core multicast routing protocol on MANETs,” *J. Internet Technology*., vol. 8, no. 2, pp. 229– 239, Apr. 2007.
4. D. Johnson and D. Maltz, “Dynamic source routing in ad hoc wireless networks,” ", *Excel Journal of Engineering Technology and Management Science,* Mobile Computer., pp. 153–181, 1996