International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Detection and Avoidance of Malicious Nodes on MANETs

Deva Priya M, Aishwarya R, Anushya S, Keerthana S
Department of Computer Science & Engineering, Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India

ABSTRACT

In Mobile Ad hoc NETwork (MANET), the primary requirement is co-operative communication among nodes. Malicious nodes in a network may lead to attacks like Black Hole, Grey Hole and Wormhole attacks. In this paper, various routing schemes like Dynamic Static Routing (DSR), 2ACK, Best-Effort Fault-Tolerant Routing (BFTR) are considered and their behaviors against attacks are also examined. To deal with these attacks in these routing schemes, Enhanced Cooperative Bait Detection Scheme (ECBDS) that integrates the advantages of both proactive and reactive defense architecture based on DSR mechanism is designed. A malicious node can attract all packets by using forged Route REPly (RREP) packet to falsely claim fake shortest route to the destination and then discard these packets without forwarding them to the destination. ECBDS rejects the alarmed and detected malicious nodes in the initial stages. It outperforms the existing Cooperative Bait Detection Scheme (CBDS) mechanism in terms of Packet Delivery Ratio (PDR), Throughput and Routing Overhead.

Keywords : Wireless Communication, MANET, CBDS, Black Hole Attack, Grey Hole Attack, Wormhole Attack.

I. INTRODUCTION

Wireless networks provide unprecedented freedom and mobility for a growing number of Personal Digital Assistant (PDA) users who no longer need wires to stay connected with their workplace and the internet. Ironically, the devices that provide wireless service to these clients need lot of wiring to connect to private networks and the internet. Unlike basic wireless networks that simply untethers the client, the wireless mesh frees the network itself giving network architects and system integrators unprecedented freedom and flexibility to build networks in record time with high performance and without expensive cabling.

Ad hoc networks also called infrastructure less networks are complex distributed systems involving wireless links between nodes. Each node acts as a router to forward the data on behalf of other nodes. The nodes are free to join or leave the network without any restriction. Thus, the networks have no permanent infrastructure.

In ad hoc networks the nodes can be stationary or mobile. Therefore, one can say that ad hoc networks basically have two forms, one is Static Ad hoc NETworks (SANETs) and the other is called Mobile Ad hoc NETworks (MANETs). With the advent of new technologies such as IEEE 802.11[2], the commercial implementation of ad hoc network becomes possible.

One of the eminent features of such a network is its flexibility in deployment. Thus, it is suitable for emergency situations. But on the other side, it is also very difficult to handle the operation of ad hoc networks. Each node is responsible to handle its operation independently. Topology changes are very frequent and an efficient routing protocol becomes essential.

II. METHODS AND MATERIAL

1. Mobile Ad Hoc Networks (MANETs)

MANETs are self-organizing and self-re-configuring multi hop wireless networks, where the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating

in a friendly manner to engage themselves in multi-hop forwarding. The nodes in the network not only act as hosts but also as routers that route data from other nodes in the network.

In MANETs, where there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transmitting packets, a routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a Base Station (BS) can reach all mobile nodes without routing via broadcast in common wireless networks. In case of ad-hoc networks, each node must be able to forward data to other nodes. This creates additional problems along with the problem of dynamic topology which includes unpredictable connectivity changes.

As MANETs rely on wireless transmission, a secured way of message transmission is important to protect the privacy of the data. An insecure ad-hoc network at the edge of an existing communication infrastructure may potentially cause the entire network to become vulnerable to security breaches. In MANETs, there is no central administration to take care of detection and prevention of anomalies.

The identities of mobile devices or their intentions cannot be predetermined or verified. Therefore, nodes have to cooperate for the integrity of the operation of the network. However, nodes may refuse to cooperate by not forwarding packets of others for selfish reasons and not want to exhaust their resources.

Various other factors like the mobility of the nodes, promiscuous mode of operation, limited processing power, and limited availability of resources such as battery power, bandwidth and memory make the task of secure communication in ad hoc wireless networks difficult.

In routing, nodes exchange network topology information to establish communication routes. This information is sensitive and may become a target for malicious adversaries who intend to attack the network or the applications running on it.

2. Attacks in MANETS

There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information or distorting routing information, an attacker may successfully partition a network or introduce a traffic overload by causing retransmission and inefficient routing. The second and more severe kind of threat comes from compromised nodes, which might misuse routing information of other nodes or act on applicative data to induce service failures.

Attacks on ad hoc networks are classified into non-disruptive passive attacks and disruptive active attacks. The active attacks are further classified into internal and external attacks. External attacks are carried out by nodes that do not belong to network and can be prevented by firewalls and encryption techniques. Internal attacks are from internal nodes which are actually authorized nodes and part of the network, and hence it is difficult to identify.

Some of the predominant attacks in ad-hoc networks include:

- ✓ Black Hole Attack
- ✓ Wormhole Attack
- ✓ Grey Hole Attack

2.1 Black Hole Attack

In Black Hole attack, the attacker drops the received routing messages, instead of relaying them, so as to reduce the quantity of routing information available to other nodes. It is a passive and a simple way to perform a Denial of Service (DoS). The attack can be done selectively by dropping routing packets destined for a specified destination or by dropping all the packets and may have the effect of making the destination node unreachable, thus downgrading communications in the network [6] (Figure 1).

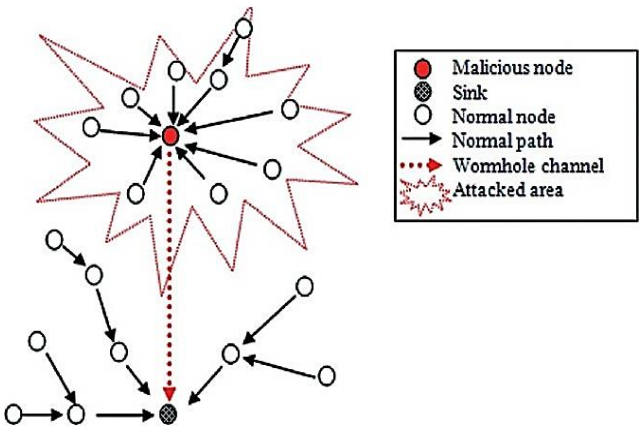

Figure 1. Black Hole Attack

2.2 Wormhole Attack

The wormhole attack is severe, wherein traffic is taken from one region of the network and replayed in a different region. For launching a wormhole attack, an adversary connects two distant points in the network using a direct low-latency communication link called the wormhole link. The wormhole link can be established by a variety of means, for example by using an Ethernet cable, a long-range wireless transmission, or an optical link. Once the wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the link and replays them at the other end. The severity of the attack comes from the fact that it is difficult to detect and is effective even in a network where confidentiality, integrity, authentication, and non-repudiation are preserved [3,5].

2.3 Grey Hole Attack

A Grey Hole attack is a variation of Black Hole attack, where an adversary first behaves as an honest node during the route discovery process, and then silently drops some or all of the data packets sent to it for further forwarding even when no congestion occurs. Detection of grey-hole attack is harder because nodes can drop packets partially not only due to its malicious nature but also due to overload, congestion or selfish nature. Grey Hole is a node that switches from showing normal behavior to depicting the behavior of a Black Hole. It is actually an attacker but acts as a normal node.

3. Routing Schemes

The behavior of existing routing schemes and their tolerance to collaborative attacks in MANETs are discussed in the ensuing section.

3.1 Dynamic Source Routing Protocol (DSR)

Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks. It forms a route on-demand when a transmitting node requests one. However, it uses source routing instead of relying on the routing table at each intermediate node. Determining source routes requires accumulating the address of each node between the source and destination during route discovery. The accumulated path information is cached by nodes processing the route discovery packets.

The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each node through which the packets traverse. This may result in high overhead for long paths or large addresses, like IPv6. The proposed Enhanced Cooperative Bait Detection Scheme (ECBDS) overcomes high overhead and circumvents intermediate attacks.

3.2 2ACK Scheme

The 2ACK scheme is a network-layer technique that is used to find links and extenuate their effects of attacks. It can be implemented as an add-on to existing path protocols in MANETs. It uses a new type of acknowledgment bundle termed as 2ACK, which is assigned a fixed path of two hops in the contrary direction of the data traffic path.

Suppose that N1, N2 and N3 are three successive clients along a path. The path from a source client ‘S’ to a destination client ‘D’ is established using the routing table information though the exchange of HELLO messages. When N1 sends a data bundle to N2 and N2 forwards it to N3, N1 is not aware of whether N3 receives the data bundle correctly or not. Such an ambiguity exists even when there is a good behavioural client. The problem becomes much more severe in open MANETs with a low potential client (Figure 2).

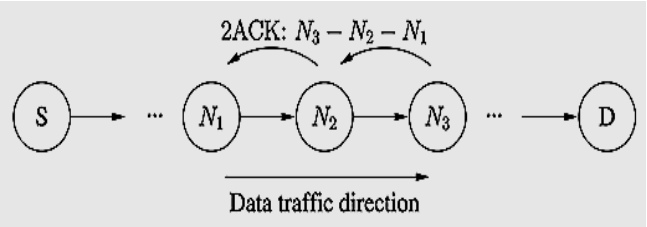

Figure 2. ACK Detection Scheme

ECBDS can be used effectively to avoid the acknowledgement problem and to increase Packet Delivery Ratio (PDR). The multi-hop bundle source maintains a record of data bundles’ IDs that have been sent out but have not been acknowledged.

3.3 Best-Effort Fault-Tolerant Routing (BFTR)

Best-Effort Fault-Tolerant Routing (BFTR) is a source-routing algorithm. The basic idea of BFTR is that, even if a bad node exhibits various behaviors, the behavior of any good node will be the same. The good node

delivers the packets correctly with high delivery ratio. Consequently, a good path consisting of purely good nodes also exhibits the same behavior pattern from the end-to-end point of view. Any path which deviates from such a pattern is considered a bad path. BFTR utilizes the existing statistics to choose the most feasible path, the one with the highest PDR in the immediate past. Likewise, a routing path is discarded when it becomes infeasible.

When there is a malicious node in a network, it results in low PDR and packet loss with high routing overhead. ECBDS can be combined with BFTR to overcome its disadvantages.

4. Cooperative Bait Detection Scheme (CBDS)

Cooperative Bait Detection Scheme (CBDS) aims to detect the collaborative Grey Hole, Black Hole and Wormhole attacks in MANET. In this scheme, the source node randomly selects the adjacent node which is used as a bait destination address to involve the malicious node in sending Route REPly (RREP) message. The malicious node in the routing operation can be found using the reverse tracing technique. The CBDS scheme integrates the advantages of proactive detection in the initial stage and the reactive defense architecture in the latter to achieve the goal.

Initially, the source broadcasts its Route REQ (RREQ) to the neighbors that are available within the source range. The neighbors receive the request and check the destination address. If a particular node is the destination, it generates RREP and sends to source through the corresponding path. If the node is not the destination node, it will forward to the neighboring nodes. After selecting the route, all the nodes update their route cache. Whenever the source node sends RREQ, it waits for RREP. After getting the RREP, the source node validates the route cache to know whether any malicious node has entered the network or not. If not, the source node generates opinion messages and broadcasts to all the neighbors about the presence of the malicious node [1 - 3].

In Grey Hole attack, the intruder depicts normal behavior, thus making it difficult for the CBDS to find the malicious node and its location. Similarly, in Wormhole and Black Hole attacks, the detection of malicious node becomes difficult since it drops both data packets and the RREQs.

5. Proposed Enhanced Cooperative Bait Detection Scheme (ECBDS)

Based on the study and analysis of CBDS against various attacks in MANETs, a new approach called Enhanced Cooperative Bait Detection Scheme (ECBDS) is defined.

The main aim of ECBDS is to discover faulty nodes on the path from the source to the destination by verifying the RREP through reply of having the shortest path to the destination. The malicious nodes are detected and put into blacklist.

In the existing CBDS mechanism, only the source node can detect the presence of malicious nodes and all the other nodes in the network will be oblivious to the location of malicious node. If the intruder nodes are dynamic as in the case of Grey Hole attack, the effectiveness of CBDS gradually decreases.

In the very first step of ECBDS, the source node sends the RREQ. Then, if the destination sends RREP, the reply packet verifier checks the threshold value for each node and rejects them if the estimated value is less than the threshold value and broadcasts alarm to other nodes. But if there is no reply from the destination node, then it checks the discovery hop limit and sends the RREQ again.

Once the alarm is broadcast to other nodes by the packet rejecter, then the system becomes regular and begins transmitting the packet data. It checks whether the PDR drops to the set threshold limit or not. If it drops to the specified threshold, then the source node randomly chooses the cooperative bait address of the one hop neighbor node ‘x’ to bait malicious node and sends the bait RREQ.

It checks whether there is any reply from other any node other than node ‘x’. If there is no reply from any node other than the node ‘x’, then it means that there is no malicious node in the network. But if any other node other than ‘x’ responds, then reverse tracing program is triggered, test packets are sent and the message is rechecked to detect the malicious node. The source node adds the malicious node into blacklist and sends an alarm packet to other nodes in the network.

There are a number of reasons why it is important to deploy ECBDS technique to detect and avoid the malicious nodes in MANETs.

i. The existing system CBDS has dealt with only the detection of Black Hole attack.

ii. The idea is to detect and overcome the Grey Hole and Wormhole attacks in MANETs by choosing the next best alternate route.

After the identification of the malicious node, the shortest path is picked from the existing routing path. These paths are checked again for any malicious activity.

If any malicious node is present, then the alarm packets are sent to all the other nodes in the network and the path containing the malicious node is rejected. This process is repeated till the alarm packet reaches the destination node. This increases the throughput of the network.

III. RESULTS AND DISCUSSION

Performance Evaluation

The schemes are simulated using ns2. The performance of CBDS and ECBDS against Black Hole, Grey Hole and Worn Hole attacks is analyzed with varying number of nodes.
The simulation parameters are listed below (Table 1).

Table 1. Simulation Parameters

Parameters	Values
MAC	802.11
Number of nodes	100
Packet size	1000 KB
Source position	Dynamic
Initial energy	0.5 unit
Simulator	ns2.3
Data rate	100 Mbps
Simulation duration	250 ms
Queue length	50

Packet Delivery Ratio: Packet Delivery Ratio is defined as the ratio of the number of packets received at the destination to the number of packets sent by the source.

Throughput: Throughput is the ratio of total number of data packets that are delivered or received per unit simulation time. Higher the throughput better is the protocol.

Routing Overhead

Routing Overhead is defined as the number of routing packets required for transferring the data over a network.

Black Hole Attack

BFTR_ECBDS offers better throughput in contrast to BFTR_CBDS, 2ACK_CBDS, 2ACK_ECBDS, DSR_CBDS and DSR_ECBDS.

It offers 4%, 19%, 14%, 7% and 3% better throughput when compared to BFTR_CBDS, 2ACK_CBDS, 2ACK_ECBDS, DSR_CBDS and DSR_ECBDS respectively (Figure 3).

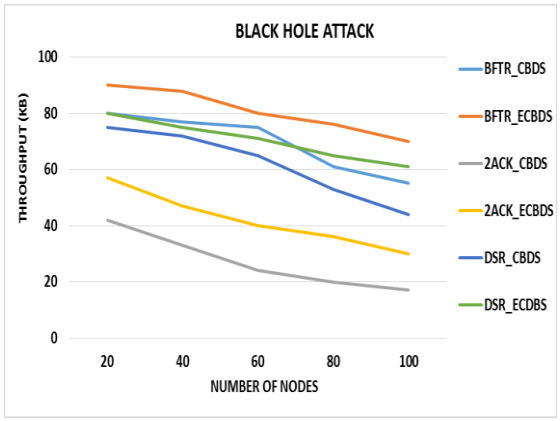

Figure 3. Black Hole Attack - Throughput

DSR_ECBDS offers better PDR in contrast to DSR_CBDS, 2ACK_CBDS, 2ACK_ECBDS, BFTR_CBDS and BFTR_ECBDS. DSR_CBDS, 2ACK_CBDS, 2ACK_ECBDS, BFTR_CBDS, BFTR_ECBDS yields 2%, 9%, 6%, 4% and 1% less PDR when compared to DSR_ECBDS respectively (Figure 4).

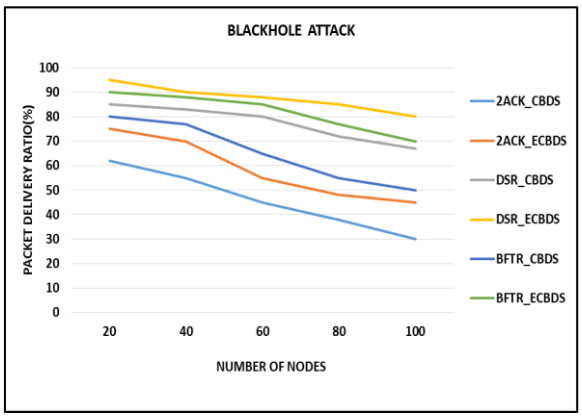

Figure 4. Black Hole Attack - PDR

2ACK_ECBDS involves less routing overhead in contrast to 2ACK_CBDS, BFTR_CBDS, BFTR_ECBDS, DSR_CBDS, and DSR_ECBDS. It involves 10%, 5%, 7%, 11% and 2% reduced routing overhead when compared to 2ACK_CBDS, BFTR_CBDS, BFTR_ECBDS, DSR_CBDS, and DSR_ECBDS respectively (Figure 5).

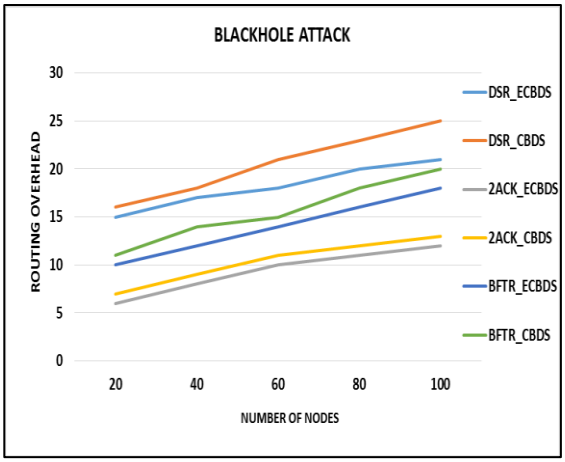

Figure 5. Black Hole Attack - Routing Overhead

Grey Hole Attack

BFTR_ECBDS offers better throughput in contrast to BFTR_CBDS, 2ACK_CBDS, 2ACK_ECBDS, DSR_CBDS, and DSR_ECBDS. It offers 1%, 9%, 4%, 5% and 2% better throughput when compared to BFTR_CBDS, 2ACK_CBDS, 2ACK_ECBDS, DSR_CBDS and DSR_ECBDS respectively (Figure 6).

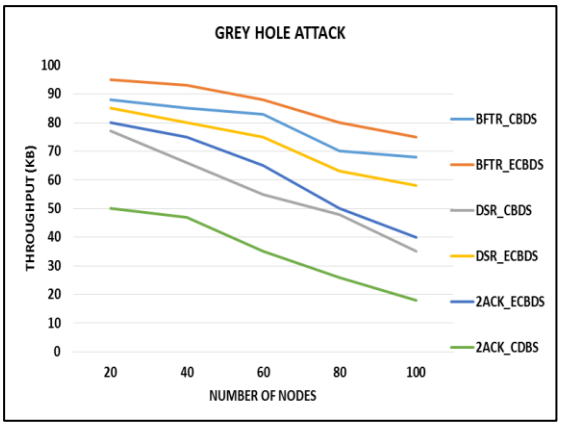

Figure 6. Grey Hole Attack - Throughput

DSR_ECBDS offers better PDR in contrast to DSR_CBDS, 2ACK_CBDS, 2ACK_ECBDS, BFTR_CBDS and BFTR_ECBDS. DSR_CBDS, 2ACK_CBDS, 2ACK_ECBDS, BFTR_CBDS, BFTR_ECBDS yields 4%, 6%, 3%, 1% and 1% less PDR when compared to DSR_ECBDS respectively (Figure 7).

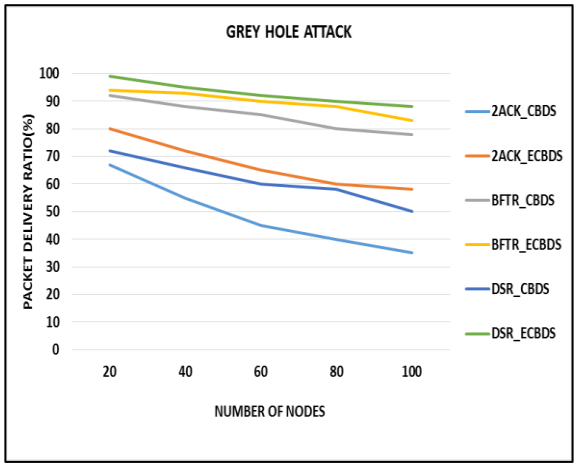

Figure 7. Grey Hole Attack - PDR

2ACK_ECBDS involves less routing overhead in contrast to 2ACK_CBDS, BFTR_CBDS, BFTR_ECBDS, DSR_CBDS, and DSR_ECBDS. It involves 15%, 6%, 9%, 16% and 4% lower routing overhead when compared to 2ACK_CBDS, BFTR_CBDS, BFTR_ECBDS, DSR_CBDS, and DSR_ECBDS respectively (Figure 8).

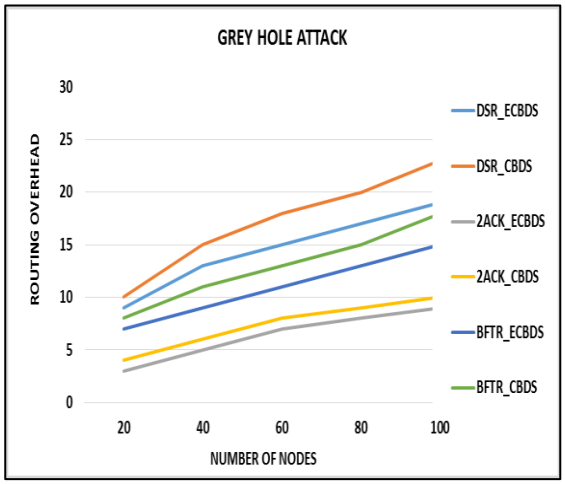

Figure 8. Grey Hole Attack - Routing Overhead

Wormhole Attack

BFTR_ECBDS offers better throughput in contrast to BFTR_CBDS, 2ACK_CBDS, 2ACK_ECBDS, DSR_CBDS, and DSR_ECBDS.

It offers 1%, 17%, 8%, 9% and 5% improved throughput when compared to BFTR_CBDS, 2ACK_CBDS, 2ACK_ECBDS, DSR_CBDS and DSR_ECBDS respectively (Figure 9).

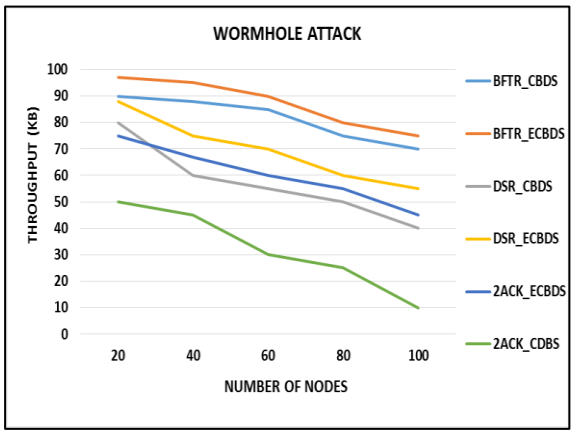

Figure 9. Wormhole Attack - Throughput

DSR_ECBDS offers better PDR in contrast to DSR_CBDS, 2ACK_CBDS, 2ACK_ECBDS, BFTR_CBDS and BFTR_ECBDS. DSR_CBDS, 2ACK_CBDS, 2ACK_ECBDS, BFTR_CBDS, BFTR_ECBDS yields 4%, 7%, 5%, 1% and 1% less PDR when compared to DSR_ECBDS respectively (Figure 10).

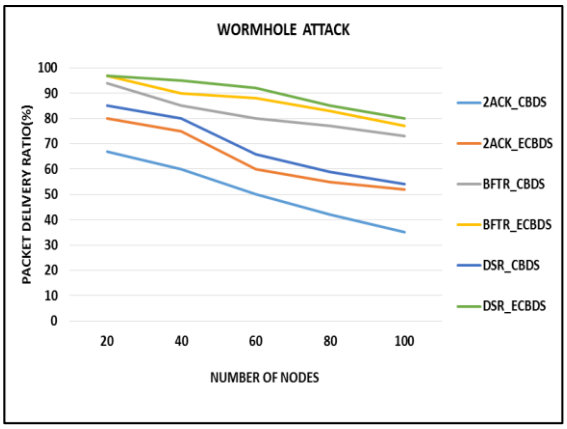

Figure 10. Wormhole Attack - PDR

2ACK_ECBDS offers less routing overhead in contrast to 2ACK_CBDS, BFTR_CBDS, BFTR_ECBDS, DSR_CBDS, and DSR_ECBDS. It offers 13%, 8%, 11%, 15% and 5% less routing overhead when compared to 2ACK_CBDS, BFTR_CBDS, BFTR_ECBDS, DSR_CBDS and DSR_ECBDS respectively (Figure 11).

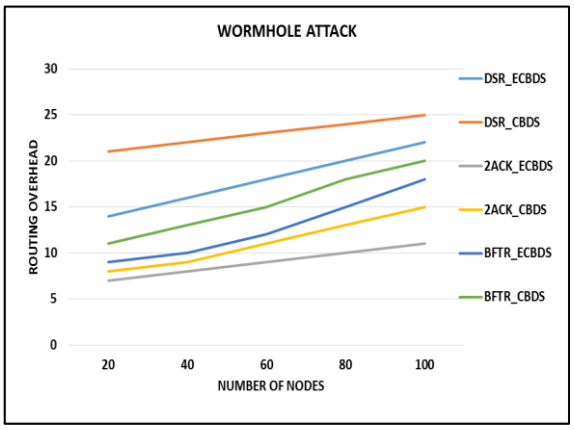

Figure 11. Wormhole Attack - Routing Overhead

IV.CONCLUSION

In this paper, Enhanced Cooperative Bait Detection Scheme (ECBDS) is proposed to overcome Black Hole, Grey Hole and Wormhole attacks. From the simulation results, it is evident that ECBDS embedded with DSR, 2ACK and BFTR outperforms the routing schemes deployed with Cooperative Bait Detection Scheme (CBDS) in terms of routing overhead, throughput and PDR.

Any detected malicious node is kept in a black list so that all other nodes that participate in the routing of the message are alerted to stop communicating with any other node in that list. The future scope could be the integration of the ECBDS with other well-known message security schemes so as to construct a comprehensive secure routing framework to protect MANETs against miscreants.

V. REFERENCES

[1] Tsou P.et al, CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture, February 2007.

[2] Corson S. and Macker J., Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, March 2008.

[3] Chang C., Wang Y. and Chao H., An efficient Mesh-based core multicast routing protocol on MANETs, April 2010.

[4] Johnson D. and Maltz D., Dynamic source routing in ad hoc wireless Networks 2010.

[5] Rubin I., Behzad A. and Caballero E., TBONE: A mobile-backbone protocol for ad hoc wireless networks, March 2011.
[6] Baadache A. and Belmehdi A., Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks, April 2011.
[7] Wankhade V., 2ACK-Scheme: Routing Misbehaviour Detection in MANETs Using OLSR, Vol. No. 1, Issue 5, July 2012.
[8] Yuan Xueand KLARA Nahrstedt, Providing Fault-Tolerant Ad hoc Routing Service in Adversarial Environments, August 2012.
[9] Shi-Chang L., Hao-Lan Y., & Qing-Sheng Z., Research on MANET security architecture design. In International Conference on Signal Acquisition and Processing. ICSAP'10, Vol 1, pp. 90-93, February, 2010.
[10] Chang J. M., Tsou P. C., Chao H. C., & Chen J. L., CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture. In 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), pp. 1-5, February 2011.
[11] Agalya A., Nandini C., & Sridevi S., Detecting and Preventing Black Hole, March 2013.
[12] Attacks In MANETS Using CBDS (Cooperative Bait Detection Scheme), International Journal of Modern Trends in Engineering and Research (IJMTER), Vol. 2, Issue 04, February 2014.
[13] Akinlemi Olushola O., & Babu K.S., Cooperative Bait Detection Scheme (CBDS) To Avoid the Collaborative Attacks of Nodes in MANET, March 2014.
[14] Sharma M., and Chander Prabha C., Byzantine, Attacks in MANET through Enhanced CBDS Technique. American International Journal of Research in Science, Technology, Engineering & Mathematics AIJRSTEM, pp. 14-543, June 2014.
[15] Chang, Jian-Ming, et al. "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach." IEEE Systems Journal 9.1, pp.65-75, January 2015.