IJITKM Volume 8 • Number 2 Jan-Jun 2015 pp. 4-7 (ISSN 0973-4414)

Security in MANET Using ECBDS on Resource Consumption Attack and Byzantine Attack

Manjeet Singh[1], Apurva Sharma[2]
[1,2]Computer Science Department, SUS College of Engineering and Technology, Tangori, Punjab.
manjeetbenipal1990@yahoo.com, apurva19.sharma@gmail.com

Abstract - Mobile Ad-hoc networks self constructing wireless networks in which nodes are free to move in any direction due to which these networks might be more prone to security issues as compared to wireless networks due to number of factors like malicious nodes in the network, changing scale and etc. This paper tries to solve the security issues with the ECBDS mechanism. ECBDS is a type of modified version of CBDS technique. This mechanism rejects the alarmed and detected malicious nodes in the initial stages. In this paper the ECBDS technique is applied on two attacks- Resource consumption and Byzantine attack.

Index Terms – Enhanced Cooperative Bait Detection Scheme (ECBDS), Resource Consumption attack, Byzantine attack.

INTRODUCTION

With the emerge of mobile technology, the wireless communication is becoming more popular than ever before. This is due to technological advances in laptops & wireless data communication devices such as wireless modems & wireless LANs. It has lead to lower prices & higher the data rates which has resulted in rapid growth of mobile computing. MANETS are self-constructing mobile networks in which each device is free to move independently in any direction & change its links to other devices frequently. Ad-hoc networks do not rely on any pre-established infrastructure, so therefore they can be even deployed on places with no infrastructure. So its useful in disaster recovery situations. Ad-hoc networks are helpful in conferences where people participating in conference can form a temporary network without engaging in services of any pre-existing network [1].

As mobile ad-hoc networks are wireless networks so they might be more prone to security issues as compared to wired networks. Here we are listing some of main vulnerabilities in the MANETs:-

- No predefined boundary- In the mobile ad-hoc networks the nodes work in the wireless environment where they are free to join and leave the wireless network. So the malicious nodes might come and communicate with the nodes in their radio range. Attacks include DOS (Denial Of Service), Eavesdropping and etc.
- Malicious nodes in the network- As there is no predefined boundary so there might be a number of malicious nodes present in the network.
- No centralized control facility- There's no centralized control facility in the MANETS which might lead to a number of security problems.
- Limited energy resource- As all mobile nodes depend upon battery power for their operation so it's another major problem when the target node remains busy in handling the traffic all the time and consuming lots of battery power.
- Changing scale- The scalability of the mobile networks keeps on changing all the time which makes to predict the number of nodes in the future time which is an another major problem. [2]

In the paper we have classified the number of attacks into two categories, namely active and passive attacks.

- Active attacks- Active attacks includes information modification, information interruption and interrupting the normal functionality of the MANET.
- Passive attacks- Passive attacks obtain the vital data exchanged within the network without disrupting the operation of communications.

Table 1: Types of attacks

Active attacks	DOS, spoofing, jamming, modification, replaying.
Passive attacks	Monitoring, eavesdropping, traffic analysis

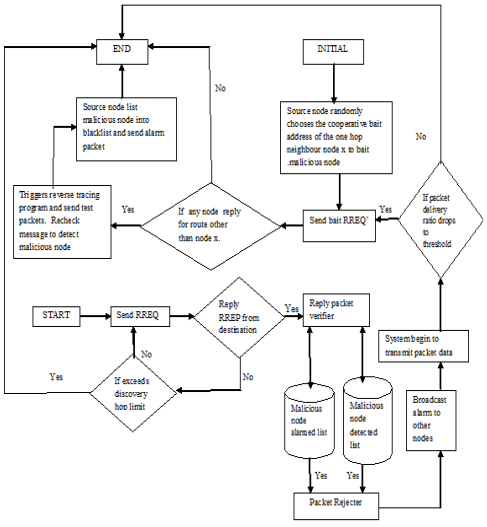
Attacks could also be classified as external or internal. In internal attacks the malicious node from the network gains unauthorized access while external attack causes congestion, sends false routing information and causes unavailability of services. Attacks could also be classified according to network protocol stacks. [3]

Table 2: Security attacks on protocol stacks in MANET.

LAYER	ATTACKS
Application Layer	Data corruption, Repudiation
Transport Layer	SYN flooding, Session hijacking
Network Layer	Location disclosure attack, Byzantine, Flooding, Blackhole, Wormhole, Resource consumption,
Data Link Layer	WEP weakness, Traffic analysis & Monitoring
Physical Layer	Interceptions, Jamming, Eavesdropping
Multi-layer Attacks	Replay, DoS, Made-in-the-middle, Impersonation,

A number of algorithms has been formulated to overcome the security issues related to the malicious nodes. In this section we discuss several security schemes to deal with the above described attacks.

- 2 ACK – In this scheme 2 hop acknowledgement packets are sent in opposite directions of routing path to indicate that data packets have been successfully received. Scheme belongs to class of proactive schemes & hence produces additional routing overhead to malicious nodes. [4]
- BFTR (Best Fault Tolerant Routing) – BFTR uses end to end acknowledgement to monitor quality of routing path to be chosen by destination node. Main drawback of BFTR is that malicious nodes may still exist in newly chosen route.
- CBDS – This technique works on DSR mechanism to detect the malicious nodes in the network. It combines the advantages of both proactive and reactive detection schemes to detect malicious nodes.[5]
- Intrusion detection - Y Zhang & W Lee proposed intrusion the approach in which they proposed distributed and cooperative framework database of previously stored detected and alarmed list as shown in flow chart.



Detected malicious nodes are kept in "malicious node detected list" and other participating routing are alarmed to stop communicate with any node in that list.

The technique is DSR based. It identifies the various addresses of the nodes in the selected routing path from the source to the destination after the RREP message has been received from the destination node. There might be the malicious nodes present in the network that may send a fake reply of having the shortest path to the destination. So with ECBDS technique these malicious nodes are detected and put into blacklist.

- to detect the attack. Each node in the MANET participates in the process & detects the sign of intrusion locally and independently and also sends the information to other nodes in the network.
- Cluster based intrusion detection - In this approach the whole network is organized as a set of clusters such that each node is member of one or more clusters. Only one node in the cluster will monitor intrusion detection. Nodes are in the same radio range.
- Defending wormhole attack using leash - Wormhole attacks are defended using packet leashes. It is the maximum information added to the packet to restrict its maximum allowable transmission distance. Receiver examines its time & distance. [2]

PROPOSED APPROACH

In the proposed work we develop a new technique named Enhanced Cooperative Bait Detection Scheme (ECBDS) by enhancing previous technique called CBDS. The main idea behind ECBDS technique is to discover faulty nodes on the path from the source to destination by verifying reply packet (RREP) through

In the very first step source node sends request RREQ. Then if there is any reply RREP from the destination then the reply packet verifier checks the previous alarmed malicious node list and malicious node detected list and rejects them with the help of packet rejecter and broadcasts alarm to other nodes. But if there is not any reply from the destination node then it checks the discovery hop limit and again sends the request RREQ.

Then after the alarm is broadcasted to other nodes by the packet rejecter then system is regular and begins transmitting the packet data. Then it checks that whether the packet delivery ratio drops to the set threshold limit or not. If it drops to threshold then the source node randomly chooses the cooperative bait address of the one hop neighbour node x to bait malicious node and sends the bait RREQ'. Then it checks that if there is any reply from other than node x. If there is no reply from any other node than node x then it means that there is no malicious node in the network. But if there is reply of any other node except x, then Reverse tracing program is triggered and test packets are sent and message is rechecked to detect the malicious node. Then source node list malicious node into blacklist and sends the alarm packet to the other nodes in the network.

PERFORMANCE EVALUATION

1 Throughput

Throughput is the ratio of total number of delivered or received data packets per unit simulation time. Higher the throughput better is the protocol. The throughput is high in case of ECBDS.

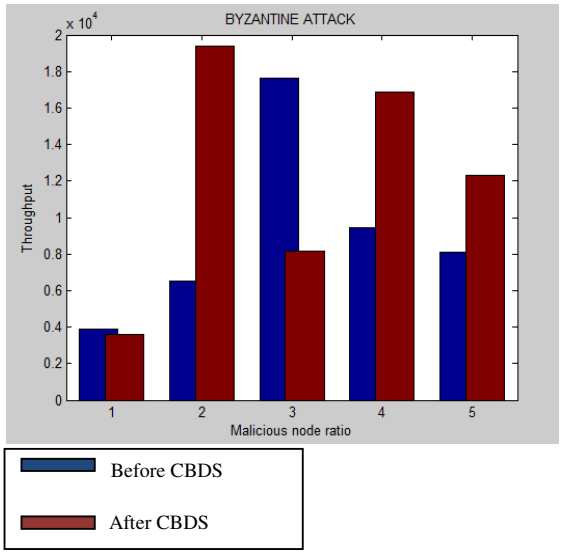


Figure 1: Throughput Graph Implementing ECBDS during Byzantine Attack

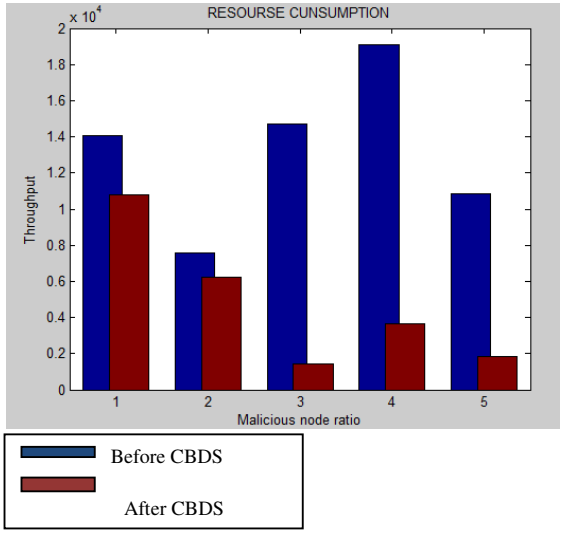


Figure 2: Throughput Graph Implementing ECBDS during Resource Consumption Attack

2 Packet Delivery Ratio

Packet Delivery Ratio is the ratio of total number of packets delivered to the total number of packets sends to the destination.

PDR = ∑ Number of packet receive / ∑ Number of packet sent

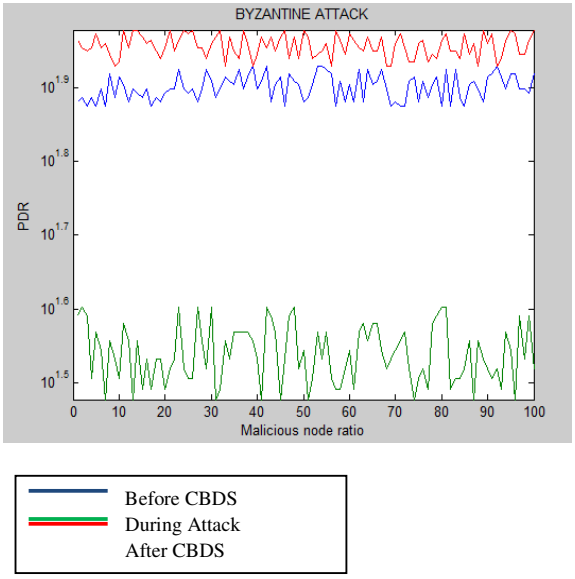


Figure 3: PDR Graph Implementing ECBDS during Byzantine Attack

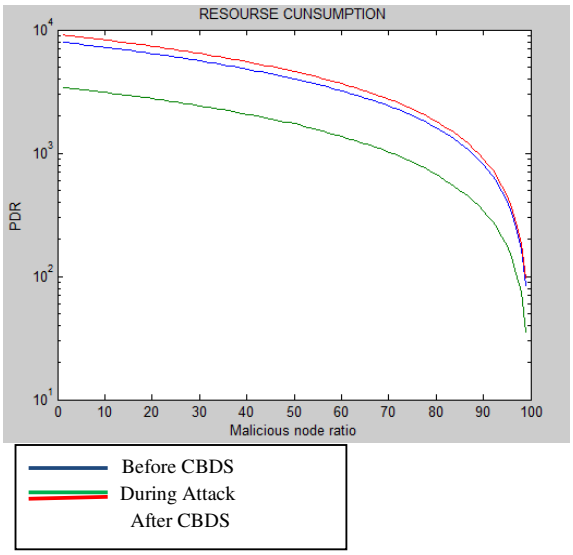


Figure 4: PDR Graph Implementing ECBDS during Resource Consumption Attack

3 End to End Delay

End-to-end delay is defined as the time taken for a packet to be transmitted in network from source to destination.

End to End delay = ∑ (arrive time – send time) / ∑ Number of connections.

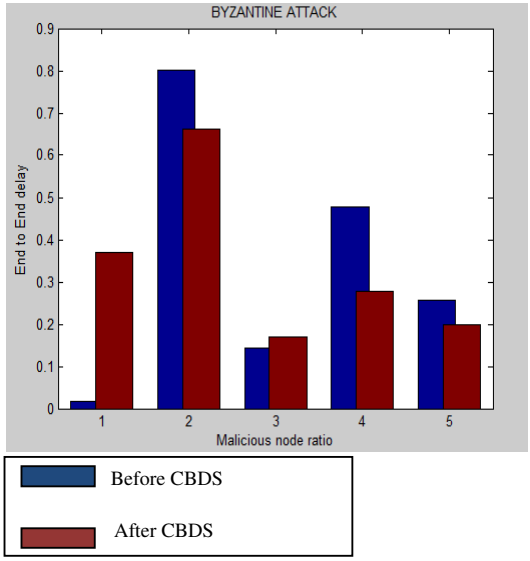


Figure 5: End to End Delay Graph Implementing ECBDS during Byzantine Attack.

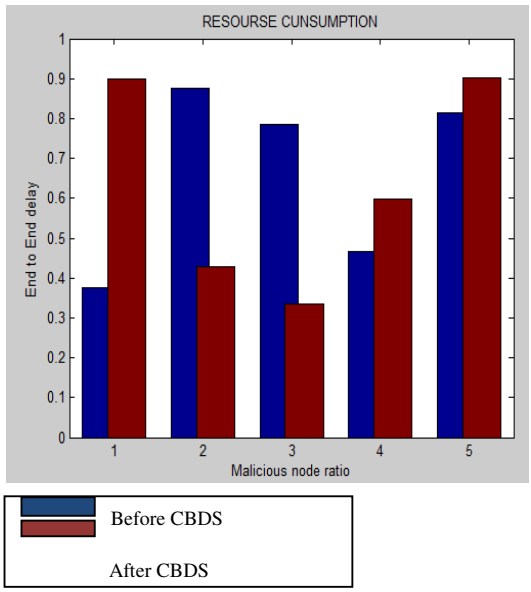


Figure 6: End to End Delay Graph Implementing ECBDS during Resource Consumption Attack.

CONCLUSION

ECBDS is a costly prevention technique used to prevent wireless system from attacks like Black Hole Attack etc. Due to its cost it is mandatory to check that is it effective for other attacks too. We have implemented ECBDS technique to prevent Byzantine and Resource Consumption Attacks. We have succeeded in preventing the nodes from malicious nodes using ECBDS. In Byzantine Attack the malicious node is identified using ECBDS and blacklisted so that system can be prevented. In Resource Consumption Attack the nodes are prevented to communicate with malicious nodes using ECBDS. Using ECBDS we are succeeded in improving throughput of the system. PDR has also increased against both the attacks with the help of this technique. End to End Delay has reduced as data reaches to receiver without communication with malicious node.

REFERENCES

1) Nicklas Hedman and Tony Larsoon:- Routing protocols in wireless ad-hoc networks.
2) Durgesh Kumar Mishra (Acropolis Institute of Technology and Research, Indore, India). Mahakal Singh Chandel (Arjun Institute of Advaced Studies and Research Centre, Indore, India),Rashid Sheikh *IEEE 2010*. Security Issues in MANET: A Review.
3) Bing Wu, Jie Wu, Jainmen Chen, Mihaela Cardie – A survey on attacks and countermeasures in Mobile Ad Hoc Networks.
4) Prof Ravindra Rathod, Prof M D Ingle, Prof R M Kawale – Detecting of routing misbehaving links in MANET by 2ACK scheme.
5) Chin-Feng Lai, Han-Chieh Chao, Jian-MingChang, Isaac Woungang, and Po-Chun Tsou, *Member, IEEE 2014*. Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach.