# An Enhanced Mechanism to Detect and Prevent Byzantine Attack in Wireless Network based on CBDS

Neha Choudhary
Dept of Comp Engg, U.I.E.T Kurukshetra University, Kurukshetra, India

Poonam Dabas
Assistant Professor, Dept of Comp Engg, U.I.E.T Kurukshetra University, Kurukshetra, India

**Abstract: In wireless networks nodes are interconnected with each other with the help of base stations. A base station takes messages from number o nodes and forward to destination node also if a node needs any message then it takes that message from base station. When messages were transmitted through intermediate nodes then security leakage chances may increases so to secure transmission of messages is a challenging task for researchers. There are different types of attacks such as black hole attack, Sybil attack, selfish node attack, denial of service attack and byzantine attack. Detection of byzantine attack is difficult because it is more complicated attack then other attacks because it combines all the features of existing attacks such as black hole attack and denial of service attack. In this paper an attempt has been made to propose a enhanced CBDS mechanism to detect and prevent byzantine attack. The main idea behind ECBDPS technique is to discover faulty nodes on the path from the source to the destination by verifying reply packet (RREP) through database of previously stored detected and alarmed list.**

**Index Terms – Wireless Networks (WNs), Byzantine attack, CBDS, ECBDPS and Alarmed list.**

## 1. INTRODUCTION

Wireless networks (WNs) are the networks in which no physical infrastructure is available through which node may contact each other. In wireless networks nodes were connected through each other via some base stations and they are not connected directly with each other. It helps nodes to move freely and extend their communication areas according to their needs. It will also causes network performance due to presence of some malwares. There are number of attacks presented in network to disturb the performance of network. Byzantine attack is one of them. In byzantine attack, attacker node provides wrong routing information or it may drop the messages in network [1]. An attacker located between multiple communicating nodes wants to waste the network bandwidth and disrupt connectivity. The malicious node can continuously send fake RREP packets of routes to other nodes, thereby overloading the network. This consumes the resources of all neighbors that communicate, overloads the network, and results in performance degradations [2]. When there is byzantine attack in networks it may cause time delay in networks and reduces throughput of the network.

## 2. RELATED WORK

Although different researchers proposed various mechanisms to detect byzantine attack in wireless networks but each technique have some advantages as well as drawbacks. One of the proposed techniques was CBDS technique [3][4].Cooperative Bait Detection Scheme (CBDS): CBDS is a mechanism which effectively detects malicious nodes that attempts to launch byzantine attacks [5]. In this scheme the address of adjacent node is used as Bait destination address to bait malicious nodes to send reply RREP message. Malicious nodes are detected using reverse tracing technique [6]. The main drawbacks of CBDS were that it only detects that there is byzantine attack in network not provides any mechanism to prevent it from network [7]. Another drawback was that it just sends some bait messages to check whether it is byzantine attack is presented or not but based on some bait messages it is very difficult to detect byzantine attack so this mechanism was not successful in the detection of byzantine attack [8]. To overcome drawbacks of CBDS we will try to propose enhanced CBDS mechanism in which we develop a new technique named ECBDPS by enhancing a previous technique called CBDS.

## 3. PORPOSED MODELLING

In the proposed algorithm initialize nodes in the network. Here sender node SN sends RREQ i.e. root request message in the network to all intermediate nodes and waits for the route reply. Whenever the RREP i.e. route reply message comes in time from the destination node itself then it can be concluded that the system is working fine over the network hence end the process. But, if the normal time to work over the network is more than the threshold time i.e. $T_h$ then just simply end the process and send a new RREQ again over the network for the packet's communication over the network. When once again a RREQ is sent over the network check for the optimal path that we can say is the best path or the error free path for the message packet traversal, must be equal to the value of number of nodes present over the network and also check for the value of the delivery ratio i.e. DR, if the threshold value is less than the $T_h$ means a bait RREQ is needed to be send over the network to bait the malicious or threat node on the network. Otherwise, end the process. Now, check the value of RREP, if it comes to be true then set the value of trace i.e. the traced path for the threat node to be detected and set trace value equals to 1, if RREP comes out to be false then just simply end the process. For the value of trace equals to 1 check traced path and detect $M_n$ i.e. the black list, it is needed to maintain the integrity, authenticity and confidentiality of nodes over the network, the black list is maintained for the malicious nodes and the list for their traced paths. While traversing over the network a value of $M_n$ is detected then simply just ignore the path of that node as it is threat node for the transmission of the packets. Otherwise, the packet transmission must be continued over the desired path for the communication process over the safe network and hence the communication will term out to be a successful process till the destination node and no loss of information and confidential data and information is lost over the network. Hence, the process is ended safely at the end [9].

```
1)  Start
2)  Initialize nodes in the network.
3)  Parameter used: SN=Sender Node, DN=Destination
    Node, RREQ=Route Request, RREP=Route Reply,
    DR=Delivery Ratio, T_h=Threshold Value, M_n=Black
    List, Time= Message Transmission Time,
    Trace=Traced Path.
4)  Send route request parameters in network.
5)  If(RREP==DN)
    {
6)   Transmission is well
7)    Else
      {
           If (Time> T_h)
           {
              Else
              {
                Send RREQ again
                }
           }
      }

8) If (number of nodes present = optimal path)
     {
      If (DR<T_h)
      {
        Send Bait RREQ
      }
     }
9)  Else If (RREP=True)
      {
       Set trace=1
8)       Else
9)          Check trace and detect M_n.
10)           If M_n=Black List
            Then
              {
                M_n detected then ignore the path
                }
            Else
              {
               Continue Packet transmission until sent to D.
11)             }
12)  }
13)  End
```

## 4. RESULTS AND DISCUSSIONS

Tool used: to implement proposed mechanism we use MATLAB. It is efficient, robust and highly reliable which grant the user the ease of graphical interface, developing and running the simulation and validation of the results.

Simulation Parameters

The performance of CBDS and ECBDPS has been analyzed with varying Number of Rounds and Adaptability to Balance Energy of nodes. The parameters used for simulation are summarized in Table 1 and positioning of nodes. Initial position of nodes in the network is shown in Figure 5.7. The performance metrics comprises of various parameters are discussed.

Table 1 Simulation Parameters

| Parameters | Values |
|---|---|
| Number of Nodes | 100 |
| Environment Size | 400x400 |
| Source Position | Dynamic |
| Initial Energy of Each Node | 0.5 Unit |
| Simulator | MATLAB 2009 |
| Operating System | Windows7 |

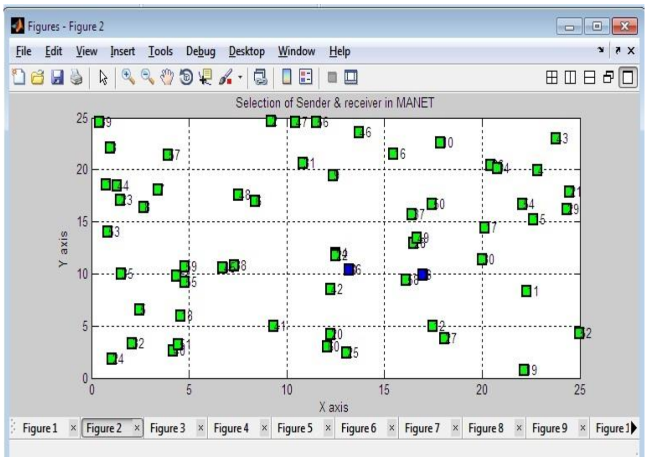
Figures - Figure 2
File Edit View Insert Tools Debug Desktop Window Help
Selection of Sender & receiver in MANET
Y axis
X axis
0 5 10 15 20 25
Figure 1 Figure 2 Figure 3 Figure 4 Figure 5 Figure 6 Figure 7 Figure 8 Figure 9 Figure 1

Fig 1 Placement of nodes in Wireless Networks

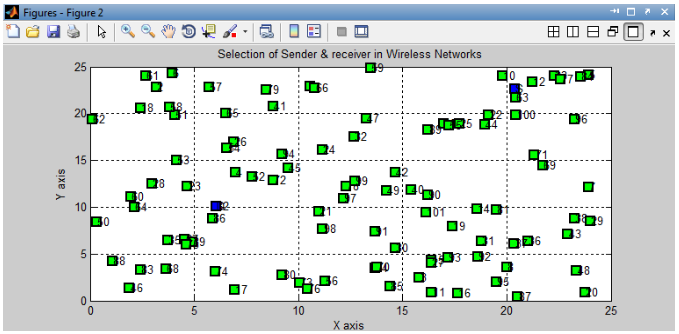

Fig 2 Selection of sender and receiver in Wireless Networks

Figure2 shows source which is blue in color transmit packets via intermediate nodes in network to destination which is green in color. Here there is no intermediate nodes which malicious.

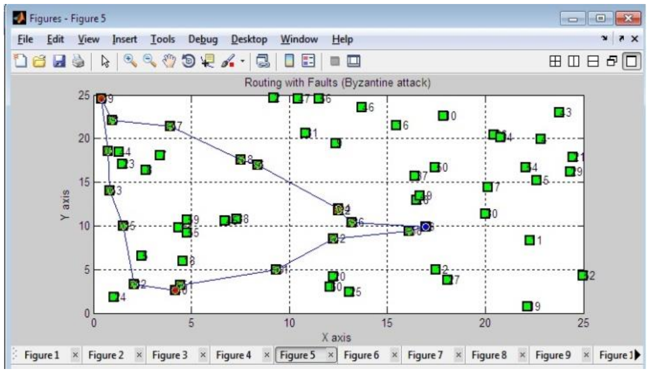
Figures - Figure 5
File Edit View Insert Tools Debug Desktop Window Help
Routing with Faults (Byzantine attack)
Y axis
X axis
0 5 10 15 20 25
Figure 1 Figure 2 Figure 3 Figure 4 Figure 5 Figure 6 Figure 7 Figure 8 Figure 9 Figure 1

Fig 3 Transmission in network during Byzantine Attack

Figure3 shows the case of Byzantine attack by two malicious nodes red in color prevent data from reaching intended destination. The malicious nodes in the network move data among them in circular fashion rather than transmitting to destination node. Transmitting node green in color send data to malicious nodes and malicious node send the data to other malicious and so on.

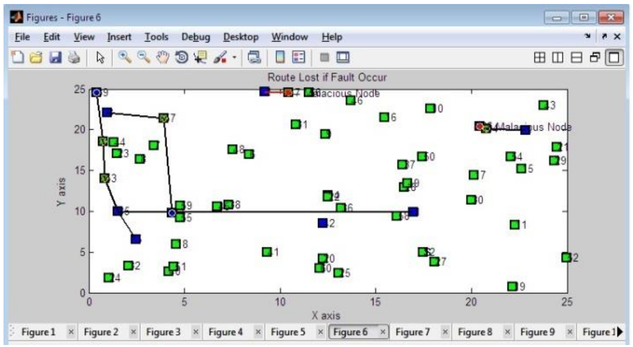
Figures - Figure 6
File Edit View Insert Tools Debug Desktop Window Help
Route Lost if Fault Occur
Malacious Node
Malacious Node
Y axis
X axis
0 5 10 15 20 25
Figure 1 Figure 2 Figure 3 Figure 4 Figure 5 Figure 6 Figure 7 Figure 8 Figure 9 Figure 1

Fig 4 Implementation of CBDS

Figure 4 shows the CBDS scheme. The route is lost when the malicious nodes get the packet. Only alarm packet is broadcasted.

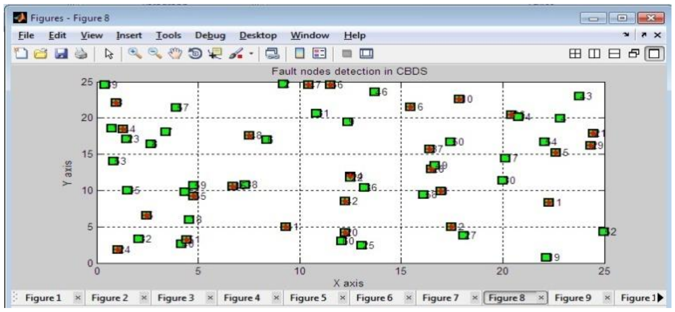
Figures - Figure 8
File Edit View Insert Tools Debug Desktop Window Help
Fault nodes detection in CBDS
Y axis
X axis
0
5
10
15
20
25
Figure 1 Figure 2 Figure 3 Figure 4 Figure 5 Figure 6 Figure 7 Figure 8 Figure 9 Figure 1

Fig 5 Faulty nodes detection

Figure 5 shows how byzantine attack is being detected by ECBDPS Scheme. So nodes detect the malicious nodes and avoid them via keeping record of node in black list. Moreover all other nodes are given information about malicious node detection.

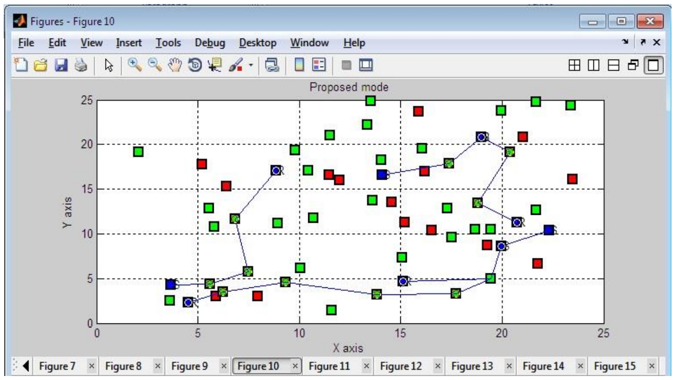
Figures - Figure 10
File Edit View Insert Tools Debug Desktop Window Help
Proposed mode
Y axis
X axis
0
5
10
15
20
25
Figure 7 Figure 8 Figure 9 Figure 10 Figure 11 Figure 12 Figure 13 Figure 14 Figure 15

Fig 6 Proposed ECBDPS

Figure 6 shows how byzantine attack is being prevented by ECBDPS Scheme. So nodes does not send data via malicious node as they detect the malicious nodes and avoid them via keeping record of node in black list. Moreover all other nodes are broadcasted physical and MAC address of malicious node on detection. This detection is purely on basis of symptoms of byzantine attack and Resource Consumption attacks.

## 5. CONCLUSION

Security in wireless networks is very challenging task for researchers. Although number of researchers provide number of techniques to deal with byzantine attack. One of them is CBDS mechanism to detect byzantine attack. In this paper we provide proposed ECBDPS mechanism to detect and prevent byzantine attack from in wireless networks. The main drawbacks of CBDS were that it only detects that there is byzantine attack in network not provides any mechanism to prevent it from network. Results shows that proposed mechanism is better than previous CBDS because delivery ratio is high and proposed mechanism also number of byzantine detection rate is also high in proposed mechanism. In future we continue working on it and propose an extended mechanism that focuses on detection and prevention of byzantine attack with minimum delay occurrence.

## REFERENCES

[1] Sara Chadli, Mohamed Emharraf, Mohammed Saber and Abdelhak Ziyyat, "Combination of hierarchical and cooperative models of an IDS for MANETs", Tenth International Conference on Signal-Image Technology & Internet-Based Systems, IEEE 2014 pp: 230-236.

[2] Nikhil R Joshi,Chandrappa D.N, "Manet Security Based On Hybrid Routing Protocol and Unique Cryptographic Identity", IEEE 2015, pp: 1-5.

[3] Jun Du, Xiang Wen, Ligang Shang, Shan Zou, Bangning Zhang, Daoxing Guo1 and Yihe Song, "A Byzantine Attack Defender for Censoring-enabled Cognitive Radio Networks", IEEE 2015 pp:1-5.

[4] Ziteng Sun, Chuang Zhang and Pingyi Fan, "Optimal Byzantine Attack and Byzantine Identification in Distributed Sensor Networks", IEEE, 2016, pp: 1-6.

[5] Mai Abdelhakim, Leonard E. Lightfoot, Jian Ren, and Tongtong Li, "Distributed Detection in Mobile Access Wireless Sensor Networks under Byzantine Attacks", IEEE Transactions on Parallel and Distributed Systems, 2014, pp: 950-959.

[6] Renu Sharma and Jitender Grover, "Mitigation of Byzantine attack using Enhanced Cooperative Bait Detection and Prevention Scheme (ECBDPS)", IEEE 2015, pp:1-6.

[7] Blaz Ivanc and Borka Jerman Blazic, "Development Approach to the Attack Modeling for the Needs of Cyber Security Education", IEEE 2016 pp:216-220.

[8] Amirmohammad Sadeghian and Mazdak Zamani, "Detecting and Preventing DDoS Attacks in Botnets by the Help of Self Triggered Black Holes", Asia-Pacific Conference on Computer Aided System Engineering (APCASE), IEEE 2014 pp: 38-42.

[9] Andrey Rukavitsyn, Konstantin Borisenko and Andrey Shorov, "Self-learning Method for DDoS Detection Model in Cloud Computing", IEEE 2017 pp: 544-547.