# Distributed Detection Methods for Byzantine Attack in Tree Topology

Apeksha.B.Dhakde
PG Student, Department of CSE
G. H. Raisoni College of Engineering

Sonali.U.Nimbhorkar
Professor, Department of CSE
G. H. Raisoni College of Engineering

## ABSTRACT
In Adhoc network the Byzantine Attack is the most safety threads as it bring to a halt in the communication of nodes in the network and behave like a fair nodes while take part normally in the network. It is very important in the network to provide the communication between the nodes is to be error free and communication takes place in a particular time period. In a tree based topology every node is take part in communication with other nodes. So it is major challenge to protect the data transmission between the nodes in the network as many types of attacks are collaborating with Byzantine attack. In order to provide optimal strategy to generate the attack in the network and also provide the good way to attack the precious node which will affect the network with a big loss. some solution is to be provided so the attack can be take place on the most important node who have the confidential data in it, with the cost associated to the node and some algorithm should provide in order to find the time delays between the nodes also provide bounds to the nodes in order to transmit the data ,detect the faulty data transmission and also limits the use of the resources by falling the investment of resources which takes part in communication. In this paper the major focus is on the cost which is provided to the nodes while differentiating with the random cost, linear cost and performance can be measures in term of minimum cost with the linearity, packet delivery,End-to-end delays, Throughput with and without attacks.

## General Terms
Polynomial time algorithm, Knapsack problem

## Keywords
Distributed detection, Byzantine attack, Tree topology, AODV (Adhoc on demand distance vector)

## 1. INTRODUCTION
In Adhoc network the data transmission process is required to capture the sending packets from one source to other destination so as to mean to provide cost to every node in the network the security to the packets in order to deal with the communication specially in the tree based network where every nodes participate in communication .As the data transmission takes place many other malicious nodes involves in the communication process and behaves like a fair nodes and always take part in communication while sending the faulty data to the other nodes and make the whole network faulty. There are many attack are generated in the network as the communication takes place between the nodes. It is very difficult to detect the malicious nodes from the whole network. In tree network the data can be distributed so that at the particular need of the data they should be available so the communication takes place smoothly but in that same condition many attacks are generated and in the case of Byzantine attack many attacks are automatically combine with it. So the main focus on this paper is to detect the attack on the network which combines with Byzantine attack and also the Byzantine attack is the most dangerous attack as it compromises the nodes in the network and behaves like a normal on. In tree network there is a relation of parent and child. So the child node always depends on the parent node for the data availability. It will overcome with the distributed environment while the data available to the nodes when it demands, while the data load on the network may decrease, resources always available for the data transmission, automatically time delays from that particular reason may also decrease, also increase the transmission area of the nodes and maintain hierarchy into the tree while levels associated to it. In this paper the different types of cost associated to the node and measure the performance with providing the linear, random. [1], [2]

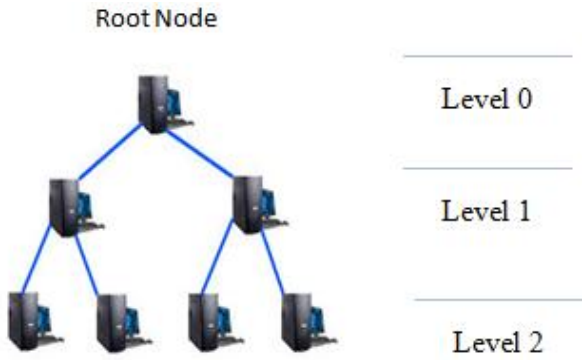


**Fig 1: Hierarchy of Tree Topology**

Tree network has the ability to provide the appropriate balance between the transmission range, functionality of the nodes in the network, reliability, random cost, linear cost association to the nodes.

The rest of this paper is as follows: Section 2 describes the Byzantine attack followed by in section 3 existing scheme comparison, methodology of work is discussed in section 4.Analysis and discussion is describe in section 5.Simulation result is describe in section 6 and conclusion is discuss in section 7.

## 2. BYZANTINE ATTACK
Byzantine attack is the most promising attack in which it compromises the nodes and the set of the compromise nodes are able to take part in communication while behaving like a normal nodes and make a communication strong but with a falsified packet delivery also associated with it. So the detection t such attack is very difficult also time consumption may take place. Major challenge in the detection of Byzantine attack is that many other attack are also deployed with it so

the work of detection also increases as the network increase therefore in some distributed detection scheme should introduce in order to deal with the situation[10].

# 3. EXISTING SCHEME COMPARISION

While dealing with the Byzantine attack many scheme, methods are introduced. Some of the schemes provide the good results in order to detect the attack, prevention also take better on it. Many time as the comparison take place the scheme always requires some modification in order to get the better result than the existing one. Here are some of the existing scheme are introduced below in table 1.

**Table 1. Comparision of Existing Scheme/Methods**

| SCHEME/ METHOD | APPROACH | LIMITATION |
|---|---|---|
| q-out-m rule[3] | Provide a good substitution between the miss detection probability and the false alarm rate. | -Fusion scheme is infeasible as the network size extended and much other attack comes in the network. -provide the high complexity in the computation. |
| AMD Code (Information Theoretical secrecy) [1] | Probability of the byzantine adversary decreases fast as the number of channel takes part in communication. while broadcasting the incorrect signal. | It cannot be more feasible in the synchronous secrecy process |
| Random linear network coding[7],[8],[11] | It doesn't require the state information it uses the encoding vector scheme in order to encode/decode the fair data | -Support the dynamic nature -Network state information is always change, unstability maintain |
| Conditional Frequency Check (CFC)[3] | Concatenated with the Markova spectrum model with one trusted sensor, while achieving the high, accuracy in the detection of malicious nodes in the network. | Modification of algorithm provides the better result than existing one. |
| End-to-end error correction[9] | It can be able to differentiate the fair node and the malicious node through which the packets are transmitted. | Redundancy may arise within the source differentiation; packet cannot able to satisfy the constraints. |
| Novel signature[6] | Avoid the receiver node fails to recover the corrupted file from the source as with the small probability of the attack the system fails with great extent. | Computationally more expensive. |
| Packet-based detection scheme[5] | Not requires intermediate nodes to decode coded packets to check the weight of a packet; therefore, it is capable in terms of computational cost, delay. | It has increase the overhead of the network as it have to subdivide the larger blocks into the sub-block |

# 4. METHODOLOGY AND WORKING

A protocol should be implemented for provide the security using identifier of node, which is generated by using some secure algorithm. The security ensures the true nature of data, non-repudiation and authentication. Where it defends data tampered or misused routing, careful forwarding the packets to the respective nodes.

## 4.1. Working steps

1. At the initial stage check the communication between the nodes in a tree topology.

2. Providing the packets on nodes in order to transmit.

3. Selecting the routing strategy for transmission.

4. Examine the packet transfer cost/time (ti) of the current nodes.

5. Generating the false data packet on the respective nodes.

6. Determine the packet transfer cost/time (ti) of the current transmission node with respect to the last packet transfer time (tj).

7. If the current packet transfer time (ti)> (tj) then delay is introduced between the nodes.

8. Detecting the falsified nodes with respect to time delays between the nodes.

9. Preventing the attacks while reducing the time delay with the existing methods, increasing throughputs.

10. Provide the non linear (random) cost to each and every node which is participating in the communication process.

11. With respect to the cost associated with each node the particular attack is generated on the nodes.

12. According to the behavior of nodes in the network determine the types of attack and comparing the performance with the measuring parameter of network as throughput, end to end delays, energy consumption.

13. Basic algorithm as polynomial time required in order to associate the cost with the nodes and also calculate the time difference between the nodes.

## 4.2. Attack Implementation

The respective attacks are implementing in this paper in order to detect the malicious nodes and also to avoid the incorrect packet transmission.

### *4.2.1. Blackhole attack*

In a Blackhole attack, the attacker attracts the data packets and then sends them by distributing incorrect routing information. The attacker notifies that it has an finest route. So, other normal nodes demand to route data packets through the malicious node [4].

### *4.2.2. Wormhole attack*

Wormhole attack is one of the most difficult forms of routing attacks. In this attack, an attacker proceedings packets at one location, tunnels them to another location of the network, where it is retransmitted by a existing attacker [4].

### *4.2.3. Grayhole attack*

In Grayhole attack a node can control from behaving correctly like a black hole that is it truly an attacker and it will proceed as a normal node [4].

# 5. ANALYSIS AND DISCUSSION

## 5.1. Analysis

1. Analyzing Byzantine attack in tree based network and consequences.

2. Simulating Byzantine attack using Adhoc on demand distance vector routing protocol.[12]

3. Comparing the performance of network parameter by means of packet delivery ratio, data rating, throughput, time delays.

## 5.2. Discussion

Performance can be measure with the network parameter as:

1. Packet delivery fraction: The ratio of the data packets elated to the destinations to those generated by the constant bit rate (CBR) sources is known as Packet Delivery Fraction (PDF).

2. End-to-End Delay: End-to-End delay is all possible delays due to buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times of data packets.

3. Energy Consumption: Before the transmission of data takes place each and every nodes have to be charged with some amount of energy in order to take part in communication process.Analyse the energy consumption of each nodes after the transmission.

# 6. SIMULATION/RESULT

Packets Transmission and receiving from the normal nodes and malicious nodes. Attacking nodes are generated with the generalized behavior of the attacks as Blackhole, wormhole, Grayhole attack.

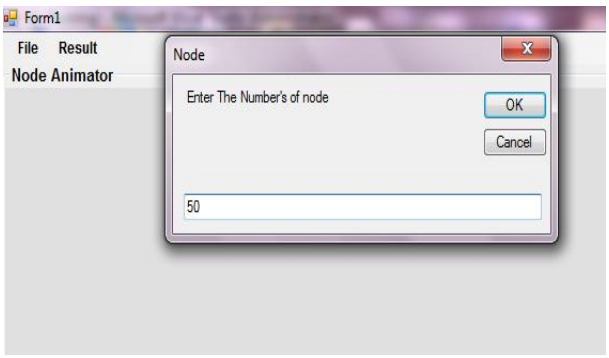


**Fig 2: Initialize the N number of nodes**

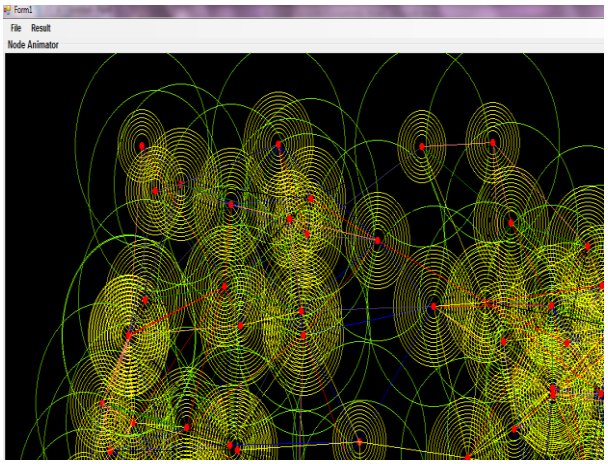


**Fig 3: Setting the transmission range and making the link between the nodes with the edges.**

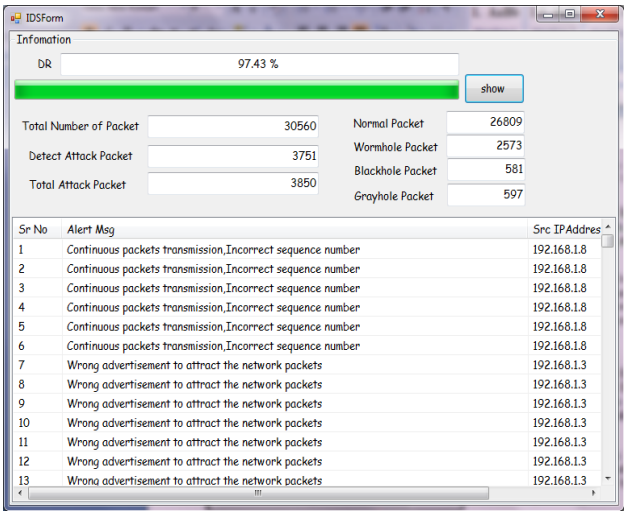


**Fig4: Shows analysis of the detected attacks as Blackhole,wormhole,Grayhole attack packets with the normal packets delivered by the respective nodes where each and every respective nodes having its own IP address through which the malicious nodes has been detected.**

With the help of the simulation result this paper can be easily identify the different types of attacks generated on the communication in an network. While specifying the total number of packets, normal packet transmission, total attack packets transmission, end-to end delays between the transmissions.

# 7. CONCLUSION

In Tree network the security of data transmission is the big issues as many innocent nodes get compromised with the malicious nodes and interrupt the process of whole network. The distributed detection process in tree topology proposed the scheme in order to bound the data transmission of the respective nodes under the Byzantine attack and also provides the cost associated to it while dealing with both random as well as linear so as to limit the usage of resources in order to increase the performance efficiency, throughput of the network, decrease the time delays. Through the scheme optimal attacking strategies introduced with decreasing the error occurs in detection, prevention process.

## 8. REFERENCES

[1] Xiang He, Aylin Yener.” Strong Secrecy and Reliable Byzantine Detection in the Presence of an Untrusted Relay,” IEEE transaction on information theory, vol. 59, no. 1, January 2013.

[2] Bhavya Kailkhura , Swastik Brahma, Pramod K.Varshney,”Optimal Byzantine Attacks on Distributed Detection in Tree based Topology,”International Conference on Computing, Networking and Communication,Workshop Cyber Physical system,2013.

[3] Xiaofan He, Huaiyu Dai, Peng Ning,” A Byzantine Attack Defender: the Conditional Frequency Check,” 2012 IEEE International Symposium on Information Theory Proceedings.

[4] Shabir Sofi, Eshan Malik, Rayees Baba, Hilal Baba, Roohie Mir,” Analysis of Byzantine Attacks in Adhoc Networks and Their Mitigation, ICCIT 2012.

[5] X. He and A. Yener, The Gaussian many-to-one interference channel with confidential messages,”IEEE Trans.Inf. Theory, vol.57, no.5,pp. 2730–2745, May 2011.

[6] Vaibhav Pandit, Jung Hyun Jun and Dharma P.Agrawal,”Inherent Security Benefits of Analog Network Coding for the Detection of Byzantine Attacks in Multi-Hop Wireless Networks,” 2011 Eighth IEEE International Conference on Mobile Ad-Hoc and Sensor Systems.

[7] MinJi Kim, Lu´isa Lima, Fang Zhao, Jo˜ao Barros,Muriel M´edard, Ralf Koetter, Ton Kalker, Keesook J. Han,” On Counteracting Byzantine Attacks in Network Coded.

[8] R. Koetter and F. Kschischang, “Coding for errors and erasures in random network coding,” IEEE Trans. Inf. Theory, vol. 54, pp. 3579–3591, 2008..

[9] S. Jaggi, M. Lang berg, S. Katti, T. Ho, D. Katabi, and M. M´edard, Resilient network coding in the presence of byzantine adversaries in Proceedings of IEEE INFOCOM, March 2007, pp. 616 – 624.

[10] B. Awerbuch, R. Curtmola, D. Holmer, et. al,” Mitigating byzantine attacks in ad hoc wireless networks,”. Department of Computer Science, Johns Hopkins University, Technical Report Version 1, March 2004.

[11] D. Lun, M. M´edard, D. Karger, and M. Effros, “On coding for reliable communication over packet networks,” in Proceedings of 42nd Annual Allert on Conference on Communication Control, and Computing Invited paper, September–October 2004.

[12] C.Perkins and P. Bhagwat.Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In Proceedings of SIGCOMM '94 Conference on Communications, Architectures, Protocols, and Applications, (London, UK, Sept 1994)