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.
Distributed Detection Methods for Byzantine Attack in Tree Topology

References

- MinJi Kim, Luísa Lima, Fang Zhao, João Barros, Muriel M´edard, Ralf Koetter, Ton Kalker, Keesook J. Han, "On Counteracting Byzantine Attacks in Network Coded.

Index Terms

Computer Science

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