IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 6, Ver. IV (Nov.- Dec. 2017), PP 60-64
www.iosrjournals.org

Distributed Detection Mechanism for Byzantine Attack in Tree-Based Topology: A Survey

Durga Shankar Baggam[1], Rajani Kanta Sahu[2]
1(Department of Computer Science & Engineering ,Gandhi Engineering College,India)
2(Department of Computer Science & Engineering ,Gandhi Engineering College,India)

Abstract: *In tree based topology each and every nodes are participating on communication with other nodes. So it is major challenge to secure the data transmission between the nodes in the network as many types of attacks are generated in between the communication. Byzantine attack is one of the most important security thread as it interrupt the communication of nodes in the network and behave like a innocent nodes while participating normally. In Byzantine attack compromisation of nodes takes place in that condition it is very difficult to detect the innocent and malicious nodes, with the byzantine nodes many other attacks are deployed as Blackhole attack, wormhole attack, gray-hole attack, flood rushing attack, sinkhole attack etc. Routing protocols helps to provide the way through which the nodes can be able to communicate with each other. Also provide the cost associated with each node so as to differentiate investment of resources from each nodes as communication takes place. For securing the data transmission in a network algorithms proposed which will bound the faulty data transmission and also limits the resources usage by decreasing the investment of resources which takes part in communication. Performance will be measures in terms of parameter as packet delivery fraction, energy consumption, End-to-end delays.*

Keywords: *Byzantine Attack, Distribution Detection, Tree Topology, AODV, Polynomial Time Algorithm.*

I. Introduction

In data transmission process user needs to take care while sending the packets from one source to other destination so as to mean to provide the security to the packets in ordertodeal with the communication specially in the tree based network where each and every nodes takes part in communication .As the data transmission takes place many other malicious nodes involves in the communication process and behaves like a innocent 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 starts between the nodes. It is very difficult to detect the malicious nodes from the whole network. Byzantine attack is important security thread as in comes into the network it is very difficult to identify as it compromise the set of nodes and treat as a innocent node because of the cooperation among these compromised nodes when they perform malicious behaviours. The compromised nodes may seemingly behave well however they may actually make use of the flaws and inconsistencies in the routing protocol to undetectably destroy the routing fabric of the network, generate and advertise new routing information that contain non-existent link, provide fake link state information, or even flood other nodes with routing traffic. In traditional approaches distributed detection mainly focused on parallel network topologies .As in Parallel networking nodes are directly transmit their data/packets to the root node. While the root nodes becomes fully loaded with number of data/packet from nodes. Hence the certain fraction of individual nodes unbalanced and incapable to make any decision and collapse the network completely.

In order to deals with the problem fully loaded nodes. Second approaches are introduced to increase the transmission area of the root nodes and make the multihop network where nodes are ordered hierarchical into multiple levels [1,2].

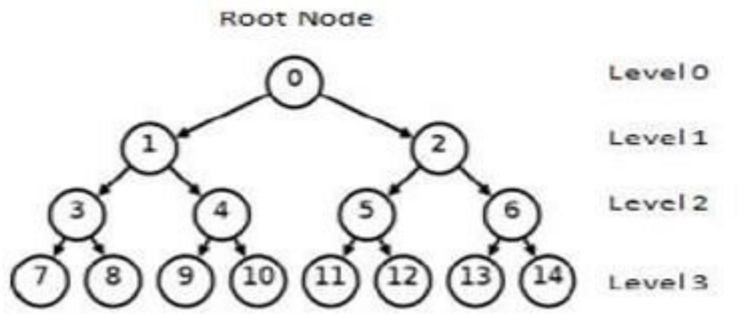

Figure 1: Structure of Tree Topology

With smart usage of resources across levels, tree networks have the potential to provide a suitable balance between cost, coverage, functionality and reliability [1, 2].

The rest of this paper is as follows: Section 2 describes the literature review followed by in section 3 general approaches. Security issues discuss in section 4. Proposed methodology of work is discuss in section 6 and conclusion is shown in section 8.

II. Literature Review

Mai Abdelhakim, Leonard E. Lightfoot, Jian Ren, and TongtongLi[3], proposed the q-out-of-m rule, which is popular in distributed detection and can achieve a good trade-off between the miss detection probability and the false alarm rate. However, a major limitation with it is that the optimal scheme parameters can only be obtained through exhaustive search, making it infeasible for large networks. Xiang He, Aylin Yener[1] proposed Gaussian two- hop network where the source and the destination can communicate only via a relay nodewho is both an eavesdropper and a Byzantine adversary. Both the source and the destination nodes are allowed to transmit, and the relay receives a superposition of their transmitted signals. Vaibhav Pandit, Jung Hyun Jun and Dharma P. Agrawal [6, 9] proposed identify an inherent security benefit of Analog Network Coding and show how it can be used to design a novel Dual Non-adjacent Watchdog scheme that can detect a set of malicious byzantine attacks. MinJi Kim, Lu´isa Lima, Fang Zhao, Jo˜ao Barros, Muriel M´edard, Ralf Koetter, Ton Kalker, Keesook J. Han [12] proposed a novel signature scheme that allows packet-level Byzantine detection. This scheme allows one-hop containment of the contamination, and saves bandwidth by allowing nodes to detect and drop the contaminated packets. We compare the net cost of our signature scheme with various other Byzantine schemes, and show that when the probability of Byzantine attacks is high, our scheme is the most bandwidth efficient. Priyank Anand, Ankit Singh Rawat[13] proposed incorrect sensing results a certain fraction of Byzantine attackers in the CR network, data fusion scheme becomes completely incapable and no reputation based fusion scheme can achieve any performance gain. Present optimal attacking strategies for given attacking resources and also analyze the possible counter measures at the fusion center (FC).StefanoMarano, Vincenzo Matta, and Lang Tong[14] proposed detection under binary hypotheses with quantized sensor observations, the optimal attacking distributions for Byzantine sensors that minimize the detection error exponent are obtained using a “water-filling” procedure. The smallest error exponent, as a function of the Byzantine sensor population, characterizes the power of attack. Also obtained is the minimum fraction of Byzantine sensors that destroys the consistency of detection at the fusion center. The case when multiple measurements are made at the remote nodes is also considered, and it is shown that the detection performance scales with the number of sensors differently from the number of observations at each sensor. Hao Chen, Pramod K. Varshney[13] proposed the performance limits of collaborative spectrum sensing under Byzantine Attacks where malicious users send false sensing data to the fusion center leading to increased probability of incorrect sensingresults.

III. General Approaches

A sender in tree network may not always be able to pass its packets directly to the intended receiver. So, routing mechanisms are required whenever an intended receiver is outside the transmission range of the sender. The goal of the routing protocol is to discover the latest topology. The routing protocols in tree network can be classified into three categories:

I. Proactive routing protocols [19]: In this family of routing protocol, all nodes exchange routing information periodically or every time the topology changes. Since each node retains a consistent view of the network, a route to the destination is always available. Examples of proactive routing protocols contain: Destination-Sequenced Distance-Vector (DSDV) or Optimized Link State Routing(OLSR).

II. Reactive routing protocols [19]: In reactive routing, the route discovery process is started by a sender whenever it wants to send packets to a destination. The route is kept until the destination becomes unreachable or is not needed anymore. Examples are: Ad hoc on demand Distance Vector (AODV) Dynamic Source Routing (DSR) and Temporally Ordered Routing Algorithm(TORA).

A. AODV (Ad hoc on demand Distance Vector) [5] is a reactive routing protocol which uses traditional routing table with one entry per destination. In this routing protocol, routes are established dynamically at intermediate nodes. Another important feature is the maintenance of timer-based state, which is required to decide whether a routing table entry is expired or not. But in (AODV) Ad hoc on demand Distance Vector the selected shortest paths to the destination may not constantly be the best, congested, contain malicious or selfishnodes.

B. The DSDV (Destination-Sequenced Distance-Vector) [19] routing protocol is based on the Bellman-Ford routing algorithm and it guarantees loop free routes. In this beating protocol, a counter of all available destinations is maintained by each node. The number of hops to reach a destination and the sequence number for a destination are also included in the routing table. In order to reduce the overhead transmitted through the network, two packet types, "full dump", and "incremental" are used in DSDV (Destination-Sequenced Distance-Vector). The full dump packet carries all the available routing information and the incremental packet carries only the information changed since the last full dump.

C. In DSR (Dynamic Source Routing (DSR)[19] , the source knows the complete hop-by-hop route to the destination and the route is stored in a route cache. When a node wants to send packets to another node for which it does not have the routing information, it starts a route discovery process by broadcasting route requests to itsneighbors.

D. ODBSR (On-Demand Secure Byzantine Resilient Routing) [16] protocol is an on-demand routing protocol for wireless networks that detects Byzantine behavior and avoids it. The protocol is intended to locate a fault free path in tree network, even when a majority of nodes have been compromised. ODBSR addresses both failures and attacks within a unified framework. While detection of the attack, ODBSR enters searching mode with the goal of discovering the attack location. In the shortest path is nominated based on a reliability metric, which captures reliability and adversarial behavior based on pasthistory.

IV. Security Issues

Ad hoc networks are self-organizing in nature, dynamic topology, peer to peer networks formed by a collection of mobile nodes and the centralized entity is not present, the Topology organized ,reorganized, Resource consumption takes place as deplete the battery power of critical nodes, flooding the routing table or consuming the data packet buffer space, compromised node can act as another node, compromised node can act as an informer, jam wireless communication by creating a wide-spectrum noise, Addressing and Service Discovery is essential because of absence of a centralized coordinator. Energy Management Requires as the radio frequency (RF) hardware design should ensure minimum power consumption. Battery energy management is aimed at extending the battery life, the CPU can be put into different power saving modes, intelligent device management can reduce power consumption of a mobile node, and scalability is expected in ad hoc wireless networks.

1) Gateways: Gateway nodes are the entry points to the wired Internet and generally owned and operated by a service provider. Perform the following tasks: keeping track of the end users, band-width fairness, address, and locationdiscovery.
2) Address mobility: Solutions such as Mobile IP can beused.
3) Routing: Specific routing protocols for ad hoc networks arerequired.
4) Transport layer protocol: Split approaches that use traditional wired TCP for the wired part and a specialized transport layer protocol for the ad hoc wireless networkpart.
5) Load balancing: Load balancing techniques are essential to distribute the load so as toavoid the situation where the gateway nodes become bottlenecknodes.

V. Attacksin Adhoc Networks [5]

Table 1: Different types of attacks on network layer

ATTACK	DEFINITION	EFFECTS
Byzantine attack	It interrupt the communication of nodes in the network, behave like a innocent nodes while participating normally.	Compromisation of nodes takes place in that condition it is very difficult to detect the innocent and malicious nodes.
Blackhole attack	In a black hole, the attacker swallows all he receives, just as a black hole absorbing everything passing through.	Efficiency of the network decreases by decreasing throughput of all the nodes around malicious node.

Wormhole attack	A Wormhole attack needs two or more adversaries have better communication resource than normal nodes, and canestablish better communication channels between them.	-Packet damage or alteration by wormhole nodes. -Normal message Stream can be change.
Gray-hole attack	In Gray hole attack a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act asa normal node.	We can't identify easily the attacker since it behaves as a normal node.
Flooding attack	Exhaust the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation.	Cause severe degradation of the performance of the network.
Sybil attack	In Sybil attack, a malicious node attract by representing multiple identities tonetwork.	-Allows other attacks. -Exploiting the routing race condition.

VI. Proposed Methodology

AdhocOn Demand Distance Vector (AODV) [5] Routing Protocol Is Proposed In Order To Provide The Route To The Nodes For Communication. AODV Is Intended To Accommodate Networks That Are As Large As SeveralThousandNodes.ItIsOneOfSeveralDemand-Driven(Oron-demand) protocols that are in existence today. Hence, the protocol is invoked only when a node (host) has data to transmit. The AODV RFC indicates that the transport layer protocol is UDP, which of course only offers best effort delivery of packets, and does not support either error recovery or flow control. Addressing is handled using IP addressing. Since each node acts as both a host and routing node, each must maintain a routing table that contains information about known destination nodes. Entries are keyed to destinations.

VII. Analysis And Discussion

Performance can be measure with the network parameter as:

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

ii) 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 datapackets.

iii) 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 thetransmission.

VIII. Conclusion

In adhoc wireless 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 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.

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, January2013.

[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]. Mai Abdelhakim, Leonard E. Lightfoot, Jian Ren, and Tongtong Li," Distributed DetectioninMobileAccessWirelessSensorNetworksunderByzantineAttacks,"

[4]. IEEE Transaction on parallel and distributed System, March 2013

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

[6]. Shabir Sofi, Eshan Malik, Rayees Baba, Hilal Baba, Roohie Mir," Analysis of Byzantine Attacks in Adhoc Networks and Their Mitigation," ICCIT2012

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

[8]. E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi- receiver wiretap channel," IEEE Trans. Inf. Theory, vol. 57, no. 4, pp. 2083–2114, Apr.2011.

[9]. 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.

[10]. 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

SensorSystems.

[11]. X. He and A. Yener, “Cooperation with an untrusted relay: Asecrecy perspective,” IEEE Trans. Inf. Theory, vol. 56, no. 8, pp. 3801–3827, Aug.2010.

[12]. X. He and A. Yener, “Providing secrecy with structured codes: Tools and applications to Gaussian two-user channels,” submitted to IEEE Trans. Inf. Theory, Jul. 2009 [Online].0907.5388.

[13]. 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 Peer-to-Peer Networks,” IEEE journal on selected areas in communication, vol. 28, no. 5, June 2010.

[14]. Priyank Anand, Ankit Singh Rawat,” Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks,” 978-1-4244-5489-1/10/$26.00 2010IEEE.

[15]. Stefano Marano, Vincenzo Matta, and Lang Tong,” Distributed Detection in the Presence of Byzantine Attacks,” IEEE Transaction on signal processing, vol. 57, no.1, January2009.

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

[17]. S. Katti, S. Gollakota, and D. Katabi, “Embracing wireless interference: Analog network coding,” in Proceedings of the 2007, ACM Conference on Applications, Technologies,

[18]. 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, March2004.

[19]. C. Adjih, A. Laouiti, P. Minet, et. al., Optimized link state routine protocol. Work in Progress, IETF draft, MANET Working Group, INRIA Rocquencourt, France,2003.

[20]. 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), p.234-244.