ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Byzantine Attack detection Techniques in Wireless Networks

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

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

Abstract: Wireless networks (WNs) provides interaction between among nodes without the use of any physical medium. Data transmission takes places between nodes through base stations. In (WNs) transmission of messages between different nodes is a challenging task. There are number of attacks presented in network that may affect routing process of networks. In this paper Byzantine attack and its detection techniques has been presented also security issues that may occurred in wireless networks will also be discussed.

Keywords: Wireless Networks (WNs), security, Byzantine and CBDS.

I. INTRODUCTION

Wireless networks (WNs) are the networks in which no physical infrastructure is available through which node may contact each other. In such networks nodes were connected among themselves by some base stations and they are not connected directly with each other. It helps nodes to move freely and expand their communication areas according to their needs. Wireless LAN offers services in offices and in building in a manner that a user can communicate to other user from the locations that they preferred [1]. Whereas Wireless Networks such as ad-hoc networks sensor networks were used for monitoring environment, home automation system, transportation and in distributed environment. The main feature of the wireless network is that it uses the available resources very efficiently and gives these resources to nodes according to their specifications. The key point is that in a network setup these tasks should be performed in a dispersed fashion through the cooperation of the nodes and based on the local information available to each node [2].

A. *Characteristics of wireless networks*

- In this part different characteristics of wireless networks will be presented. These are as follows:
- The nodes can interact in the arrangement anytime, building the network topology active in nature.
- Itinerant nodes are distinguished with low memory, command and low burden features.
- Mobile and spontaneous behavior which demands minimum human intervention to configure the network.
- All nodes have same features with comparable tasks and abilities and thus it creates a fully similar situation.
- Mobility of nodes is high.
- Interaction between nodes is intermittent [3].

B. *Technical Challenges of Wireless Networks: This section covers various technical challenges that are occurred during data transmission in wireless networks.*

- Limited data transfer capacity: Wireless interaction keep on having essentially brought down limit than infrastructure networks. Furthermore, the acknowledged throughput of wireless correspondence in the wake of representing the effect of different get to, blurring, commotion, and obstruction conditions, and so on., is frequently a big pact not as much as a radio's most extreme transmission rate.
- Dynamic topology: Dynamic topology enrollment may exasperate the faith connection among nodes. The faith may likewise be irritated if a few nodes are identified as traded off.
- Routing Overhead: In wireless specially appointed networks, nodes regularly change their area inside system. In this way, some stale courses are created in the steering table which prompts pointless directing overhead.
- Hidden terminal problem: The concealed terminal issue alludes to the effect of parcels at an accepting node as the synchronous transmission of those nodes that are not inside the immediate transmission scope of the sender, however are inside the transmission scope of the beneficiary.
- Packet losses due to transmission errors: Ad hoc wireless networks encounters a significantly higher bundle misfortune due to components, for example, expanded crashes because of the nearness of concealed terminals, nearness of obstruction, unidirectional connections, visit way breaks because of portability of nodes.
- Mobility-induced route changes: The system topology in a specially appointed wireless system is profoundly powerful because of the development of nodes; subsequently an on-going session endures visit way breaks. This circumstance regularly prompts visit course changes.
- Battery constraints: Devices worked as a element of these networks have confinements on the power source observing in mind the last objective to look after compactness, size and weight of the gadget.
- Security threats: The wireless flexible especially agreed nature of MANETs conveys new security difficulties to the system outline. As the wireless medium is

defenseless against spying and impromptu system usefulness is built up through node participation, flexible especially agreed networks are naturally presented to various security attacks.

- Frequent network partitions: The arbitrary development of nodes frequently prompts parcel of the system. This for majority of fraction influences the moderate nodes [4].

II. RELATED WORK

Sun et.al.[5] studied the trouble of disseminated sensing in the existence of Byzantines when the number of sensor nodes was finite. The optimal attacking strategy and percentage of Byzantines needed to shade the FC are showed.

Saini and Singh [6] presented the solution to the dilemma of Byzantine attack that arises in most of network scenarios.

Sukhpreet et al.[7] proposed A DSR related energy competent malevolent node recognition method called Extended Cooperative Bait Detection Scheme (ECBDS). In this ECBDS scheme, the passive and immediate protection architectures are integrated and random cooperation was done with the adjacent node.

Zhang et al.[8] Proposed a taxonomy of the accessible Byzantine attack behaviors and indicates the parallel attack points, that tells how to, and when to open attacks.

Saxena et.al.[9] proposed the investigation of security attacks in MANET.A review of diverse attack in MANET is presented.

Ivanc and Blazic[10] presented a proposal of progress advance to attack modeling based on the breakdown of nodes and their importance regarding the node-level within the tree structure of the model.

Rukavitsyn et al. [11] proposed selflearning method that allows adapting a detection model to network changes. This was minimized the false detection and reduce the possibility to mark legitimate users as malicious or not.

Hu et al.[12] designed an appraisal method by utilizing performance feedbacks provided by user vehicles as the trust metrics to measure the quality of services of platoon head vehicles.

III. VARIOUS ATTACKS IN WIRELESS NETWORKS

Here different attacks that may affect data transmission occurred in wireless networks. These attacks violate security of a network for example: a malevolent module may disturb routing process by either dropping some messages or manipulating messages. A lot of attacks these are as follows:

- Black hole attacks:
  Black hole attack is like that of a byzantine attack where attacker does not send data packets. Facts modules are missed in this attack without being in knowledge of the sender party that the data has not sent to receiver. These can be termed as a packet dropping attacks and are invisible in nature.

- Gray hole attacks:
  This attack is similar to selfish node attack but the difference is just it selectively drops some packets and data into a dim gap, for instance sending parcels but not sending any information parcels related to that. These attacks are not distinguishable by security features as they act as a ordinary node in the network as they compromise the steering table.

- Selfish node attacks:
  Selfish node is a node that does not forward any packet to next node so as to keep their resources and time. Selfish node takes packets from sender node and saves the buffer memory to gain more benefits.
- Denial of Service:
  Denial of service attack may prevent normal nodes from using information of data transmission or may create some delays for their accessing time of network resources. In this flooding of messages can take place on recipient's node to shut down the network.

IV. BYZANTINE ATTACKS

These are the attacks in which the attacker nodes have a full authority over the network objects and act in an arbitrarily manner to disturb the network. Traditionally the secured routing protocols thought that the authenticated nodes are the trusted nodes that can execute a information traversal over a network efficiently. This attack creates loopholes in the network and thus these attacks are desired to be in use into consideration and all nodes are needed to be back traversed to find the malicious nodes. But, this duty is not a trouble-free one and requires lot of implementation is needed to be done.

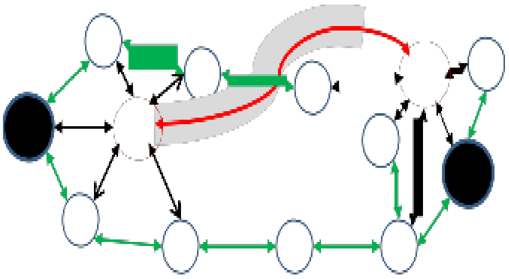

Figure1: Byzantine Attack

Byzantine Fault Tolerance

The main purpose is to protect from byzantine failures, in which failed node acts a normal node thus making fault tolerance difficult.

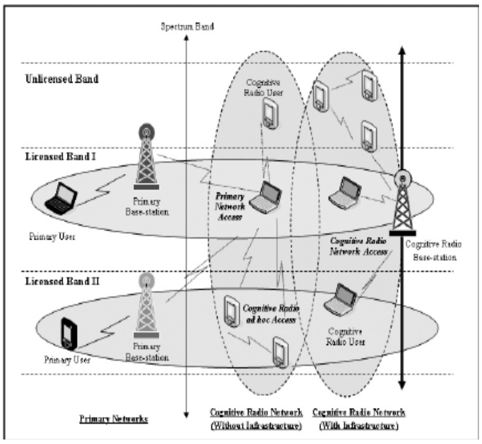

Figure 2: Distributed detection in the presence of cooperative (Byzantine) attack

The sensors that keep a check on errors can be altered by attacking nodes, and can be falsified to transmit modified data. To estimate binary data for quantized sensor, optimal attacks distributions for byzantine sensors to reduce the error probability are extracted by "water-filling" method.

V. VARIOUS TECHNIQUES TO DETECT BYZANTINE ATTACKS

Random Linear Network Coding

It is a method in which instead of simply transmitting a network packet to sender node, all packets are combined together to a node to check appropriate data flow in a network and thus data flow over nodes are saved. Various manipulation of data can be occurred over a network, thus network coding can expose these errors.

Cooperative Bait Detection Scheme (CBDS)

Chang et al. [13] proposed a suspicious node detection mechanism called Cooperative Bait Detection Scheme (CBDS) that coordinates both receptive and proactive recognition conspires and identifies the noxious nodes that cause grayhole and blackhole attacks by utilizing a switch following system. The CBDS is a DSR-based plan that makes utilization of draw bundles to allure the malignant nodes to send a course answer parcel for the trap RREQ send and from the course answer got the questionable way framed by the malevolent node is followed out and the pernicious node that causes the dark and grayhole attacks is recognized. However, it is found that the steering overhead of the CBDS achieves the most noteworthy esteem when the threshold is set to 95%. This is credited to the way that the discovery plan of CBDS triggers speedier when the threshold esteem is set to95%. Subsequently, the trap parcels to recognize noxious nodes will be sent ordinarily in the system.

Table1 Comparative Analysis of various Byzantine attack detection techniques

Techniques	***Additional packet Transmission***	***Detection***	***Prevention***	***Neighbor Monitoring***
Random Linear Network Coding	No	Yes	No	No
Cooperative Bait Detection Scheme	Yes	Yes	Yes	Yes
Credit Based	Yes	Yes	Yes	Yes
Trust Based	Yes	Yes	No	Yes
Hash Based	No	No	Yes	No

VI. CONCLUSION

In this paper different attacks that are presented in WNs are discussed. Wireless networks security issues some technical challenges were also discussed. The central theme of this paper was to study Byzantine Attack and its detection technique called CBDS. The drawback of CBDS system was that end to end message delay was high and overhead ratio was also high. In future we must try to improve the CBDS by adding some backbone nodes that will help in reduction of path link failure.

References:

[1] Muneer Bani Yassein, Qusai Abuein, Deya Alzoubi, "Dynamic Probabilistic Flooding in DSR Routing Algorithm for Wireless Network", Journal of Emerging Technologies in Web Intelligence, Vol. 4, No. 4, November 2012.

[2] 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.

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

[4] 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.

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

[6] Sukhpreet Kaur Saini and Parminder Singh, "Analysis and Detection of Byzantine Attack in Wireless Sensor Network", International Conference on Computing for Sustainable Global Development (INDIACom) IEEE 2016, pp: 3189-3191.

[7] R.Sukanesh, Eisha Edsor and Aarthylakshmi.M, "Energy Efficient Malicious Node Detection Schem in Wireless Networks", IEEE 2016 pp:1-5.

[8] Linyuan Zhang, Guoru Ding and Qihui Wu, "Byzantine Attack and Defense in Cognitive Radio Networks: A Survey", IEEE Communications Surveys & Tutorials 2015, pp:1-23.

[9] Nidhi Saxena,Vipul Saxena, Neelesh Dubey, Pragya Mishra, "Attack Analysis In Mobile Ad Hoc Network Based On System Observations", IJARCSSE, Vol. 3, Issue 7, pp. 618-623, July 2013.

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

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

[12] Hao Hu, Rongxing Lu, Zonghua Zhang and Jun Shao, "REPLACE: A Reliable Trust-based Platoon Service Recommendation Scheme in VANET", IEEE Transactions on Vehicular Technology, 2016 pp: 1-11.

[13] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai ,"Defending Against Collaborative Attacks By Malicious Nodes In Manets: A Cooperative Bait Detection Approach", IEEE Systems Journal ,Vol.9, No.1, March 2015.