ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A DETAILED SURVEY ON MALICIOUS NODE DETECTION AND MITIGATION IN LARGE SCENARIO WIRELESS NETWORKS

J. Santhosh *, A. Rajivkannan, R. Vijayarajeswari
Department of Computer Science & Engineering, KSR College of Engineering, Tiruchengode, India- 637 215

DOI: 10.5281/zenodo.231525

ABSTRACT

As of date, wireless sensor systems (WSNs) have gotten much consideration as methods for gathering and using information from the real world. The quantity of WSN applications is being expanding broadly and the application range is required to spread. WSN is a system made out of a substantial number of sensor hubs with restricted radio capacities and one or few sinks that gather information from sensor nodes. Remaining nodes are the vindictive nodes in WSN which corrupts the execution of the WSN. The unwanted node recognition is a perplexing issue in WSN because of its comparative qualities with different nodes in WSN. In this paper, different systems for the identification and relief of malicious nodes in remote sensor network environment are examined.

KEYWORDS: Wireless sensor networks, malicious nodes, performance, mitigation.

INTRODUCTION

Wireless Sensor Network (WSN) is a collection of spatially distributed sensor nodes in large space environment. The main application of deploying WSN are military and environmental monitoring as T-sunami alert and Earth Quake in various regions of the earth. The sensor node contains an inbuilt sensing element which is used to sense the surrounding information and these informations may be either analog or digital depends on the environment. These sensed informations are converted into digital form information using analog to digital converter. These converted digital informations are sent to processor unit which performs some mathematical manipulations on the sensed data which is suitable for data transmission and reception through the antenna element to remote area. The main contribution of this sensor node is to collect and propagate the data to the remote unit in wireless manner. The transmitted data may be passed through some medium which affects the performance of the data transmission in the form of noises and some environmental flutuations. Hence, the received data in the receiver section is affected by noise. These noise contents are suppressed in the receiver side and then the data from the transmitted packets are recovered.

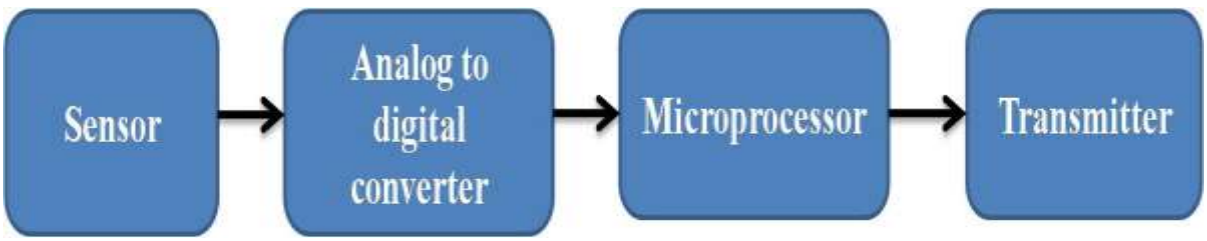

Figure 1 Internal architecture of node

The performance of the sensor node is affected in another way by attackers. The attacker attacks the sensor either in direct or indirect way. In direct way, the attacker from outside environment affects the data transmission and reception on sensor node such as Distributed Denial of Service (DDOS) attack. In indirect

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

attack mode, the behaviour of the sensor node is controlled by attacker through the nearby nodes. The attacker may be active or passive. In active mode, the data transmission is altered by attacker. In case of passive attack, the attacker can able to capture the data transmission only. They are not able to alter any data passage.

SURVEY BASED ON CLUSTERING APPROACH

Hossein Jadidoleslamy (2011) proposed hierarchical Intrusion Detection algorithm to detect and mitigate the untrusty nodes in WSN environment. The cluster-based Intrusion Detection System was established to analyze the charecteristics of the nodes in WSN. Seo Hyun Oh et al. (2012) used dual-weighted trust evaluation methodology to detect both malicious nodes and malfunctioning nodes in WSN. Mis detection rate was high due to the presence of large number of malicious nodes. The trust worthy scheme was developed to classify the nodes behaviour in WSN environment. Sung-Jib Yim et al. (2012) detected malicious nodes using neighbor based authentication algorithm in larger network deployment scenario.The fault status of the node was sent and recorded to the centralized node, which further categorized the node into either trusty or malicious. Bhakti Thakre, S.V.Sonekar (2014) used clustering technique for the detection of malicious nodes in wireless networks. The connected clustering method determined the suspecious nodes in wireless networks using Acknowledge scheme. Nidhi Lal et al. (2015) used Watchdog Protocol for the detection of malicious nodes and its behaviour was analyzed with respect to cluster head. Destination sequenced distance vector algorithm was used in cluster head to detect the untrusty behaviour of the nodes in sensor networks. Kresimir Grgic et al. (2016) proposed an adaptive distributed algorithm for the detection of malicious nodes in WSN. The authors estimated the probability of the nodes in sensor environment and their trust behaviour was analyzed. The authors achieved 82% of average accuracy for malicious node detection in WSN environment.

S.Gopala Krishnan et al. (2014) enumerated that the malicious nodes which were distinguished and evacuated utilizing grouping approach. Every hub inside the bunch gets the group key from the bunch head and this key was utilized for the information exchange between group head and nodes. The cluster head checked this key for each information exchange from hub and matches with their group table. In the event that the match is legitimate, then just it perceived that this hub has a place with this bunch, else it is chosen as malicious hub. This work additionally analyzed about finding the connection disappointment because of the nearness of malicious hubs by deciding the pickup of every connection in the system. R Vijayarajeswari et al. (2016) deveoped image security based data transmission and reception scheme in WSN environment. The author's embeded the secret image or information into the cover image which hide the information into some one data. The authors analyzed their work interms of Peak Signal to Noise Ratio (PSNR) and unified average changing intensity (UACI). The security of the information in WSN can be achieved in this way by super imposing the secret or important informations into some one un-important information.

The following points are acquired from the survey on various clustering methods as,

- High latency
- Low packet delivery rate
- Low throughput
- Low datarate

SURVEY BASED ON FEATURES

Abdelhakim et al. (2014) proposed a trust based evaluation technique which detected the faulty nodes in wireless environment. The fuzzy hypothesis were constructed and used in the wireless network to utilize the band of inner capacity to keep efficient searching techniques. The authors conducted various kinds of research experiments using their proposed work and compared their experimental results with large set of conventional methods results. Chang et al. (2015) utilized hypothesis protocol to detect and mitigate different set of attacks in larger network node scenario. This lead to high network congestion rate and reduced the overall average packet delivery ratio. The authors analyzed different multidimensional elements furthermore with the coordinating data, along these lines; the ordinary operation of the entire system can be checked.

In Xu et.al (2009), recognition conventions algorithm was developed to have the hash security method which overlayed the key based steering to detect and mitigate the various attacks in network environment. Somasundara et al. (2006) developed a method to perceive/find the dim opening ambush (malevolent center point) by the help of the direct/execution of the widely appealing centers. Creators proposed methodology called Support Vector Machine (SVM) on using AODV controlling convention.

Ahmad et al (2015) introduced the noval methodology for counting the HELLO packets in wireless sensor networks using AODV protocol and this lead to heavy loading capacity which turned off the switching capability of the network. This was followed by a 32-bit length HELLO packets whil tranformed from one node to another node using this kind of protocol. Fenye Bao et al. (2012) developed a gathering approach which was based on trust evaluation system. In this work, the authors collected various datas from distinct points and these datas were transferred to the center node of the network system. This kind of reputation work followed certain unique rules for the data transmission from one node to another set of nodes in wireless networks in large remote environment.The Watchdog protocol was used in this work which supported large number of nodes in the network.

The following points are acquired from the survey on various feature extraction methods as,

- The complex feature set
- Required larger features for classification
- Complex classification algorithms.

CONCLUSION

The malicious node recognition and moderation assumes a vital part to improve the execution of the wireless sensor systems. In this paper, different strategies for the location and alleviation of malicious nodes in WSN environment are talked about. The detection of malicious nodes in a system consequently diminishes the vitality utilization of different hubs and undesirable transmissions, along these lines expanding the system lifetime. This paper analyzed about different works of bunching based malicious node discovery to secure hubs in WSNs against noxious hubs.

REFERENCES

[1] Abdelhakim, M., Lightfoot, L., Ren, J., Li, T., 2014, Distributed detection in mobile access wireless sensor networks under byzantine attacks, IEEE Transactions on Parallel and Distributed Systems, 25(4), 950–959.
[2] Ahmad, Rathore, M.M., Paul, A., Chen, B.W., 2015, Data transmission scheme using mobile sink in static wireless sensor network, Journal of Sensors, 2015.
[3] Bhakti Thakre, Sonekar, S.V., 2014, An Algorithmic Approach for the Detection of Malicious Nodes in a Cluster Based Wireless Networks, International Journal of Computer Science and Information Technologies, 5(3), 3220–3223.
[4] Hossein Jadidoleslamy, 2011, A Hierarchical Intrusion Detection Architecture For Wireless Sensor Networks, International Journal of Network Security & Its Applications (IJNSA), 3(5).
[5] Kresimir Grgic, Drago Zagar, and Visnja Krizanovic Cik, 2016, System for Malicious Node Detection in IPv6-Based Wireless Sensor Networks, Hindawi Publishing Corporation, Journal of Sensors, 2016(6206353), 1-10.
[6] Nidhi Lal, Shishupal Kumar, Aditya Saxena, Vijay Km. Chaurasiya, 2015, Detection of Malicious Node Behaviour via I-Watchdog Protocol in Mobile wireless Network with DSDV Routing Scheme, Procedia Computer Science, 49, 264-273.
[7] Seo Hyun Oh, Chan O. Hong, Yoon-Hwa Choi, 2012, A Malicious and Malfunctioning Node Detection Scheme for Wireless Sensor Networks, Wireless Sensor Network, 4, 84-90.
[8] Somasundara, Kansal, A., Jea, D., Estrin, D., Srivastava, M., 2006, Controllably mobile infrastructure for low energy embedded networks, IEEE Transactions on Mobile Computing, 5(8), 958–973.
[9] Sung-Jib Yim, Yoon-Hwa Choi, 2012, Neighbor-Based Malicious Node Detection in Wireless Sensor Networks, Wireless Sensor Network, 4, 219-225.
[10] Xu, X., Zhou, B., Wan, J., 2009, Tree Topology Based Fault Diagnosis in Wireless Sensor Networks, International Conference on Wireless Networks and Information Systems, Shanghai, pp. 65-69.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

[11] Fenye Bao, Ing-Ray Chen, Moon Jeong Chang, & Jin-Hee Cho 2012, Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection, IEEE Transactions on Network and Service Management, 9(2), pp.1-18.

[12] Chang, JM, Tsou, PC, Woungang, I, Chao, HC, & Lai, CF 2015, Defending Against Collaborative Attacks by Malicious Nodes in MANETs: Cooperative Bait Detection Approach, IEEE Systems Journal, 9(1), pp.67-74.

[13] R. Vijayarajeswari, A. Rajivkannan and J. Santhosh, A Simple Steganography Algorithm based on Lossless Compression Technique, Circuits and Systems, 2016, pp. 1-9.

[14] Gopalakrishnan, S & Ganeshkumar, P 2014, Intrusion detection in mobile Adhoc Network using secure routing for attacker identification protocol, American Journal of Applied Sciences, 11(8), pp. 1391-1397.