International Journal of Emerging Technology and Innovative Engineering
Volume 2, Issue 6, June 2016 (ISSN: 2394 – 6598)
Date of Publication:20.06.2016

SURVEY OF MALICIOUS NODE DETECTION IN WIRELESS SENSOR NETWORKS

R. Vijayarajeswari
Department of Computer Science & Engineering,
KSR College of Engineering,
Tiruchengode,
vijiraji0505@gmail.com

A. Rajivkannan
Department of Computer Science & Engineering,
KSR College of Engineering,
Tiruchengode,

J. Santhosh
Department of Computer Science & Engineering,
KSR College of Engineering,
Tiruchengode,
vijiphd0505@gmail.com

ABSTRACT

In recent times, wireless sensor networks (WSNs) have received much attention as a means for collecting and utilizing data from real world. The number of WSN applications has been increasing widely and the application range is expected to spread. WSN is a network composed of a large number of sensor nodes with limited radio capabilities and one or few sinks that collect data from sensor nodes. Residual nodes are the malicious nodes in WSN which degrades the performance of the WSN. The malicious node detection is a complex problem in WSN due to its similar characteristics with other nodes in WSN. In this paper, various methodologies for the detection and mitigation of malicious nodes in wireless sensor network environment are discussed.

Keywords
Wireless sensor networks, malicious nodes, performance, mitigation.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) can be defined as large networks consisting of nodes that have sensor functions. The change in topology, broadcast network and resources make the wireless network different from the adhoc network. Whenever a node wants to send the data to another node, in between node called as co-operator node act as an intermediate for receiving or sending the packet to destination. In contrast to traditional wireless sensor networks, special security and performance related issues need to be considered for the modern sensor networks. For instance, an attacker could instigate various attacks over an unattended sensor network, and even make the sensor device without being detected. Therefore, the design of a sensor network must be made robust to attacks, even if an attack succeeds, its impact should be minimized. In simple, a single sensor node or few sensor nodes should not crash the entire network after an attack. Another concern is about energy efficiency. These attacks lead to anomalies in the network behaviors, the monitoring of which can be detected by some reported solutions to identify these attacks. Fig. 1 shows the basic architecture of WSN.

Besides, the traditional network security threats occurring in the WSN, it faces many new security problems, such as passive attacks and active attacks; host and network attacks; internal and external attacks. Attack can be divided into layers corresponding to different protocols.

- Attacks in Physical layer: Radio signal interference and physical capture, etc.
- Attacks in Data link layer: These types of attacks are based on their energy consumption or utilization level by a node in the network.
- Attacks in Network layer: This type of attacks alters the transmitting information and thus increases the error rate of the system.
- Attacks in Transport layer: This layer is attacked or affected due to the unsynchronization of the nodes in the network.

Secure communication is much essential in the transmission of data to be securely transmitted between the sensor nodes. All the nodes in wireless sensor networks distribute the common extracted features in sensor networks which has the same properties in the network.

COPYRIGHT TO IJETIE

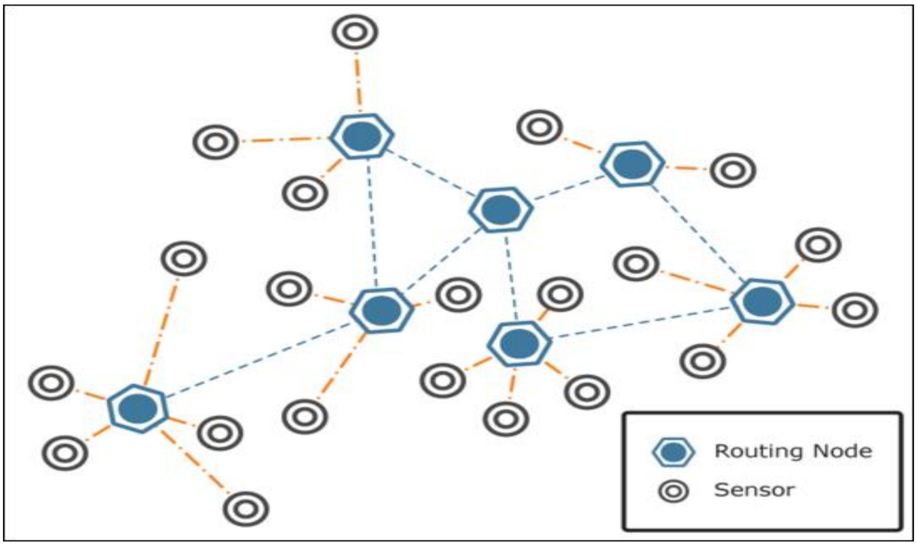

Fig 1: WSN Architecture

2. LITERATURE SURVEY

Denko et al. (2011) investigated a probabilistic trust management scheme to be implemented in pervasive computing environments. The authors argued that in addition to allowing a device to find other suitable devices for interaction, while detecting those that were malicious. This trust model was capable of allowing a device to judge the trustworthiness (i.e. reliability) of another device with which it interacts by means of the recommendations from its peers. The behavior changes as expected depending on the proportion of malicious devices, and when a device gains enough experience of interactions with other devices in the environment, it starts to protect against false recommendation attacks depending on the proportion of false recommenders. Fenye Bao et al. (2012) proposed a novel system to identify the malicious nodes using clustering approach which based on trust system. In this work, the authors derived the properties of each node in the wireless environment system to classify the nodes behaviours in an effective and simple manner. The authors developed probability distribution density function for the nodes in heterogeneous network and each node in the wireless network environment derives the quality of service (QoS) properties. Nodes were classified based on this derived set of features.The authors also designed a reputation-based framework to ensure data integrity in WSNs, which collects information from each node by means of a Watchdog technique which identifies the malicious nodes or hidden nodes in structured or unstructured wireless sensor network environment.

Bo Sun et al. (2013) presented an anomaly detection technique for Wireless Sensor Networks. By means of various aggregation functions like sum, average, max, and min, the authors presented how to obtain a theoretical threshold. The authors implemented an algorithm to increase detection sensitivity by the integration of generalized likelihood ratio and cumulative summation. The authors proposed a new system integrating both system monitoring modules (SMM) and intrusion detection modules (IDM) for implementation in Wireless sensor networks. This combination helps to classify the malicious events and other emergency events. In practice, WSNs are made use in monitoring significant emergency events, such as battlefield monitoring and forest fires.

Gopalakrishnan and Ganeshkumar (2014) have proposed different detection methods for attackers who hacked the packets in networks. The authors proposed Secure Routing for Attacker Identification (SRAI) protocol to detect and mitigate the attackers in the network environment. This proposed system automatically detected the attacks in the network and thus periodically generates the attacker identification report. This report was sent to all the nodes in the network environment and thus the attacks were identified in each node of the network. The protocol developed in this method obtained threshold value from the node which was transmitted the packet. For instance, the authors considered a node which had the deterministic threshold value as 50. When the value of initial threshold value reached the threshold value of the destination node, it checked the threshold value of the current state of the node in sensor network environment. If it is constant, then the receiver assumed the received packet was original and generated an acknowledgement which was sent to the source. If the packets were viewed or modified by an attacker through the way to reach destination, its threshold value may change and then it transmitted to the destination that checks the threshold value and identified the received packet was duplicate. Then, it generated the misbehavior report to the source node via the intermediate nodes. The authors analyzed the performance of their proposed system in terms of end to end delay, throughput and packet delivery ratio.

Chang et al. (2015) devised a methodology to classify the nodes behaviour based on their cooperative bait approaches which predicted the attacks in the network. The problems of the conventional malicious node detection system were tolerated by implementing cooperative bait detection scheme (CBDS).The anomaly nodes were detected based on fuzzy theory and revised evidence theory. The malicious nodes in a network can be identified by monitoring the behaviors of the evaluated nodes with multidimensional features and integrating this information, thus, the normal operation of the whole network can be verified.

Renyong Wu et al. (2015) proposed an anomaly node detection in networks using trust based authentication algorithm. The anomaly nodes were detected based on fuzzy theory and revised evidence theory. The frequent observation and integration of the behavior of the evaluated nodes with multidimensional characteristics helps to detect the malicious nodes in a network. The authors also devised a system which detected intrusion based on Neighbor Node Trust algorithm. Each node examines the trust level of its neighbor nodes. Depending on the obtained trust values, the neighboring nodes may be classified into risky, malicious or trustworthy. Trustworthy nodes were recommended to the forwarding engine for the purpose of packet forwarding. Their scheme successfully detected HELLO flood attack, selective forwarding attack, and jamming attack by analyzing the malicious node behavior and other network statistics.

Wagner (2004) made use of statistical estimation techniques against malicious attacks by designing flexible aggregation schemes. The security of various aggregation schemes were assessed using a mathematical framework proposed in that work. Haripriya et al. (2015) proposed a framework to detect and mitigate the malicious nodes. The authors detected the malicious nodes in prior to the routing using consensus based algorithm and then that route is prevented for transmitting data between nodes in mobile adhoc networks.

Stetsko et al. (2010) proposed statistical based intrusion identification system which uses the spatially features of each sensor node in the wireless network environment. The node in the network were clearly classified into either malicious or trusty nodes based on their neighbors features.The signals strength was analyzed based on the proposed Tiny OS system in this paper and the authors were well analyzed the packet delivering and packet losses in every intermediate nodes in the network environment with less number of flood type of distributed attacks. The authors were observed their results using TOSSIM tool in Tiny OS environment.The proposed methodologies in this paper were detected the distributed type’s attacks with less number of error rates and false rates if there were large number of nodes in the network.

Muktikanta Sa et al. (2011) developed an algorithm for detecting the misbehaviour of the node based on the Bayesian methodologies. The authors analyzed their performance improvement based on their agent based approaches over the conventional methods.Song et al. (2010) proposed a simple and efficient malicious node classification system based on the markov model for the nodes in network.The malicious node classification system is categorized into learning and classification phases. The authors increased their classification rate of their proposed malicious node taxonomy system based on their extracted scores from each node in the network environment.

3. CONCLUSION

The malicious node detection and mitigation plays an important role for improving the performance of the wireless sensor networks. In this paper, various methodologies for the detection and mitigation of malicious nodes in wireless sensor network environment are discussed. The detection of malicious nodes in a network automatically reduces the energy consumption of other nodes and unwanted transmissions, thereby increasing the network lifetime. This paper discussed various works of clustering based malicious node detection to protect nodes in WSNs against malicious nodes.

4. REFERENCES

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

[2] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and 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).

[3] Bo Sun, Xuemei Shan, Kui Wu, and Yang Xiao 2013. Anomaly Detection Based Secure In-Network Aggregation for Wireless Sensor Networks. IEEE Systems Journal, 7(1).

[4] Chang, J.M., Tsou, P.C., Woungang, I., Chao, H.C., and Lai, C.F. 2015. Defending Against Collaborative Attacks by Malicious Nodes in MANETs: Cooperative Bait Detection Approach. IEEE Systems Journal, 9(1).

[5] Mieso K. Denko, Tao Sun, and Isaac Woungang 2011. Trust management in ubiquitous computing: A Bayesian approach. Computer Communications 34(2011) 398–406.

[6] Renyong Wu, Xue Deng, Rongxing Lu, and Xuemin (Sherman) Shen 2015. Trust-Based Anomaly Detection in Emerging Sensor Networks. International Journal of Distributed Sensor Networks. 2015(363569), 1-14.

[7] Wagner, D., “Resilient aggregation in sensor networks,” *Proc. ACM SASN*, pp. 78–87, 2004.

[8] Stetsko, A., Folkman, L., and Matyas, V. 2010. Neighbor-based Intrusion Detection for Wireless Sensor Networks. 6th International Conference on

COPYRIGHT TO IJETIE

Wireless and Mobile Communications (ICWMC), 420-425.

[9] Muktikanta Sa, and Amiya Kumar Rath 2011. A Simple Agent Based Model for Detecting Abnormal Event Patterns in Distributed Wireless Sensor Networks. Proceedings of the 2011 International Conference on Communication, Computing & Security, ACM, 67-70.

[10] Song, X., Chen, G., and Li, X. 2010. A Weak Hidden Markov Model Based Intrusion Detection Method for Wireless Sensor Networks. International Conference on Intelligent Computing and Integrated Systems (ICISS). 887-889.

[11] Haripriya, Y., Bindu Pavani, K.V., Lavanya, S., and Madhu Viswanatham, V., "A Framework for detecting Malicious Nodes in Mobile Adhoc Network," *Indian Journal of Science and Technology*, vol. 8, no. S2, pp. 151–155, 2015.

COPYRIGHT TO IJETIE