Techniques for Malicious Node Detection in Wireless Sensor Networks - A Survey

Azna Asharaf
M. Tech Scholar
Department of Computer Science
School of Computer Sciences, Mahatma Gandhi University, Kerala, India

Abstract— Maintaining a protected, malicious free environment is essential for any kind of network in order to preserving security and network lifetime. Even though it is a challenging task the demand of mechanisms for preserving such a network is high. In the case of wireless sensor network, nodes are placed in an open, unprotected and hostile environment, which gives an effective way for the intruder to get in to it. Since the main aim of wireless sensor network is monitoring, information gathering and reporting, the need for secure space is crucial for authenticated data transfer. This survey describes about various methods of detection for malicious activities in a wireless Sensor network.

Key words: Wireless Sensor Network (WSN), Malicious Network, Compromised Nodes, Types of Attacks, Intruders

I. INTRODUCTION

Wireless Sensor Network, is an emerging technology which advances its vigorous application in various fields of health care, logistics, Telematics, surveillance etc. The requirements of applications like fewer amounts of memory, lower energy consumption and for small area of communications hike the demand of wireless sensor network. Wireless Sensor networks can be defined as a distributed network comprised of a collection of inexpensive devices called sensor nodes which are connected to each other to coordinately working for a particular task. Each sensor nodes is featured with low power, limited storage area and processing capability, whose function is to sense a physical quantity and transfer the information to the base station. The base station can also be referred to as gateway is with high processing power and memory space that receives the sensed data from each nodes, process it and sent to the outside wired world. The network does not involve any pre-described structure and no centralized controlling exists. The communication between sensors is within a limited transmission range using radio link, through either direct as peer to peer fashion or multihop strategy.

Basically, a wireless sensor network is amenable to glut of intrusion due to its broadcasting nature of transmission. This feature gives the gap for an adversary to eavesdrop the data transfer and fault data spreads across the network. The minimum and non-rechargeable battery capacity and storage area act as a hinder to proper security measures by sensor nodes. Thus vulnerability in wireless network is high than wired habitat. Hence preserving the integrity and authentication in wireless sensor network is a burdensome and of course, difficult. There are different types of attacks commonly speaks as active and passive. Active attacks are easier to detect since its effects can be easily monitored due to the changes occurred in the network and over its elements. Alternatively, passive attack accounts for a silent killing approach; it neither shows its presence nor can be easily detected. So it is more strenuous to capture it.

S. Rajasegarar et al. [1], shows an overview of various existing anomaly detection schemes in wireless sensor networks and describes two approaches for intrusion detection. The first approach is misuse or signature based detection, where signature of known attack is stored and compares the monitored attack. The second approach is anomaly detection where deviation in the behavior of monitored data is checked to detect an attack. Anomaly detection is categorized into statistical and non-parametric techniques. Statistical techniques are application dependent and are used when prior knowledge about data distribution is available. While non parametric is used where there is dynamic data distribution without any prior knowledge.

G. Padmavathi et al. [2], conducted survey deals with different attacks and their effects in wireless sensor networks. It also describes various challenges faced by WSN. In this article mainly, illustrates some of the techniques for detection of malicious activities in wireless sensor networks.

II. TECHNIQUES AGAINST MALICIOUS BEHAVIOR IN WIRELESS SENSOR NETWORKS

A. Neighbor based malicious node detection in Wireless Sensor Networks

Sung-Jib Yim et al. [3], proposed a neighbor node based malicious detection system. Here malicious node can be faulty nodes which generate wrong decision while intelligently behave like normal nodes. Decision making process in each node is carried out through the wrong readings from itself and neighbors.

Fault in a network can be either transient, responsible for incorrect readings and performance loss or permanent fault responsible for unreliability in network. Transient fault occurs abundantly and smoothing filter is used to remove it where it avoids unnecessary alarms in event driven detection. Permanent fault can be detected using confidence level evaluation such that each node maintains confidence level of its own and its neighbors and thus evaluates trustworthiness between them. After each periodic and event driven cycles each node updates its own confidence level and also its neighbors for further decision making. Updation procedure is carried out by two parameters that differentiate malicious nodes from normal nodes from their behavior. The simulation results shows the detection accuracy with low false alarm rate.

B. Malicious Node Detection in Wireless Sensor Networks Using an Auto regression Technique

Malicious detection through a time series evolution of sensor data is presented by D. I. Curiac et al. [4]. Initially each sensor node is assigned with a threshold value depending on its type.

Malicious sensor node is diagnosed by comparing the value provided by the sensor at the moment with the predicted output value which is obtained from the past/present values of the same sensor through an auto regressive predictor. If the comparison shows a harsh difference from threshold value the node is considered to be malicious and decision block is activated. A case study is also described to show the effectiveness of this method.

C. Cluster-based Reputation and Trust for Wireless Sensor Networks

G. V. Crosby et al. [5] , proposes a novel approach for preventing election of compromised or malicious cluster heads. A secure cluster formation algorithm is developed for the establishment of trusted cluster through pre-distributed keys. After the formation of cluster, whenever the current cluster head's power fails new cluster is then selected by passing a new cluster election message to cluster members. Through a voting approach from these members a new candidate with top ranked in trusted neighbors list chosen as new cluster head. Before establishing it as cluster head it then undergoes a challenge - response stage with current cluster head. If it pass it is selected else it is moved to blacklist and its trust level is set to -1 .Once a node is set to -1 which implies there is no trust level updation or no further relation with that node. The experimental analysis concludes that this approach reduces the chances of making compromised nodes as cluster head.

D. Distributed Reputation-based Beacon Trust System (DRBTS)

A novel distributed security protocol that enhances beacon nodes to monitor each other in order to detect inaccurate location information from malicious beacon nodes is proposed by Avinash Srinivasan et al [6],. Beacon nodes are mainly placed to assist sensor node for initialize location. Here each beacon node uses second hand information for maintaining reputation after passing through a deviation test. Every beacon node monitors its neighborhood to identify misbehaving beacon nodes and accordingly updating reputation of that node in the neighbor-reputation table. This table is used by each sensor node to determine whether or not to use the location information of corresponding beacon node using a majority voting approach. DRBTS use first and second hand information to maintain the trust in a network.

E. An Improved Intrusion Detection Scheme Based on Weighted Trust Evaluation for Wireless Sensor Networks

L. Ju, H. Li et al. [7], developed a weighted-trust application (WTA) scheme to detect the compromised nodes from reporting false data and preventing base station from accepting it. The schemes works by assigning each sensor node with a weight value ranging from 0 and 1. Weight value will act as an interface to the base station thus mainly placed to enhance reliability and trust. Initially the value is 1 and goes on changing in every cycle. A node is detected to be malicious if the weighted value falls below a threshold value and a more accurate aggregation result can be obtained by comparing node's weight sum value. The simulation results of this approaches claim with robustness in different network scale

F. A Review Paper on Watchdog Mechanism in Wireless Sensor Network to Eliminate False Malicious Node Detection

Jijeesh Baburajan et al. [8], presented a review paper showing the limitations of watchdog mechanism and the countermeasures to overcome those. Watchdog is an intrusion detection mechanism in a wireless sensor network which monitors the malicious nodes from their misbehavior. The mechanism involves nodes as watchdogs that may overhear the message between other nodes and decides whether to discard or forward them. This occurs mainly due to the broadcast nature of network.

The main limitations reviewed as Ambiguous collision, Receiver collision, Limited transmission power, false misbehavior and partial dropping. This problem can overcome through improved version of watchdog technique.

G. An improved watchdog technique based on power-aware hierarchical design for ids in wireless sensor networks

Inorder to maintain security and networks lifetime by removing the limitations in an ordinary watchdog mechanisms, an improved version was implemented by A.Forootaninia et al. [9]. It is a power aware hierarchical model such that cluster head node will act as watchdog and perform the operation. For effectiveness the model is simulated using TinyOS simulator thereby compare it with non-hierarchical model.

The work describes about hierarchical design based on intrusion detection system and comparison of ordinary Watchdog with improved mechanism. The results shows that majority of drawback in ordinary watchdog is resolved in the improved technique while ambiguous collision is not been solved.

G. Malicious Node Detection Using a Dual Threshold in Wireless Sensor Networks

SungYul.Lim [10], developed an advanced form of malicious node detection through dual threshold structure mainly applicable in fault prone network rather than single threshold. The first threshold uphold event detection by reducing false alarm rates and the second threshold makes event nodes to pass the test resulting in exact event region detection accuracy. To clarify the instability between the nodes each node posses a trust values along with threshold values for decision making.

III. CONCLUSION

As increasing the application of WSN with emerging technologies, its security is also on great demand. Even though a vast number of techniques are developed for preserving protected WSN they are not fall under complete protection mode. Cryptographic and authentication methods are also facing limitations in the hostile and open terrain of WSN. This article surveys some of the malicious node detection techniques for WSN. In this document, some of the issues in WSN, methods for overcome it and their evaluations is outlined. The survey summarize that node can refer to be malicious if it is:

- Faulty and thus produces wrong data.
- Showing fluctuations in the predicted value.
- Providing false report on data transmission.
- Fluctuating in threshold value.

REFERENCES

[1] S. Rajasegarar, C. Leckie and M. Palaniswami, "Anomaly Detection in Wireless Sensor Networks," IEEE Wireless Communications, Vol. 15, No. 4, 2008, pp. 34-40.
[2] G. Padmavathi, D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," International Journal of Computer Science and Information Security, IJCSIS, Vol. 4, No. 1 & 2, August 2009.
[3] Sung-Jib Yim, Yoon-Hwa Choi, "Neighbor-Based Malicious Node Detection in Wireless Sensor Networks" Vol.4 No.9(2012), Article ID:22509,in Scientific Reasearch, September 2012.
[4] D. I. Curiac, O. Banias, F. Dragan, C. Volosencu and O.Dranga, "Malicious Node Detection in Wireless Sensor Networks Using an Autoregression Technique," 3rd International Conference on Networking and Services, Athens, 19-25 June 2007, p. 83.
[5] G. V. Crosby and Niki Pissinou, "Cluster based Reputation and Trust for Wireless Sensor Networks", in the proceedings of the IEEE Consumer Communications and Networking Conference, January2007.
[6] Avinash Srinivasan, Joshua Teitelbaum, and Jie Wu "DRBTS: Distributed Reputation-based Beacon Trust System" Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, 19 December 2006.
[7] L. Ju, H. Li, Y. Liu, W. Xue, K. Li and Z. Chi, "An Improved Intrusion Detection Scheme Based on Weighted Trust Evaluation for Wireless Sensor Networks," Proceedings of IEEE 5th International Conference on Ubiquitous Information Technology and Applications, December 2010.
[8] Jijeesh Baburajan, Jignesh Prajapati, "A Review Paper On Watchdog Mechanism In Wireless Sensor Network To Eliminate False Malicious Node Detection", Volume: 03 Issue: 01 , Jan-2014
[9] Forootaninia, M. B. Ghaznavi-Ghoushchi, "An Improved Watchdog Technique based on Power-Aware Hierarchical Design for IDS In Wireless Sensor Networks", International Journal of Network Security & Its Applications (IJNSA), 2012.
[10] SungYul,Lim and YoonHwaCho, "Malicious Node Detection Using a Dual Threshold in Wireless Sensor Networks", J. Sens. Actuator Netw. 2013, 2,70-84; doi:10.3390/jsan201007, 5 February 2013.

