ISSN:0975-9646

A Survey on Detecting Compromised Nodes in Wireless Sensor Networks

K.Sumathi[1] & Dr.M.Venkatesan[2]
Assistant Professor[1], EBET Group of Institution, Kanga yam, Tamilnadu,India.
Principal[2], K.S.R Institute for Engineering and Technology, Thiruchengodu, Tamilnadu,India

Abstract: **The Wireless sensor networks are popular and frequently used in many applications. The WSN are deployed in open and unprotected environment. The sensor nodes have limited resources and communication capability so each node is easily captured by an adversary and launching several malicious software inside the network. There are number of cryptographic and authentication protocols have been proposed to protect these networks from outsider attack but Fail to protect them from insider attack.** ***In this article, we surveyed about the intrusion detection schemes in WSN.***

Keywords: **wireless sensor network, security, sensor node.**

I INTRODUCTION

Recent trends in micro electro mechanical systems and less amount of power and highly integrated electronic devices lead to develop a more number of applications in a wireless sensor networks. The wireless sensor network consists of sensor node with low power, data processing unit with small storage area and also short range wireless communication. Generally numerous sensor nodes are deployed in hostile environment, it led to unattended nature of wireless network, which collect information from the different sensor nodes in the field, aggregate them partially and sent them to the sink node, which is responsible for data fusion. Based on applications the sensor network can be classified into C1WSN (Category 1Wireless sensor network) and C2WSN (Category 2Wireless sensor network). C1WSN is mesh based multi hop radio connectivity and C2WSN is a P2P or with single hop radio connectivity.

The wireless sensor networks are used in many fields like Energy management, Emergency response networks, Medical field, inventory management, High way monitoring, military application, and Battle field management.

II RESEARCH ISSUES AND RESOURCE CONSTRAINS

The various research issues include Biological applications, smart vehicular parking, Event detection, Structural health monitoring, Green house monitoring etc.The various resource constraints in sensor networks such as energy, memory and computational power. The series issues in the sensor network are the nodes get compromised and perform various attacks.

The attacks are as follows

1. Sniffing attack: Overhear valuable information of the nearer sensor nodes.
2. Bad mouthing attack: Propagate negative information about the legal sensor nodes.
3. Good mouthing attack: Propagate positive information about the illegal sensor nodes.
4. DOS attack: Prevent the functioning of entire WSN.
5. Sybil attack: Clone illegal nodes and replicate the information.
6. Black hole attack: Attract the traffic and drop the valuable information of the packets.

These attacks lead to anomalies in network behaviors that are detectable in general. There are some reported solutions to detect these attacks by monitoring the anomalies. In the following sections deals various compromised node detection strategies.

III SUMMARY OF VARIOUS COMPROMISED NODES DETECTION TECHNIQUES

Many techniques have been proposed till now for detection and recovery of compromised node. This paper gives some idea regarding various compromised node detection and recovery schemes and their pros and cons.

1. Weighted Trust Evaluation Scheme

The author introduced weighted trust evaluation scheme in hierarchical network architecture, which consists of three different sensors at three different layers. In the trailing position of the architecture contains low power Sensor Nodes (SN), which gathers the information about various sensors at this lower layer level. The middle layer contains the Forwarding Node (FN), assume that who is trustful and won't be compromised. The FN is responsible for collect information from the lower layer and compute aggregation result and commit the information to Access point (AP).The FN is also responsible for verifying correctness of the information gathered from SN. The Access point or Base station is placed at the leading position of the architecture and assume who is also trustful, who is responsible to transfer the output to the outside world.

This scheme is based on the assumption FN and Base station, both are trusted. In fact the adversary can gain control over the BS then it leads to create any possible attacks in the network. Another critical assumption is that most of the sensor nodes are work in proper condition .If number of compromised nodes are more than number of normal nodes then there may be a chance to choose normal node as compromised node and it will create number of

false positive. Through simulation result the author verified that correctness and effectiveness of the compromised node detection scheme.

2. STL Approach

Generally WSN consists of hundreds or thousands of sensor nodes and to create effective topology as well as to protect all nodes from vulnerable attacks are impractical. To overcome this situation the author introduced Stop Transmission and Listen approach, which is the one of the simple and effective technique for detecting a malicious node. In this number of sensor nodes are deployed in an environment and each sensor nodes having a built in time limit to stop their transmission. Each node starts their sensing process with in their sensing region and each node has the capability to detect the malicious node. After sensing the sensed data is forwarded to sink node and each node has stop their transmission in every few seconds and listen malicious behavior. The malicious nodes are transmitting a data at the non-transmission time period because those nodes are not aware this non-transmission built in time period. If malicious nodes are not transmitting any data during non-transmission time then they will be caught another frequent non-transmission time.

This approach having some disadvantages such as the whole network stopped their transmission at a time and start suddenly will cause congestion and unwanted delay in the network operations. Simulation result shows the effectiveness of the approach.

3. Auto regression technique

In this paper, the author considered the following assumption for detecting maliciousness of the different sensor nodes in the same network.

The sensor network is static as well as each sensor node passed a onetime authentication procedure. Every sensor node has the capability to store up to hundreds of bytes of keying material in order to secure the transfer of information through symmetric cryptography. Base station will not be compromised at any cost. Due to this assumption the networks avoid various attacks such as eavesdropping, traffic analysis, spoofing, sinkhole, selective forward attack, wormhole attack, Sybil attack and Hello flood attack.

The biggest threat for wireless sensor network is the node capturing attack, where an adversary gains full control over sensor nodes through direct physical access. To avoid these kind of attack the author introduced Auto Regression model (AR model).In this the time series of measured data provided by each sensor node and relies on an autoregressive predictor placed in base station. The basic principle followed is: For each sensor nodes collect past and present values and it will be compared with the threshold and detect whether that sensor node behave normally or abnormally.

This scheme has some disadvantages, it follows symmetric key cryptography for transmission of information causes key exchange problem, and it is an open issue in network security. Another important consideration is choosing an effective threshold for comparing present and past behavior of the sensor nodes. Through case study author shows the effective nests and efficiency of the AR model.

4. Dual Threshold

In this work the author considered the following assumptions:

The n numbers of sensors are deployed in the monitored area and having the transmission range r_c.Each node knows its neighbors and their transmission range. If two nodes are neighbors of each other if their distance is less than or equal to r_c.

The trust values of the neighbor is calculated based on Weighted directed graph and its lies between 0 and 1.If W_{ij}=0 means node v_i does not trust node v_j at all, where as W_{ij}=1 means node v_i totally trust node v_j. In addition, v_i also has its own trust value and its ranging from 0 to 1. Once w_{ii} reaches 0, means node v_i is faulty.

The event region is assumed to be a circle with radius r_e. If any event occurred in the region then nodes in the region generate an alarm to its neighbors. In event detection, each sensor node makes a local decision based on the sensor readings of its own and its neighboring nodes.

The malicious nodes are detected based on two thresholds θ1 and θ2. The role of the θ1 is to minimize the false alarm rate. The role of the θ2 is to enhance the malicious node detection accuracy. In which, for each node collecting binary reading of all of its neighbors and then compute U1 /U0+U1 to determine which group it belongs to. Generally there are three groups: R1, R2 and R3. If a particular node v_i at the region R1 if its computed value of U1 /U0+U1 is greater than θ1. If a particular node v_i at the region R2 if its computed value of U1 /U0+U1 is lies between θ1 and θ2. All the remaining nodes are in the group R3.After division of the region, apply the hypothesis test and decide the behavior of each node as normal or up normal.

Through simulation results the author evaluates the performance of the malicious node detection using a Dual Threshold scheme.

5. SWATT: Software based ATTestation for Embedded Devices

Our environment is surrounded by number of embedded devices ranging from java enabled cell phones to sensor networks and smart appliances. If an adversary can compromised one of our devices and modifying the memory contents. To avoid this kind of maliciousness the author introduced Software based ATTestation (SWATT) to verify the memory contents of the embedded devices. SWATT can be applied in varies field such as network printers, smart cell phones, Electronic voting machines, smart cards etc.

A verifier is used to verify the expected memory contents of embedded device, which generates a random MAC key and sends this key to embedded device. The device computes MAC on the entire memory using the key and returns MAC value. The random keys are used to avoid replay attacks .The embedded device contains some empty memory which is filled with number of zeros. If an intruder

alters the memory content, an intruder used this memory location for storing their contents and compute MAC function. The verifier uses the checksum and verifies the memory content .If the checksum is true only if the memory content of the device is same as expected memory content. Otherwise the checksum will be false.

The author desired some of the properties for verification procedure such as pseudorandom memory traversal, the verifier sends the device a randomly-generated challenge. The challenge is used as a seed to the pseudorandom number generator (PRG) which generates the addresses for memory access. The verification procedure then performs a pseudorandom memory traversal, and iteratively updates a checksum of the memory contents. This property is used to know the single byte changes in the memory content. The second property is resistance to pre-computation and replay attacks in which the author used Pseudo random generator for generating the random key and avoid pre-computation and replay attacks.

The disadvantages in this paper are the author cannot give a clear idea about how to prevent and recovery of compromised node detection. The second problem is the periodic attestation of any devices increases the verification cost and time. Through pseudo code and experimental results the author shows the correctness of the procedure.

6. Sequential Probability Ratio Testing

A wireless sensor network consists of 100 to 1000 of sensor nodes which are used to transmit the sensitive information from one location to another location. Generally these sensor nodes are unattended in nature therefore which are easily compromised by an adversary and make many replicas of them. Using this replicas the adversary take control over the entire network communication. To overcome this kind of replicas a number of software based replica detection scheme have been proposed for static sensor nodes.

The author introduced sequential probability ratio test (SPRT) for mobility based sensor nodes. In this work the author considered the following assumptions: The sequential probability ratio test is comes under the centralized detection scheme and it is also depends on hypothesis testing method. In which uncompromised nodes are taken as null hypothesis and compromised nodes are taken as alternative hypothesis.

The author considers normal node's speed is always nearly or less than system configuration speed, where as the compromised node's speed is exceeds the threshold level.

The base station is responsible for identifying compromised nodes by computing the speed of observed sample nodes and decides which nodes speed are exceeded decided threshold speed.

Simulation result shows the effectiveness of the approach.

7 Trust Based Approach

In this paper the author consider a composite trust metric which is derived from both quality of service trust and social trust for identifying malicious nodes.

By statically analyzing peer to peer trust evaluation results which are collected from different sensor nodes, the cluster head is used to apply intrusion detection in those sensor nodes and assess the trust worthiness as well as maliciousness of the sensor in its cluster.

The cluster heads are analyzed by the base station. The performance evaluation of proposed system is depends on the analytical model based stochastic pertinet, stastical method are used to calculate false alarm probability. Through simulation results the author evaluates the effectiveness of the approach.

IV CONCLUSION

The intrusion detection system is very essential issue due to the un attended nature of the wireless sensor networks. In this document we discuss some of the security issues in WSN, evaluate several basic methods for identifying compromised nodes and various research work under each category been addressed.

ACKNOWLEDGEMENT

We'd like to thank the anonymous reviewers for their valuable comments and suggestions.

REFERENCES

[1] Idris M. Atakli, Hongbing Hu, Yu Chen, Wei- Shinn Ku, Zhou Su, "Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation", Jan. 11, 2008 to *The Symposium on Simulation of Systems Security* (SSSS'08), Ottawa, Canada, April 14 –17.

[2] T.Sathyamoorthi, D.Vijayachakaravarthy, R.Divya, M.Nandhini," A simple and effective scheme to find malicious node in wireless sensor network", International Journal of Research in Engineering and Technology eISSN 2319-1163 | pISSN: 2321-7308.

[3] Daniel-Ioan Curiac, Octavian Dranga," Malicious Node Detection in Wireless Sensor Networks Using an Auto regression Technique".

[4] Sung Yul Lim and Yoon-Hwa Choi," Malicious Node Detection Using a Dual Threshold in Wireless Sensor Networks", Journal of Sensor and Actuator Networks ISSN 2224-2708.

[5] Arvind Seshadri, Adrian Perrig, Leendert van Doorn, Pradeep Khosla," SWATT: Software based ATTestation for Embedded Devices", Center for Computer and Communications Security at Carnegie Mellon under grant DAAD19-02-1-0389.

[6] T. Nidharshini1, V. Janani2," Detection of Duplicate Nodes in Wireless Sensor Networks Using Sequential Probability Ratio Testing", International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 10, December 2012.

[7] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, Jin-Hee Ch, "Trust-Based Intrusion Detection in Wireless Sensor Networks", IEEE International Conference on Communications (ICC), 2011, pp. 1-6

AUTHOR PROFILE

K.Sumathi received her B.E. degree in Computer Science and Engineering from Anna University Chennai in 2005 and M.E Degree in Anna University Coimbatore in 2010 and currently working as Assistant Professor in EBET Group of Institution. She can be reached at thirusumathi83@gmail.com.

Dr.M.Venkatesan completed his Ph.D in Anna University Coimbatore in 2011 and he has published 20 research papers in both conference and international journal. Nearly 10 candidates are doing their research work under his super vision and he is working as Principal in K.S.R Institute for Engineering and Technology. He can be reached at venkatesh.muthusamy@gmail.com