International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 6, June 2016

Detection of Malicious Node in Wireless Sensor Networks - A Survey

[1] Asha R N [2] Jyothi R [3] Kiran Kumar K [
[1][2][3] Asst. professor, Computer Science & Engineering, Global Academy of Technology, Bangalore
[1]harshaaru@gmail.com, [2] jyothir.gat@gmail.com, [3]kkirankumarm.e@gmail.com

***Abstract:* — Wireless sensor network becomes popular both in civil and jobs in military. WSNs are of particular interest to adversaries due to their frequent deployments in open and unprotected and low computation resources so each node is weak entity, that software inside the network As security mechanism is not enough to sensor network from external attacks, introduction of intrusion detection system is needed. Many mission critical wireless sensor networks require an lightweight, efficient and flexible intrusion detection algorithm to identify malicious attackers. Intrusion detection in a wireless sensor network is of significant importance in many applications to detect malicious or unexpected intruder(s). The intruder can be an enemy in a war field or an unusual environmental change in a chemical or any industry etc. Our intrusion detection system is based on specific detection rules.**

***Keywords:* Security, Wireless Sensor Network, Sensor Node,, Intrusion detection.**

I. INTRODUCTION

Wireless Sensor Networks (WSN) is a kind of networks that constitutes by a large number of small mobile devices with sensor functions. It is mainly used to collect, disseminate and process sensor information. It is large- scale, wireless, self-organizing, multi-hop, no-partition, no infrastructure support, its nodes are isomorphic, lower cost, smaller size, and most of them can't move. Wireless sensor network are differ from other wireless ad hoc network in the sense that they are resource limited, they are often prone to failure, they are densely deployed, their topology often changes, they are remotely managed. They use broadcast mechanism instead of point to point. Wireless communication is often unreliable. So there is a chance of dropping the packets.

Intrusion detection systems (IDS) according to collect data in different ways can be classified based on host and network- based intrusion detection. IDS of traditional wired network cannot be directly used to wireless sensor networks, because of its characteristics of "wireless", autonomy, and multiple nodes distributed in unattended environment , not the central node , but consider the issue of energy consumption, the system should be as much as possible to avoid excessive complexity in the design and communication.

II. SECURITY ISSUES OF WSN

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

- Physical layer attacks: Radio interference and physical capture, etc.
- Data link layer attacks: Frame the conflict, unfair attacks and energy depletion attacks.
- Network layer attacks: Network layer is the research focus and most of attacks from this layer. For example: a) False messages, modify, or replay routing information; b) Sinkhole attack; c) Selective forwarding attack; d) Sybil attack; e) Wormholes attack; f)Hello flood attack.
- Transport layer attacks: It main has not synchronized attack and run out of memory attack.
- Application layer attacks, such as data gathering, task distribution, target tracking, etc which all need security.

Secure communication is required for transmitting data securely between sensor nodes. Setting security goals for sensor networks will depend on knowing what it is that needs protecting. Sensor networks share some of the

features of mobile ad hoc networks but also add some unique challenges. The security goals encompass both those of the traditional networks and goals suited to the unique constraints of sensor networks. The four security goals for sensor networks are determined as Confidentiality, Integrity, Authentication and Availability (CIAA).

1. *Confidentiality*

Confidentiality is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. This is the most important issue in network security. Carman et al. [2000] and Perrig et al. [2002] have said the following about confidentiality in sensor networks. A sensor node should not reveal its data to the other nodes in the network. For example, an adversary has injected some malicious nodes into the network in a sensitive military application; confidentiality will not allow them from gaining access to information about other nodes.

Establishing and maintaining confidentiality is extremely important when node identities and keys are being distributed to establish a secure communication channel among sensor nodes.

2. Integrity

Data integrity in sensor networks is needed to ensure the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed while on the network. Even if the network has confidentiality measures in place, there is still a possibility that the data's integrity has been compromised by alterations. The integrity of the network will be in question if a malicious node present in the network injects bogus data or turbulent conditions due to wireless channel cause damage or loss of data.

III. AUTHENTICATION

Authentication indicates the reliability of the message. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject additional bogus packets. So the receiving node needs to be able to confirm that a packet it has received is actually comes from the node who have claim to sent it. In other words, data authentication verifies the identity of senders. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys to compute the message authentication code (MAC).

- ❖ It is extremely challenging to ensure authentication because of the wirelessness of the media and the unattended nature of sensor networks.
- ❖ The energy and computational limitations of sensor nodes makes it impractical to deploy complex cryptographic techniques.

1. Availability

Availability means the service should be available all the time. It means whether a node has the ability to use the resources and whether the network is available for the messages to communicate. Complex security measures require a higher consumption of energy and computation power. It keeps availability of the network challenging. However, failure of the base station or cluster leader's availability will eventually threaten the entire sensor network. therefore availability is most important factor for maintaining an operational network.

The study for the applicable of WSN security programs and security technology is the urgent needed, routing, various security authentications, time synchronization for example: security architecture, key management, secures, and security localization of nodes, intrusion detection of network and prevention strategies

2. The Intrusion Detection of WSN

An intrusion is defined as a set of actions that compromises confidentiality, availability, and integrity of a system. Intrusion detection is a security technology that attempts to identify those who are trying to break into and misuse a system without authorization and those who have legitimate access to the system but are abusing their privileges. The system can be a host computer, network equipment, a firewall, a router, a corporate network, or any information system being monitored by an intrusion detection system.

An IDS dynamically monitors a system and users' actions in the system to detect intrusions. Because an information system can suffer from various kinds of security vulnerabilities, it is both technically difficult and economically costly to build and maintain a system that is not susceptible to attacks. Experience teaches us never to rely on a single defensive technique. An IDS, by analyzing the system and users' operations, in search of undesirable and suspicious activities, may effectively monitor and protect against threats.

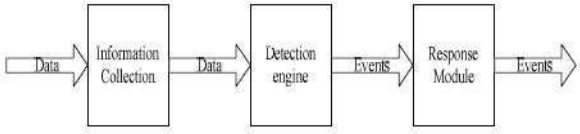

Figure 1: The basic form of IDS

IDS are a proactive intrusion prevention technology, such as figure 1. The WSN are usually deployed in harsh environments, or even the enemy area, so vulnerable to enemy capture and invasion. The IDS of WSN is varying widely from traditional network, mainly three aspects: No fixed network infrastructure; Communication type; Available resources (such as energy, CPU, memory, etc.).

With limited resources, some effective security defense techniques for traditional LAN/WAN/Internet are no longer suitable for wireless sensor network. For example, asymmetric cryptography is often too expensive for many WSN applications. Intrusion detection, as another layer of security, plays a more important role to secure wireless sensor networks. However, the low computational power and the insufficient available memory pose big challenges to the design of an intrusion detection system for WSNs: the intrusion detection components should optimize resource consumption, and it might sacrifice its performance to fit the resource constraints. Another challenge is only limited log/audit data could be used for intrusion detection due to low available storage. Sensor nodes use wireless communication in WSNs. Any information over the radio can be intercepted and the private or sensitive information could be captured by a passive attacker. An aggressive attacker can easily inject malicious messages into the wireless network to perform varied attacks.

IV. RELATED WORK

In this section we have discuss existing method that are used for secure data aggregation.

1. Weighted Trust Evaluation Approach

The basic idea in [1] is that forwarding node give trust values to each of the nodes in the cluster, if a node sends incorrect information which implies that a node has been compromised the forwarding node (aggregator node) directly lowers that node's trust level. It is much easier and less complex to keep track of the nodes and it is harder to compromise most of the node unless an attacker compromises the base stations. This approach is based on the assumption that base stations are trusted. In fact, if the adversary can gain control over the base stations, he/she can do any possible attack against the WSN. This is an interesting open problem. Another critical assumption is that the majority of the sensor nodes are working properly. If the number of compromised nodes is more than the number of normal nodes, the legal nodes will be reported as malicious one and being isolated. Through intensive simulation, the author has verified the correctness and efficiency of the detection scheme.

2. Ant Colony Based Approach

The proposed model in [2] has two phases. The first phase is initial configuration of the network, and the second phase performs identification of attacks and routing of data. Proposed intrusion detection model consists of four stages:

Formation of Cluster

To form clusters, the WSN is divided into different geographical regions G. Within each geographical region G a node N is chosen randomly and a parameter L that indicates the level of neighbor in the cluster is decided. Further to avoid HELLO flood attack only M neighbors are sent the Hello message. The neighbor list exchange process starts from the node N and goes up to L levels.

Identification of cluster head within the cluster

Once the cluster is formed, the cluster head selection process starts. Three random nodes H1, H2, and H3 are chosen within the cluster. The resources of H1, H2, and H3 are then computed and compared with a predefined threshold value of resource. A node with highest resources is then selected as a cluster head. This process is applied to select a cluster heads of all available clusters.

Deployment of Ant pheromone on cluster heads

Once the pheromone is deployed over all the cluster heads, the routing process can begin. The routing process is now a two stage process. In the first stage, data is sent to respective cluster head by the source node. The cluster head then sends Hello message along with pheromone request to its neighbor cluster heads. The entire neighbor cluster heads reply with their current pheromone value. This process is repeated until an optimal path from source cluster head CH to destination is found. It is capable of taking care of internal as well as external attack. Further the conformity check after the formation of cluster makes sure that no malicious node becomes part of WSN.

3. Data Mining Based Approach

A sensor based online mining wireless intrusion detection system is proposed in [3]. It applies data mining clustering technique to wireless network data which is captured through hardware sensors and detection of anomalous behavior in wireless packets is done. Using hardware sensors to capture network packets enables detection of attacks before they reach access points. All packets transmitted in the networks are analyzed for more complete attack detection. Experiments show that the system can detect intrusions without undergoing any training and has a higher detection rate.

4. Agent Based Approach

In the agent based approach as in [4], the author has evaluated the performance of the agent based abnormal detection model, which is implemented by rule base and naive Bayesian technique. Throughout experiment the simulation results shows that the performance of the proposed agent based model is better compare to existing methods. Proposed model identifies the abnormal event pattern sensor nodes in a largely deployed distributed sensor network under a common anomaly detection framework which will design by agent based learning and distributed data mining technique.

5. Trust Based Approach

In a trust-based intrusion detection scheme as in [5], the author has considered a composite trust metric deriving from both social trust (honesty) and QoS trust (energy and cooperativeness) as an indicator of maliciousness. By statistically analyzing peer-to-peer trust evaluation results collected from sensor nodes,each cluster head applies trust-based intrusion detection to assess the trustworthiness and maliciousness of sensor nodes in its cluster. Cluster heads themselves are evaluated by the base station. An analytical model based on stochastic Petri nets is developed for performance evaluation of the proposed trust-based intrusion detection scheme, as well as a statistical method for calculating the false alarm probability. Simulation results show the effectiveness of the approach.

6. Weak Hidden Markov Model Based Approach

A weak hidden markov model based intrusion detection method for wireless sensor networks is proposed in [6]. State transition probabilities are reduced to rules of reach ability in weak Hidden Markov model (W-HMM). Intrusion detection algorithm can be divided into two stages: training and learning stage and real time intrusion detection stage. The author has introduced scoring scheme nd deviation alarm mechanisms to enhance the state transition accuracy of W-HMM. Simulation results show that the methodology is efficient.

7. Neighbor Based Approach

The Neighbor-based intrusion detection method proposed in [7] explores the principle that sensor nodes situated spatially close to each other tend to have a similar behavior. A node is considered malicious if its behavior significantly differs from its neighbors. The author has implemented IDS for the Tiny OS which uses the received signal strength, packet delivery ratio as well as proposed packet dropping ratio and received to sent ratio to detect selective forwarding, jamming and hello flood attacks. They have evaluated the implemented IDS in the TOSSIM simulator. The proposed IDS are capable of detecting the attacks with reasonably low occurrence of false positives and negatives when collaboration among nodes is employed.

8. Game Theory Based Approach

A theoretical signaling game model for intrusion detection in wireless sensor networks is proposed in [8]. A signaling game is used to model the interactions among nodes of a wireless sensor network. The interaction between an attacker and an individual node is as a Bayesian game with incomplete information. The author has proposed a signaling Bayesian game to model the interaction between a notorious node and IDS.

9. Hybrid Approach

A hybrid intrusion detection system for enhancing the security of a cluster-based wireless sensor network is proposed in [9]. Proposed hybrid intrusion detection system consists of three modules: The anomaly detection module is used to filter the normal or abnormal packet. Then, the abnormal packets are judged through the misuse detection module for type detection. Finally, the results of the two detection module are integrated by the decision-making module to determine whether the intrusion and the type of intrusion, and return to the manager to follow-up treatment. Simulation result shows the efficiency of the proposed system.

V. CONCLUSIONS

Intrusion detection is very crucial issue due to the nature of wireless sensor nodes. In this paper first we have discuss the security issues in WSN, then various challenges associated with intrusion detection system and the existing methods to detect the malicious node in wireless sensor network.

REFERENCES

[1]Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation, Idris M Atakli, Hongbing Hu, Yu Chen, Wei-Shinn Ku, Zhou Su The Symposium on Simulation of Systems Security (SSSS'08), Ottawa, Canada, April 14 –17, 2008, pp. 836-843.

[2]Ant Colony based Approach for Intrusion Detection on Cluster Heads in WSN Harshal A Arolkar, Shraddha P Sheth, Vaidehi P Tamhane, International Conference on Communication, Computing & Security ICCCS'11, February 12–14, 2011, Rourkela, Odisha, India, ACM ISBN: 978-1-4503-0464-1, pp. 523-526.

[3]WIDS: A Sensor-Based Online Mining Wireless Intrusion DetectionSystem, C.I. Ezeife, Maxwell Ejelike, A.K. Aggarwal, Proceedings of the 2008 international symposium on Database engineering & applications

IDEAS '08, September 10-12, ACM ISBN: 978-1-60558-188-0, pp. 255-161.

[4]A Simple Agent Based Model for Detecting Abnormal Event Patterns in Distributed Wireless Sensor Networks, Muktikanta Sa, Amiya Kumar Rath, Proceedings of the 2011 International Conference on Communication, Computing &
Security, ACM ISBN: 978-1-4503-0464-1, pp. 67-70 .

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

[6]A Weak Hidden Markov Model Based Intrusion Detection Method For Wireless Sensor Networks, Xianfeng Song, Guangxi Chen, Xiaolong Li, International Conference on Intelligent Computing and Integrated Systems(ICISS) 2010, pp. 887-889.

[7]Neighbor-based Intrusion Detection for Wireless Sensor Networks, Andriy Stetsko, Lukas Folkman, Vashek atyas, 6th International Conference on Wireless and Mobile Communications (ICWMC), 2010, pp. 420-425.

[8]A Theoretical Signaling Game Model for Intrusion Detection in Wireless Sensor Networks, Mohsen stiri, Ahmad Khademzadeh, 14th International Telecommunications Network Strategy and Planning Symposium (NETWORKS), 2010, pp. 1-6 .

[9]Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network, K Q Yan, S C Wang, S S Wang, C W Liu, 3rd IEEE International Conference on Computer Science and Informational Technology (ICCSIT), 2010, pp.114-118.