Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.810 – 813

REVIEW ARTICLE

A Review on Intrusion Detection Schemes in Wireless Sensor Network

Nidhi Aley[1], Shruti Kolte[2]
[1]Department of CSE, GHREAT, Nagpur, India
[2]Department of CSE, GHREAT, Nagpur, India
[1] nidhi.a02@gmail.com, [2] shrutikolte32@gmail.com

Abstract— Modern wireless sensor networks require specific and high degree of security due to their limitation and versatility tasks. Their limited computational ability and battery resources restrictions make them vulnerable to many kinds of attacks. Little real-world data is available about the insider threat. This "insider threat" has received considerable attention, and is cited as one of the most serious security problems. The goal of this paper is to provide a detailed review about different techniques available for detecting an intrusion along with their characteristics and advantages.

Keywords— Watchdog, Insider threats, Trust mechanism, WSN, IDSs

I. INTRODUCTION

In today's world, advances in electronic technology have invented the new ways for the development of new inventions in wireless sensor networks. It consist of large number of low-power, low-cost sensor node that communicate wirelessly. When the nodes in WSN are situated far away from each other, transmitting data using multihop may weaken the security strength (e.g. intermediate nodes may modify data, or capture/harm the sensor nodes, or may launch the attacks, etc.). These types of problems generally increase the node's energy consumption or may reduce the lifetime of network.

Many security solutions for WSN have been proposed. They are authentication, key exchange and security routing. They cannot detect or eliminate all the security attacks since an intrusion detection system is considered as the foremost solution to address wide range of security problem. Authentication and authorization can prevent the network from outsider attacker, but they cannot catch the insider attackers who are the legal members of the network. These legal members are the insider threats, and insider threat is an important security in WSN. A trust mechanism system is developed to defend the insider attacker.

A trust mechanism is often implemented as distributed system where each sensor can evaluate, update and store trustworthiness of other nodes based on trust model [1].

II. LITERATURE REVIEW

a. Watchdog Three-Tier Technique to Secure Wireless Sensor Network-

[2] Uses a pair wise key distribution scheme as its basic component, this key provide the basic authentication and pair wise key establishment between sensor node and MSS plus they refine the general three-tier security framework. A special kind of node is implemented which is called as watchdog, that doesn't involve in communication. An access point detects intrusion and passes information to watchdog, further it check and matches keys and permit the respective node in network, otherwise throw node out of network.

This will increase the flexibility of network, Improve the network resilience to mobile sink replication attack. This system throws the detected node out of network completely; the current operation being performed by that node remained undone, since a routing algorithm is needed.

b. Hybrid Intrusion Detection System for enhancing Security of a cluster-based wireless sensor network-

[3] Creates two basic models viz. Anomaly detection- build a model of normal behaviour and compare with detected behaviours. And it filters a large number of packet records. Misuse detection- detect attack type by comparing past attack behaviour and current behaviour. Also perform a second detection when the packet is determined to intrusion. Result of these two is integrated by decision making module to determine intrusion and type of intrusion. Since an IDS system act as a network monitor or an alarm.

It efficiently detects intrusion and avoids the resource waste. It prevents destruction of system by raising an alarm before intruder start to attack. Anomaly detection have high detection rate but high false positive rate, whereas misuse detection have high accuracy but low detection rate.

c. Hybrid Intrusion Detection for Anomaly detection & Misuse Attack using Clustering in wireless sensor network-

[4] Proposed a HIDS system with two techniques- Cluster based and Rule based. Network is divided into cluster head (CH) and member nodes.CH transfer and collect information to and from node members. A rule based system is divided into 3 phases of intrusion detection, in first supervised node data, in second node operation failure, and in third compare number of failure with estimated occasional failure in network.

The rule based techniques are simple, faster and require minimum data. This decreases the threat of attack in the system helps user to handle and correct the system further with hybrid detection. The feature selection method and rule based method is fully dependent on expert.

d. Intrusion Detection & fault Tolerance in Heterogeneous Wireless Sensor Network: A survey-

[5] Proposes a dynamic trust management protocol, In that there are 2 ways for intrusion detection- single sensing and multiple sensing. They propose a work that consider smart and insidious attacker which can perform more targeted attacks, capture certain nodes with high probability alternates between benign and malicious behaviour and concatenate with other attackers to avoid intrusion detection. Also it investigate the use of trust/reputation management, strengthen intrusion detection through "weighted voting" by leveraging knowledge of trust/reputation of neighbour nodes.

It reduces all false positive and negative rates, also provide shortest path routing. These studies largely ignored energy consumption which can adversely shorten the system lifetime.

e. Advanced Intrusion Detection System for Wireless Sensor Network-

[6] Proposed an Advanced IDS which is a combination of energy prediction based IDS and hybrid intrusion detection as well cross layer IDS. The system is capable of detecting almost all intrusion but also applicable to small, medium and large sized wireless Sensor Network. One advantage of it is that, it improves the detection rate and efficiency, so that almost all the intrusion can be detected.

Energy efficiency and lifetime is improved. IDSs will work efficiently for small or medium sized network but for a large network with many numbers of sensors it will not be suitable.

IDSs proposed for WSNs are summarized in Table 1 including their detection technique, advantages and limitation of each scheme. Accordingly, the following conclusions can be drawn for the proposed IDSs in WSNs:

TABLE I

COMPARISON OF THE IDSs PROPOSED FOR WSNS

Sr. No.	***Detection Technique***	***Description***	***Advantage***	***Limitation***
[2]	Pair wise Key distribution	A key is matched and permit the node for further operation.	Increase networks' flexibility.	It throws the detected node out of network completely
[3]	Anomaly and misuse detection based approach	Compare normal behaviour with detected behaviour and filter the records. In next step detect attack type by comparing both behaviours.	Anomaly detection have high detection rate, misuse detection have high accuracy.	Anomaly detection have high false positive rate, Misuse detection have low detection rate.
[4]	Cluster based and Rule based approach	A cluster head monitor, collect and send the information to and from member nodes of the network.	Decrease the threat of attack in the system helps user to handle and correct the system.	The feature selection method and rule based method is fully dependent on expert.
[5]	Single sensing and multiple sensing trust management	Strengthen the network through weighted waiting algorithm by using the knowledge of neighbour nodes reputation system.	Reduces false positive and negative rates, provide shortest path routing.	These studies largely ignored energy consumption which can adversely shorten the system lifetime.
[6]	Energy prediction based IDS and hybrid intrusion detection, cross layer IDS	It gets the advantage of hybrid intrusion detection plus energy prediction based system is used to manage the energy resources.	Improves the detection rate and efficiency.	IDSs will work efficiently for small or medium sized network but for a large network with many numbers of sensors it will not be suitable.

III. CONCLUSIONS

This paper introduces different techniques for intrusion detection, their advantages and limitations. While sensing the surrounding environment, processing the sensed information and transmitting the resultant data WSNs consume high amount of energy. Therefore, the IDSs need to spend the least amount of energy as possible to spare enough energy for the crucial operations of the WSN. As energy is the scarce resource, energy consumption of the IDSs is an important issue from a system design point of view. So, if high energy consuming IDS algorithms are only run on watchdog node, this can surely save energy of the rest of the nodes and ultimately increase the total lifetime of the network.

REFERENCES

[1] Y. Cho and G. Qu, Y Wu. "*Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks*", IEEE CS Security and Privacy Workshops 2012.

[2] Pramod D Mane, Prof. D.H.Kulkarni,"*Watchdog Three-Tier Technique to Secure Wireless Sensor Network*", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (6) , 2013.

[3] K.Q. Yan, s.c. Wang, S.S. Wang and C.W. Liu, "*Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network*", IEEE, 2010.

[4] Mr. Ansar S, Prof. Pankaj K, Prof. Hitesh Gupta, "*Hybrid Intrusion Detection for Anomaly & Misuse Attack using Clustering in Wireless Sensor Network*", IJARCET, Volume 2, Issue 11, November 2013.

[5] Sneha Dhage, Purnima Soni, "*Intrusion Detection and Fault Tolerance in Heterogeneous Wireless Sensor Network: A Survey*", International Journal of Scientific and Research Publications, Volume 4, Issue 2, February 2014.

[6] Joseph RishSimenthy, K. Vijayan, "*Advanced Intrusion Detection System for Wireless Sensor Networks*", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Special Issue 3, April 2014.

[7] Ravi Kumar, Sunil Kumar, Prabhat Singh, "*Enhanced Approach for Reliable & Secure Wireless Sensor Network*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013.

[8] Shaila Ket al."*Probabilistic Model for Single And multi-sensing Intrusion Detection in Wireless Sensor Networks*", IOSR Journal of Computer Engineering, Volume 16, Issue 1, Ver. IX Feb. 2014.

[9] HamedKhanbabapour, Hamid Mirvaziri, "*An Intelligent Intrusion Detection System Based On Expectation Maximization Algorithm in Wireless Sensor Networks*", ICT, Volume 4, January 2014.

[10] Hamed Khanbabapour Hamid Mirvaziri, "*An Intelligent Intrusion Detection System Based On Expectation Maximization Algorithm in Wireless Sensor Networks*", International Journal of Information and Communication Technology Research, Volume 4 No. 1, January 2014.

[11] Ismail Butun et al., "*A Survey of Intrusion Detection Systems in Wireless Sensor Networks*", IEEE, 2013.

[12] Hassen Mohammed Abduallah Alsafi. "*A Review of Intrusion Detection System Schemes in Wireless Sensor Network*", CIS Journal, Vol. 4, No. 9 September 2013.

[13] Hichem Sedjelmaci, and Mohamed Feham, "*Novel Hybrid Intrusion Detection System for Clustered Wireless Sensor Network*", IJNSA, Vol.3, No.4, July 2011.

