IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

A review on Intrusion Detection system in WSN

Manoj Kumar Gupta[1], Lokesh Singh[2]

M. Tech Scholar, Computer Science & Engineering, TIT, Bhopal, India [1]

Assistant Professor, Computer Science & Engineering, TIT, Bhopal, India [2]

Abstract: Intrusion detection is the one of the major problem in network security, as the use of computer system and network increases, securing data is one of the important in order to achieve secure data transmission without hacking. Various numbers of methods and intrusion detection systems have been proposed to detect intruder and anomaly detection, but most of the methods and system tries to detect the rates of the attackers and positive rates in different types of attacks. In this paper a study of various intrusion methods have been analysed and their comparison is also shown.

Keywords: IDS, Attacker, WSN, Security.

I. INTRODUCTION

A Wireless Sensor Network (WSN) [1] monitor the conditions for physical and environmental, the WSN consist of autonomous sensors which are structural distributed and works cooperatively to monitor applications like temperature, sound, military and vibrations. Some applications have diverse data traffic which has different quality of service (QoS) requirements. There are three different QoS requirements: 1) Energy Efficiency 2) Scheduling based on traffic priority and 3) Latency 4) Security. Based on these requirements the data traffic can be split into:

- Regular traffic
- Reliability sensitive traffic, in this traffic the data is to be delivered without loss, but it can have little delay.
- Delay sensitive traffic, in this traffic data has to be delivered within deadline, but can tolerate minimum packet losses. Critical Traffic has high importance, which requires high reliability and short delay

The main objective of a wireless sensor node is to collect information from there surrounding environment and transmit it to the sink. WSNs have many applications that are used in many scenarios such as detecting climate changed, monitoring environments and habitats, and other surveillance and military applications. Mostly sensor nodes are used in such areas where wired networks are impossible to be setup. WSNs are setup in physical harsh and unfriendly environments where nodes are always bare to physical security risks damages. Furthermore, self-organizing nature, low battery power supply, limited bandwidth support, distributed operations using open wireless medium, multi-hop traffic forwarding, and dependency on other nodes are such aspect of sensor networks that expose it to many security attacks at all layers of the OSI model. Various security-related solutions for WSNs have been proposed such as authentication, key exchange, and secure routing or security mechanisms for individual attacks. D. Baghyalakshmi [2] proposed an hierarchical routing model in WSNs in which the sensor network divided into various cluster, the packet forwarding takes place from the first level cluster head to second level cluster head and reaches to final destination.

An IDS is used to detect the intruder in the network while communicating, since this is only used to detect the intruder this does not used to prevent the intruder. When the attack is detected in the network, the IDS trigger an alarm which informs the network controller management to take particular actions. IDS can be classified into two types 1) IDS based on Rules and 2) IDS based on anomaly [3,4]. Rule based IDS is also known as signature based IDS, where the digital signatures are used to detect the intruder. The rule based IDS detects the intruder very accuracy, which uses the built in signatures as a parameters to detect the intruder, but if any new attacks is launched this fails to detect the intruder. The anomaly IDS works based on the traffic patterns in the network, this IDS system can detect the new attacks as they can identify the false claim in the traffic patterns.

This paper gives the review of the existing IDS and their data set, we examine existing security attacks. We analyze and discuss some already proposed IDSs. We make comparison of existing IDSs on the basis of detection. We highlight some open research issues and directions, and finally we conclude the paper.

II. SEURITY IN WSN

One security condition that receives a great deal of attention in the wireless sensor network is the area of key management. WSNs are unique (among embedded wireless networks) in this aspect due to their size, mobility and computational power constraints. Even, researchers envision wireless sensor networks to be orders of magnitude larger compare to their traditional/embedded counterparts. This, coupled with the operational constraints makes secure key management an absolute necessity in most wireless sensor network designs. Because encryption and key management establishment are so crucial to the defense of a wireless sensor network, with nearly all aspects of wireless sensor network defences relying on solid encryption, we first begin with an overview of the unique key and encryption issues surrounding WSNs before discussing more specific sensor network defences.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

There are many key management issues in to wireless sensor networks. Indeed, key establishment and management problems have been studied in deep outside of the wireless networking area. Traditionally, key establishment is done by using one of many public-key protocols. Commonly Diffie-Hellman public key protocol is used, but also there are many others.

Many traditional techniques are unsuitable in low power devices such as wireless sensor networks. This is due largely to the fact that typical key exchange techniques use asymmetric cryptography, also called public key cryptography. In this type, it is necessary to maintain two mathematically key related to each other, one of which is public while the other is private. These allow data to be encrypted with the public key and decrypted only with the private key. The problem occurs with asymmetric cryptography, in a wireless sensor network, is that it is typically too computationally intensive for the individual nodes in a sensor network.

Symmetric cryptography is typical choice for applications that cannot afford the computational complexity of asymmetric cryptography. Symmetric schemes use a single shared key known only between the two communicating hosts. The key that is share with communication host, is used for both encrypting and decrypting of data. The traditional example of symmetric cryptography is Data Encryption Standard. The Data Encryption Standard is used, however, is quite limited due to the fact that it can be easily broken. In light of the shortcomings of Data Encryption Standard, other symmetric cryptography systems had proposed including 3DES (Triple DES), RC5, AES, and so on.

Most WSNs use contention based carrier sense multiple access with collision avoidance mechanism (CSMA/CA). This method tries to avoid collision; however it includes more complications in the form of collision, hidden-node problem, MAC selfishness, and unfairness. There are possible countermeasures against such kind of attacks are small frames and rate limitations.

III. INTRUSION DETECTION SYSTEM (IDS)

In WSN communication nodes communicate through single and multihop to transfer the data, while communicating the security issues for wsn is a one of the parameter to be considered because of its distributed environment, where the attackers cannot be tracked or located easily. Many authors have proposed how to handle the security attacks, Encryption mechanisms are designed and used to protect data against passive attacks. Hence, one can say that there is a need to design mechanisms that are capable enough of detecting and preventing multiple security attacks in WSNs. An Intrusion Detection System (IDS) is one possible solution to it.

IDS operation modes can be based on stand alone and cluster based operation. Standalone operation works on every node to identify the malicious activities in the network, whereas the cluster based operation is based on distributed where every node monitors its neighbor node, if in case any malicious activity is detected, the node informs to its cluster head.

The components of IDS can be defined in three

1) Monitoring
2) Analysis and Detection
3) Alarm

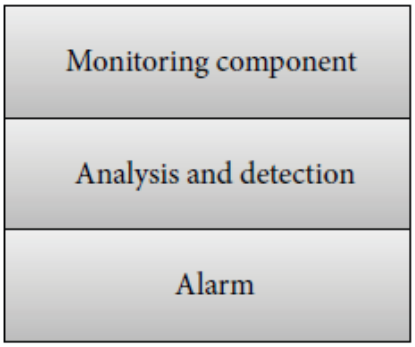

Fig.1. Components of IDS

In monitoring component the node monitors its neighbor local events, the event may be a traffic pattern, change in an action and resource utilization.

In analysis and detection module, the network operation and behaviour is analysed and based on the analysis the decisions are made.

In the alarm component, the alarm or the trigger is generated whenever the malicious activity is detected and it is sent to the processing unit.

- **Signature-Based Intrusion Detection Systems**

Signature based IDS, which is also known as rule-based IDS, having predefined rules of different security attacks. When the network's behavior shows any variance from the predefined rules, it is classified as an attack. Signature-based IDSs are well work with for known intrusions; however they cannot detect new security attacks or those attacks having no predefined rules.

In [5], a rule-based IDS for WSNs is presented. It is host based in which every node has IDS. The architecture of the proposed IDS has different type many modules like packet monitoring, cooperative engine, detection engine, and response unit. The IDS is generally designed for routing attacks and is capable for detecting packet-dropping attacks. An IDS for detection of sink-hole attack is presented in [6]. The proposed IDS are hosted on each sensor node and requires TinyOS with the combination of Mint Route routing protocol. It is an advanced version of [5] with narrow approach; that is, the former can trace many packet-dropping and misdirecting attacks while the latter is only designed for detection of sink-hole attacks.

A decentralized rule-based IDS is proposed in [7]. This mechanism has three main phases, namely, data acquisition, rule application, and intrusion detection. The proposed mechanism is capable of detect many routing attacks such as worm-hole, black-hole, selective-forwarding, and delay attacks. The authors also claim that the proposed solution is capable of detecting jamming attack as well; however they did not explain how jamming attacks are detected as it is a physical layer attack.

- **Anomaly-Based Intrusion Detection Systems.**

IDS monitors network activities and classify them as either normal or malicious using heuristic approach. Most

DOI 10.17148/IJARCCE.2016.5128

of anomaly-based IDSs identify intrusions through threshold values; that is, any activity below a threshold is normal, while any condition above a threshold is known as an intrusion.

The main advantage of anomaly-based IDS is its capability to detect new and unknown attacks; however sometimes it fails to detect even well-known security attacks. A cluster based IDS for routing attack is proposed [8]. This mechanism is capable of building a normal traffic model, which is used to differentiate between normal and abnormal traffic. The normal traffic model consists of number of packets received and sent, number of route requests and sent, and so forth. The IDS can detect many attacks such as periodic route error attack and sink-hole attack. A support vector machine based IDS [9] is used to detect routing attacks such as black hole.

Characteristics	**Anomaly based IDS**	**Signature based IDS**
Detection rate	Medium	Medium
False alarm	Medium	Medium
Computation	Low	Low
Energy consumption	Low	Low
Attack detection	Few	Few
Strength	Capable of detecting new attacks	Detects all those attacks having signatures
Weakness	Misses well known attack	Cannot detect new attacks
Suitable for WSN	Yes	Yes

Table 1: Comparison of IDSs.

IV. COMPARISION AND DISCUSSION

The Wireless Sensor Networks are distributed in nature using multi-hop communication model. These networks are usually used in such areas where direct human communication is either impossible or difficult. Furthermore, WSNs have some limitations in terms of computation, bandwidth, memory, and energy. These limitations are considered when designing any proposal for such networks. Due to the unfriendly environments of WSNs, security is one of their most important aspects. IDSs are generally used for securing WSNs. IDS able to detect an intrusion and raise an alarm for appropriate action. Due to the limitation of energy and computational power, designing appropriate IDS for WSN is a challenging task.

The anomaly-based IDSs are suitable for small-sized WSNs in which few nodes communicate with the base station. In small sized WSNs, the traffic pattern is mostly same, so unusual traffic pattern or changing behavior treated as an intrusion. However this type of IDS may generate more false alarms and may not be able to detect well-known intrusions. Anomaly-based IDSs are generally lightweight in nature and mostly use statistical, probabilistic, traffic analysis or intelligent techniques.

The signature-based IDSs are suitable for large sized WSNs, where more security threats and attacks can compromise network operations. Signature-based IDS required more resources and computations as compared to anomaly based IDS. Among one of the most important and complex activities is the compilation and insertion of new attack signatures in the databases. Such IDSs generally use data mining or pattern matching techniques.

V. CONCLUSION

When designing a security mechanism, we must assume the limited resources of WSNs. Anomaly-based IDSs are lightweight in nature; however they can create more false alarms. Signature-based IDSs are suitable for large-sized WSNs; however they have few overheads such as updating and inserting new signatures.

REFERENCES

[1] Li Qun Zhuang, Jing Bing Zhang, Dan Hong Zhang and Yi Zhi Zhao "Data Management for Wireless Sensor Networks: Research Issues and Challenges" International Conference on Control and Automation (ICCA2005), Budapest, Hungary, June 27-29, 2005.

[2] D.Baghyalakshmi, Jemimah Ebenezer, S.A.V. Satyamurty "Low latency and energy efficient routing protocols for wireless sensor networks" IEEE Second International Conference on Computer and Network Technology, IEEE, pp 1-6,2-4 Jan 2010

[3] S. Northcutt and J. Novak, Network Intrusion Detection, SAMS, 3rd edition, 2002.

[4] S. Khan, K. K. Loo, and Z. U. Din, "Framework for intrusion detection in IEEE 802.11 wireless mesh networks," International Arab Journal of Information Technology, vol. 7, no. 4, pp. 435–440, 2010.

[5] I. Krontiris, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in Proceedings of the 13th EuropeanWireless Conference, Paris, France, April 2007.

[6] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "Intrusion detection of Sinkhole attacks in wireless sensor networks," in Algorithmic Aspects of Wireless Sensor Networks ALGOSENSORS, vol. 4837 of Lecture Notes in Computer Science, pp. 150–161, Springer, 2008.

[7] A. P. R. Da Silva, A. A. F. Loureiro, M. H. T. Martins, L. B. Ruiz, B. P. S. Rocha, and H. C.Wong, "Decentralized intrusion detection in wireless sensor networks," in Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks (Q2SWinet '05), pp. 16–23, Montreal, Canada, October 2005.

[8] C. E. Loo, M. Y. Ng, C. Leckie, and M. Palaniswami, "Intrusion detection for routing attacks in sensor networks," International Journal of Distributed Sensor Networks, vol. 2, no. 4, pp. 313–332, 2006.

[9] H. Deng, Q. A. Zeng, and D. P. Agrawal, "SVM-based intrusion detection system for wireless ad hoc networks," in Proceedings of the 58th IEEE Vehicular Technology Conference (VTC '03), pp. 2147–2151, October 2003.