Evaluation of Intrusion Detection Schemes in Wireless Sensor Network

Ishu Gupta[1], Kishu Gupta[2]
[1]*(Computer Application, National Institute of Technology (Kurukshetra), India,*
[2]*(Computer Application, Kurukshetra University (Kurukshetra), India,*

Abstract: *Wireless Sensor Network (WSN) consists of sensor nodes, which communicate wirelessly in order to perform some specific operation. Wireless Sensor Network (WSN) is implemented in open medium environment and the sensors nodes are fully distributed in nature. In order to communicate with each other a multi hop communication should be used. Moreover, WSNs have limitations in terms of computations, memory, bandwidth, and energy. The distributed nature, multi hop data forwarding, and open wireless medium are the factors that make WSNs highly vulnerable to security attacks at various levels. Intrusion Detection Systems (IDSs) can play an important role in detecting and preventing security attacks. IDS is capable to detect an intrusion and raise an alarm for appropriate responses. The aim of this paper is to provide a detailed review about current IDS schemes for WSN. Finally we focus on comparison of recent Intrusion Detection Schemes in WSNs.*

Keywords: *Anomaly-based IDS, Cluster-based IDS, Intrusion Detection System, sensor node, Signature-based IDS, Wireless Sensor Network*

I. Introduction

A Wireless Sensor Networks (WSN) consists of large number of low-power, low-cost sensor node that communicate wirelessly. These sensors are self-organized and deployed automatically in highly distributed and homogenous network environment. Also, it does not require any predefined infrastructure. The aim of using such sensors is to collect and process information about the surrounding environment. The packets will be transmitted from one node to another via multi-hope communication. The computation and energy resources are restricted in WSN.

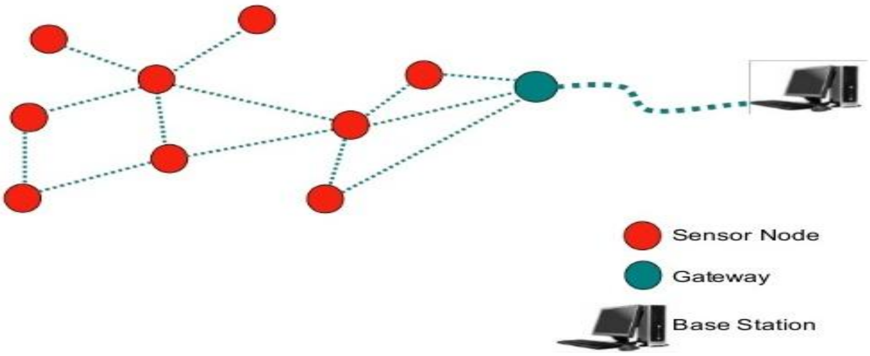

Fig 1: Wireless Sensor Network [1]

As the sensor nodes are deployed in open wireless medium, multi-hop data forwarding and the distributed nature, thus WSN becomes highly venerated towards security attacks. It can be attacked either by passive or active attacks. In passive attacks, attacker attempts to acquire imperative information by listening the stream of data sent via the communication channel while in active attacks, attacker has the ability to modify or delete the data in the network.

The prevention-based techniques such as cryptography, key management, and authentication have been implemented to secure and protect the network from malicious activities. Yet, these techniques will not be able to secure the network from internal attack that leads to extract some sensitive information [2] [3] [4] [5]. Detection-based techniques are introduced to overcome the limitation of the prevention-based technique. IDS are capable to detect an intrusion. This technique will be placed as second layer of defense to detect the internal as well the external attacks and keep the network secure from any malicious activities.

The aim of this paper is to provide a detailed review about the current IDS for WSN. Furthermore, we classified the IDS based on the detection techniques. Finally we discussed and concluded work.

II. Defense Mechanisms Against Attacks In WSN

The defense techniques that used to overcome the vulnerabilities in WSN are categorized into prevention-based security approaches and detection-based approaches. Prevention-based mechanism is formed as first defense line for WSN. It is used to protect the sensor networks from different types of attacks however this mechanism is not sufficient to secure the entire system from internal attacks because the insider attacks may capture some sensitive data. Hence it is only effective to prevent against external or outsider attacks [6]. On the other hand, detection-based mechanism has been proposed to overcome the limitation in the prevention-based technique. It is used to secure and monitor the WSNs from internal or insider attacks. IDS plays significant role as second line of defense and its major aim is to detect the abnormal or malicious activity in the network system.

III. Intrusion Detection System

Intrusion Detection System (IDS) is in charge of detecting, analyzing and reporting unwanted intrusion that exploited the vulnerabilities of the networks and computer system. It acts as second line of defense against attacks that preventive mechanism fail to address [6]. The collected information and logs from the IDS needs to be interpreted by skilled and experienced person [7].

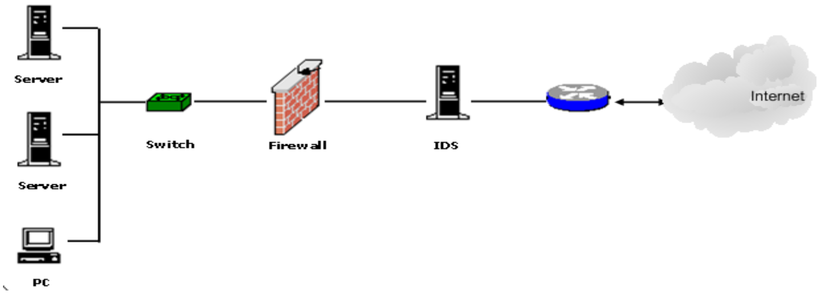

Fig 2: Intrusion Detection System (IDS) [8]

IV. Classification Of IDS

IDS can be classified in two categories on the basis of different features as shown in Fig. 3

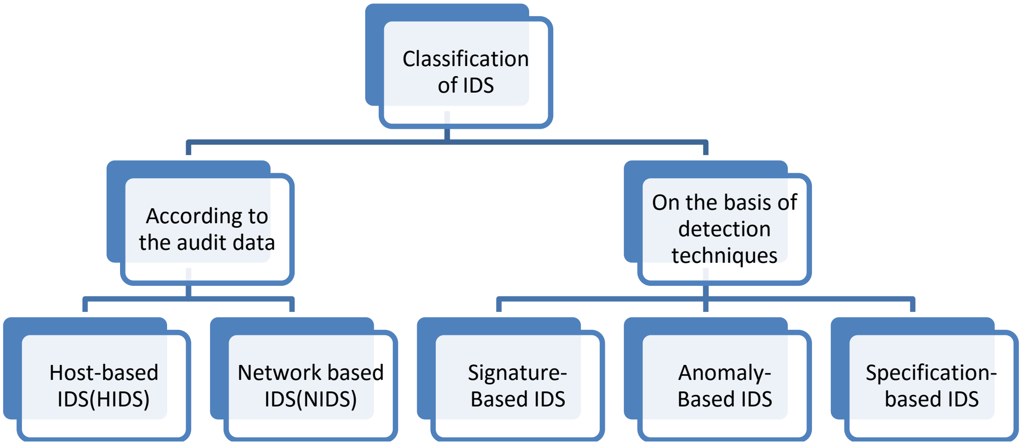

Fig 3: Classification of IDS

4.1 According To The Audit Data

(IDS) are classified according to the audit data into two main parts: **host-based IDS and network based IDS**. The host-based IDS uses application logs in the analysis whereas the network-based operates by capturing and evaluating the networks packet received from network traffic.

4.2 On The Basis Of Detection Techniques

On the basis of detection techniques IDS are categorized into three main classes **signature-based IDS, anomaly-based IDS and specification based IDS** as follows [9].

4.2.1 Signature-Based IDS

Signature-based IDS are also known as rule-based IDS because it consists of prior stored rules of security attacks. These rules are kept in the database. Once the network's behavior displays any matches to the fixed rules, it is classified as attack. Signature-based IDS are well suitable for known intrusions however they are not able to identify the latest security attacks or attacks having no predefined rules [10] [11].

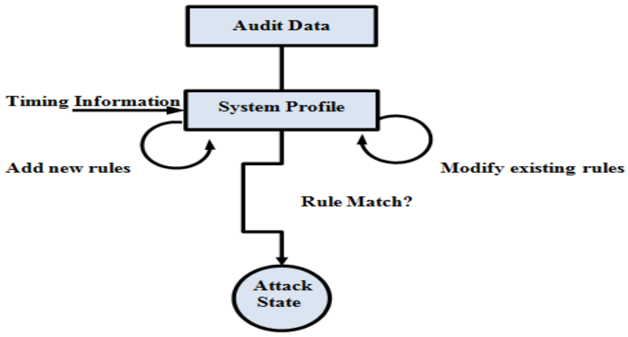

Fig 4: Signature-based Detection System (SDS) [12]

4.2.2 Anomaly-Based IDS

It is the second type of detection technique in IDS. In this technique there are reports or normal logs that are stored in the system. Then the system starts evaluating and comparing the captured data against the stored one in the normal profile and monitors network behavior deviation from normal profile. If the network's behavior deviates from the normal profile then there is possible intrusion occurred. Finally the system administrator should be informed about the status and take proper reaction [13][14]. This technique is much effective to detect new security attacks. Since this technique does not maintain any database to store the signature, the probability to miss detecting well-known security attack is high however, it keeps continuously monitor the traffic patterns [15][10].

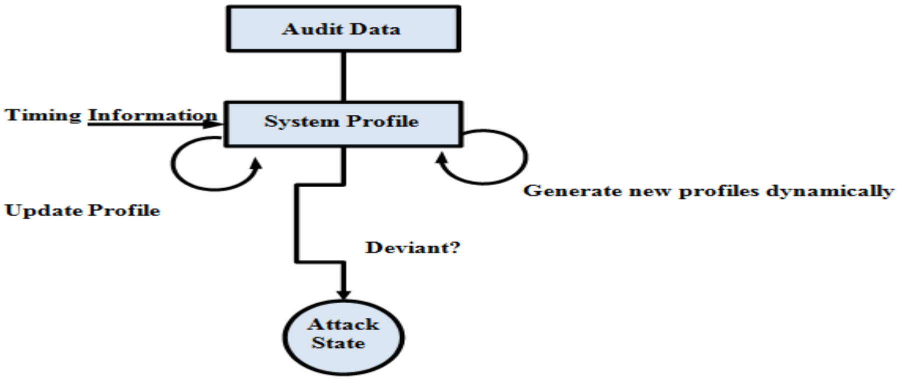

Fig 5: Anomaly-based Detection System (ADS) [12]

4.2.3 Specification-Based IDS

This technique is also known as hybrid IDS. It is the combination of signature-based and anomaly-based techniques. This technique involves two detection components. The first component known as signature-based is in charge of identifying well-known security attacks using signatures. On the other hand, the second component known as anomaly- based is in charge of identifying new security attacks by learning and detecting normal and abnormal patterns. This scheme is suggested if we want security attack detection contains less number of false positives however it is advisable not to use such scheme for the networks such as WSN that suffers from restricted energy and resources because hybrid mechanism may consume extra energy and extra resources.

V. Comparison Of Different IDS Scheme Used In WSN

TABLE 1 shows the comparison of different IDS scheme used in WSN. Signature-based IDS are well suitable for large-sized WSNs and effective to detect known intrusions however it requires extra resources and computation power as compared to anomaly-based IDS and one of the complicated and critical activities is the complexity of insertion of new attack patterns in the database. From the table we can see that memory required, energy consumption, resource consumption and computation power is less in anomaly-based IDS as compare to other two IDS. Anomaly-based IDS are suitable for small- sized WSNs and effective to detect latest intrusions however they have some limitation also. It is the complicated task to update the profile in the system. Hybrid IDS are suitable for large-sized and sustainable WSNs and used in cluster based or hierarchical WSNs however hybrid-based IDS is not recommended because of High consumption of energy and resources.

Table 1: Comparison of different IDS scheme used in WSN

IDS Characteristic	Signature-based IDS	Anomaly-based IDS	Hybrid-based IDS
Memory	Low	Low	Medium
Resource consumption	Medium	Low	High
Computation power	Medium	Low	High
Energy consumption	Low	Low	Medium
Detection rate	Medium	Medium	High
False alarm	Medium	Medium	Low
Network size	Suitable for large sized WSNs	Suitable for small-sized WSNs	Suitable for large-sized and sustainable WSNs
Technique used	Pattern matching techniques or data mining	Probabilistic, statistical, traffic analysis	Contain both signature-based and anomaly-based schemes
Intrusion detection	Effective to detect well-known intrusions	Effective to detect new intrusions	Effective to detect well-known as well as new intrusions

VI. Conclusion

While designing a security mechanism for the IDS in WSN, we have to take special care of the limitations that exists in the WSNs. IDS are widely used for securing WSNs and are capable to detect an intrusion. This paper introduces different techniques for intrusion detection system for wireless sensor networks. Each technique has its own superiority and limitations, so that we should be cautious about selecting the technique. Signature-based IDS are suitable for large-sized WSNs and effective to detect known intrusions however it require extra resources and computations power as compared to anomaly-based IDS. Anomaly-based IDS are suitable for small- sized WSNs and effective to detect latest intrusions however they have some limitation also. It is the complicated task to update the profile in the system. On the other hand, hybrid-based is not recommended because of its high consumption of resources and energy.

References

[1]. https://www.google.co.in/search?hl=en&site=imghp&tbm=isch&source=hp&biw=&bih=&q=wireless+sensor+network&btnG=Search+by+i mage#btnG=Search+by+image&imgrc=ok-Eklg0v_LAGM%3A.

[2]. Zapata, Manel Guerrero. "Secure ad hoc on-demand distance vector routing."ACM SIGMOBILE Mobile Computing and Communications Review 6, no. 3 (2002): 106-107.

[3]. Hu, Yih-Chun, David B. Johnson, and Adrian Perrig. "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks." Ad Hoc Networks1, no. 1 (2003): 175-192.

[4]. Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Ariadne: A secure on-demand routing protocol for ad hoc networks." Wireless Networks 11, no. 1-2 (2005): 21-38.

[5]. Perrig, Adrian, Ran Canetti, J. Doug Tygar, and Dawn Song. "The TESLA broadcast authentication protocol." (2005).

[6]. da Silva, Ana Paula R., Marcelo HT Martins, Bruno PS Rocha, Antonio AF Loureiro, Linnyer B. Ruiz, and Hao Chi Wong. "Decentralized intrusion detection in wireless sensor networks." In Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, pp. 16-23. ACM, 2005.

[7]. Alsafi, Hassen Mohammed, Wafaa Mustafa Abduallah, and Al-Sakib Khan Pathan. "IDPS: an integrated intrusion handling model for cloud computing environment." International Journal of Computing & Information Technology (IJCIT) 4, no. 1 (2012): 1-16.

[8]. https://www.google.co.in/search?hl=en&site=imghp&tbm=isch&source=hp&biw=&bih=&q=Intrusion+detection+system&btnG=Search+by +image#btnG=Search+by+image&imgrc=bgoc5oyiXo2hwM%3A.

[9]. Walters, John Paul, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary. "Wireless sensor network security: A survey," in book chapter of Security." In in Distributed, Grid, and Pervasive Computing, Yang Xiao (Eds. 2007).

[10]. Abduvaliyev, Abror, A. Pathan, Jianying Zhou, Rodrigo Roman, and W. Wong. "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks." (2012): 1-15.

[11]. Mamun, Mohammad Saiful Islam, and AFM Sultanul Kabir. "Hierarchical design based intrusion detection system for wireless ad hoc sensor network."International Journal of Network Security & Its Applications (IJNSA) 2.3 (2010): 102-117.

[12]. Hassen Mohammed Abduallah Alsafi, and Saeed Salem Basamh. "A Review of Intrusion Detection System Schemes in Wireless Sensor Network." Journal of Emerging Trends in Computing and Information Sciences, ISSN 2079-8407.

[13]. Karlof, Chris, and David Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures." Ad hoc networks 1, no. 2 (2003): 293-315.

[14]. Khan, Shafiullah, and Kok-Keong Loo. "Real-time cross-layer design for a large-scale flood detection and attack trace-back mechanism in IEEE 802.11 wireless mesh networks." Network Security 2009, no. 5 (2009): 9-16.

[15]. Wang, Shun-Sheng, Kuo-Qin Yan, Shu-Ching Wang, and Chia-Wei Liu. "An integrated intrusion detection system for cluster-based wireless sensor networks." Expert Systems with Applications 38, no. 12 (2011): 15234-15243.