Review on Intrusion Detection System Architectures in WSN

Ishu Gupta
Research Scholar, Department of Computer Applications, National Institute of Technology, Kurukshetra-136119, Haryana
Email: ishugupta23@gmail.com
Kishu Gupta
Research Scholar, Department of Computer Science & Applications, Kurukshetra University, kurukshetra-136119, Haryana
Email: kishugupta2@gmail.com

Abstract
Wireless Sensor Networks (WSNs) consist of sensor nodes deployed in a manner to collect information about surrounding environment. Wireless Sensor Network (WSN) is implemented in open medium environment and the sensors nodes are fully distributed in nature. Moreover, WSNs have limitations in terms of energy, bandwidth, computations and memory. Their limited computational ability and battery resources restrictions make them vulnerable to many kinds of attacks. Intrusion Detection Systems (IDSs) can play an important role in detecting and preventing security attacks. The aim of this paper is to provide a detailed review about current IDS and its architectures for WSN. Finally we focus on comparison of recent Intrusion Detection architectures in WSNs.

Keywords - ***Cluster-based or Hierarchical IDS, Cooperative or Distributed IDS, Intrusion Detection System, Stand-alone or Non-collaborative IDS, Wireless Sensor Network.***

1. Introduction

Wireless Sensor Networks (WSNs) are composed of large number of low-power, low-cost sensor node that communicate wirelessly. These Sensor nodes have the capability of self-organizing. They are decentralized and distributed in nature where communication takes place via multihop intermediate nodes. The main objective of a sensor node is to collect information from its surrounding environment. The computation and energy resources are restricted in WSN.

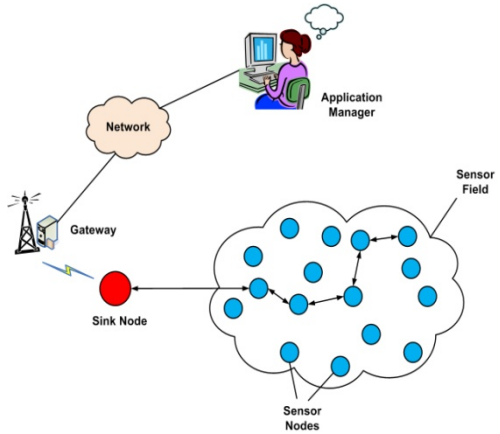

fig 1: wireless sensor network [7]

Their limited computational ability and battery resources restrictions make them vulnerable to many kinds of attacks. It can be attacked either by active or passive attacks. In active attacks, attacker has the ability to delete or modify the data in the network while in passive attacks, attacker attempts to acquire imperative information by listening the stream of data sent via the communication channel.

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 [5][6][11][14]. Detection-based techniques are introduced to overcome the limitation of the prevention-based technique. IDS is 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 and components of IDS. Furthermore, we presented

the architectures of IDS in WSN. Finally we discussed and concluded work.

2. 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 [4]. The collected information and logs from the IDS needs to be interpreted by skilled and experienced person [2].

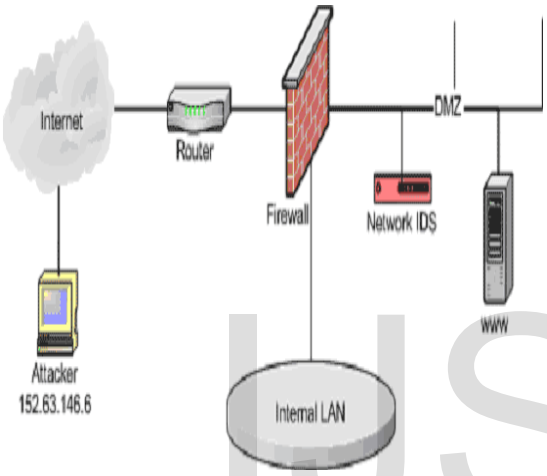

fig 2: intrusion detection system (ids) [8]

3. Components of IDS

IDS consist of three major components as shown in the Fig. 3 [10].

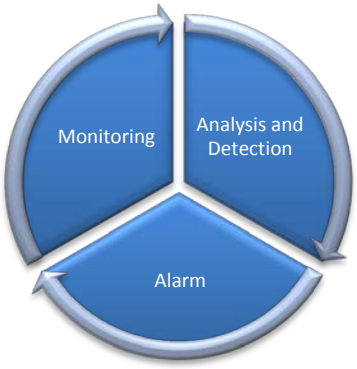

fig 3: ids component

Table 1: Component of IDS

Component	Characteristics
Monitoring	• It is used to monitor internal events and traffic Patterns [9]. • It is used to monitor both local and neighbor events in the node.
Analysis and detection	• It includes analysis of the Network operation, behaviors and activities and on the basis of analysis logs are prepared. • Uses IDS approach to detect the intrusions if present. • In IDS approach the decision is made based on the logs.
Alarm	• It is the element that generates the response and alerts the system if it detects any intrusions.

4. Architectures of IDS in Wireless Sensor Network

IDS can work in several modes. There are three main modes classifications: **standalone or non-collaborative IDS, cooperative or distributed IDS and cluster based IDS or hierarchical IDS** [3][12][13]. The architecture in WSN is based on the distribution and cooperation of different nodes. Every node will have its own IDS agent running on node.

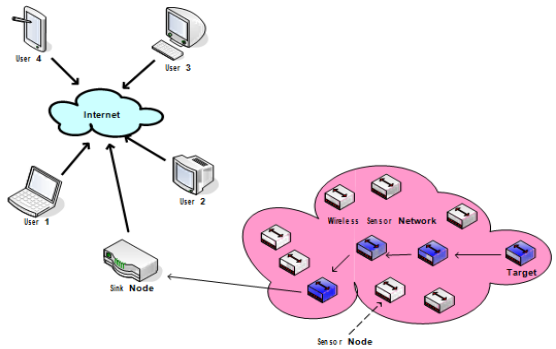

fig 4: wireless sensor network architecture [1]

The following are some of architecture for IDS in WSN:

4.1 Stand-alone or Non-collaborative Intrusion Detection Systems

In this architecture, the IDS work on each node independently to detect any malicious activities occurring in the victim node. In it different information will be collected from different node and the decision is made separately on each node based on the system logs.

This architecture would be efficient in a network where IDS is not configured on every node of the network. This architecture is suitable for flat infrastructure network because all nodes are assumed to be equal to each other.

This architecture has many limitations-

1. There is no sharing of data among the nodes in the network [3][12].
2. The collected data on every node will not be enough without sharing to determine an intrusion occurred or not.
3. Nodes belong to identical network will not know any information regarding the condition on other nodes.

That is why this infrastructure is not useful because of its limitations. Finally this network is not suggested to be chosen as optimal solutions to design the IDS architecture for WSN [1].

4.2 Cooperative or Distributed Intrusion Detection Systems

In the cooperative or distributed –based IDS the data is shared among the nodes [3]. In this architecture every node monitors and controls its close neighbor and surrounding nodes activities and operation, if any node has been violate then cluster head will be updated.

IDS agent running on each node is in charge for identifying and collecting local events i.e. monitor only their own data and communication to detect possible intrusions as well as initiating a response independently [1], however the IDS agents cooperatively participate in global communication by monitoring its surrounding nodes activities when the evidence is inconclusive. Like the stand-alone IDS infrastructure, this scheme is suitable for flat network infrastructure [12].

4.3 Cluster-based or Hierarchical Intrusion Detection Systems

Hierarchical architecture is extended from the cooperative or distributed IDS architecture and it is introduced for multilayer network. The multilayer networks are divided into clusters. Each cluster in the network has cluster head which act as central point and monitors all its sub-related nodes and response to detect the intrusions.

IDS agent running on every node locally monitors and detects all the intrusions. However, cluster head is responsible for both local and global communication for its cluster. It monitors and controls the network packet traffic and then initiate global reaction when intrusion in the network is identified or detected [3]. This architecture is deployed in multilayer infrastructure because some nodes are considered different in the multilayer infrastructure network.

5. Comparison of the Architectures used in WSN

Stand-alone or Non-collaborative IDS is not suitable architecture for WSN as in this architecture there is no sharing of data among the nodes in the network. The architecture in WSN is deployed as **distributed IDS** if the network infrastructure is flat infrastructure while **hierarchical IDS** should be deployed in WSN if network infrastructure is multilayer infrastructure. **TABLE 2** shows the comparison of different architectures used in WSN.

6. Conclusion

WSN have limitations in terms of energy, bandwidth, computations and memory. As the sensor nodes in WSN are deployed in open wireless medium, multi-hop data forwarding and the distributed nature thus WSN becomes highly venerable towards security attacks. IDS are widely used for securing WSNs and are capable to detect an intrusion. The architecture in WSN is based on the distribution and cooperation of different nodes. Stand-alone or Non-collaborative IDS is not suitable architecture for WSN as in this architecture there is no sharing of data among the nodes in the network. Thus while designing the architecture for WSN, distributive IDS architecture is suggested to be chosen as optimal solutions in case of flat infrastructure network and hierarchical IDS is suggested to be chosen as

optimal solutions for multilayer infrastructure network.

Table 2: Comparison of the Architectures used in WSN

Characteristic / Architecture	Sharing of data among the nodes	Network support	Commu-nication	Deployment
Stand-alone or Non collaborative IDS	No	This architecture would be efficient for a network where IDS is not configured on every node of the network.	Local	In flat infrastructure
Cooperative or Distributed IDS	Yes	This architecture would be efficient for a network where all nodes belong to the identical network.	Local as well as global	In flat infrastructure
Cluster-based or Hierarchical IDS	Yes	This architecture would be efficient for a network where network is divided into cluster.	Local as well as global	In Multilayer infrastructure

References

[1] Alsafi, Hassen Mohammed Abduallah, 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.

[2] 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.

[3] Anantvalee, Tiranuch, and Jie Wu. "*A survey on intrusion detection in mobile ad hoc networks*." In Wireless Network Security, pp. 159-180. Springer US, 2007.

[4] 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.

[5] 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.

[6] 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.

[7] http://www.cse.unr.edu/~arslan/pmwiki/pmwiki.php?n=Main.ResearchOverview.

[8] https://www.sans.org/securityresources/idfaq/what-is-the-role-of-security-event-correlation-in-intrusion-detection/5/9.

[9] 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.

[10] Khan, Shafiullah, Kok-Keong Loo, and Zia Ud Din. "*Framework for intrusion detection in IEEE 802.11 wireless mesh networks*." Int. Arab J. Inf. Technol. 7, no. 4 (2010): 435-440.

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

[12] Rassam, Murad A., M. A. Maarof, and Anazida Zainal. "*A Survey of Intrusion Detection Schemes in Wireless Sensor Networks*." American

Journal of Applied Sciences 9, no. 10 (2012): 1636.

[13] Siddiqui, Muhammad Shoaib, and Choong Seon Hong. "*Security issues in wireless mesh networks*." In Multimedia and Ubiquitous Engineering, 2007. MUE'07. International Conference on, pp. 717-722. IEEE, 2007.

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