Review Article

iMedPub Journals
http://www.imedpub.com

American Journal of Computer Science and Information Technology

2021
Vol. 9 No. 8: 108

Intrusion Detection System-IDS

Estifanos Tilahun Mihret*

Engineering and Technology College, Mettu University (MeU), Mettu, Ethiopia

Corresponding author:
Estifanos Tilahun Mihret, Engineering and Technology College, Mettu University (MeU), Mettu, Ethiopia

E-mail: amirelove03@gmail.com

Citation: Mihret ET (2021) Intrusion Detection System-IDS. Am J Compt Sci Inform Technol Vol.9 No.8: 108.

Abstract

Today's world has made up of electronic networks. Everyday huge amount of sensitive data passed through the networks. These networks are the backbones of the industries and different sectors like banking, transportation, health-care, military, communication etc. Thus securing the data passed through those networks is mandatory. Organizations are investing more and more money to secure their data from the attackers. Simultaneously, the attackers are raising their knowledge and getting strength time to time. Thus, to overcome this problem in some extents, IDS techniques have contributing a vital role as one of security tools. The IDS techniques have used to protect the network whether wired or wireless from the attackers. Moreover, due to their unique characteristics, wireless ad hoc networks (MANETs) are more vulnerable to malicious attack and the absolute security in the mobile ad hoc network is very hard to achieve. Prevention methods as cryptography techniques alone are not sufficient to make them secure; therefore, efficient intrusion detection must be deployed and elaborated to facilitate the identification of attacks. In this paper, I made survey of different architectures, techniques, types and approaches of intrusion detection systems (IDSs) as general and for MANETs accordingly to some literatures as shown below. Besides, in the coming days, the researchers would focus on building an improved system to detect the intruders and more secure the network from the attackers by the integrating of different IDS tools and with various security methods.

Keywords: Intrusion Detecion system (IDS); Survey of IDS; Mobile ad hoc networks (MAN)

Received: August 17, 2021; **Accepted:** August 31, 2021; **Published:** September 07, 2021

Introduction

In the past two decades, computer-networking technology has been growing dramatically. Generally, computer networking has classified into two kingdoms, wired and wireless network respectively. Though on the one hand the technology improves time to time, on the other hand the security challenges have widely enhanced in different directions. Such as, intrusion problems, DOS, eavesdropping and so forth. For all of those security problems, many authors and researchers have trying to propose and develop different security mechanisms and approaches. However, novel security attacks and malicious activities have emerging rapidly and due to this it is a very tough to make a complete secure system. This paper tried to prepare a survey of intrusion detection system and recommendation of its future works. Thus, I have reviewed basic journals of intrusion detection system and presented IDS types, techniques and some IDS approaches regarding to wireless network (ad hoc) as shown as below. Intrusion is an attempting to break into or misuse our system and it can be a physical, system or remote intrusion. Intruders are a person who does intrusion, may be from outside the network or legitimate users of the network (internal intruder). Intrusion detection system (IDS) is an art of detecting unwanted traffic on a network or a device. It can be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable use policies. The first IDS had implemented in early 1980's in US Air Force and Navy [1]. Intrusion prevention as using cryptography techniques is not always practical that is why intrusion detection becomes an important second line of defense. Generally the intrusion detection techniques used for wired networks may no longer be effective and sufficient when adapted directly to a wireless ad-hoc network, thus existing methods of intrusion detection have to be modified and new methods have to be defined in order to work effectively and efficiency in this new network architecture [2]. The paper has presented the general concept of IDS with regarding to their types, techniques and wireless ad hoc networks (MANETs) [3].

The paper is organized in seven sections followed by conclusion, recommendation, acknowledgement and references. Section II describes about types of intrusion detection system in detail. Section III gives a detailed explanation about responses of intrusion detection system. Section IV and V talks about intrusion detection system techniques and functional blocks respectively. And, section VI, VII talks about architecture of IDS and IDS in MANET respectively [4-6].

Literature Review

Intrusion detection system types

Intrusion detection systems consists of two main types, Network based (NIDS) and Host based (HIDS) intrusion detection systems [7].

Network based Intrusion Detection System (NIDS): It is looks for attack signatures in network traffic via a promiscuous interface. It can only see the packets that carried on the network segment its attached to. NIDS cannot scan protocols or content of network traffic if encrypted. Besides, it is analyses network packets at all layers of OSI (Open System Interconnection) and in many vendors NIDS well known as "Wireless Intrusion Prevention System" (WIPS) [8].

Host based Intrusion Detection System (HIDS): It is a software application and operates based on operating system audit trails, logs and process trees. It only scans the independent hosts or devices on the network and will not scan the entire network. A HIDS monitors the packets from the tool/device and will alert the administrator if malicious activity has detected. If any modification has done, an alert has sent to the administrator [3]. Besides, it has a platform specific, large overhead OS and higher management (deployment costs), and it can operate in encrypted environments. As a remark, the two types of intrusion detection systems differ significantly from each other, but complement one another well. The best IDS tools combine both approaches under one management console. In this way, the user gets comprehensive coverage, making sure to guard against as many threats as possible [9,10].

Intrusion detection system responses: Intrusion detection systems has classified into two in terms of their response. They are passive and reactive system

Passive IDS system: In this system, the IDS detect a potential security breach, logs the information and signals an alert.

Reactive IDS System: In this system, the IDS respond to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source [11,12].

Intrusion detection system techniques

There are two basic IDS techniques, which used to detect intruders: misuse and anomaly detection systems respectively.

Misuse detection system (Signature detection or pattern detection): It is monitor network traffic and analyses this traffic against specific predefined attacks. Almost all IDSs are signature based, also known as knowledge based. It has programmed to interpret a certain series of packets, or a certain piece of data contained in those packets, as an attack. Most signature analysis systems are working based of simple pattern matching algorithms. In most cases, the IDS simply look for a sub string within a stream of data carried by network packets. As drawbacks, they are unable to detect novel attacks, suffer from false alarms and have to program again for every new pattern to detect. In addition, this detection technique has used a few approaches. For instance, ID Expert System, Keystroke Monitoring, model based ID, State Transition Analysis and Pattern Monitoring. As a remark, most anti-virus software works based on a signature based IDS (a database of signature) **(Figure 1)**.

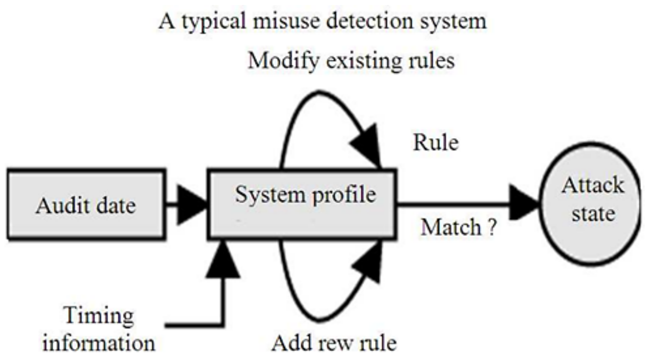

Figure 1 **A typical misuse detection system.**

Anomaly detection system (Behavior detection): It is a model of the normal usage of the network as a noise characterization. Anything distinct from the noise has assumed as an intrusion activity. Behaviour-based intrusion detection techniques assume that an intrusion can detect by observing a deviation from normal or expected behaviour of the system or the users. As pros, it has an ability to recognize novel attacks. As drawback, they would generate many false alarms and hence compromise the effectiveness of the IDS. In addition, this detection technique has used a few approaches. For instance, statistical approaches, predictive pattern approaches and neural networks **(Figure 2)**.

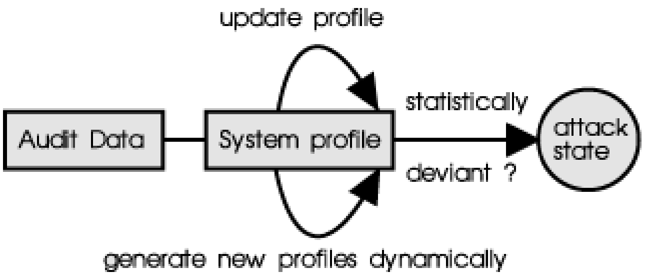

Figure 2 **A typical anomaly detection system.**

Intrusion detection system functional blocks

The functional blocks of IDS have classified into four. These are sensor, monitor, resolver and controller

Sensor: It is a system specific data gathering component and it can track network traffic, log files and system behavior **(Figure 3).**

Monitor: It is a correlates event against behavior-model, supervise components, get events from sensor and produce alerts **(Figure 4)**.

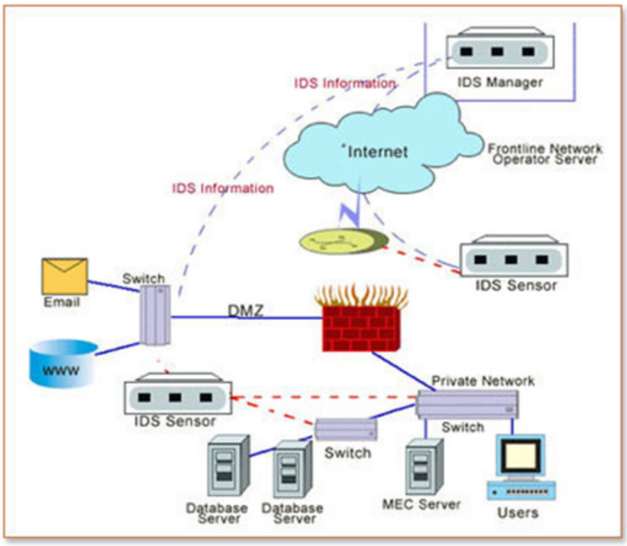

Figure 3 IDS model with sensors.

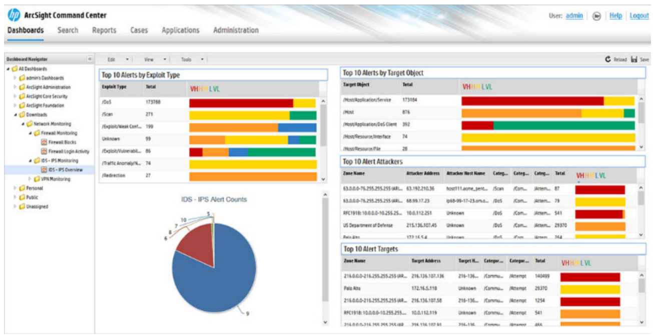

Figure 4 IDS monitoring sample from arch sight Hp.

Resolver: It can determine response against alerts (use for reactive IDS). IDS is working with the collaboration of Identity resolution to resolve the users' identification **(Figure 5)**

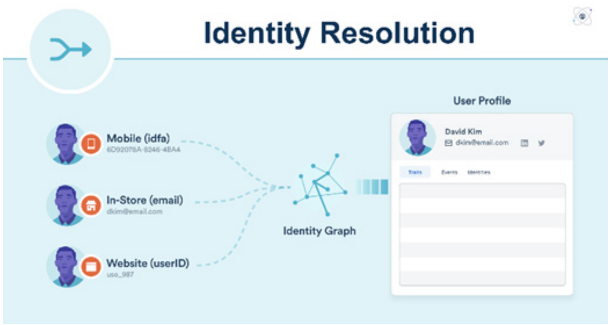

Figure 5 IDS on identity resolution.

Controller: A system operates a coordination and administration of IDS. As shown in IDS controlling model can be applied on virtual machine integrated system to manage the VM activities **(Figure 6)**.

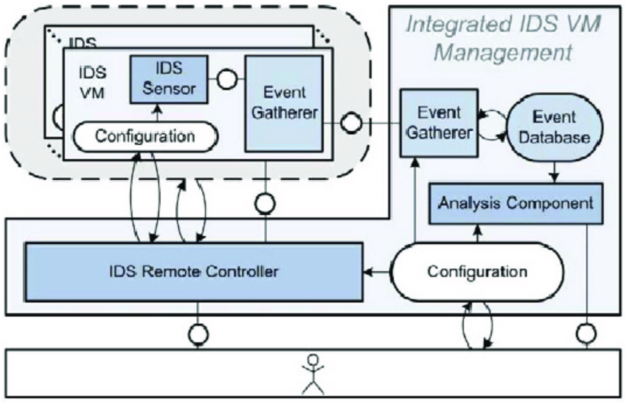

Figure 6 IDS controlling model on VM integrated system.

Intrusion detection system architecture

The architectures of IDS have broadly classified into four; monolithic, hierarchic, agent-based and distributed architectures respectively.

Monolithic IDS architecture: It is a single application contains sensor, monitor, resolver and controller. It is the simplest architecture, unable to detect attack made by distributed normal events **(Figure 7)**.

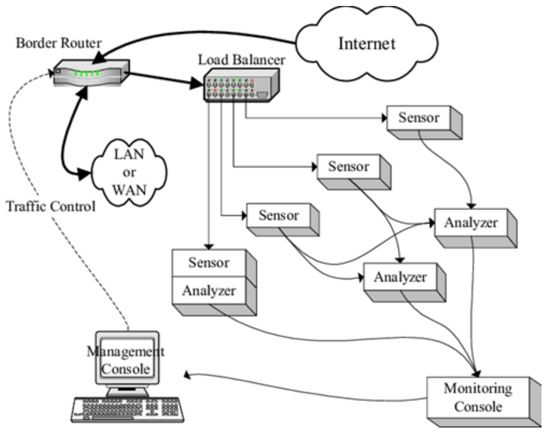

Figure 7 Monolithic IDS model.

Hierarchic IDS architecture: It is a centralized controller correlates information from different monitors and resolver take decision. A resolver and controller exist at root of hierarchy, monitors exist at sub-system (logical group) level and finally sensors have found where at node-level **(Figure 8)**.

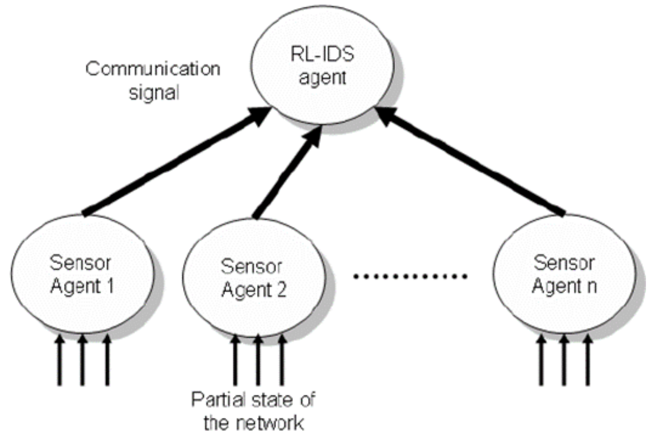

Figure 8 Hierarchic IDS model.

Hierarchic IDS architecture: It is a multi-hierarchy of monitors. It has a distributed sensors, monitors, resolver and controller. Besides, recently it is very widely used in various IDS **(Figure 9)**.

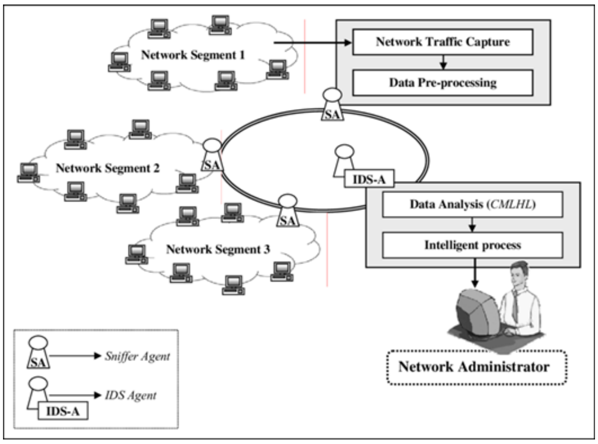

Figure 9 Agent-based IDS architecture.

Distributed IDS architecture: It allows us to improve the IDS efficiency with regard to several aspects. First, a distributed system allows the separation of concerns among a well-defined set of entities, each suited to deal with a particular aspect of the problem. This on one side simplifies the task of each involved entity, and on the other side allows a deeper specialization of each module, which can thus be modified without necessarily affecting the performance of the overall system **(Figure 10)**.

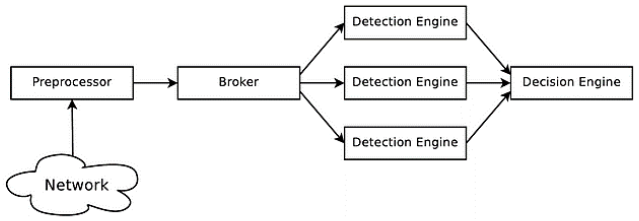

Figure 10 Distributed IDS architecture.

Intrusion detection system in wireless ad hoc network (MANET)

As I perceived, most Intrusion Detection System in Wireless Ad hoc Networks deals to detect the misbehaving nodes (selfish nodes) or to discovery a secure route rather than detect the packet related attacking.

In MANET, anomaly-detection-based-scheme more likely to be more applicable because of its collaborative and distributed nature. Generally, many authors have proposed a various IDS approaches for MANETs. From those I have listed a few approaches as shown as below [13].

The authors proposed two IDS techniques for MANET to add on the top of the standard routing protocol DSR (Dynamic Source Routing) [14]. Those techniques are Watchdog and Path rater respectively. The authors of have presented IDS approach called CONFIDANT (Cooperation Of Nodes, Fairness In Dynamic Ad-hoc Networks) to overcome the drawbacks of the Watchdog and Path rater. In the first sensor-based approach had developed to detect intrusion in MANETs. A non-overlapping Zone-Based Intrusion Detection System (ZBIDS) approach was proposed [15]. The researchers of had developed a neural network approach for anomaly intrusion detection in ad hoc network using mobile agents. In the researchers elaborated a dynamic hybrid approach based on the artificial bee colony (ABC) and negative selection (NS) algorithms, named Bee ID, for intrusion detection in AOOV-based MANETs. The approach designed of three phases: training, detection, and updating respectively [16,17].

Conclusion

In summary, IDS is not a “Silver Bullet” that means it doesn't fully guarantee security by itself due to its cannot tell us who and how and what the intentions of the attackers. However, when used with security policy, vulnerability assessments, data encryption, user authentication, access control and firewalls, they are greatly enhancing network safety. Even though research in intrusion detection started earlier in the wired world, its application to wireless ad hoc networks is a rather recent development. Intrinsically, wireless ad hoc networks are resource constrained, and this makes several of the schemes proposed in the wired world inadequate. The solutions, which require analysis of large trace data, attack signatures used by misuse detection techniques, or require centralized analysis engines are not suitable. However, the scheme that are collaborative and distributed (e.g. anomaly-detection-based schemes).

References

1 Harale DN, Meshram DB (2016) Data mining techniques for network intrusion detection and prevention systems. Int J Innov Res Comput Sci Tech 7: 2347-5552.

2 Şen S, Clark JA (2014) Intrusion Detection in Mobile Ad Hoc Networks. In Guide to Wireless Ad Hoc Networks 8: 427-454.

3 Soniya SS, Vigila SM (2016) Intrusion Detection System Classification and Techniques. International Conference on Circuit, Power and Computing Technologies 1: 1-7.

4 Marti S, Giuli TJ, Lai K, Baker M (2000) Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks. International Conference on Mobile Computing and Networking 5: 255-265.

5 Buchegger S (2002) Performance Analysis of the Confidant Protocol: Cooperation of Nodes-Fairness in Distributed Ad-Hoc Networks.

6 Kachirski O, Guha R (2003) Effective Intrusion Detection using Multiple Sensors in Wireless Ad Hoc Networks. International Conference on System Sciences 8: 120-125.

7 Sun B, Wu K, Pooch UW (2006) Zone-Based Intrusion Detection for Mobile Ad Hoc Networks. In Semantic Scholar 2: 297-324.

8 Sahu S, Shandilya SK (2020) A comprehensive survey on intrusion detection in manet. Int J Inf Technol Manag 2: 305-310.

9 Barani F, Abadi M (2012) Intrusion Detection in Aodv-Based Manets using Artificial Bee Colony and Negative Selection Algorithms Int J Inf Secur 3: 1-4.

10 Pattnaik O, Pattanayak BK (2010) Security in Vehicular Ad Hoc Network based on Intrusion Detection System. Am J Appl Sci 14: 337.346

11 Xie Y, Wu Y, Feng D, Long D (2019) Provenance-based gaussian distribution for detecting intrusion behavior variants using high efficient and real time memory databases. Transactions on Dependable and Secure Computing 9: 45-49.

12 Jurgen (2014) Red Socks Malware Threat Detector with Hp Archsight Siem.

13 Segment (2021) Personas Identity Resolution Overview.

14 Modi C, Patel D, Borisaniya B, Patel H, Patel A, et al. (2013) survey of intrusion detection techniques in cloud. J Netw Comput Appl 36: 42-57.

15 Fink GA, Chappell BL, Turner TG, O'Donoghue KF (2002) A metrics-based approach to intrusion detection system evaluation for distributed real-time systems. Int J Parallel Distr Pro Symp 8: 118-120.

16 Servin A, Kudenko D (2005) Multi-agent reinforcement learning for intrusion detection. In adaptive agents and multi-agent systems adaptation and multi-agent learning. 21: 211-223.

17 Dibaei M, Zheng X, Jiang K, Abbas R, Liu S, et al. (2020) Attacks and defences on intelligent connected vehicles a survey digital communications and networks. 6: 399-421.