International Journal of Computer Science and Engineering Communications
Volume.6, Issue.1 (2018): Page.1830-1837
www.ijcsec.com

Intrusion Detection System for Wireless Network based on Classifier Ensemble

D.Karthikeyan[1], K.P.Gowshick Raja[2], V.Menaga[3]

Assistant Professor[1], PG Scholar, Assistant Professor[2]

[1,2]Kongunadu College of Engineering and Technology, Trichy, India.

[1]duraikkeyan@gmail.com, [2]gowshick1994@gmail.com

Abstract- *An intrusion detection system is used to detect several types of malevolent actions that can compromise the security and trust of a computer system. An IDS 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 intrusion detection system detects network attacks against vulnerable services, data drove attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files and malware. It operates either at the host level or at the network level using either misuse or signature-based detection or anomaly detection. Normally, attacks that cannot be detected by network-based intrusion detection system can be detected by a host-based intrusion detection system and vice versa. In each level, the attacks can be detected by intrusion detection technique namely, misuse detection or anomaly detection. Misuse detection can detect only known attacks with high detection accuracy whereas anomaly detection can detect both known and unknown attacks with the high false positive rate. To Resolve the shortcomings of these individual intrusion detection systems; this paper proposes a novel data mining based hybrid intrusion detection system.*

Keywords: *Intrusion Detection System; Anomaly Detection; Misuse Detection; Data mining; hybrid intrusion detection system.*

Citation: D.Karthikeyan, K.P.Gowshick Raja, and V.Menaga. **"**Intrusion Detection System for Wireless Network based on Classifier Ensemble." *International Journal of Computer Science and Engineering Communications* 6.1 (2018): 1830-1837.

1.INTRODUCTION

This paper boon the results of a literature review of machine learning (ML) and data mining (DM) procedures for cyber security applications. The ML/DM methods are described, as well as some applications of each method to cyber intrusion detection difficulties. The complexity of different ML/DM algorithms is discussed, and the paper provides a set of comparison criteria for ML/DM methods. Recent days we communicate on networks to receive emails, banking, stock price, news and online shopping. The unnecessary use of the communication networks leads to intimidation. Due to that, it raises the need for the secure and safe system.

Because of the dependence on the computer technology, we have to radically improve computer network security, so that data integrity, confidentiality, and availability do not hinder. Many papers describing these methods have been published, including several reviews. In contrast to previous reviews, the focus of our paper is on publications that meet certain criteria. Malicious users or hackers use the organization's internal systems to collect information's and cause vulnerabilities like Software bugs, Lapse in administration, leaving systems to default configuration [8]. As the internet emerging into the society, new stuff like viruses and worms are imported.

Hence, security is needed for the users to secure their system from the intruders. Firewall technique is one of the popular protection techniques and it is used to protect the private network from the public network. In addition, societies use IDPSs for other determinations, such as identifying difficulties with security policies, recording surviving threats and daunting individuals from impious security policies. IDPSs have become a necessary addition to the security infrastructure of nearly every organization. IDPS typically record info related to experimental events, notify security supervisors of significant observed events, and produce reports. Many IDPSs can also respond to a detected threat by attempting to prevent it from succeeding. An intrusion is defined as any kind of action that compromises the integrity, confidentiality or Availability. Although it plays a very significant role to define and protect in security architecture, IDS is still immature and not considered as a complete defence, IDS identify or monitor any kind of intrusion and notify immediately in the form of alert so that resources never get compromised. An IDS is deployed to cover unauthorized access to resources or data. It can be hardware and/or software. IDS can be used to protect a single host or a whole computer network. IDS provides a user-friendly interface to non-expert staff for managing the systems easily. The Basic Components of intrusion detection system (IDS).

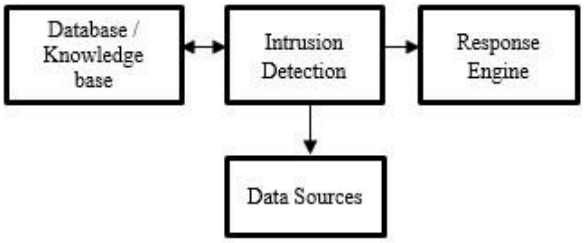

Fig.1: Components of IDS.

Data Source: Data Source is responsible for collecting and providing the audit data that will be used by next component to make decisions.
Intrusion Detector: The intrusion detector is the core component which analyzes the audit patterns to detect attacks.
Database or knowledge base: This is used to characterize the normal and anomalous behaviour. It is the knowledge base for attacks, configuration information about the current state of the system and audit information describing the events that are occurring in the system.
Response Engine: The response engine controls the reaction mechanism and regulates how to respond. The system may raise an alarm and report to the administrator.

2. INTRUSION DETECTION SYSTEM

Intrusion is any kind of prohibited activity on a computer network. An IDS is a processor device that monitors actions occurring on a network and analyzing it to identify any kind of activity that violate computer security policies. The IDS device can be hardware, software or a combination of both that monitors the computer network against any prohibited access. The main

purpose of the IDS is to catch the intruder before a real and serious damage to a computer network. To protect from the attack and malicious activity IDS provides following features:

- Monitoring and analyzing network user and computer system activity
- Auditing computer system policy configurations and vulnerabilities
- Accessing integrity of critical data server and file system
- Statistical analysis of pattern matching to the known attacks
- Unauthorized activity analysis
- Operating system auditing
- Record information on abnormal events
- Alert administrators about malicious activity
- Producing reports

Intrusion is any kind of prohibited activity on a computer network. An IDS is a processor device that monitors actions occurring on a network and analyzing it to identify any kind of activity that violate computer security policies. The IDS device can be hardware, software or a combination of both that monitors the computer network against any prohibited access. The main purpose of the IDS is to catch the intruder before a real and serious damage to a computer network. Intrusion Detection Technique can be classified into following categories.

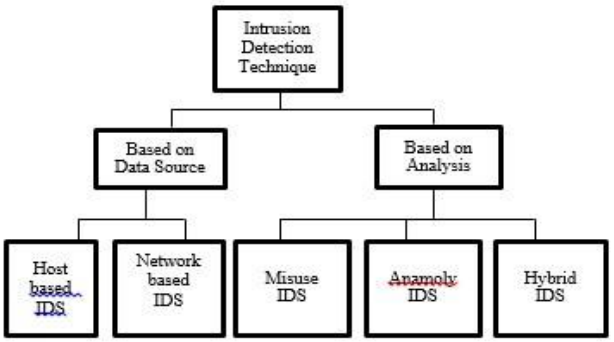

Fig.2: Classification of IDS.

Host-Based Intrusion Detection System

A host-based intrusion detection system is a system that monitors malicious activities. It monitors application logs, file system modification configuration changes in the host.

Network-Based Intrusion Detection System

A network-based intrusion detection system is used to monitor and analyze network traffic to protect a system from network-based threats.

Misuse Intrusion Detection System

This detection technique uses specifically known patterns to detect malicious code. These specific patterns are called as signatures. if current activity matches with any of known signatures an alarm is triggered.

Characteristics	Limitations
Identifies intrusion by matching captured patterns with the preconfigured knowledge base	Cannot detect new or variant of known attacks
High detection accuracy for previously known attacks	High false alarm rate for unknown attacks

2.1 Anomaly Intrusion Detection System

These techniques are designed to detect abnormal behaviour in the system. The normal usage pattern is baselined and alerts are generated when usage deviates from the normal behaviour.

The anomaly is indicated as an outlier, peculiarities or exceptions are the data pattern which performs abnormally. Anomaly detection technique is designed to uncover the patterns that are far from the normal and others are flagged as an intrusion. Anomaly detections are categorized into static and dynamic detectors. Static anomaly detector is assumed as a portion of the monitored system which remains constant. The static portion is possessed into two parts, i.e. system code and system data. Static portions of the system can be represented as a binary bit. If any divergence from its original form occurs when the error has been indicated or the burglar has reshaped the portion of the system. In dynamic detector, the definition of the system behaviour is included. The system behaviour is defined as an order of different event. For example, audit records produced by the operating system are used by IDS to define the events of interest. In this case, the behaviour can be observed only when audit records are created by OS and the events occur in strict sequences. If the uncertain behaviour is considered as anomalous, then the system administrators may be alerted by false alarms.

.Characteristics	Limitations
Use Statistical test on collected behaviour to identify intrusion	More time is required to identify attacks.
Can lower the false alarm rate for unknown attacks.	Detection accuracy is based on the amount of collected behaviour or features.

2.2 Hybrid Intrusion Detection System

Hybrid Intrusion Detection System Consists following six components i. Data Source. ii. Analyser. iii. Anomaly Detector iv. Signature Detector v. Signature Database vi.Counter-measure module

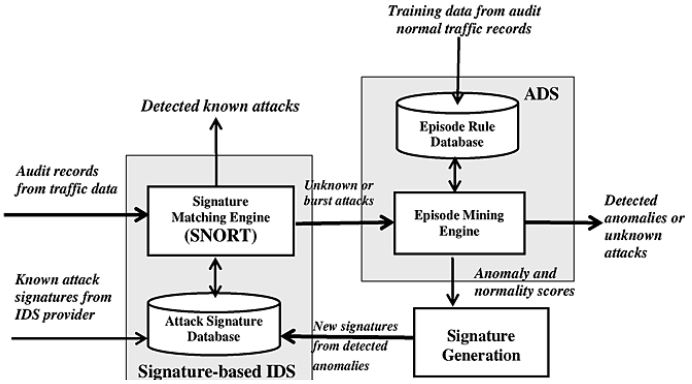

Fig.3: Hybrid IDS.

Data Source: In this module have multiple sensors. Sensors are placed either on the individual host or in particular network sector. The sensors need to be placed in locations where they will be able to capture all of the packets entering and leaving a host or network sector.
Anomaly detector: Its finds any anomaly then send a suitable message to the Signature Generator.
Signature generator: Its creates a signature and create a new entry in the Signature database.
Signature database: It's stored in the created signature.

3. FUNCTIONS OF IDS

The IDS consist of four key functions namely, data collection, feature selection, analysis and Action,

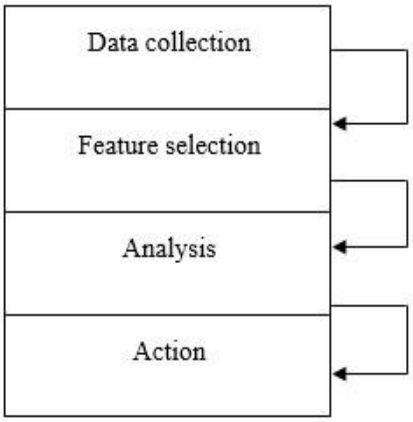

Fig.4: Functionality of IDS.

Data collection

This module passes the data as input to the IDS. The data is recorded in a file and then it is analyzed. Network-based IDS collects and alters the data packets and in host-based IDS collects details like usage of the disk and processes of the system**.**

Feature Selection

To select the particular feature large data is available on the network and they are usually evaluated for the intrusion. For example, the Internet Protocol (IP) address of the source and target system, protocol type, header length, and size could be taken as a key for the intrusion.

Analysis

The data is analyzed to find the correctness. Rule-based IDS analyze the data where the incoming traffic is checked against predefined signature or pattern [15]. Another method is anomaly based IDS where the system behaviour is studied and mathematical models are employed to it.

Action

It defines the attack and reaction of the system. It can either inform the system administrator with all the required data through email/alarm icons or it can play an active part in the system by dropping packets so that it does not enter the system or close the ports

4. IDS LIFE CYCLE

Vendors frequently release new IDS products aggressively and compete for market shares [19]. Estimating the new systems is not a relevant task and product calculation information is imperfect. Hiring and retaining the workers to administer security and intrusion detection are the challenging tasks [19]. Faster changes in IT make it problematic for the firm to implement long-term security strategy.

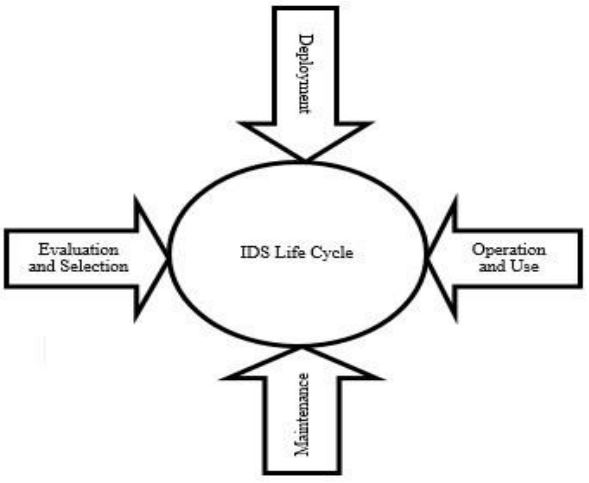

Fig.5: Function of IDS.

If an organization plans to get IDS it should examine the resources available for the systems operation and maintenance [19]. The lifecycle of a product for economic IDS is accelerated. The third-party evaluation is available and their reports are generally on the surface [19]. This process illustrates about the finding of the intruder and the amount of work required for maintaining the system in the network with traffic and the selection process defines about the identification of character, approaches, accuracy, usability, and effectiveness.

4.2 Deployment

Deployment phase includes the working of sensors to maximize protection for the critical assets by configuring the IDS to reflect security policy and installing signatures [19]. Users must develop rules for handling the alerts and to associate alerts with other systems. The Intrusion Detection Working Group of the Internet Engineering Task Force (IETF) is developing a common alert format that uses the IDS to alert from different systems and they are reported to a common display console [19].

4.3 Operation and use

The organization administers the IDS to monitor the host and to respond the report as an alert. It establishes the roles and responsibilities for analyzing and monitoring the outcomes of both manual and automatic responses [19]. Smart intruders who realize that IDS has been deployed on a network attack that they force it to provide a false report.

5. DATA MINING BASED INTRUSION DETECTION SYSTEM

Data mining is the activity of extracting relevant information from a large amount of data. Network traffic is massive and information comes from different sources, so the dataset for IDS becomes large. Hence the analysis of data is very sharded in case of a large dataset. Data mining techniques are applied to IDS because it can extract the hidden information and deals with a large dataset. Presently Data mining techniques play a vital role in IDS. By using Data mining techniques, IDS helps to detect abnormal and normal patterns. This section describes different Data mining techniques such as clustering and classification, which are used in IDS to obtain information about vulnerability by monitoring network data.

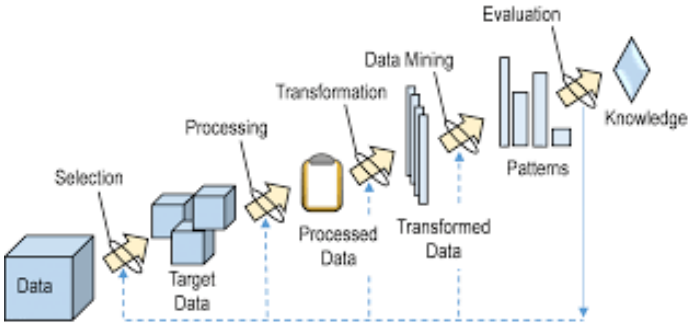

Fig.6: Data Mining

Network traffic is massive and information comes from different sources, so the dataset for IDS becomes large. Hence the analysis of data is very sharded in case of a large dataset. Data mining techniques are applied to IDS because it can extract the hidden information and deals with a large dataset. Presently Data mining techniques play a vital role in IDS. By using Data mining techniques, IDS helps to detect abnormal and normal patterns. This section describes different Data mining techniques such as clustering and classification, which are used in IDS to obtain information about vulnerability by monitoring network data.

6. CONCLUSION

The main objective of this paper is to provide an overview of the necessity and utility of intrusion detection system. This paper provides a complete and enough study about types of IDS, life cycle, various domains, types of attacks and tools. IDS are becoming essential for the day today security incorporate world and for network users**.** IPS defines the preventing measures for the security. In the lifecycle, the phases developed and the stages are illustrated. Still, there are more challenges to overcome.

REFERENCES

[1] A. Mukkamala, A. Sung, and A. Abraham, "Cybersecurity challenges: Designing efficient intrusion detection systems and antivirus tools," in *Enhancing Computer Security with Smart Technology*, V. R. Vemuri, Ed. New York, NY, USA: Auerbach, 2005, pp. 125–163.

[2] M. Bhuyan, D. Bhattacharyya, and J. Kalita, "Network anomaly detection: Methods, systems and tools," *IEEE Commun. Surv. Tuts.*, vol. 16, no. 1, pp. 303–336, First Quart. 2014.

[3] T. T. T. Nguyen and G. Armitage, "A survey of techniques for internet traffic classification using machine learning," *IEEE Commun. Surv. Tuts.*, vol. 10, no. 4, pp. 56–76, Fourth Quart. 2008.

[4] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Comput. Secur.*, vol. 28, no. 1, pp. 18–28, 2009.

[5] A. Sperotto, G. Schaffrath, R. Sadre, C. Morariu, A. Pras, and B. Stiller, "An overview of IP flow-based intrusion detection," *IEEE Commun. Surv. Tuts.*, vol. 12, no. 3, pp. 343–356, Third Quart. 2010.

[6] S. X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," *Appl. Soft Comput.*, vol. 10, no. 1, pp. 1–35, 2010.

[7] Y. Zhang, L. Wenke, and Y.-A. Huang, "Intrusion detection techniques for mobile wireless networks,"*Wireless Netw.*, vol. 9, no. 5, pp. 545 – 556, 2003.

[8] U. Fayyad, G. Piatetsky-Shapiro, and P. Smyth, "The KDD process for extracting useful knowledge from volumes of data," *Commun. ACM*, vol. 39, no. 11, pp. 27–34, 1996.

[9] C. Shearer, "The CRISP-DM model: The new blueprint for data mining," *J. Data Warehouse.*, vol. 5, pp. 13–22, 2000.

[10] A. Guazzelli, M. Zeller, W. Chen, and G. Williams, "PMML an open standard for sharing models," *R J.*, vol. 1, no. 1, pp. 60–65, May 2009.

[11] M. Hall, E. Frank, J. Holmes, B. Pfahringer, P. Reutemann, and I. Witten, "The WEKA data mining software: An update," *ACM SIGKDD Explor. Newslett.*, vol. 11, no. 1, pp. 10–18, 2009.

[12] M. Graczyk, T. Lasota, and B. Trawinski, "Comparative analysis of premises valuation models using KEEL, RapidMiner, and WEKA,"*Computational Collective Intelligence. Semantic Web, Social Networks and Multiagent Systems*. New York: Springer, 2009, pp. 800–812.