A REVIEW ON INTRUSION DETECTION AND ITS ANALYSIS

A. Pradeep Kumar¹, N. Sreema Iswarya², S. Sharmila Jeyarani³

¹Assistant Professor, Dept. of Computer Science, NPR Arts & Science College, Natham, Dindigul.
²Assistant Professor, Dept. of Computer Science, NPR Arts & Science College, Natham, Dindigul.
³Assistant Professor, Dept. of Computer Science, NPR Arts & Science College, Natham, Dindigul.
¹pradeepmahesh094@gmail.com, ²sreemamca@gmail.com, ³sharmimca85@gmail.com

ABSTRACT

Now a day wireless detection network could be a unit that is loosely used in environmental management, investigation tasks, observing military applications, health connected applications, pursuit and dominant etc. A wireless intrusion detection additionally aids among the detection of a range of attacks, so as to identify gaps and attacks in wireless network intrusion detection analysis, this paper survey the literature of this area. This paper is to classify existing up to date wireless intrusion detection system (IDS); techniques based on target wireless network, detection technique, assortment method, trust model and analysis technique. This paper summarize pros and cons of a similar or differing types of considerations and concerns for wireless intrusion detection with respect to specific attributes of target wireless networks together with wireless local area networks (WLANs), wireless personal area networks (WPANs), wireless sensor networks (WSNs), ad hoc networks, mobile telecommunication, wireless mesh networks (WMNs) and cyber physical systems (CPSs). This paper is to outline the fundamentals of intrusion detection in wireless network, describing the kinds of attacks and state the motivation for intrusion detection in wireless network.
A REVIEW ON INTRUSION DETECTION AND ITS ANALYSIS

[1] INTRODUCTION
Intrusion detection is a significant exploring topic with many prospective applications. Along with intrusion prevention, response and tolerance, intrusion detection is one tool that can defend against the real-world cyber attacks threatening critical systems. Vulnerabilities in most computer systems. And, it can be exploited by either non-authorized or authorized users. Having said that, several tools are being designed and implemented for a variety of exploitations in diverse range of security attacks. Among these tools is the intrusion detection systems (IDS) which allow us to monitor a range of computer systems: an information system, a network or a cloud computing. These IDS detect intrusions and defined as attempts to break the security objectives such as confidentiality, integrity and availability and non-repudiation. The objective of this paper is to compare the different type of intrusion detection systems and describe their mode of use. In addition, we will include the different approaches currently proposed by others on IDS system, network and cloud computing based vulnerabilities in most computer systems. And, it can be exploited by either non-authorized or authorized users.

[2] LITERATURE REVIEW
Wireless networks are not immune to the risks of destruction and decommissioning. Some of these risks are identical to those in Ad-Hoc networks, and others are specific to the sensors. Several articles [1][2][3][4][5] have presented security attacks and issues in WSNs. Intrusion detection system (IDS) defined as the second line of defense after cryptography, allows the detection and prevention of internal and external attacks. In [6], it is presented a Rule-based IDS called also Signature-based. Most of the techniques in these schemes follow three main phases: data acquisition phase, rule application phase and intrusion detection phase. In [7], it is proposed two approaches to improve the security of clusters for sensor networks using IDS. The first approach uses a model-based on authentication, and the second scheme is called Energy-Saving. IN [8] a hybrid intrusion detection system (HIDS) model has been anticipated for wireless sensor networks. The paper does not promote a solution. Rather, it is a comparative study of existing model of intrusion detection in wireless sensor networks. The paper aim is to provide a better understanding of the current research issues in this field.

The paper [9] focus on detecting intrusion or anomalous behavior of nodes in WLAN’s Using a modular technique. We explore the security vulnerabilities of 802.11, numerous intrusion detection techniques, and different network traffic metrics also called as features. Based on the study of metrics, propose a modular based intrusion detection approach. The intrusion detection is a mechanism for a WSN to detect the existence of improper, inaccurate, or anomalous moving attackers. In the paper [10], consider the issue according to heterogeneous WSN models. Furthermore, consider two sensing detection models: single-sensing detection and multiplesensing detection.

[3] SURVEY ON SECURITY ATTACKS AND INTRUSION TYPES

3.1 INTRUDER TYPE: Computer security specialists normally distinguish between internal and external network attacks. This is because intruder profiles, methods of attack and intruder objectives can vary significantly between internal and external attacks.
3.1.1 External intruder

- External intruder attacks can be made against the internal network, using the target’s own computers.
- This is often done with the active or passive collusion of the members of the target’s own staff. However, if the ultimate initiator of the attacks is someone holding no legitimate privileges on the network, then it is considered an external attack. Attacks where the intruder has no privileges on the target network, and either gains access from outside the network perimeter or by evading or undermining the target’s physical and/or network security measures to achieve some degree of access to the target’s internal network.

3.1.2 Internal intruder

- Attacks where the intruder has legitimate privileges on the target network.
- Access is obtained using existing privileges, privileges the intruder has extended without permission, or privileges stolen from other users. To gain access to data and resources to which the intruder is not authorized.
- Internal attacks are typically far more common than external ones.

3.2 INTRUSION TYPE

Several kinds of IDS technologies exist because of the variance of network configurations. Mainly, there are 3 necessary distinct families of IDS: the categories of IDPS technologies are differentiated primarily by the types of events that they monitor and therefore the ways that during which they're deployed.

3.2.1 Attempted break-in

- A Firewall has the task to examine data traffic across borders between networks, and to reject those packets, which do not have a permission for transmission.
- Beside attempts to access directly a computer in the protected network, there are also attacks against the Firewall itself, or attempts to outwit a Firewall with falsified data packets. Such break-in attempts are recognized, repelled and logged by the Intrusion Detection system (IDS).
- Thereby it can be selected between logging within the device, email notification, SNMP traps or SYSLOG alarms. IDS checks the data traffic for certain properties and detects in this way also new attacks proceeding with conspicuous patterns.

3.2.2 Masquerade

- A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification.
- If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack.

3.2.3 Leakage

- DoS Attack designed to cause an interruption or suspension of services of a specific host/server by flooding it with large quantities of useless traffic or external communication requests. When the DoS attack succeeds the server is not able to answer even to legitimate requests any more - this can be observed in numbers of ways: slow response of the server, slow network performance, unavailability of software or web page, inability to access data, website or other
resources. ➢ Distributed Denial of Service Attack (DDoS) occurs where multiple compromised or infected systems (botnet) flood a particular host with traffic simultaneously.

3.2.4 Phishing attack
➢ This type of attack use social engineering techniques to steal confidential information - the most common purpose of such attack targets victim's banking account details and credentials. ➢ Phishing attacks tend to use schemes involving spoofed emails send to users that lead them to malware infected websites designed to appear as real on-line banking websites.
➢ Emails received by users in most cases will look authentic sent from sources known to the user (very often with appropriate company logo and localised information) - those emails will contain a direct request to verify some account information, credentials or credit card numbers by following the provided link and confirming the information online.
➢ The request will be accompanied by a threat that the account may become disabled or suspended if the mentioned details are not being verified by the user.

3.3 DETECTION METHODOLOGIES
The Attempt The d Information Leak rule deals with signatures from potent detection method defines the characteristics of analyzer. It is categorized on the basis of information being used by IDS.

3.3.1 Anomaly based detection
➢ The anomaly based detection is based on defining the network behavior.
➢ The network behavior is in accordance with the predefined behavior, then it is accepted or else it triggers the event in the anomaly detection. ➢ The accepted network behavior is prepared or learned by the specifications of the network administrators.

3.3.2 Misuse based detection
➢ Misused based detection involves searching network traffic for a series of malicious bytes or packet sequences.
➢ The main advantage of this technique is that signatures are very easy to develop and understand if we know what network behavior we are trying to identify.
➢ For instance, we might use a signature that looks for particular strings within exploit particular buffer-overflow vulnerability.

3.3.3 Specification based detection ➢ Specification-based techniques have been proposed as a promising alternative that combine the strengths of misuse and anomaly detection.

3.4 ANALYSIS TECHNIQUE

3.4.1 Pattern matching analysis techniques
➢ The pattern Matching is a problem to find the first occurrence of given pattern in a stream of given text but the match should be exact which is known as Exact Pattern Matching.
After the dynamic organization and analysis of rules and data package processing by package capture and analysis module and preprocessor are finished, the detection engine is called to carry out the real-time matching of data packages and rules.

### 3.4.2 Data mining analysis techniques

**Feature selection data analysis:**

The main idea in feature selection is to remove features with little or no predictive information from the original set of features of the audit data to form a subset of appropriate features [24].

**Classification analysis:**

The goal of classification is to assign objects (intrusions) to classes based on the values of the object’s features. Classification algorithms can be used for both misuse and anomaly detections [16].

### 3.4.2 Combined analysis techniques

- This technique proposes combining two or more algorithms for analyze intrusion.

## 4 CONCLUSION

The paper analyzes the intrusion detection problem by describing intrusion detection probability with respect to the intrusion distance and the network parameters (i.e., node density, sensing range, and transmission range) and then prevents the problem. The analytical model for intrusion detection allows us to analytically formulate intrusion detection possibility within a certain intrusion distance under various application scenarios. Once the intruders are found than the technique used to stop intruders over the network. Our goal was to present the existing security mechanisms for Wireless Networks, specifically focusing on intrusion detection systems (IDS), and consider existing approaches to provide a fairly comprehensive and effective model.

## REFERENCES


