A Survey on Intrusion Detection System for Wireless Network

Ajita Mishra
PG Scholar, CSE
NIIST Bhopal, India

Ashish Kumar Srivastava
Associate Professor, CSE
NIIST Bhopal, India

ABSTRACT
Security of Wireless network becomes associate in nursing woeful necessary issues with the speedy development of wireless network that is in danger for an honest vary of attacks due to preparation among the hostile atmosphere and having limited resources. Now a day wireless detection network is a unit which is loosely utilized in environmental management, police investigation tasks, monitoring military applications, health connected applications, pursuit and dominant etc. A wireless intrusion detection also aids among the detection of a variety of attacks. Wireless intrusion detection system cannot exclusively notice scoundrel WAPS, establish non-encrypted 802.11 traffic, and facilitate isolate associate attacker's physical location. We have a tendency to define the basics of intrusion detection in wireless network, describing the varieties of attacks and state the motivation for intrusion detection in wireless network. This paper, firstly indicates the developing history of WIDS, and then summarizes the related work on Wireless Intrusion Prevention System through RF jamming technique.

Keywords
WNS, IDS, attacks, SID, WIPS .

INTRODUCTION
Wireless network could be a speedily growing space as new technologies square measure rising. New applications square measure being developed, like traffic, setting observance, healthcare, military applications, home automation. A wireless network is susceptible to numerous attacks like jam, battery avoidance, routing cycle, Sybil, cloning. To protect Wireless network against completely different varieties of vulnerabilities, preventive mechanisms like cryptography and authentication will be applied to stop some sorts of attacks. However, some attacks like wormholes, sinkhole, couldn't be detected exploitation this sort of preventive mechanisms. Additionally, these mechanisms square measures solely effective to stop from outside attacks and didn't guarantee the interference of intruders from within the network. Due to that, it's necessary to use some mechanisms of intrusion detection. Associate degree Intrusion detection system is outlined in [6] as A system that dynamically monitors the events going down on a system's associate degree decides whether or not these events square measure symptoms of an attack or represent a legitimate user of the system. However, there square measure several challenges posed against the appliance of the IDS for Wireless network. These challenges square measure thanks to the dearth of resources like, energy, process and storage. Wireless networks square measure assortment of nodes wherever every node has its own detector, processor, transmitter and receiver and such sensors sometimes square measure low price devices that perform a selected variety of sensing tasks. Being of low price such sensors square measure deployed densely throughout the world to watch specific event.

The Wireless network largely operates publicly and uncontrolled space, thence the safety could be a major challenge in detector applications. Today Intrusion used as a security resolution in a much wired network within the type of software/ hardware by that one will sight unwanted services happening the system by the approach of enhanced/abnormal network activity and determine suspicious patterns that will indicate whether or not the network/system is beneath attack? For Wireless network many schemes were projected however they need restricted options like solely a concern for attacks on a specific layer.

A wireless IDS may aid within the detection of a variety of attacks. Not solely will a wireless IDS Sight knave WAPS, determine non-encrypted 802.11 traffic, associate degree facilitate isolate an attacker's physical location, as mentioned earlier - a wireless IDS will cite several of the quality (and not-so standard) wireless attacks and probes still. In an attempt to spot potential WAP targets, hackers ordinarily use scanning computer code. Hackers or curious people can use tools like Netstumbler or Kismat to plan a given area's WAPs. Wireless network refers to a system that consists of variety of inexpensive, resource restricted detector nodes to sense vital information associated with setting and to transmit it to sink node that gives entranceway practicality to a different network, or associate degree access purpose for human interface.

1. LITERATURE REVIEW

1.1 Types of Wireless Networks

- **Adhoc Network: -**Wireless ad hoc network [11] is a type of wireless network and decentralized in nature. It is a set of wireless mobile nodes forming a momentary network without any centralized access point. Decentralized nature of wireless ad hoc networks makes them suitable for multiple applications, where central nodes can't be relied on and may develop the scalability of networks as compared to wireless networks. Ad hoc network is also referred as IEEE 802.11 wireless networks. Ad-hoc network suffer from the lot of issues and congestion and security are the major issues of ongoing research, which leads to severe degradation of network throughput and increases the routing overheads. Mobile ad hoc networks (MANET) are an application of Ad - hoc networks.
- **Sensor Network: -**A wireless sensor network (WSN**) [3]** consists of spatially disseminated autonomous sensors to monitor physical or environmental conditions, such as sound, temperature, pressure, etc. The further modern networks are bi-directional, also enabling control of sensor activity. Intrusion detection in Wireless Sensor Network is of practical concern in many applications such as detecting an

intruder in a battleground. Today such networks are used in many consumer and industrial applications, such as machine health monitoring, industrial process monitoring and control and so on. But, wireless sensor networks are now used in many healthcare applications, house automation, and traffic control resident application areas, including environment and locale monitoring.

- Area monitoring
- Environmental/Earth monitoring
- Air quality monitoring
- Air pollution monitoring
- Forest fire detection
- Agriculture
- Passive localization and tracking

1.2 Types of Wireless network for Intrusion Detection

We introduce the basics of the intrusion detection in Wireless network, which has the definition of the intrusion, kinds of intrusions/attacks in Wireless network, the motivation and want for intrusion detection and therefore the challenges of developing an honest candidate intrusion detection theme for Wireless network. The definition of the Intrusion/Attack: [4] defines the intrusion as any set of actions that try to compromise the most parts of the safety system: the integrity, confidentiality or handiness of a resource. Within the same work, the interloper so was outlined as a personal or a cluster of people who take the action within the intrusion. [5] Adds the statement of success or failures of those actions thus it additionally refers to the attacks against the PC system. Within the theme of wireless detector network, the conception stills constant since the intrusion additionally target any of the parts mentioned on top of. The character of Wireless network and its special characteristics just like the harsh readiest, energy constraints and therefore the media of communication makes them terribly liable to the intrusions quite different networks.

Types of attacks in Wireless network:

- **Probing & Network Discovery:-**

Before an attacker is capable to attempt any kind of wireless harm one of the main activities would be for him to recognize the various wireless targets in range. This type of attack is described amongst the first activities engaged by any attacker. There are two types of probing- active and passive probing. Active probing involves the attacker actively sending probe needs with no SSID configured in order to request a probe reaction with SSID information and other information from any access points in range. Active probing cannot detect for access points that are covered or out of range of the attacker's wireless transmission range. When an attacker engages in passive probing, he/she is listening on all channels for all wireless packets receive and send without sending an only packet, thus the detection capacity is not limited by his transmission power. A superior example of a tool that uses active probing is NetStumbler and for passive probing, Wirehsark tool is used .

- **Surveillance:-**

Once the wireless aim has been recognized, the attacker can continue to gather information about the network using tools like airodump or kismet. The gathered data can be saved in pcap format for following offline analysis. If the traffic stream is not encrypted, directly the attacker could look at the traffic stream and recognize the network parameters (e.g. IP address range, gateway, MAC address, etc.) from the traffic. If the traffic stream is WEP encrypted, there are WEP crackers which are available for him. Airodump is used to collect all the encrypted packets and aircrack is then used to attempt to crack the WEP key given enough WEP that are gathered.

- **DOS (Denial of Services) attack:-**

Denial Of Service (DOS) attack make an attempt to prevent legitimate users from accessing some services, which they are eligible for. For instance, an unauthorized user might send too many login requests to a server using random user ids one after the other in quick succession, so as to flood the network and deny other legitimate users from using the network facilities.

- **Impersonation:-**

Another category of attacks that can be simply executed in a wireless network is the impersonation attack. In such an attack, the attacker adjusts his MAC address to a MAC address which he found prior during the surveillance state. This MAC address would most positively belong to an authorized client in the network. This is generally done to overcome the MAC filtering abilities of access points where only a list of authorized MAC addresses is allowed to use the wireless network. To adjust the MAC address manually in the windows, locate the registry settings for your wireless NIC and add a new string call network address with the new MAC address information to it.

Key fingerprint = AF19 FA27 2F94 998D FDB5 EE3D F8B5 06E4 A169 4E46

- **Man in the middle and Rouge AP:-**

In this type of attack, the attacker attempts to introduce himself in the middle of a communication for purposes of catching client's data and could potentially adjust them by discarding them or sending them out to the real target. In order to insert oneself in the middle of the communication, one has to achieve two tasks, first, the suitable AP allocates the client must first be brought down or made "extremely hard" so as to create a "complex to connect" scenario for the wireless client. Secondly, the attacker must set up an interchange rouge AP with the same records as the original for purposes of allowing the client to connect to it.

1.3 Intrusion Detection System

An **Intrusion detection system** (**IDS**) is hardware and/or software designed to sense superfluous attempts at accessing, manipulating, and/or disabling of computer through a network, such as the Internet. These attempts may take the form of attacks like crackers, malware and/or dissatisfied employees. IDS indirectly detect attacks within properly encrypted traffic. An intrusion detection system is used to detect several types of nasty behaviors that can give and take the security and trust of a computer system. This comprises network attacks against data determined attacks on applications, host based attacks such as unauthorized logins and access to sensitive files, privilege escalation, susceptible services, and viruses.

IDS can be classified into two **approaches**: anomaly detection and misuse detection. Misuse Detection also referred to as Signature based Intrusion Detection (SID) and Anomaly based Intrusion Detection (AID). In SID detection, each network traffic record is recognized as either normal or one of many predefined intrusion types. In contrast, anomaly detection amounts to training models for learning normal traffic behavior and then classifying, as intrusions, any network behavior that considerably deviates from the known normal network traffic patterns.

Intrusion signatures have been characterized as a string, event sequences, graphs, and intrusion scenarios (consisting of target states, event sequences, and their preconditions). FSM (finite-state-machine), colored Petri Nets, associate roles and

production rules of expert systems have been used to represent and recognize intrusion signatures. Intrusion signatures are either physically encoded or manually learned through data mining. But, signature recognition techniques have a limitation in that they cannot detect original intrusions whose signatures are unknown.

1.4 Requirements of IDS in Wireless Network

There area unit 2 key needs that any IDS should discover a considerable share of intrusions into the supervised system, whereas keeping the warning rate at a suitable level at a lower cost. It's expected that a perfect IDS is likely to support many of the subsequent needs :

- The IDS mustn't introduce a brand new weakness infrastructure. In the painter. That is, the IDS itself ought to not build a node any weaker than it already is.
- Associate in Nursing IDS ought to run ceaselessly and stay transparent to the system and users.
- The IDS ought to use as very little system resources as potential to observe and stop intrusions. IDS that need excessive communication among nodes or run advanced algorithms square measure not fascinating.
- It should be fault-tolerant with in the sense that it must be ready to pass though system crashes, hopefully recover to the previous state, and resume the operations before the crash
- Excluding sleuthing and responding to intrusions, Associate in Nursing IDS ought to conjointly resist subversion. It should monitor itself and observe if it's been compromised by Associate in Nursing offender.
- Associate in Nursing IDS ought to have a correct response. In other words, Associate in Nursing IDS mustn't solely observe but conjointly answer detected intrusions, preferably while not human intervention.
- Accuracy of the IDS is another major consider MANETs. Fewer false positives and false negatives square measure desired.

1.5 Wireless Intrusion Prevention System

Wireless Intrusion Prevention System (WIPS) is a network device that monitors the radio spectrum for the existence of un-authorized access points , and can do automatic intrusion prevention. The main purpose of a WIPS is to prevent un-authorized network access to local area networks and other information resources by wireless devices. WIPS which is an extension of WIDS not only detects wireless intrusions, but also can prevent them.

2. RESEARCH SCOPE

With the fast development of wireless network, the problems on wireless security have become more and more prominent. And the technologies of firewall and intrusion detection cannot solve these problems satisfactorily. However, wireless intrusion prevention systems which can prevent attacks for WLAN excellently have become the research hotspot. This paper, firstly indicates the developing history of WIPS, and then summarizes the related work on WIPS in academic and engineering application area respectively. Based on this work, propose a common wireless intrusion prevention framework (CWIPF), and describe some key technologies used in this framework. Finally, we proposed some research issues should be focused on in the future. Index Terms-intrusion prevention, wireless LAN, CWIPF, network security [1].

The increasing confidence upon wireless networks has put remarkable emphasis on wireless network security. Intrusion detection for wireless network has become an essential component of any helpful wireless network security system, and has recently gained attention in both research and industrial communities due to widespread use of wireless local area network (WLAN). Although some intrusion prevention systems have recently appeared in the market, their intrusion detection capabilities are limited. This paper 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. [2]

Intrusion detection in Wireless Sensor Network (WSN) is of useful attention in various applications such as detecting an intruder in a battlefield. The intrusion detection is a mechanism for a WSN to detect the existence of improper, inaccurate, or anomalous moving attackers. In this paper, consider the issue according to heterogeneous WSN models. Furthermore, consider two sensing detection models: single-sensing detection and multiple-sensing detection [3]

In this approach, wireless traffic data are clustered and use heuristic to label each instance as intrusive or normal. The heuristic used is the execution of modules for individual features in intrusion detection system. In which we search for the specific features collectively defined an activity (i.e. Pattern) followed by an attack. Then we put these results of features in a table consist list of features with respect to MAC or IP address of a node (i.e. We maintain a check list for individual node), so we can calculate the intrusive behavior of a node rather than a particular attack.

A technique adopted for the detection of features is tabular in which we create a list of features vertically and on the basis of detecting features the alarm can generate for the respective attacks. It is a reverse approach than the usual Intrusion Detection Systems in which they detect specific attacks. In the earlier, IDS two checks were needed for the same feature in two different attacks but in proposed Modular Approach there is only a single check required to detect same feature in both attacks. The following steps are followed to implement modular approach for intrusion detection in wireless environment

- Generate algorithm to implement modular approach.
- Collecting knowledge of signature of attacks used in wireless networks.
- Capture database of wireless network.
- Implement approach in system compatible platform.

3. FUTURE WORK

In this research wireless intrusion detection and prevention algorithm has been developed which proves to be effective in detection and prevention of intrusions. The intrusion detections are applied in internet application and parallel computer interconnection network. The Algorithm can be extended and compare with real time work such as WEKA tools.

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 is RF jamming through salutatory-style channels i.e changing by spacing a channel. RF jamming means block the whole RF medium when intrusion is detected. But it has the obvious limitation of blocking all the traffic on the medium.

5. REFERENCES

[1] Y. Zhang, G. Chen, W. Weng, and Z. Wang, "An Overview of Wireless Intrusion Prevention Systems,"*IEEE ICCSNA* , vol. 3, no. 12, pp. 147–150, 2010.

[2] T. Badal, D. Verma, "A Modular Approach for Intrusion Detection System in Wireless Networks", *IJACNS*, vol. 1, pp. 57-61, 2011, ISSN:2250-3757.

[3] K. Suresh, A. Sarala Devi, and Jammi Ashok, "A Novel Approach Based Wireless Intrusion Detection System", *IJCSIT*, Vol. 3 (4) , 2012,4666 – 4669, ISSN:0975-9646.

[4] Heady, R., "The Architecture of a Network-level Intrusion Detection System."1st Edn., Department of Computer Science, Mexico, pp: 18, 1990.

[5] Zamboni, D., 2001. Using internal sensors for computer intrusion detection. Purdue University.

[6] Debar, H. M. Dacier and A. Wespi, 1999. Towards at taxonomy of intrusion-detection systems. Comput. Netw., 31: 805-822.

[7] S. Zhong, T. M. Khoshgoftaar and S. V. Nath, "A Clustering Approach to Wireless Network Intrusion Detection", in proceedings of the 17th IEEE International Conference on Tools with Artificial Intelligence (ICTAL'O5), PP. 54-60, 2005.

[8] V. Gupta and S. Gupta, "Experiments in Wireless Internet Security", Wireless Communications and Networking Conference, (WCNC 2002), IEEE Volume 2, pp. 860-864, 2002.

[9] Z. Li, A. Das and J. Zhou, "Theoretical basis for intrusion detection," Information Assurance Workshop, (IAW 2005), proceedings from the sixth Annual IEEE SMC, pp. 184-192, 2005.

[10] Aleksandar Lazarevic, Vipin Kumar, Jaideep Srivastava, "Intrusion Detection: A Survey", Managing Cyber Threats: Issues, Approaches and Challenges, Vol. 5, 2005, Springer Publisher.

[11] P. Brutch and C. Ko, "Challenges in intrusion detection in wireless ad-hoc networks," IEEE Proceedings of Workshop on Security and Assurance in Ad hoc Networks, 2003, pp368 - 373, Jan. 2003.

[12] Tsakountakis, G. Kambourakis, S. Gritzalis, "Towards effective Wireless Intrusion Detection in IEEE 802.11i," in: Security, Privacy and Trust in Pervasive and Ubiquitous Computing, (SECPerU 2007), Third International Workshop, pp. 37-42, 2007.

[13] N. Ye, SM. Emran, Q. Chen and S. Vilbert,"Multivariate statistical analysis of audit trails for host-based intrusion detection", Computers, IEEE Transactions on Volume 51, Issue 7, pp. 810 – 820, July2002.