Analysis for Improving Intrusion Detection System in Wireless Network

Ashu Raghav
Research Fellow
KIIT College of Engineering
Gurgaon, Haryana - 122102
Email: ashu22raghav@gmail.com

Shambhu Sharan
Research Fellow
KIIT College of Engineering
Gurgaon, Haryana - 122102
Email: reachshambhu@gmail.com

Namrata Wadhwa
M.Tech (CSE)
KIIT College of Engineering
Gurgaon, Haryana - 122102
Email: namrata.it03@gmail.com

***Abstract*—The Wireless is word that defined as "having no wires. Wireless is the term used to define in a computer network where there is no physical wired assembly between sender and receiver, but somewhat the network is subordinated with radio waves and microwaves to maintain transportations. Wireless is a term used to describe communications in which electromagnetic carry the signal over part or the entire communication path.Wireless networking utilizes specific tools such as NICs, APs and routers instead of wires for linking the network. WLAN is commonly referred to as wireless fidelity (WI-Fi). This paper focus on detecting intrusion or jarring (abnormal) behavior of nodes in WLANs using signature based Intrusion detection method. We explore the security susceptibilities of 802.11 and numerous intrusion detection methods. This paper, indicates the developing history of the Wireless Intrusion detection system (WIDS), and then sum up the connected work on Wireless Intrusion Prevention System (WIPS) through an RF jamming method.**

Keywords*—*Intrusion detection system, Signature based Intrusion Detection, Wireless Network System,Attacks, WIPS

I. Introduction

Interest in wireless network security has been rising in existing years. Though several security-defense systems have been recognized such as encryption, verification, firewall, and VPNs, maximum of the wireless systems are silent vulnerable to attacks. Unluckily, complete attack expectation in wireless networks is not accurately possible because it is exposed for wireless medium, system difficulty, configuration and management errors, misuse by authorized users, lack of federal observing and management points, vigorously changed network topologies, etc. The wireless network is a speedily developing new knowledge square measure. New requests square amount being industrialized like in traffic, setting adherence, healthcare, military applications, and home mechanization. A wireless network is vulnerable to numerous attacks like jam, battery evading, routing series, Sybil, duplicating. To guard Wireless network against different diversities of susceptibilities, preventive contrivances like cryptography and verification will be functional to break some kinds of attacks. Additionally, these mechanisms are efficiently use to guard from outside attacks and didn't promise the intrusion of interlopers from outside or within the network. Today Intrusion detection is introduced as a security determination in a much wired networks within the type of software/ hardware by that one will sight unsolicited services fashionable in the system by the method of improved/irregular network activity and control distrustful/suspicious designs that will designate whether or not the network/system is beneath outbreak? For Wireless network many schemes were predictable however they need controlled choices like apprehension for occurrences on a specific coating. A wireless IDS may aid within the discovery of a various kind of attacks. In an attempt to spot possible WAP targets, hackers normally use scanning computer code. Hackers or inquiring persons can use tools like Netstumbler or Kismat to plot a given area's WAPs. Many classes of wireless networks are used e.g an ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to subordinate with any other ad hoc network device in link range. Ad hoc network frequently refers to a mode of operation of IEEE 802.11 wireless networks. Operating in ad-hoc method permits all wireless strategies within range of each other to control and connect in point to point fashion without connecting central access points. Dispersed nature of wireless ad hoc networks makes them suitable for multiple applications, where central nodes can't be trusted on and may develop the scalability of networks as compared to wireless networks. Ad hoc network refers to a mode/form of operation of IEEE 802.11 wireless networks.

II. INTRUSION DETECTION SYSTEM (IDS)

An intrusion detection system is a trick or software application that screens network or system activities for nasty actions or policy destructions and produces reports to a management station. IDS come in varieties and method the goal of spotting doubtful traffic in different ways. There are network based and host based intrusion detection systems. Some systems may effort to stop an intrusion attempt but this is neither obligatory nor predictable of a checking system. Intrusion detection and prevention systems are mainly attentive on classifying likely incidents, logging evidence about them, and reporting efforts. In addition, organizations use IDPSes for other determinations, such as classifying problems with security rules, documenting existing extortions and daunting persons from violating security rules. IDPSes have become an essential adding to the security infrastructure of nearly every association.

Components of IDS: The typical components in an IDS solution are as follows:

- Sensor or Agent : Sensors and agents space and review activity. The term sensor is typically used for IDSs that screen networks, including network-based, wireless, and network presentation inspection tools.

- Management Server : A management server is a consolidated device that obtains info from the devices or supervisors and completes them. Some organization servers attain analysis on the event indication that the sensors or administrators provide and can classify accounts that the distinct devices or agents cannot. Identical event suggestion from frequent sensors or agents, such as detection events activated by the same IP address, is known as connotation. Management servers are available as both application and software-only products.
- Database Server : A database server is a basis for occurrence material confirmed by devices, agents, and/or organization servers. Many IDPSs provide support for file servers.
  1) Autonomous IDS: In autonomous IDS manner, each network node functions autonomously/distinctly and is answerable for detecting attacks, there is no communication between the nodes of the network. This architecture is more appropriate for the flat networks than multi-layered networks.
  2) Distributed IDS: It includes a number of the network nodes which are responsible for gathering local audit data autonomously and then collaboratively observe it in a wider range in order to carry out a global Intrusion Detection System. This architecture is appropriate for flat networks and also for multilayered networks.

III. LITERATURE REVIEW

There are common practices applied in the safety of the wireless network and attacks that affect the safety of wireless system, so experts have prearranged some of methods to introduce the fundamentals of the intrusion detection in Wireless network, the definition of the intrusion, kinds of intrusions/attacks in Wireless network, the motivation and want for intrusion detection and therefore the competitions of emerging an honest intrusion detection theme for wireless network. The definition of the Intrusion/Attack: defines the intrusion as any set of movements that try to collaboration the most parts of the safety system: the honesty, privacy or convenience of a resource. Within the same work, the intruder so was sketched as a personal or a bunch of people who take the exploit within the intrusion.

Once the wireless aim has been documented, the attacker can endure to gather information about the network using tools like air dump. If the traffic stream is not encrypted, directly the assailant could look at the traffic stream and recognize the network limitations (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. Airo dump is used to gather all the encrypted packets and air crack is then used to crack the WEP key given if sufficient WEP are collected.

- DOS (Denial of Services) attack : Denial Of Service (DOS) attack make an attempt to prevent genuine users from retrieving some services, which they are eligible for. For instance, an unauthorized user might send too many login requirements to a server using random user ids one after the other in quick sequence, so as to flood the network and deny other genuine users from using the network facilities.
- Man in the middle and Rouge AP : In this type of attack, the invader efforts to introduce himself in the middle of a communication for purposes of infectious clients data and could hypothetically adjust them by clearance them or sending them out to the real target.

In this paper, a novel framework to detect wireless network attacks based on anomaly analysis of the behavior of wireless networks and data mining techniques. The primary experiment shows that the isolation table can detect and prevent intrusions attacks effectively. But this method is not good enough to detect anomaly using IDS.

IV. PROPOSED METHODOLOGY

In our methodology, bunch the wireless traffic data and then use the empirical function to make each occurrence aggressive or standard. The heuristic function is used in the operation of components for separate features in intrusion detection system. In which we search for the specific topographies obligingly defined an activity 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, so we can calculate the disturbing behavior of a node relatively than a particular attack. A technique accepted for the detection of features is tabular in which create a list of features vertically and on the basis of detecting features the alarm can be generated for the respective attacks The following steps are followed to implement modular approach for intrusion detection in wireless environment:

- Generate algorithm to device modular approach.
- Collecting information of signature of attacks used in wireless networks.
- Implement approach in system well-matched platform.

Algorithm for Intrusion Detection and Prevention

1) Initiate.
2) Snort for 802.11 frames.
3) Save data in a file that can be recovered through the system and in the required format.
4) Open file includes data of the network.
   a) Change hexadecimal code in decimal arrangement.
   b) Purse frames and cutting MAC headers from the frames.
   c) Check 802.11 frame types.
   d) The extract feature needs to detect intrusion.
   e) Search for the predefined signature of attacks in the database.
5) Log packet content.
6) Send out an alarm if interruption found (i.e. Signature match).
7) Analysis data packet with remote from (Analysis illegal behaviors).
8) Save all the intrusion data in the event catalogue.
9) Set occupied Occurrence of monitoring channel.
10) Exit and Repeat.

V. RESULT

We have plan and implement the CWIPF with Snort-wireless. We have formed measuring experiments, based on the performance of CWIPF with Snort-Wireless. In our experiment, twenty wireless terrorizations square measures hurled against the WLAN, together with DoS, MAC spoofing, MITM, rogue AP, misconfigured AP attacks. When CWIPF is applied on 20 threats file then it detect 19 threats file which can prevent attackers from destructive wireless networks.

VI. CONCLUSION

This paper inspects the intrusion detection problematic by symbolizing intrusion detection likelihood with respect to the intrusion distance and the network limitations like sensing range, node thickness and transmission series. The analytical model for intrusion detection allows us to analytically articulate intrusion detection likelihood within an assured intrusion distance under various request situations and then authenticate our method on real network data in which a a database of 20 files is used and then positively detect the signature that are provided in our experiment.

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. 147150, 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] G.C.Tjhai, M.Papadaki, S.M.Furnell, N.L.Clarke, Investigating the problem of IDS false alarms An experimental study using Snort, internet, 253-267, 2008.

[4] James Kelly, An Examination of Pattern Matching Algorithms for Intrusion Detection Systems, Internet,1-208, August 2006 11. SIDDHARTH SAHA, Network Intrusion Detection System Using String Matching, Internet, 1-46, 2010.

[5] Craig Labovitz, G. Robert Malan, and Farnam Jahanian, Origins of Internet routing instability, in Proc. IEEE INFOCOM, 1999.

[6] Ricardo Oliveira, Beichuan Zhang, Dan Pei, Rafit Izhak-Ratzin, and Lixia Zhang, Quantifying path exploration in the Internet, in Proc. ACM SIGCOMM/USENIX IMC, 2006.

[7] W. Lu, I. Traore, Detecting New Forms of Network Intrusion Using Genetic Programming. Computational Intelligence, vol. 20, pp. 3, Blackwell Publishing, Malden, pp. 475-494, 2004.

[8] M. M. Pillai, J. H. P. Eloff, H. S. Venter, An Approach to Implement a Network Intrusion Detection System using Genetic Algorithms, Proceedings of SAICSIT, pp:221-228, 2004.

[9] A Survey of Intrusion Detection Systems Douglas J. Brown, Bill Suckow, and Tianqiu Wang.

[10] A Survey of Modern Advances in Network Intrusion Detection V. Kotov, V. Vasilyev Department of Computer Engineering