International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-2 Issue-5, November 2013

An Efficient Modular Approach of Intrusion Prevention in Wireless Sensor Networks

Varsha Nigam, Saurabh Jain

Abstract: Security of wireless sensor network becomes crucial issue in the latest research with the fast deployment of wireless sensor network.The latency between an attack detection and corrective action taken by the administrator is usually high and therefore ,at the time the administrator notices an attack and take some suitable action the damage was done by the attacker. Depandig on this requirement the need for Intrusion Prevention System which can not only detect attacks but also able to actively respond in malacious activities.Intrusion prevention is a preemptive approach in a system security which is used to identify malacious activities and respond quickly to mitigate anamolous behaviour. In this research paper we actively proposed a new modular approach in intrusion prevention by analyzing past approaches.A wireless IPS can also aid among the prevention of a variety of attacks.. 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. In this paper, we firstly indicate the developing history of WIDS, and then summarize the related work on WIPS.On these work, we propose a algorithm for wireless intrusion prevention framework.

Index Terms: WSN, IDS, Attacks, WIPS.

I. INTRODUCTION

The wireless sensor networks (WSNs) are often deployed in physically insecure environment where we can hardly prevent attackers from the physical access to the devices. Since making nodes resistant to physical tampering would make them much more expensive, we have to think that an attacker may capture the nodes and retrieve the cryptographic material via physical tampering.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 sight 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. Utilized in conjunction with a worldwide Positioning System (GPS) these scans not solely find WAPs,
however additionally log their geogr aphical coordinates. These tools became thus well-liked that they're square measure websites dedicated to mapping the world's WAP earth science. A wireless IDS will cite these and other scans, serving two to boost awareness of the threats to the wireless fidelity.

Revised Manuscript Received on 30 November 2013.
* Correspondence Author
Varsha Nigam, Research Scholar,Department of CSE,OCT,Bhopal, India.
Saurabh Jain, AP,Department of CSE,OCT,Bhopal, India.

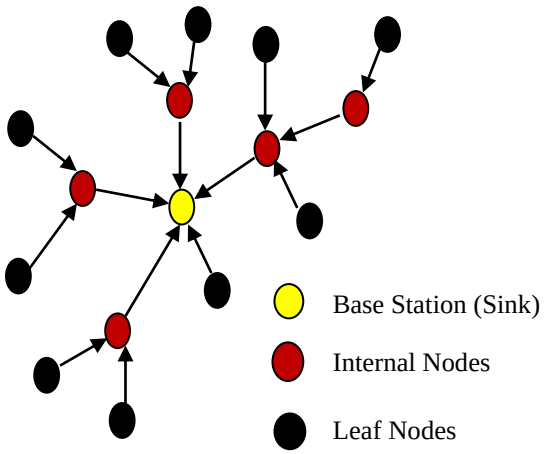

Figure 1.1 :Wireless Sensor Network

A wireless network could be a wireless network consisting of spatially distributed autonomous devices exploitation sensors to hand in glove monitor physical or environmental conditions, like motion, temperature, pressure, sound, vibration, , or pollutants, at completely different locations the event of wireless networks was originally driven by military applications like field of battle police investigation. However, wireless networks square measure currently utilized in several civilian application areas, as well as setting and surround observance, control, home automation, and health care applications.
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. 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. Thanks to limitation of computation, memory and power resource of detector nodes, advanced security mechanism can't be enforced in Wireless network. So energy-efficient security implementation is a very important demand for Wireless network. 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.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

This sort of preventive mechanisms fashioned the primary defense line for Wireless network. 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 (Silva et al., 2005). Due to that, it's necessary to use some mechanisms of intrusion detection. Intrusion Detection Systems (IDS) square measure thought of to act because the second defense line against network attacks that preventive mechanisms fail to deal with (Silva et al., 2005). Associate degree Intrusion detection system is outlined in (Debar et al., 1999) as A system that dynamically monitors the events going down on a system associate degreed decides whether or not these events square measure symptoms of an attack or represent a legitimate use 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 task. Being of low price such sensors square measure deplokyed densely throughout the world to watch specific event.

The Wireless network largely operate publicly and uncontrolled space, thence the safety could be a major challenges in detector applications. Today Intrusion used as a security resolution in a very wired network within the type of software/ hardware by that one will sight unwanted services happening the system by 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 concern to attacks on a specific layer.

1.2 Intrusion Signature

There are two types of approaches based on the detection technique in wireless network: 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 rules 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.

1.3 Wireless Intrusion Prevention System(WIPS)

A WIPS is a network device that monitors the radio spectrum for the existence of un-authorized access points , and can do automatically intrusion prevention by generating alerts accurately. 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.

1.4 Types of Wireless Intrusion Prevention System

In the following subsections we briefly describe some commercially available WIPS.

1.4.1Juniper Intrusion Prevention and Detection System

It is a network based IPS.It has three tier architecture and having three main components: Intrusion detection and prevention sensors(IDPS),central server and a graphical user interface.It uses a rule based policy management to examines the network traffic and responds to detected intrusions.

1.4.2Attack Mitigator Intrusion Prevention System

It is able to provide both content based and rate based intrusion prevention The rate based IPS blocks traffic based on network load.This funtionality is useful for stoping Denial of Service (DoS) attacks. The content based IPS blocks traffic using IDS-signatures,searching for a specific content in a network packets.

1.4.3Symantac Host-Based Intrusion Prevention System

This IPS monitors the activities of the host in which it is installed.Due to its policy based processing engine it processes the received events from the detecting four collector components of the Symantac Host Based IPS.

II. FUNDAMENTALS OF INTRUSION DETECTION IN WIRELESS NETWORK

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: Heady (1990) et al. [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 cluster of people WHO take the action within the intrusion.

Zamboni (2001) et al. [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 readying, energy constraints and therefore the media of communication makes them terribly liable to the intrusions quite different networks.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

A. Types of attacks in Wireless network:

Outsider versus business executive attacks: supported the node that's launching the attack, if it happiness to the network thus it's thought-about as business executive attack, otherwise it's thought-about as outsider attack.

Passive versus active attacks: supported the impact that results from AN attack. Passive attacks simply monitor or pay attention to the info packets, whereas the active attacks do modify the info streams or according false alarms to the bottom station.

Mote-class versus laptop-class attacks: supported the potential of the wrongdoer in compromising the network. In mote-class attacks, some nodes with an analogous capability to the network nodes are used as attackers, whereas in laptop-class, AN wrongdoer uses powerful devices like laptops with higher transmission varies, processing power and energy to compromise the network.

III. EXISTING WORK

With the fast development of wireless network, the problems on wireless security have become more and more prominence. 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. In this paper, we firstly indicate the developing history of WIPS, and then summarize the related work on WIPS in academic and engineering application area respectively. Based on these work, we 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

The increasing reliance upon wireless networks has put tremendous emphasis on wireless network security. Intrusion detection in 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 we 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]

IV. EXTRACT FROM PREVIOUS PAPER AND ALGORITHM

In our approach, we cluster wireless traffic data 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 detected features the alarm can be 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 single check required to detect same feature in both attacks. 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.

Generate algorithm to implement modular approach:

As discussed[2] MID and AID both have problems of higher false alarm rate due to inappropriate threshold value to generate alarms for intrusion. An approach is needed that uses the combination of both of these techniques. In modular approach we are using the signature based detection approach by detecting the feature listed for known attacks as well we are checking for the abnormal behavior through a table of feature detected so we can detect the unknown attacks. During algorithm design we take care of follow the basic terminology of modular approach that can detect known as well as unknown attacks. Because that system is designed to implement for wireless network one more thing that is crucial to remember is that it should not increase the CPU overhead more than 5-6%.

Algorithm to implement modular approach with least increase in computational complexity is given below:

A Novel Solution for Intrusion Prevention.

1. Begin
2. Sniff for 802.11 frames.
3. Save data in a file that can be accessed through system and in required format
4. Open file contains data of the network
   - 4.1. Change hexadecimal code in decimal format
   - 4.2. Parse frames and extract MAC headers from the frames
   - 4.3. Check 802.11 frame types.
   - 4.4. Extract feature require to detect intrusion
   - 4.5. Search for the predefined signature of attacks in the database
5. Log packet content
6. Send out an alarm if intrusion found (i.e. Signature match)

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

7. Analysis data packet with isolated from (Analysis illegal behaviors).
8. Save all the intrusion data in the event database.
9. Set working Frequency of monitored channel.
10. Exit and Repeat

V. FUTURE WORK

Our Future enhancements are intrusion detections in internet application and parallel computer interconnection network.

VI. CONCLUSION

Here we are analyzing the intrusion detection problem by characterizing intrusion detection probability with respect to the intrusion distance and the network parameters (i.e., node density, sensing range, and transmission range).The analytical model for intrusion detection allows us to analytically formulate intrusion detection possibility within a certain intrusion distance under various application scenarios. Once we find the intruders than technique is used to stop intruders is RF jamming through salutatory-style channels i.e changing by spacing a channel.

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. 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.
3. Heady, R., 1990. The Architecture of a Network-level Intrusion Detection System.1st Edn., Departmentof Computer Science, Mexico, pp: 18.
4. Zamboni, D., 2001. Using internal sensors for computer intrusion detection. Purdue University.
5. Debar, H. M. Dacier and A. Wespi, 1999. Towards at axonomy of intrusion-detection systems. Comput. Netw., 31: 805-822.
6. 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.
7. V. Gupta and S. Gupta, "Experiments in Wireless Internet Security", Wireless Communications and Networking Conference, (WCNC 2002), IEEE Volume 2, pp. 860-864, 2002.
8. Z. Li, A. Das and J. Zhou, "Theoretical basis for intrusion detection," Information Assurance Workshop, (IAW 2005), Proceedinggs from the sixth Annual IEEE SMC, pp. 184-192, 2005.
9. Aleksandar Lazarevic, Vipin Kumar, Jaideep Srivastava, "Intrusion Detection: A Survey", Managing Cyber Threats: Issues, Approaches and Challenges, Vol. 5, 2005, Springer Publisher.
10. P.Brutch and C.Ko, "Challenges in intrusion detection for wireless ad-hoc networks," IEEE Proceedings on Workshop on Security and Assurance in Ad hoc Networks, 2003, pp368 - 373, Jan. 2003.
11. 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.
12. 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, July 2002.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)