Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Wireless Intrusion Detection System using Reputation

Sagar C. Gavande, Dr. V. K. Pachghare, Rahul Adhao
Computer Engineering & COEP
India

Abstract— with growing technologies, use of internet is also increasing. To access internet more rapidly the wireless technology is being used, as it is free from complex network of wires. Due to non-existence of physical medium in this technology, it is vulnerable to various kinds of attacks. A group of processes which try to violate the confidentiality, integrity or accessibility of data on a computing platform is known as intrusion. An Intrusion Detection System (IDS) monitors the network activities and detects the known and unknown attacks all over the network. Wireless IDS have different approaches for detecting the intrusions and in this paper we have talked about reputation based Wireless IDS for fast intrusion detection.

Keywords— Wireless IDS, Reputation, Intrusion, Attacks, Internet.

I. INTRODUCTION

Today use of Internet is going at its highest rate at the same time the terminologies to use it are also changing. The modern technologies such as Wi-Fi are getting used tremendously as it is easy to use without any wired network. Hence to achieve the risk or bug free access and network security is one of the most important issues. To do this, there is a technique called Wireless Intrusion Detection System which is discussed in this paper. Intrusion Detection is a type of security management system for computers and network. A group of processes which try to violate the confidentiality, integrity or accessibility of data on a computing platform is known as intrusion [2]. The software or hardware tool which is used by the system to find an unofficial access into the computer network is known as an Intrusion Detection System (IDS) [6]. IDS monitor the network traffic and looks for the threats as well as for logging threats and send signals to the system regarding the same. There are basically two ways to do this, one is anomaly based detection and another one is signature-based detection. At present all the detection systems are based on signature-based detection. Usually, the known attacks and its tools have the same signature from which IDS can find or detect the attack by looking for these signatures. Though it is mostly used one, it has some downsides. This technique is easy to fool as it only works on the past data and only detects the attacks for which it has a signature. As discussed above, another technique to detect the intrusion is the anomaly-based-IDS. This technique is not get used generally, as it generates high amount of the false alarms. It is totally based on the techniques of analysing the network traffic. When the network traffic seems to be different from the considered traffic, it generates an alarm. It has advantage over the signature-based IDS; it can capture new or unknown attacks by analysing traffic which might not be seen by the signature-based IDS. The main drawback of this technique is that, it requires lot of time to train and retrain the IDS and also need to examine the false alarm which generates while analysing the traffic. There is also the concept of hybrid system which uses the both signature -based and anomaly-based techniques.

II. RELATED WORK

The following section reviews various researches which have been done in past few years on Wireless Intrusion Detection System by using different approaches. Also how these researches distinguish from previous research work.

Keldor Gerrigagoitia et al. have proposed Reputation-based Intrusion Detection System for wireless sensor networks by using the cooperative approach in between distributed architecture and nodes. To find an intrusion they used an idea of hybrid approach i.e. Anomaly based IDS and Signature based IDS. While finding the behaviour of the node, they used reputation and trust mechanism. As they used Anomaly-based and Signature-based approaches together, it is quietly secure one proposed system. Use of reputation in it, makes system more faster and reliable one. [4]

Ismail Butun et al. have written the paper on a Survey of Intrusion Detection Systems in Wireless Sensor Networks. In this paper, they have mentioned the detail information about intrusion detection techniques. They have also given the different types of IDS and approaches to define it. This paper talked about intrusion detection systems such as Anomaly-based, Signature-based, Specification-based, Flow-based and Reputation based approaches in details. It also talked about how to make decision in IDS and gave the proposed systems for infrastructure based and non-infrastructure- based wireless system [3].

Jeff Dixon has given detailed idea about Wireless Intrusion Detection Systems including Incident Response & Wireless Policy. In this paper, he mentioned the need of IDS for wireless technology and gave information about IDS,[5].

Yongguang Zhang et al. have proposed an idea for Intrusion Detection in Wireless Ad-Hoc Networks. They gave the distributed and cooperative architecture for better intrusion detection which is based on statistical analysis and anomaly based IDS. The proposed architecture consists of four modules which are data collection, local detection, cooperative detection and intrusion response [11].

III. WIRELESS TECHNOLOGY

In recent years, in computer network, wireless technology has appeared as the most popular technology which is best alternative to an existing wired technology, because it is easily available for the computer networks anywhere for example-in home, offices or in any organization. Wi-Fi technology is the new way of connecting the number of hosts without using the wires. It uses the concept of radio frequency to obtain the wireless connection hence user gets the choice of connecting his/her device from anywhere in an office or a home network. Wireless technology works same as that of how the cordless phone works which uses the radio signals to transmit data from one place to another. Though it is an advanced technology, it has range problem which restricts an access of the particular network. Wireless Local Area Network (WLAN) and Wireless Personal Area Network (WPAN) are the two basic types of wireless networks.

There is little difference between configurations of Wireless LAN compared to the regular LAN, where WLAN uses the radio signals or waves instead of the traditional cables or wires. Wireless LAN and mobile phones have the large frequency gap between them which gives less risk of crossing the transmission of signals while communicating with the other network devices. As WLAN uses the radio waves for transmission, there is a chance of accessing those signals by third party i.e. an intruder. Hence to save the network from intruder required a tool called Wireless Intrusion Detection Technique (WIDS).

A. Need for Wireless Intrusion Detection System

The existing wired IDS system gives best solution for detecting an intrusion, but unfortunately it is not applicable for wireless world. The problem with wireless technology is that, it doesn't have any physical medium as that of wired LAN, hence protecting the medium for Wi-Fi technology (i.e. Air) is a great issue. There are many measures to protect the Wireless technology, but at same time there are more tools to break them. Because of the nature of Wi-Fi technology, it is hard to control the area of access. Most of the time, the range of the Wi-Fi reaches out of an organization's boundaries. Due to the limited control on medium of wireless technology, an attacker can access the network a mile away from the original network. Because of an above discussed problem regarding the Wi-Fi technology, developing and implementing WIDS systems is definitely a step in the right direction. If we are using Wi-Fi technology and have fear about attacks and intruders, the Wireless IDS may be a great idea.

B. Architecture of wireless IDS (WIDS)

Basically, WIDS can be deployed by using two approaches one is centralized and another one is decentralized. In decentralized approach each WIDS operates independent of other, also does logging and sends alert on its own. It means we need to administer each WIDS independently. But in a large wireless network it is very difficult to handle with this approach, hence this technique is not recommended for the network which has more than two Access Point. The other architecture to deploy WIDS is centralized approach. In this approach, the sensors which are deployed in the wireless network, sends the information back to one central point. Then this central point sends alert to all the sensors, log events and serve as the single administration for all sensors. It has one advantage that, sensors in a network communicate with other sensors and detect a wider range of events with more accuracy.

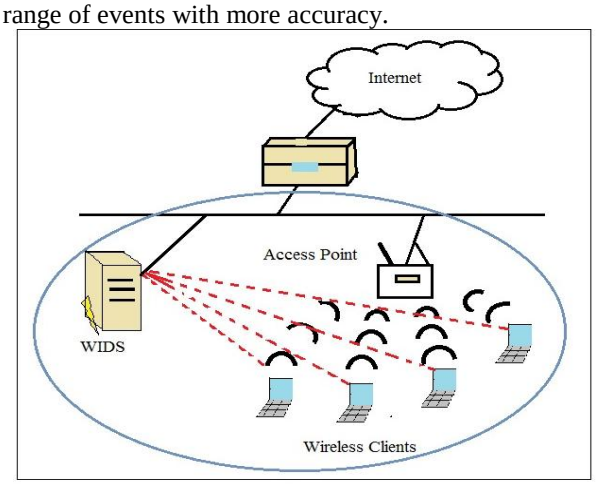

Fig. 1 Architecture of WIDS

IV. REPUTATION AS AN INTRUSION DETECTION APPROACH

As discussed earlier, the detection methodologies such as Anomaly-based, Signature-based, Semantics based and Flow-based are not efficient when it used individually to detect the intrusion. Hence to have secure wireless network which is free from intrusions, we need more advanced and fast detection methodology. Therefore, reputation based approach has this features which is discussed below in detailed.

A. Reputation

Defining the reputation for finding an intrusion is same as that of the reputation which has defined for human in the society. Reputation is nothing but the collective observations which is given by society about particular person based on his/her past behaviour in the society [7]. The publicly available values of the person such as trustworthiness is used to rate the person's reputation. Reputation system works on the mechanism of collecting information about an agent based on other agent's experience or observations with that agent. This experience or their observations are obtained in the form of rating, which means how the other agents in the society value an agent after an interaction with them. So Reputation model work for defining the reputation of a target agent based on observations which are collected from other agents without interacting with the target agent, and it is as close as that of actual trustworthiness of agent in society. Reputation model provides rule of procedure, which helps an individual agent to obtain information about another agents in the society without any direct contact with that particular agents. Finding the reputation of the agent to detect an intrusion in a network is a new approach in computer network field

B. Approaches to define Reputation

There are mainly three approaches to define reputation i.e. 1.Centralized approach, 2. Distributed approach and 3. Hybrid approach.

1) Centralized approach: In this approach, there is a use of central database, in which reported observations are getting stored. The reputation system is nothing but the database itself. From that database, information is used to calculate the reputation of an agent whenever such a request comes from another agent. This kind of approach is mainly used in on-line shopping sites. This approach is not applicable for open multi agent system, as the agents are widely distributed.

2) Distributed approach:

In this approach, the agent itself has an observation about another agent. Suppose, agent ONE want to know the reputation of the agent TWO, in this situation agent ONE will look for the agent with whom agent TWO has interacted and ask its review or observation about agent TWO. By using graphs or chaining, the neighbour of the targeted agent can find; which help to define the reputation. As it is operated in distributed manner, the drawback of centralized approach can get over come.

3) Hybrid approach:

It is a combination of above both approaches i.e. Centralized and distributed approach. In this approach as name suggest, the information is get stored in centralized format and get accessed in the distributed manner.

V. PROPOSED SYSTEM

Reputation System is nothing but the database which consists of pool of IP addresses of the well-known attackers and botnets. Classifier module basically analyses the incoming packets and extracts the Source and destination IP addresses from it. Then these IP addresses get check with the Reputation system and if the system finds these addresses, then discard the packets from that particular IP addresses as they are malicious one. If extracted IP addresses are not in Reputation System then it will send to another module i.e. Signature Creation. Signature creation module takes the packet of respective IP address from the classifier and creates its signature. This signature further sends to another module i.e. Signature level to check the maliciousness of the packet. Signature level module is divided into 4 levels according to false positive rate (incorrectly identified) of the signatures i.e. from low level to high level. It checks the signature of the incoming packet with these levels and decides the maliciousness of each packet.

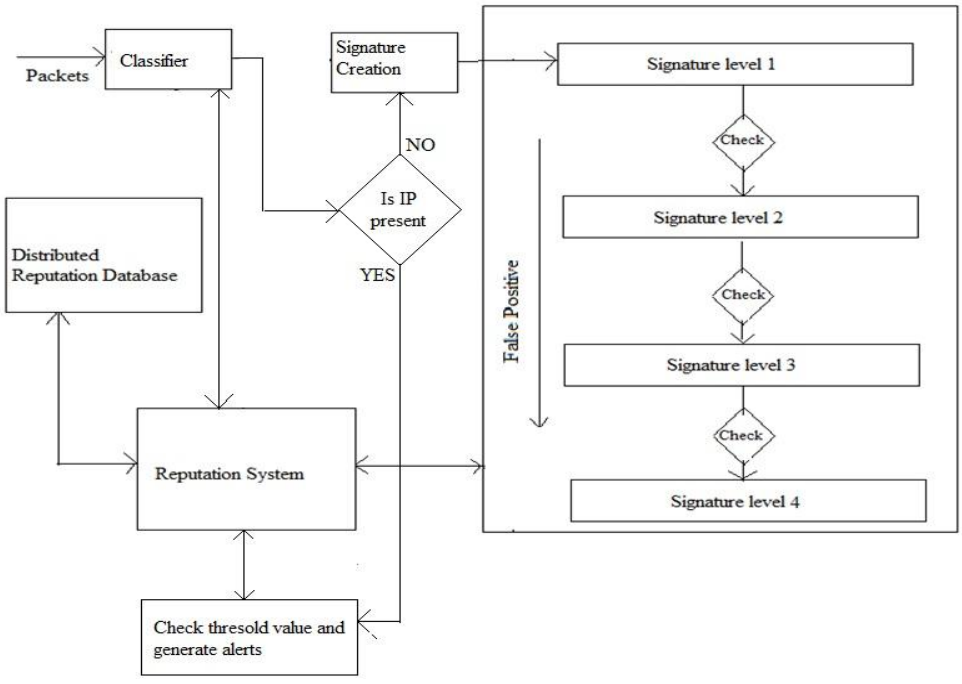

Fig 2. Proposed System

After this, each checked packet, get assigned some value according to respective levels. And final average value sends to the Reputation system to update a database. These updates will be sent to last module for generation of alerts. The final module checks the updated value and compares it with system's threshold value, if it crosses, the alert will generate and it will send to network administrator else alert will not be generated.

VI. CONCLUSIONS

Wireless network are used widely for providing network connectivity because of its convenience and ease of access. As discussed above, there is rapid proliferation in network technology which results out through higher speed networks like 3G, 4G. Also there is increase in number of Internet users. This leads to high fluctuation of data flowing through a network, which gives burden on the traditional Intrusion Detection System. Because of this, anomaly based IDS and flow-based IDS are not compatible with rapid intrusion detection for wireless technology. The proposed solution is reputation based intrusion detection system which uses the reputation for detecting the intrusions based on their past behaviours in the network.

REFERENCES

[1] Ashley Thomas, "*RAPID: Reputation based Approach for Improving Intrusion Detection Effectiveness*", 6th International Conference on Information Assurance and security.

[2] Dr. V. K. Pachghare, "*Cryptography and Information Security*", PHI Publication.

[3] Dr. S. Madhavi1 and Dr. Tai Hoon Kim, "*An Intelligent Distributed Reputation Based Mobile Intrusion Detection System"*, International Journal of Computer Science and Telecommunications, 2011.

[4] Ismail Butun, Salvatore D. Morgera, and Ravi Sankar, *"A Survey of Intrusion Detection Systems in Wireless Sensor Networks"*, IEEE Communications Surveys &Tutorials, 2013

[5] Jeff Dixon, *"Wireless Intrusion Detection Systems Including Incident Response & Wireless Policy*", unpublished.

[6] Keldor Gerrigagoitia, Roberto Uribeetxeberria, Urko Zurutuza, and Ignacio Arenaza, *"Reputation-based Intrusion Detection System for wireless sensor networks*", IEEE Communications Surveys &Tutorials, 2012.

[7] Rahul B. Adhao, Avinash R. Kshirsagar and Dr. V. K. Pachghare, *"Reputation Based Fast Intrusion Detection"*, International Conference on Information Technology, Computer Science & Management(ICITCSM), Goa 2014.

[8] Rahul B. Adhao, Avinash R. Kshirsagar and Dr. V. K. Pachghare , "*NIDS Designed Using Two Stages Monitoring*", International Journal of Computer Science and Information Technologies, 2014

[9] V. Jyothsna and V. V. Rama Prasad, *"A Review of Anomaly based Intrusion Detection Systems",* International Journal of Computer Applications, September, 2011.

[10] X. Wang, *"Intrusion Detection Techniques in Wireless Ad Hoc Networks"*, IEEE Inter National Computer Software and Applications Conference, 2006.

[11] Yongguang Zhang and Wenke Lee, *"Intrusion Detection in Wireless AdHoc*", 6th Annual International Conference on Mobile Computing and networking, Boston, Massachussetts, August 2000.

[12] Y. Mao, "A Semantic-based Intrusion Detection Framework for Wireless Sensor Network", 6th International Conference on Networked Computing(INC), Korea, South 2010.

