IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN ANALYSIS ON MOBILE AGENT FRAMEWORK FOR NETWORK INTRUSION DETECTION SYSTEM

[1]Author Kamal Kishore Prasad- [2]Author Rajendra Singh Kushwar

[1]Author Research Scholar and [2]Author Professor –Computer Application & Science department of Sri Satya Sai University of Technology & Medical Sciences-Sehore-MP

ABSTRACT

An Intrusion Detection System (IDS) monitors network traffic for dubious movement and alarms the system or network manager. Software agents can be treated as a mobile agent, as they can migrate starting with one computer then onto the next computer. Mobile agents are incredible projects, which can act even without the machine that started them. After completion of their doled out undertakings, the mobile agent's re-visitation of the host machine to report the outcome or just end. The Intrusion detection system for this environment is proposed based on the mobile agent, which utilizes the data mining procedure to identify the intrusions in the wireless environment. There are various agents utilized for identifying intrusions to be specific Collector agent, Misuse detection agent, Anomaly detection agent, Classifier agent and Alert agent. These agents gather and dissect the data gathered from the wireless environment to distinguish the attacks abused by the intruders.

KEYWORDS: Agent, Misuse, Mobile, Intrusion, Detection, Wireless.

1. INTRODUCTION

An Intrusion Detection System (IDS) monitors network traffic for dubious movement and alarms the system or network manager. At times, the IDS may likewise respond to anomalous or malicious traffic by making moves, for example, impeding the client or source IP address from getting to the network. The objective of the IDS is to distinguish dubious traffic. A few kinds of IDS are accessible for performing the detection in an unexpected way. There are network based and host based intrusion detection systems. network based IDS and host based IDS recognizes based on explicit marks of known dangers like the way antivirus software identifies and ensures against malware. Here network based IDS and host based IDS distinguish based on contrasting traffic designs against a gauge and pays special mind to anomalies. Network based IDS and Host based IDS just monitor and alarms and perform an action or actions in response to a distinguished danger. An attack against a wireless computing system can be quiet for network-based IDS conveyed in its environment, since node communication is typically encoded. Attacks can likewise be imperceptible to host-based IDS, since explicit attacks don't really leave follows in the nodes working system, where the host – based IDS dwells. In this manner, traditional IDS can't fittingly recognize dubious attacks in the wireless environment. The mobile agent is an agent having the capacity of moving starting with one host then onto the next. It collaborates with other nodes to gather the data. The advantages of

mobile agent innovation in a heterogeneous environment are diminishing the network over-burden, beating network idleness, heartiness and fault tolerance. The mobile agent innovation has been demonstrated to be truly reasonable to tackle the intrusion detection in a distributed environment. The proposed system utilizes the mobile agent innovation to recognize the known and obscure attacks abused by the attacker. The new expectations of the examination local area from a mobile agent are more realistic. 10 years after the introduction of mobile agents, it is currently certain that mobile agent is most appropriate for distant information recovery. Considering the idea of mobile computing where computing hosts are away from one another and in such situations on the off chance that we need to realize what's going on at the distant host, utilization of a mobile agent become unavoidable. Therefore detection of the presence of maverick passageways in wired, wireless or hybrid (wired and wireless joined) kind of network is an appropriate case for the utilization of mobile agent.

2. LITERATURE REVIEW

Mishra, Ajita and Srivastava, Ashish (2013) Security of Wireless network gets associate in nursing woeful necessary issues with the rapid development of wireless network that is in danger for an honest varies of attacks because of preparation among the hostile atmosphere and having restricted assets. Presently a day wireless detection network is a unit which is approximately used in environmental management, police investigation tasks, monitoring military applications, health connected applications, pursuit and dominant and so forth Wireless intrusion detection also aids among the detection of a variety of attacks. Wireless intrusion detection system cannot solely see heel WAPS, establish non-scrambled 802.11 traffic, and facilitate isolate associate attacker's physical location. We have a propensity 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, right off the bat indicates the developing history of WIDS, and then summarizes the related work on Wireless Intrusion Prevention System through RF jamming method.

Milliken, Jonny (2014) IDS (Intrusion Detection System) is a common means of protecting networked systems from attack or malicious misuse. The development and rollout of IDS can take many various forms regarding gear, protocols, connectivity, cost and automation. This is particularly valid for WIDS (Wireless Intrusion Detection Systems) which have many more chances and challenges associated with data transmission through an open, shared medium. The operation of a WIDS is a multistep cycle from origination of an attack through to human readable evaluation. Attention to the performance of each of the cycles in the chain from attack detection to evaluation is imperative if an ideal solution is to be sought. As of now, research focuses particularly on each discrete aspect of a WIDS with little consideration to the operation of the entire system. Taking a holistic perspective on the innovation shows the interconnectivity and inter-reliance between stages, leading to enhancements and novel research areas for investigation. This chapter will outline the general construction of Wireless Intrusion Detection Systems and momentarily portray the functions of each development stage, categorized into the following 6 areas: Threat Identification, Architecture, Data Collection, Intrusion Detection, Alert Correlation, and Evaluation. These topics will be considered in broad terms intended for those new to the area. Spotlight will be placed on ensuring the readers are aware of the impact of decisions made at early stages in WIDS development on future stages.

AlShourbaji, Ibrahim and Al-Janabi, Samaher (2017) society today, public and personal communication are often carried out through wireless innovation. These advances can be vulnerable to various kinds of attacks. Attackers can access the signal to listen or to cause more damage on the wireless networks. Intrusion Detection and Prevention System (IDPS) innovation can be used to monitor and analyze the signal for any infiltration to forestall interception or other malicious intrusion. An overview description of IDPSs and their center functions, the primary sorts of intrusion detection mechanisms, and the limitations of IDPSs are discussed. This work sees the prerequisites of developing new and sophisticated detection and prevention methods based on, and managed by, combining smart procedures including machine learning, data mining, and game theory along with risk analysis and assessment strategies. This assists wireless networks to remain secure and aids system administrators to successfully monitor their systems.

Shukla, Piyush (2015) organizations focuses IDPSes

for separate purposes, for example identifying issues with security strategies, manually introduced threats and deterring individuals from violating security approaches. IDPSes have become a necessary strategy to the security infrastructure of approximate each association. IDPSes typical record information interrelated to practical occasions, security administrators of essential noticed occasions and construct review. Many IDPSes can also respond to a detected threat by attempting to thwart it succeeding. These use several response strategies, which involve the IDPS restricting the attack, changing the security environment or the attack's content. Sensor node ought to wander in size from a shoebox down to the small size, although functioning "bits" of genuine tiny dimensions have to be formed. The expense of sensor nodes is variable, from a couple to thousands of dollars; rely upon the unpredictability of the sensor nodes. Size and cost constraints on sensor nodes address in corresponding constraints on assets, for example, energy, memory, computational speed and communications bandwidth. The arrangement of the WSNs alters itself from a star network to efficient multi-bounce wireless mesh network. The proliferation procedure between the jumps of the network can be routing or flooding

Yassine, Maleh and Ezzati, Abdellah (2014) Wireless Sensor Networks (WSNs) are as of now used in various industrial and consumer applications, for example, earth monitoring, health related applications, natural disaster prevention, and many other areas. Security is one of the major aspects of Wireless sensor networks because of the asset limitations of sensor nodes. Nonetheless, these networks are facing several threats that affect their functioning and their life. In this paper we present security attacks in wireless sensor networks, and we center on an audit and analysis of the new Intrusion Detection conspires in WSNs.

3. RESEARCH METHODOLOGY

The Intrusion detection system for this environment is proposed based on the mobile agent, which utilizes the data mining procedure to identify the intrusions in the wireless environment. There are various agents utilized for identifying intrusions to be specific Collector agent, Misuse detection agent, Anomaly detection agent, Classifier agent and Alert agent. These agents gather and dissect the data gathered from the wireless environment to distinguish the attacks abused by the intruders

3.1 Collector Agent

The agent in this architecture is started on a timely premise to record user movement and program operation related information from various hosts in the network. The collector agent in this architecture gathers user and cycle related information and passes the gathered information to the misuse detection agent for further processing.

3.2 Misuse Detection Agent

The misuse detection agent breaks down the gathered data and distinguishes the realized attacks by checking the likenesses between the gathered data with the data accessible in the centralized database; if the gathered data matches with the data accessible in the centralized database then it reports the attack as example matching attack with the assistance of alert agent.

3.3 Anomaly Detection Agent

The anomaly detection agent gathers the data from the misuse detection agent and examines it to recognize the obscure attacks. In the event that the gathered data isn't matching with the data accessible in the centralized database, the misuse detection agent takes care of the gathered data to the anomaly detection agent. The rationale is characterized for the attacks, for example, Ping of Death, Land, Teardrop, TCP flooding. In the event that the gathered data abuses or surpasses the constraints characterized in the rationale then the data is distinguished as another or obscure attack and the recognized new attack is updated in to the centralized database.

3.4 Classifier Agent

It arranges the data based on the dataset accessible in the centralized database. On the off chance that the approaching data is identified as an attack, then it reports this to the anomaly detection agent, which thusly reports to the alert agent about the attack. It additionally updates the distinguished attack in the centralized database.

3.5 Alert Agent

An alert agent gets alerts generated from misuse and anomaly detection agent. The alert agent sends these alerts to an IDS console that can be utilized by the security director to see alerts generated from the IDS. The alert agent is likewise responsible for keeping various alerts from being generated. The alert agent additionally stores the information gathered from a misuse and anomaly detection agent for further investigation.

4. DATA ANALYSIS

To dissect the strength of the improved construction, this section plans a test to keep down certain sorts of attack exercises with two unique systems. One is the improved intrusion detection system based on agent, and the other is an overall Rule-based intrusion detection system. Then, the part arrives at a conclusion by dissecting and contrasting the outcome and the test outcome. In this system, agents can speak with one another utilizing UDP and TCP. Communication between agents is fundamental. On the off chance that the issue happens in the middle of two agents, then the whole IDS is in a dilemma. A basic model to assess the performance of the TCP is an extension of the packet-misfortune model. The misfortunes in the internet should be free and they are often hurried and associated. Therefore, new models are expected to catch the effect of random corresponded misfortunes on the TCP performance.

4.1 RTT

Sending a TCP fragment contingent on the modulation and coding plans utilized on the radio interface is done utilizing the "stop and pause" convention. The quantity of retransmissions needed to convey the TCP fragment is a random variable because of fluctuating radio channel conditions. The time expected to send a blunder free TCP section is given in equation (1),

$$RTT = \frac{\sum_{i=1}^{n_s} NTTI(i)}{n_s} T_j + RTT_{wired} = RTT_{wireless} + RTT_{wired} \quad (1)$$

Where

$$N_i = \frac{\sum_{i=1}^{n_s} NTTI(i)}{n_s}$$

Is the number of transmissions of a TCP portion?

n_s (variable) is the number of TTI expected to communicate a TCP portion when no mistakes happen on the radio interface;

NTTI (i) is the number of transmissions of TTI because of HARQ;

Tj is the transmission time of a portion on the radio interface.

4.2 Number of Transmissions of Packets

Since in each record, packet call or TCP portion is communicated over a specific number of Trail Traces Identifier (TTIs), the utilization of booking on a shared channel makes the mistakes on each TTI autonomous (the progressive TTIs are allotted to different users), and the number of retransmissions of each TTI data free of the other TTIs.

4.3 Forward Percentage (FP)

FP processes the proportion of really forwarded packets to the packets that are sent from the sender to the moderate node and that halfway node ought to forward. The FP proportion is determined in equation (2),

$$FPm = \frac{\text{Packets actually forwarded}}{\text{Packets to be forwarded}} \quad (2)$$

FP determines the ratio of actually forwarded packets to the packets that are transmitted from M to m and that m should forward. If the denominator is not zero and FPi =0, the attack is detected as unconditional packet dropping and m is identified as the attacker. Throughput performance increases network performance and packet delivery ratio and minimizes packet delay. It is the ratio of data packets delivered to the destination to those generated by the sources. It is calculated by dividing the number of packets received by the destination by the number of packets originated from the source.

Finally, evaluation of the performance of two experiments using Detection Rate (DR), False Positive Rate (FP) and accuracy is done according to the formulae specified in the equation (3)

$$\text{Detection Rate} = \frac{\text{Number of Detected Attacks}}{\text{Number of Attacks}} \times 100\% \quad (3)$$

4.4 Attack Detection Rate (ADR)

It is the proportion of the absolute number of attacks detected by the system to the all out number of attacks present in the dataset. False sure rate is determined in the equation (4),

$$\text{False Positive Rate} = \frac{\text{Number of misclassified connections}}{\text{Number of normal connections}} \times 100\% \quad (4)$$

4.5 False Alarm Rate (FAR)

It is the proportion of the complete number of misclassified occasions to the absolute number of normal cases examined in the equation (5).

$$\text{Accuracy} = \frac{\text{Number of correct classified connections}}{\text{Number of connections}} \times 100\% \quad (5)$$

To test the legitimacy of the improved system, this study plans an analysis to keep down some sort of attack exercises with two unique systems. One is the improved intrusion detection system based on Agent and the other is an overall Rule-based intrusion detection system. Then, it concludes by dissecting and contrasting and the test outcome.

5. DISCUSSION AND RESULTS

The standard network intrusion dataset included is commonly utilized in network security research for preparing and assessing IDSs. Attacks in the location of information can be isolated into five gatherings in particular Denial of Service (DOS), Remote to User (R2L), User to Root (U2R), Probing (Probe) and Normal. DoS attacks are performed on a host by spending its assets so it won't have the option to give network service to the legitimate users. R2L attacks are conducted by sending packets to a focused on machine in a computer network to obtain entrance as though the intruders own a record in the focused on machine.

R2L attacks can be performed in many forms. It exploits feebly configured security highlights, perform cradle flood attacks and theory or catch secret phrase of hosts in computer networks. For U2R attacks, a nearby user may abuse defects in ineffectively planned systems so that root-level advantages can be gotten. Probing normally goes before a genuine access or DoS attack.

- **DOS:** (BackSide, Ground, Neptune, Shell, Smurf, Slant Crash, Processor Table, UserDataGram Protocol, Mailbomb, Apache2)
- **R2L:** (File-Transfer, Protocol Write, Password Guessing, Image map, Multihop, Email Master, Mails Sending Block Messages, Worm Messages, Send Number of Messages Protocol, Named Data)

- **U2R:** (Buffer Overloading, Load Section, Perl Model, Source Kit, Xname, Protocol Server, Hypertext Transfer Protocol Channel, Structure Query Language Attacking)

- **PROBING:** (Internet Protocol Cleaning, Network Mapping, Port Cleaning, Mscan)

5.1 Intrusion detection attack result

Figure 1 is a depiction of the comparison between the number of attacks detected among the four main sorts of attacks to be specific DOS, R2L, U2R and Probing attack.

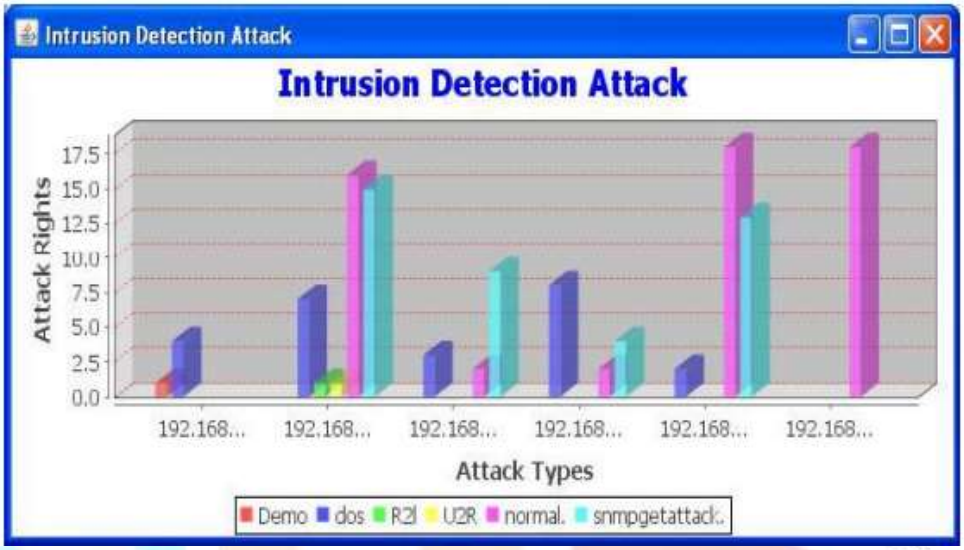

Figure 1: Intrusion Detection Attacks Comparison Chart

Table 1 indicated the summary report of different intrusion detection attacks. The customer data is investigated to check for any attack by utilizing the misuse detection agent. In the event that the misuse detection agent finds any match with the attacks characterized in the centralized database then the alert agent alerts the system by communicating something specific.

Table 1 Intrusion Detection Attack Summary Report

Table - dbo.tbl_IntrusionData | Summary

Sno	Attackservice	Attack	Land	IPAddress	Sourcebytes	Destinationbytes	TimeOfAttack	Data
1	dos	TearDrop Attack	http	192.168.1.109	3	86	2012-03-12 14:...	(ACCEPT-PROP...
2	dos	TearDrop Attack	http	192.168.1.109	23	87	2012-03-12 16:...	(ACCEPT-PROP...
3	dos	TCPFlooding	http	192.168.1.109	24	94	2012-03-13 10:...	(ACCEPT-PROP...
4	dos	TearDrop Attack	http	192.168.1.109	25	95	2012-03-13 10:...	(ACCEPT-PROP...
5	dos	TCPFlooding	http	192.168.1.108	3	87	2012-03-13 11:...	(ACCEPT-PROP...
6	dos	PingOfDeath	http	192.168.1.108	30	87	2012-03-13 11:...	(ACCEPT-PROP...
7	dos	TCPFlooding	http	192.168.1.109	3	86	2012-03-12 14:...	(ACCEPT-PROP...
8	dos	TearDrop Attack	http	192.168.1.109	23	87	2012-03-12 16:...	(ACCEPT-PROP...
9	dos	TCPFlooding	http	192.168.1.109	24	94	2012-03-13 10:...	(ACCEPT-PROP...
10	dos	Neptune	http	192.168.1.109	25	95	2012-03-13 10:...	(ACCEPT-PROP...
11	dos	TearDrop Attack	http	192.168.1.108	3	87	2012-03-13 11:...	(ACCEPT-PROP...
12	dos	PingOfDeath	http	192.168.1.108	30	87	2012-03-13 11:...	(ACCEPT-PROP...
13	dos	TCPFlooding	http	192.168.1.109	3	86	2012-03-12 14:...	(ACCEPT-PROP...
14	dos	TCPFlooding	http	192.168.1.109	23	87	2012-03-12 16:...	(ACCEPT-PROP...
15	dos	TCPFlooding	http	192.168.1.109	24	94	2012-03-13 10:...	(ACCEPT-PROP...
16	dos	TCPFlooding	http	192.168.1.109	25	95	2012-03-13 10:...	(ACCEPT-PROP...
17	dos	TCPFlooding	http	192.168.1.108	3	87	2012-03-13 11:...	(ACCEPT-PROP...
18	dos	Neptune	http	192.168.1.108	30	87	2012-03-13 11:...	(ACCEPT-PROP...
19	dos	TCPFlooding	http	192.168.1.109	3	86	2012-03-12 14:...	(ACCEPT-PROP...
20	dos	Neptune	http	192.168.1.109	23	87	2012-03-12 16:...	(ACCEPT-PROP...
21	dos	TCPFlooding	http	192.168.1.109	24	94	2012-03-13 10:...	hai
22	dos	TCPFlooding	http	192.168.1.109	25	95	2012-03-13 10:...	chennai
23	dos	TearDrop Attack	http	192.168.1.108	3	87	2012-03-13 11:...	welcome
24	dos	PingOfDeath	http	192.168.1.108	30	87	2012-03-13 11:...	android
25	dos	PingOfDeath	http	192.168.1.108	1	477	2012-03-22 12:...	(ACCEPT-PROP...

The IDS for wireless computing makes the mobile agent distinguish notable and anonymous attacks. The results delivered show that the proposed model professionally orders the flightiness profile from the normal profile as restricted by the centralized controller. Additions of new hosts are not an issue for this architecture on the grounds that the architecture makes the IDS adaptable. Communication with the server can't over-burden portions of the network in view of the utilization of mobile agent. The proposed IDS don't contain platform components. The IDS for wireless networks is proposed which utilizes the mobile agent innovation to detect known and new or obscure attacks. Because of the distributed idea of wireless networks, it is an obvious objective for intruders to misuse the attack; thus security is a major issue. To defeat the security issues in the wireless networks, the intrusion detection system is sent. Therefore, mobile agents are utilized to detect the known and new or obscure attacks abused by the intruders. Consequently the attacks are detected by the mobile agents and the attacks are updated in the centralized database and the wireless network environment is alerted about the intrusion. The eventual outcome of the proposed architecture is that the known and obscure or new attacks are detected by the mobile agent innovation.

6. CONCLUSION

Assessment of the mobile agent server with other progressive introductions makes this model to conquer the issue of single purpose of disappointment. Notwithstanding hypothetical investigation, the model likewise incorporates a complete precision testing that can be performed with pivotal measurements that are both host-based and network-based. This system gives high intrusion detectivity. Sending a mobile agent has empowered this system to examine and order the condition of encroaching action in real time and thus recognize the attack effectively. A relative report dependent on the presentation of the mobile agent system over the customary customer server approach was accomplished for an intrusion detection system. It has been seen that the free-meandering mobile agents can diminish the network traffic and generally trip time.

REFERENCES

[1]. Mishra, Ajita & Srivastava, Ashish. (2013). A Survey on Intrusion Detection System for Wireless Network. International Journal of Computer Applications. 73. 37-40. 10.5120/13021-0221.

[2]. Milliken, Jonny. (2014). An Introduction to Wireless Intrusion Detection Systems (WIDS). 10.1201/b16390-19.

[3]. AlShourbaji, Ibrahim & Al-Janabi, Samaher. (2017). Intrusion Detection and Prevention Systems in Wireless Networks. 2. 6.

[4]. Shukla, Piyush. (2015). Intrusion Detection and Tolerance in Next Generation Wireless Network.

[5]. Yassine, Maleh & Ezzati, Abdellah. (2014). A Review of Security Attacks and Intrusion Detection Schemes in Wireless Sensor Network. International Journal of Wireless & Mobile Networks. 5. 10.5121/ijwmn.2013.5606.

[6]. Mitchell, Robert & Chen, Ing-Ray. (2014). A Survey of Intrusion Detection in Wireless Network Applications. Computer Communications. 42. 10.1016/j.comcom.2014.01.012.

[7]. Yang, Hongyu & Lixia, Xie & Sun, Jizhou. (2004). Intrusion detection solution to WLANs. 553 - 556 Vol.2. 10.1109/CASSET.2004.1321948.

[8]. Makhlouf, Amel & Boudriga, N.. (2008). Intrusion and Anomaly Detection in Wireless Networks. 10.4018/9781599048994.ch006.

[9]. Ghosal, Amrita & Halder, Subir. (2013). Intrusion Detection in Wireless Sensor Networks: Issues, Challenges and Approaches. 10.1007/978-3-642-36169-2_10.

[10]. Ponomarchuk, Yulia & Seo, Dae-Wha. (2010). Intrusion detection based on traffic analysis in wireless sensor networks. 1 - 7. 10.1109/WOCC.2010.5510642.