A New Approach of Intrusion Detection System with a Combination of Multilevel and Multiagent

Arpita Biswas, Meenakshi Sharma

Abstract— the internet systems are attacked by many intruders and the information in the network is not safe here. So we need to protect the network from intruder and the intrusion detection system is needed to detect the intrusion in the network. It monitors the information and detects the intrusion. In this paper used the Multiagent technique with multilevel system to improve the existing Intrusion Detection System. Proposed detection process is very easy and error free. By this process all the high level and low level attacks are detected because information are checked in different levels thoroughly and the time and work burden is also less because multiple agents work together for the same goal.

Index Terms: Multilevel, Multiagent, Security.

I. INTRODUCTION

Network attacks are increasing day by day and whole world is affected by it. Security is a critical issue for today's life. Many technologies have been applied in protecting network environment. The technology which we used is vulnerability, authentication, firewall, encryption etc. By using these techniques we want to secure the network resources but there have been an unauthorized access in the system because attackers are very intelligent and they take advantage of any defect or social engineering process. Another important process is if one employee is unsatisfied and they misuse the company resource, is the process of unauthorized access or attracts. In the intrusion detection system it collects information from a network resource and attacks and stores it and detects intrusion on the basis of this information. In this paper we use the intrusion detection system in a Multiagent based. By this process the transmission speed is improved. Multiagent used same information system and detects intrusion by the own way. That's why the process is so easy because here the whole burden is not dependent on one agent. Here different agent done the work in different way and complete the whole task. In this paper we also used multilevel detection systm.hre different agent detect intrusion in different level, so the detection is also error free. The concept of Intrusion detection system was first introduced by Anderson to complement conventional computer security approaches in 1980[1].To improves the existing intrusion detection system this paper introduces multilevel attached with Multiagent intrusion detection system. When information are send from one server to another then before receiving this information it is checked by the proposed Intrusion Detection architecture. Where information checked through different level that's why we get more secure information and here the total information is divided into different agent who works together and completes the whole task. In this process less time is needed.

Manuscript published on 30 July 2014.
***Correspondence Author(s)**

Arpita Biswas, Department of Computer Science & Engineering, Sri Sai College of Engineering & Technology, Badhani, India.
Meenakshi Sharma, Department of Computer Science & Engineering, Sri Sai College of Engineering & Technology, Badhani, India.

II. INTRUSION DETECTION SYSTEM

Intrusion Detection process is a very useful process.IDS is a self operating system by which the detection process is done automatically. If any error is detected then it also attempts any solution process. By the process of IDS we get the information more accurate and practical. There are two types of IDS system present here-

A. Network Based IDS: In network based IDS data monitor from the network. Network data are collected from different host and all data are analyzed.

B. Host Based IDS: In the host based IDS only the one host's data are monitor and detect the intrusion. Any network encryption does not affect the work of host based intrusion detection.

C. Router Based IDS: In the router based IDS the computers on large network are analyzed and detect intrusion.

There is some method present for detecting intrusion in different situation. These are:

A. Abnormality Check: In this process we detect the intrusion very easily. When normal behavior is changed and abnormal behavior is found then it is called intrusion. In this process we test the data flow and find the abnormality. Means if their behavior is deviate from the normal it is called abnormal behavior. By the abnormality check process we can solve the intrusion with known pattern means we know some behavior like execution time, CPU usage. If this behavior is not like exactly this then we call the behavior is abnormal and detects intrusions.

B. Misuse Detection: In the misuse detection system we stored known patterns and basis of this pattern we detect intrusion. It only detects the known attack pattern. Sequence of action is stored in the known pattern dataset. Here data monitored on the basis of this dataset but new attacks are not detected by it.

III. MULTIAGENT TECHNIQUE

Multiagent means more than one agent work together and complete task and also use same resource [1],[2],[4].in this paper three types of agents are used. This agents divide the task among them and work individually for same goal. They work independently and not interfere in one another's work.

IV. MULTILEVEL TECHNIQUE

Multilevel means intrusion is detected in different level [3, 6].1st of all here information is encrypted and divided among the agent. Agent sends this information. Before receiving the information receiver decrypt the information and matched the integrity. If it is not matched then generates an alarm to the administrator about intrusion and stops the work otherwise it sends the information to the next level where Bayesian theory is used [8]. By this algorithm the information are checked 2nd time and we get the better result

V. RELATED WORK

To provide network security here need of Intrusion Detection System. By the Intrusion Detection System Intrusion is detected and generate a safety alarm to the administrator. But Intrusion Detection System has some limitations. That's why there introduce Distributed Intrusion Detection System [1],[2],[4].In this technique Intrusion is detected in distributed network. Here multiple agents are used to detect intrusion means different agent work together to produce same goal. They use same resource also. By using Multiagent system less time is needed to complete the task and agent solve easily any problem by working together. They work independently. Intrusion is detected by the multilevel technique [3],[6].here information is passed to the 1st level then to the 2nd level. Information are checked in different level so all low level and high level attacks are detected. When information is passed to the 1st level then if there detect any intrusion then generate an alarm to the administrator otherwise information is passed to the next level where this information is checked 2nd time. If intrusions detected then generate an alarm otherwise the information is stored as a normal. In the Intrusion Detected System information are collected 1st then divide among the agents [5].Intrusion is detected by using Bayesian theory [7], [8].in this technique use database and find the probability of intrusion. Information is encrypted and encryption decryption process is used to provide better security [9],[10], [11].

VI. PROPOSED WORK

1st of all encrypt the collected information then divide among agents. Agent receives information and they decrypt this information and check the integrity of this information. If integrity matched then this information is attack free and sends this to the next level, otherwise if any intrusion detected then send an alarm to the administrator and block the attack packet. In the 2nd level information are checked again. Here used Bayesian theory to check information. If intrusion detected then send an alarm to the administrator and block the attack packet otherwise store the information as a normal data. Figure 1 is the proposed Intrusion Detection Architecture.

A. *Algorithm Used by Agents:*

1st level: In this level agent use their own rule. Which describe bellow –

Encryption process of the file:

1. User prepares a message for sending.
2. User calculates the size of the received message.
3. User than calculates the hashes of the received message. This hash values will be used for integrity checking.

Any changes in the data will change the hash value of the same file.

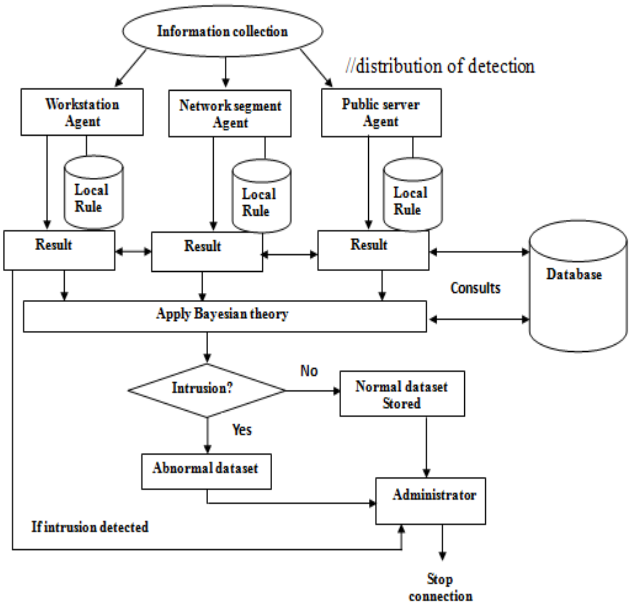

Fig. 1 Architecture of Intrusion Detected System

4. User then encrypts the Message and sends the encrypted message to the server.

Decrypt process of the file:

1. Server first requests for the intended message and key.
2. User sends the key.
3. Sever decrypts the message.
4. Here for integrity verification Server performs the following tasks:

i) Server first calculates the size of the received message. If the file size is matched with the previously stored one, then Server performs (ii) Else the integrity of the message has been lost.

ii) Server calculates the hash of the received message and matches it with the stored one. If it matches then the message is ok, else its integrity has been lost.

5. After verification Server sends the data to next level if its integrity is not lost.

Server decrypts the message with the same password as provided by the user.

B. Algorithm Used by Agent:

In the 2nd level agent use the algorithm to detect the intrusion. Agents use their own rule to detect the intrusion. In this paper agent use the Bayesian filtering technique to detects the intrusion [8]. The technique is described below. Assume the word tourist (t) present in an attacked packet. By this process we get the chance of intrusion. Let 5 packets are present here. These are p1, p2, p3, p4, p5. Now we find the probability of packet p1 is attack packet. The probability,
$P\ (p1/t) = P_A\ (p1)\ x\ P_A\ (t/p1) \div P_A\ (p1)\ x\ P_A\ (t/p1) + P_N\ (p1)\ x\ P_N\ (t/p1)$ where

P_A (p1) = overall probability that p1 is an abnormal packet,

P_A (t/p1) = probability that the word tourist present in the abnormal packet p1,

P_A (p1/t) = probability that the packet is abnormal and the word tourist is in it,

P_N (p1) = probability that the packet is normal,

P_N (t/p1) = probability that the word present in normal packet.

Here the probability that the packet is abnormal is 65 % means P_A (p1) = .65 and P_N(p1) = .45, then by using the Bayesian filtering technique we get the solution that the packet p1 is abnormal or not.

If P_A (p1) = .65 and P_N (p1) = .45, then P_A (t/p1) = .65 and P_N (t/p1) = .45.

By putting these value we get,

P_A (p1/t) = .65 x .65 / .65 x .65 ± .45 x .45 = 0.676 = 68%, means chance of the abnormal packet 68% and chance of the normal packet 32 % or the intrusion is detected in this packet and immediately blocks this packet and back to the source for resend the packet.

VII. CONCLUSION

In this paper the Multi-agent and multilevel system work together for improving the intrusion detection system. The Multi-agent works in different level and for this the detection process results better. In one level it checks the integrity of the information. If there is any malicious activity presents then generate an alarm about intrusion. If no attacts are detected then this information is passed through the level where the information is checked 2nd time. So by this process we get the better intrusion free information. This approach is very helpful to us because here data is checked by different level and also less time required because the use of multi-agent. They divide their work and easily detect the intrusion. After finishing these two levels we get the final result and store it in the database.

REFERENCES

1. Ran Zhang', Depei Qian, Chongming Bao, Weiguo Wu, "Multiagent Based Intrusion Detection Architecture", pp 494-501, IEEE 2001.
2. Siham benhadou, Driss raoui Hicham medromi, "New Methodology for Intrusion Detection based on Multi-Agents System", Architecture Systems team ENSEM.
3. Gargi Agrawal, Megha Kamble, "Proposed Multi-Layers Intrusion Detection System(MLIDS) Model", Gargi Agarwal et al, / (IJCSIT) International Journal of Computer Science and Information Technologies 2012, Vol. 3(5),5040 - 5042
4. Nita Patil,Chhaya Das, Shreya Patankar, Kshitija Pol, "Analysis of Distributed Intrusion Detection Systems using Mobile Agents", Datta Meghe College of Engineering, Airoli , Navi Mumbai- 400708, First International Conference on Emerging Trends in Engineering and Technology,pp 1255-1260, IEEE 2008.
5. Sarit Kraus, Tatjana Plotkin, "Algorithms of distributed task allocation for cooperative agents" ,Department of Mathematics and Computer Science, Bar-Ilan University, 52-900 Ramat- Gan, Israel,Theoretical Computer Science 242 ,Elsevier Science (2000) pp.1-27.
6. Mueen Uddin, Kamran Khowaja, Azizah Abdul Rehman, "Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents",Department of Information System, UTM, Malaysia ,International Journal of Network Security and Its Applications(IJNSA),Vol.2, No.4, October 2010, pp.129-141.
7. Tatsuya Baba,Shigeyuki Matsuda , "A Proposal of Protocol and Policy-Based Intrusion Detection System" SYSTEMICS,CYBERNETICS AND INFORMATICS, pp 57-62.
8. Farah Jemili,Dr. Montaceur Zaghdoud,Pr. Mohamed Ben Ahmed "A Framework for an Adaptive Intrusion Detection System using Bayesian Network",2007 IEEE, pp 66-70.
9. "Encryption Basics | EFF Surveillance Self-Defense Project." (06 Nov. 2013) Encryption Basics | EFF
10. Robert Richardson, 2008 CSI "Computer Crime and Security Survey",at 19.i.cmpnet.com
11. Goldreich, Oded. "Foundations of Cryptography" Volume 2, Basic Applications. Vol. 2. Cambridge university press, 2004.

AUTHOR PROFILE

Arpita Biswas, is pursuing M.Tech in Computer Science & Engineering at SSCET, Badhani, Punjab, India under Punjab Technical University, Jalandhar. Her ongoing research area is on Intrusion Detection System and her areas of interest are Network Security, Distributed Networking.

Meenakshi Sharma, is working as Associate Professor in Department of Computer Science & Engineering, SSCET, Badhani, Punjab, India. She has more than 16 years of teaching experience. Her areas of interest are Parallel Computing, Cloud Computing, and Network Security.