Journal of Computer and Communications, 2016, 4, 93-98
Published Online April 2016 in SciRes. http://www.scirp.org/journal/jcc
http://dx.doi.org/10.4236/jcc.2016.44008

General Study of Mobile Agent Based Intrusion Detection System (IDS)

Chandrakant Jain, Aumreesh Kumar Saxena

CSE SIRTE, Bhopal, India
Email: ckjain20@gmail.com, aumreesh@gmail.com

Received 5 February 2016; accepted 10 April 2016; published 13 April 2016

Abstract

The extensive access of network interaction has made present networks more responsive to earlier intrusions. In distributed network intrusions, there are many computing nodes that are assisted by intruders. The evidence of intrusions is to be associated from all the held up nodes. From the last few years, mobile agent based technique in intrusion detection system (IDS) has been widely used to detect intrusion over distributed network. This paper presented survey of several existing mobile agent based intrusion detection system and comparative analysis report between them. Furthermore we have focused on each attribute of analysis, for example technique (NIDS, HIDS or Hybrid), behavior layer, detection techniques for analysis, uses of mobile agent and technology used by existing IDS, strength and issues. Their strengths and issues are situational wherever appropriate. We have observed that some of the existing techniques are used in IDS which causes low detection rate, behavior layers like TCP connection for packet capturing which is most important activity in NIDS and response time (technology execution time) with memory consumption by mobile agent as major issues.

Keywords

Intrusion Detection System, Mobile Agent, Intrusion, Network, Attack, Security

1. Introduction

These days' threats have become prominent. To have a better knowledge, controlling and managing cyber security risks have become utmost demand of time for the representatives of either government, or the private firms. Various organizations responses are reflected by their action. Moreover, they are stepping towards the new and innovative ideas or technologies like cloud-enabled cyber security, Big Data analytics, IDS, IPS, Firewalls and advanced authentication to reduce cyber-risks and improve cyber security programmers. Businesses are also covering up a more cooperative approach to cyber security; one way is to share the potential threats and responses

How to cite this paper: Jain, C. and Saxena, A.K. (2016) General Study of Mobile Agent Based Intrusion Detection System (IDS). *Journal of Computer and Communications*, **4**, 93-98. http://dx.doi.org/10.4236/jcc.2016.44008

with external partners. As per the recent market research worldwide spending on IT security is set to increase 4.7 percent in 2015 to $75.4 billion, and it is projected to spend $101 billion on information security in coming 2018 [1]. We may expect that this cyber security market will have an exponential growth of $170 billion (USD) by 2020, at a Compound Annual Growth Rate (CAGR) of 9.8 percent from 2015 to 2020, it has figured out from the market reports that the expertise, like the aerospace, defense, and intelligence, is likely to be the largest contributor to cyber security solutions [1]. Intrusion detection system (IDS) is required, whenever the Affinity, integrity, and availability of computer resources are under attack, it will help to expose and respond completely. From all such affected nodes the evidences of intrusions have to be combined. An intruder may move in multiple nodes in the network. Due to this the root of attack is concealed [2].

2. Intrusion Detection System

Most necessary task of Intrusion Detection System (IDS) is the analysis on computer networks [2]. Intrusion Detection Systems (IDS) is considered as one of security tools there are few other measures such as anti-virus software, firewall, digital signature scheme and access control scheme, it has widely used for enhance computer security .it can be done in two ways: the analysis approach and the placement of this method [2] [3]. IDS are of two types one is anomaly detection and the other is misuse detection. Of normal behavior model is made by anomaly detection system, and any deviation from it is automatically detected, Rendering the latter as suspect [4] abnormal behaviors and deviations from normal activities are detected by this system using methods such as statistical analysis, machine learning, neural networks, and sequential analysis. It is also efficient to identify previously unknown attacks, but also led to false alarm rates because of the anomalies. Each part of misuse detection system in a data set is designed as normal or intrusion and a learning algorithm is applied over the labeled data [4] [5]. Misuse detection systems is that its use patterns of well known attacks or weak spots use this system to match and identify known intrusions, say for example we cite the network IDS SNORT. SNORT is configured by making use of database signatures which characterize network packets that have the potential of being malicious [6]. SNORT monitors a network connection by using this database and marks the network packets that match any of the configured signatures. However, this techniques, in general, are not effective against novel attacks without any matched rules or patterns [6]. Traditionally the IDS are classified as either network-based or host-based. Network-based systems control and monitor the network traffic and identify packet transmissions for any suspicious behavior. On the other hand Host-based systems are made for single hosts, and operate on system data of low label, such as patterns of system calls, file access, or process usage. They can monitor for suspicious behavior, or they can scan configurations to detect potential threats [6] [7]. The existing IDS models have same features: (1) a database containing few thousand patterns, of different lengths, and (2) the patterns may be seen anywhere in any packet payload. For instance, Snort is an open-source (NIDS), Network-based Intrusion Detection System which has proven utility to listen in packets on a network link, characterize anomalous intruder behavior with a set of patterns, and generate logs and alerts by predefined actions [8].

3. Agent Based IDS

The performance of IDS can be increased by using an agent. Agent Based IDS has following advantages which are following [10]:

- Decrease Network Flow: the process functions of central node to network nodes are distributed by systems and computed by agents in network nodes. Malicious data package can be identified by system and send computing result to other nodes in network if there is abnormal information in data flow.
- Improvement Autonomous Computing and Adaptation Capacity: Agent is autonomous independent unit. Other agents remain effective even though a few agents do not work for some reasons.
- Platform Irrelevance: agent based on IDS can work in diverse environment and implement interoperation on the application layer for agents are independent of the computer and transformation layer and work in nodes with agent.
- Better Maintainability: Agent can response network topology dynamic changing as system can independent start and stop agent so IDS is configured dynamically.

4. Mobile Agent

Mobile Agent is a self-contained and easily detectable computer autonomous program, outfitted with their code, data, and execution state that can move within a heterogeneous network of computer systems [9]. Such agents are useful in various industrial applications like automation of spacecraft, game playing, steering cars, medical diagnosis, robotics, language understanding and problem solving. Following are the advantages of using mobile agents in IDS [9].

- Overcoming Network Latency
- Reducing Network Load
- Autonomous Execution
- Platform Independence
- Dynamic Adaptation
- Static Adaptation
- Scalability

5. Related Work

The use of mobile agent in computer networks has proved its utility and being used extensively in computer networks to detect threats. There are many present mobile agent based intrusion detection systems (IDS) are lagging behind due to its bed response time and big size [10]. Description of existing mobile agent based intrusion detection system is as followed:

- [11] described the prototype of an agent. This prototype used with HSA. The prototype makes use of both anomaly and misuse based models. The normal range of values for a selected set of system parameters is stored here. It also collects signatures of different attacks. At the time of scan, the agent verifies the log file and identifies the parameters which are outside the range of normal values. Then the lists of parameters which have abnormal values are matched against the signature of known attacks in order to identify the types of attack [11].
- [12] represents the multi-agent design that uses distributed IDS based on ACC to identify a new and coordinated attack, and the movement of large data handling, capabilities of synchronization, the cooperation between components without the presence of centralized computing components, good detection performance to turn on warning alarm in real time. ACC is very fruitful to be applied in the method of detection of attack. To represent large dimension of data clustering process into a two-dimensional grid space, also create chances in process of controlling to improve ACC performance further on its application in the Distributed IDS. ACC as a metaphor is able being controlled and is designed its behavior as per the needs in this case the application of DIDS. Its Ability of clustering data without guiding, movement in the unlimited search space, patterns of movement can be controlled, is used to create clusters of different types of data for normal and attack connections.
- [13] proposes a multilayer technique with a Multi-agent and multilevel technique. In the 1st level the information is collected then this information is divided among the multiple agents. They have their own rule to verify this. Now in the 2nd level resulting information are gathered and pass it to the different layers such as application, session and transport. Then in the 3rd level another algorithm is detect the intrusion by agent. The benefit of multilevel detection process here is that detection is error free and all the low-level and high level intrusion is detected by the different level. In this system the attacks are completely discussed and detected.
- [14] presented a multi-agent based approach to generate an Intrusion Detection System (IDS) using data mining concept. IDSs based on Data mining have demonstrated a considerable accuracy, good generalization to novel types of intrusion, and robust behavior in an environment changing permanently. Development of IDS using the agent technology has many advantages such as add or remove the agents without changing other system components, modifying the agents to latest versions without affecting the rest of the system, the capacity of transfer information between groups of agents, obtaining more complex results than any one of them could obtain on its own. Finally intrusion detection system obtained as a result of intelligent agents and data mining techniques combination can be utilized with significant results to enhance the immunity of computer systems/networks. The framework shown here should be considered a step forward towards a complete multi-agent based system for the purpose of network security
- [15] described a simple system based on multi agents for Intrusion Detection, utilized to run on general purpose devices such as web servers, this system with considerable knowledge is capable to detect port scans

and "syn" attacks against a specific port, and it is capable to perform actions to prevent the suspicious attack. Also, by using its feature of mobility which is characteristics to mobile agents, the system has capability to protect several hosts in a small time frame, by triggering agents which go onto the hosts and reply the protection actions has done on the place where the attack was detected initially.

- [16] proposed a mixed approach depending on the mobile agents for the detection of intrusion (HAMA-IDS). The design of the system allows the treatment of information directly to the place where it is present via the utilization of mobile agents (aglets). Thus, the method is based on the platform Aglets for the creation and distribution of agents. These last ones can move from one post to other to analyze packets collected by the collector agents. The hybrid analysis is assured by the analyzers and redirectors agents, so that possible attacks could be detected. The proposed approach has the following postulates [16]:

o The application for detection of intrusion by mobile agents for the detection of intrusion allow distribution of the Intrusion Detection system (IDS) (distinct from the centralized systems)

o The use of a mixed approach make use of both type of intrusion detection (scenario and behavioral method)

o The platform Aglets allow of this method to be use as a manager of the mobile agents and for their distribution.

- In [17], intrusion detection model based on multi-agents uses four kinds of agents are defined in this system, which are organized in a particular structure. The basic agents in every host or at the beginning of subnets are usually responsible for performing the simple detection and some separate coordination agents performs the response task; they are also responsible for analyzing the suspicious behavior synthetically that is not possible by lower level agents. Coordination agents are also capable to assign the task to the lower-level associated agents. Based on the hierarchical structure, the general description of the model is given. By adaptable protocols and association among some elements, this model provides dynamic adaptability to the changing environment and attacks. Apart from this the concept of coordination domain which facilitates the management of collaborative detection is also proposed. The model provides a theoretical foundation for creation of dynamically adaptive intrusion detection system.
- [18] is multi-agent based technology and designs an adaptive distributed IDS model. It has good adaptive capacity and grater response and treatment on the network environment and arbitrary attack methods, also utilizes various data mining algorithm with linking detection mechanism to void the new invasion behavior. The latest mechanism of rule library adopts LFU for the goal of elimination of pervious rules; efficiently customize the misuse detection of matching speed. Meanwhile, the source of alarm, secondary detection can effectively avoid the many times alarm phenomenon caused by the same attack, it can also reduction the rate of wrong alarms. When the system is attacked or collapsed, dynamic election algorithm of management agent with the improved algorithm Bully timely recovery system, make the simple operation of the system has good anti-destruction ability and self-restoration ability.

Based on the characteristic in the categorization of IDS using mobile agent, **Table 1** summarizes analysis report of existing MA-IDSs.

From the **Table 1** we can improve existing intrusion detection system using mobile agent by focusing on implementation of LSA and MSA for the agents and compare the performance of LSA, MSA. Designing IDS agent is in a distributed network, which communicates using a framework of Cooperative agent using interest. Implementations of hybrid IDS can be raise the detection rate of intrusion. Increase the full Architecture of the system, by granting fault tolerance in Control component, secured communication distribution across a network. Provide batter security of agents over network. The latest way of rule library adopts LFU for the purpose of elimination of past rules; efficiently update the misuse detection of matching speed which can be increase the efficiency of exiting intrusion detection system.

6. Conclusion

Literature survey of mobile agent based existing intrusion detection system using their calculative analysis and the big issues has been presented. On the basis of type of intrusion detection system, comparative analysis of various IDS using mobile agents based has been done. Different characteristics like the technique (NIDS, HIDS or Hybrid), behavior layer, detection techniques for analysis, uses of mobile agent and technology used by existing IDS, detailed comparative analysis is shown in **Table 1**. From **Table 1** we have observed that some of the existing techniques are used in IDS which causes low detection rate, behavior layers like TCP connection for

Table 1. Analysis report.

Model Mobile	Nids, hids or hybrid	Behavior layer	Detection technique	Mobile agent	Technology	Strength
Banik, s.m.; pena, l-2015	Nids	Tcp Connection Based	Scanning Algo.	Deploying Agents.	Heavy Scan algorithm (hsa), medium scan algorithm (msa), And light scan algorithm (lsa)	Detect the Distributed Attack
Abdurrazaq m.n., bambang r.t., rahardjo b.-2014	Hybrid	(foraging Behavior)	Agent based on ant colony clustering	Jade (java agent development Environment) cooperative agent	Clustering	Recognize a new And coordinated attack,
Biswas, a.; sharma, m.; poddder, t.; kar, n.-2014	Hybrid		Multi-agent based detection	Coordination agent Monitoring agent	Multilayer technique	Less time is to be taken to detect Intrusion.
Ionita, i.; ionita, l.-2013	Hids,nids	Tcp Connection Based	Multi Agent based with data mining	Classification agent	Intelligent agents and data mining framework g	Hybrid intrusion detection system improving the immunity of computer systems/networks.
Gutierrez, s.a.; branch, j.w-2013	Hids		Multi-Agent based ids	Jade (java agent development Environment) cooperative agent triggering agents	Jade platform was used to establish the multi-agent Platform.	Very desirable Having more robust analysis mechanisms to provide Pro-activeness in attack detection, and even prediction from the analysis of collected data related to previous attacks.
Djemaa, b.; okba, k-2012	Hybrid	Tcp Connection Based	Hama-ids	Mobile agent (aglets) Generator agent Collector agent Analyzer agent Redirector agent	Hybrid approach based on The mobile agents	Hybrid intrusion detection system improving the anomaly detection rate
Zhang ran-2012	Hybrid		Collaborative Detection; coordination domain	basic agents Coordination agent interface agents	Collaborative intrusion Detection model based on multi-agent	Provides dynamic adaptability to the changing environment and attacks.
Huailin; Tianmao; qingfeng; yangbin-2011	Not Specified		Multi-agent technology	Management agent	Adids (adaptive distributed Ids model based on multi-agent.)	It has better adaptive capacity and better response and treatment on the network environment and changeful attack methods

packet capturing which is the most important activity in NIDS and response time (technology execution time) with memory consumption by mobile agent as major issues. In the future we will implement a technique or suggest some specific solutions to conquer these issues.

References

[1] Steven, C. (2015) Morgan Editors Cyber Security Ventures. http://cybersecurityventures.com/cybersecurity-market-report/

[2] Du, X.F. and Qiang, Z.X. (2010) A Model of Intrusion Detection System Based on Aglet with Multi-Agent. *International Conference on Computer Application and System Modeling* (*ICCASM*), Volume: 6, Taiyuan, 22-24 October 2010, V6-232-V6-234. http://dx.doi.org/10.1109/ICCASM.2010.5620503

[3] Huang, W., An, Y. and Du, W. (2010) A Multi-Agent-Based Distributed Intrusion Detection System. 3*rd International Conference on Advanced Computer Theory and Engineering* (*ICACTE*), Volume: 3, Chengdu, 20-22 August 2010, V3-141-V3-143. http://dx.doi.org/10.1109/ICACTE.2010.5579686

[4] Wang, Y., Cheng, X. and Wang, S. (2011) Anomaly Network Detection Model Based on Mobile Agent. 3*rd International Conference on Measuring Technology and Mechatronics Automation* (*ICMTMA*), Volume: 1, Shanghai, 6-7 January 2011, 504-507. http://dx.doi.org/10.1109/ICMTMA.2011.128

[5] Dong, H., Xu, T., Wu, Q. and Liu, Y. (2011) Research on Adaptive Distributed Intrusion Detection System Model Basedon Multi-Agent. *IEEE International Conference on Computer Science and Automation Engineering* (*CSAE*), Volume: 1, Shanghai, 10-12 June 2011, 182-185. http://dx.doi.org/10.1109/CSAE.2011.5953199

[6] Hancock, D.L. and Lamont, G.B. (2011) Multi Agent System for Network Attack Classification Using Flow-Based Intrusion Detection. *IEEE Congress on Evolutionary Computation* (*CEC*), New Orleans, 5-8 June 2011, 1535-1542.

[7] Brahmi, I., Yahia, S.B. and Poncelet, P. (2011) A SNORT-Based Mobile Agent for a Distributed Intrusion Detection System. *Proceedings of the International Conference on Security and Cryptography* (*SECRYPT*), IEEE Conference Publications, Seville, 198-207.

[8] Wang, J.-H., Dong, Y.-F. and Liu, H.-F. (2012) On Intrusion Detection Matching Algorithm from the Perspective of Multi-Agent. *International Conference on Machine Learning and Cybernetics* (*ICMLC*), Volume: 2, Xi'an, 15-17 July 2012, 601-606. http://dx.doi.org/10.1109/ICMLC.2012.6358991

[9] Patil, T.T.K. and Banchhor, C.O. (2012) A Survey on Mobile Agent Based Intrusion Detection System. *International Journal of Advanced Research in Computer and Communication Engineering*, **1**, 773-777.

[10] Shah, B. and Trivedi, B.H. (2015) Improving Performance of Mobile Agent Based Intrusion Detection System. 5*th International Conference on Advanced Computing & Communication Technologies* (*ACCT*), Haryana, 21-22 February 2015, 425-430. http://dx.doi.org/10.1109/acct.2015.118

[11] Banik, S.M. and Pena, L. (2015) Deploying Agents in the Network to Detect Intrusions. *IEEE*/*ACIS* 14*th International Conference on Computer and Information Science* (*ICIS*), Las Vegas, 28 June-1 July 2015, 83-87. http://dx.doi.org/10.1109/ICIS.2015.7166574

[12] Can, O. (2014) Mobile Agent Based Intrusion Detection System. 22*nd Signal Processing and Communications Applications Conference* (*SIU*), Trabzon, 23-25 April 2014, 1363-1366. http://dx.doi.org/10.1109/SIU.2014.6830491

[13] Abdurrazaq, M.N., Bambang, R.T. and Rahardjo, B. (2014) Distributed Intrusion Detection System Using Cooperative Agent Based on Ant Colony Clustering. *International Conference on Electrical Engineering and Computer Science* (*ICEECS*), Kuta, 24-25 November 2014, 109-114. http://dx.doi.org/10.1109/ICEECS.2014.7045229

[14] Biswas, A., Sharma, M., Poddder, T. and Kar, N. (2014) An Approach towards Multilevel and Multiagent Based Intrusion Detection System. *International Conference on Advanced Communication Control and Computing Technologies* (*ICACCCT*), Ramanathapuram, 8-10 May 2014, 1787-1790. http://dx.doi.org/10.1109/icaccct.2014.7019417

[15] Ionita, I. and Ionita, L. (2013) An Agent-Based Approach for Building an Intrusion Detection System. *RoEduNet International Conference* 12*th Edition on Networking in Education and Research*, Iasi, 26-28 September 2013, 1-6. http://dx.doi.org/10.1109/RoEduNet.2013.6714184

[16] Gutierrez, S.A. and Branch, J.W. (2013) A Preliminary Application of Mobile Agents to Intrusion Detection. 47*th International Carnahan Conference on Security Technology* (*ICCST*), Medellin, 8-11 October 2013, 1-4. http://dx.doi.org/10.1109/ccst.2013.6922045

[17] Djemaa, B. and Okba, K. (2012) Intrusion Detection System: Hybrid Approach Based Mobile Agent. *International Conference on Education and e-Learning Innovations* (*ICEELI*), Sousse, 1-3 July 2012, 1-6. http://dx.doi.org/10.1109/iceeli.2012.6360647

[18] Ran, Z. (2012) A Model of Collaborative Intrusion Detection System Based on Multi-Agents. *International Conference on Computer Science & Service System* (*CSSS*), Nanjing, 11-13 August 2012, 789-792. http://dx.doi.org/10.1109/csss.2012.202