Parallel Component Agent Architecture to Improve the Efficiency of Signature Based NIDS

Hafiz Gulfam Ahmad Umar, Chuandong Li, and Zeeshan Ahmad

***Abstract*—To avoid increasing threats of intrusion or vulnerabilities, networks require flexible and efficient security systems. Intrusion detection system (IDS) is the basic component of any network defense scheme. Different IDS use several techniques for Intrusion detection. Signature base detection techniques are widely used in networks for fast response to detect threats. Regarding the intrusion detection technique, one of the main challenges is to control the huge traffic volume where each packet needs to be compared with the known signature database and reduce the comparison time of signatures in it. In this paper we analyze different techniques and proposed a new architecture that can handle the attacks by using multiple agents with small databases at high success rate by dynamically updating the signature database. Proposed method reduces the IDS processing time and improves its efficiency.**

***Index Terms*—IDS, signature base, agent.**

I. Introduction

Networks Security threats become more common on networks, so IDS are now transforming from host base IDS to Network based IDS. Detection at network level is a difficult task because at network level the amount of audit data is more as compared to the host level and events related to a same intrusion can be visible at different nodes on network [1]. Network IDS are the first defense line of any network, and to monitor the network traffic becomes more complicated and thorny as the new vulnerabilities and intruders enters the system. These issues become more compounded because of such sites that contain malicious code [2].Symantec report 2011 indicates that Symantec had blocked a total of over 5.5 billion malware attacks in 2011, an 81% increase over 2010, and Web based attacks increased by 36% with over 4,500 new attacks each day. 403 million new variants of malware were created in 2011, a 41% increase as compared with 2010 [3].

In the increasing complexity of today's computing environment Intrusion detection system become a key component for system security threat landscape. Recently the information security research has been focusing much attention on the Intrusion detection system. Intrusion detection is defined as the process of identifying unauthorized use, misuse, and abuse of the computer system [4].To act appropriately against the attacks, currently security solutions are relying on the intrusion detection system. To detect the pattern and signatures of these malicious worms attacks normally IDS parameters divided into signature based or misuse detection and anomaly based systems [5]. Signature base intrusion detection system defines the set of rules that are used to recognize the given pattern by intruder. The main advantages of Signature base system are effective and accurate results against the known security threats and minimize the false positive for intrusion identification [2]. The less fortunate ramification of this technique is that a detection system is incapable of detecting intrusions that are not present in its knowledge base. The other drawback of this technique is that if there is a little change in known attack, it will affect the analysis and identification when the detection system is not updated [6].

For effective intrusion detection, system needs some significant resources such as SNORT. It is an open source network-based intrusion detection system (NIDS) performs real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching, and content matching. The program can also be used to detect probes or attacks, but not limited to stealth port scans [7]. Mostly Snort used the signature header and its option used to determine that Network traffic is corresponds to a known signature or not [8].

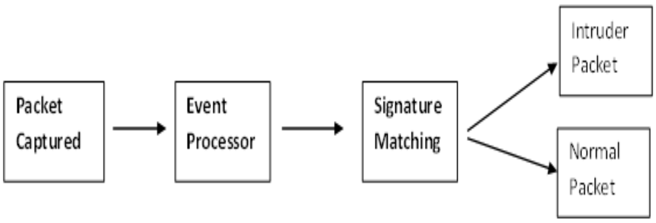

Fig. 1. Signature based IDS working mechanism.

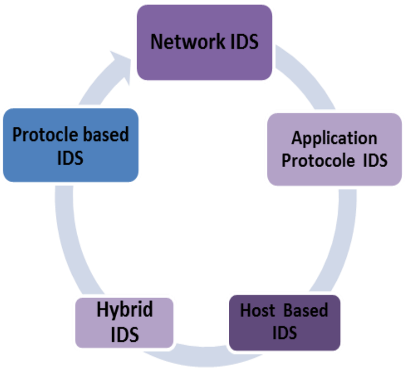

Fig. 2. Types of IDS system.

Fig. 1 shows the working mechanism of signature based

Manuscript received January 12, 2014; revised March 24, 2014.

Hafiz Gulfam Ahmad Umar is with the College of Computer Science, Chongqing University, Chongqing, 400044, China (e-mail: gulfamahmad@uaf.edu.pk).

Chuandong Li is with the College of Computer and Information Science, Southwest University, Chongqing, 400044, China (e-mail: cdli@swu.edu.cn).

Zeeshan Ahmad is with the School of Communication Engineering, Chongqing University, Chongqing, 400044, China (e-mail: engr.zeeshan@hotmail.com).

DOI: 10.7763/JACN.2014.V2.124

intrusion detection system where the recognized captured packets are compared against the intruder packets. Widely deployed intrusion system needs to match the packet header against thousands of header rules defined by the attacking signatures that is an expensive task as compare to typical header processing [9]. Network IDS scan the network traffic and monitors multiple hosts. Protocol Based IDS work on certain protocol(s) for a specific service. Application Protocol IDS monitors the dynamic behavior and state of the protocol. Host-Based IDS monitors and analyzes the internals of a computing system. Hybrid IDS combines one or more approaches and provide multiple protection mechanisms. Prelude Hybrid IDS is the example of the Hybrid IDS. Fig. 2 depicts different types of IDS.

In order to protect the network, we consider the ways of boosting the IDS performance and its efficiency. In this process we argue that the agent based framework is highly efficient to boost the system performance.

II. Related Work

In network intrusion detection one of the most important weaknesses is the processing of whole network traffic that is a time consuming job. The network speeds rises day by day, so need of efficient intrusion detection techniques that reduce the processing time for more traffic emerges. To solve this problem different researchers give different techniques and IDS models. Ref. [5] proposed a dynamic multilayer signature based IDS by using mobile agents, where each packet is compared with the database that can slow down the detection process. The other problem in this approach is the introduction of new services and need of a network administrator who manually updates or adds the signature. This process is error prone to overcome. The researcher have proposed a new model by using mobile agents that focus on dynamic and automatic use of small and efficient multiple databases. These databases are updated by mobile agents at particular interval of times.

Ref. [10] proposed a survival architecture that introduces network intrusion detection system which used packet splitter to send every packet to every node and its two major analysis methods. WinPlap used as a tool in the present scheme, which capture network traffic in windows environment. Packets are distributed between sensors on their ports numbers, to detect attack from the depicted packet. Generate alerts on attack recognition; otherwise pass the packet to distribution. But this model has several inabilities like many sensors are required if the traffic increases and there is no mechanism to update the signature information. Sensor recognized the attack that aimed specific port numbers and there is no string matching algorithm is used here in above scheme.

Ref. [11] performed a great job in this regard especially improving the content matching algorithm which is the intensive task for signature base IDS and parallel processing at component level and the sub component level.

Ref. [12] proposed an Intrusion detection design that use capture module and Packet pre-processor module categorized the packet and then pass it to the Intrusion detection module. They proposed an algorithm by using multithreading techniques which count the 1 ton number packets that handled under a single thread. After every n packets, a new thread is generated and so on. They suggest an agent that depicts three modules, frequently attack database detection and updating module also enhance the architecture at distributed network intrusion system. In this model the researcher suggest that this will improve the efficiency of the intrusion detection by using multithreading technique but each packet that is captured will be compared with every signature in database to detect intrusion attack, that is a time consuming process. This can slow down the intrusion detection process because of huge load of Network traffic.

The present intrusion detection system either they are commercial base or research base mostly used the hierarchal structure that has host based and network based characteristics. We used agents in our proposed architectures so it is necessary to give the brief introduction of agents. We can define agent as an application that can run automatically, a predefined goal such as monitor an environment and then generate alerts based on given instructions [13]. In IDS they are used as monitors that can retrieve information for analysis to generate real time alerts. This research paper presents an efficient scalable architecture for host and network based intrusion detection system.

The remaining paper proceeds as follows. Second section present the related work and section three show the architecture of the proposed IDS. In Section IV the performance of the proposed system is analyzed by experimental work and last section offer some conclusion based on proposed architecture and some future work.

III. Proposed Architecture

The proposed architecture is shown in Fig. 3. It develops a framework by combining the two approaches, multithreading [11] and parallelizing IDS [12]. The main focus of the research is how to reduce the time needed to compare the signatures and update the small databases in agents. We use a duplicator module, UDP packet duplicator which is used to send same packet to every agent. Instead of the UDP packet duplicator it is possible to use a system with Linux. The Linux kernel version 2.6.35 introduces a new configuration option CONFIG_NETFILTER_XT_TARGET_TEE:

This option adds a "TEE" target with which a packet can be cloned and this clone can be rerouted to another next hop.

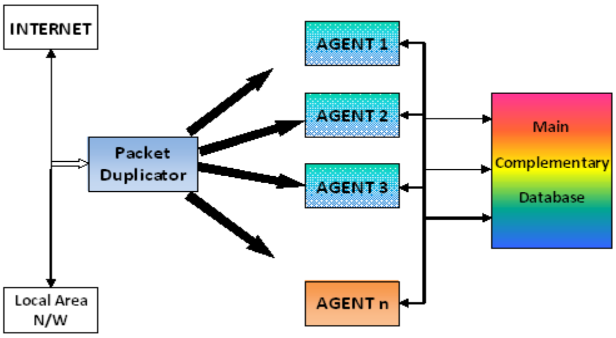

Fig. 3. Proposed architecture model for intrusion detection.

By using this method, agents can detect intrusions more quickly by comparing each network packet with the small agent's databases. Then agent follow the complete process, compare the signature in the frequent database, in positive case packet will be intruder and in negative case the packet is considered to be a normal packet. But the main challenge is how to update the database of agents and maintain the complementary main server databases.

In our proposed study we divide the main database in small databases. These small databases connected with a complementary database on the server. We use agents as the main entity in this model. While there are multiple definitions of agents, their essential characteristic in intrusion detection is that agents are software computing entities that perform intrusion detection tasks autonomously and need to be able to affect environment using some type of predefined mechanisms [13]. The proposed architecture is flexible, we can increase or decrease the number of agents depends on the network traffic. In agent architecture, intrusion detection module takes packet as input and extracts the signature and compares it with available signatures in the small databases. If there is any match occur the input packet consider as the intruder and create the log record of that intrusion packet at the main server database, generate alarm and send request to the proxy server block the traffic. If there is no match, the packet is considered to be a normal packet and passed to the network. The second module is SSD update module which updates the small signature databases that depends on the algorithm based on different parameters like most frequent attacks and log record and the age of the signature alert. The updating module is responsible to update the small databases from the main server database.

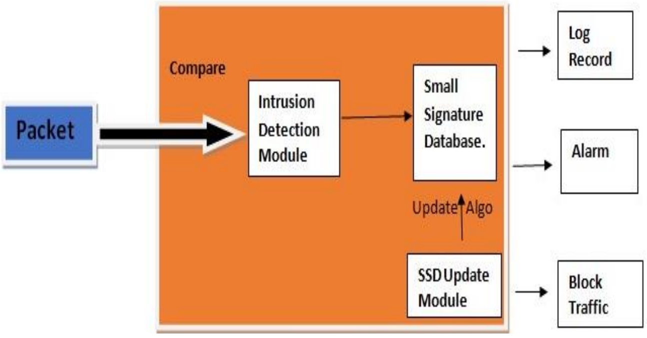

Fig. 4. Agent architecture.

Fig. 4 represents the structure of agent deployed in intrusion detection system. The agent consists of Capture module, signature database with an update algorithm. For the implementation of any architecture in real time many challenges involves. Some of these challenges were resolved and some remain still unsolved for future work. For prototype model we choose snort as our signature database platform, and configure the snort with the My SQL.

TABLE I: DESCRIBE THE PORT AND RULES SET

Agent Number	Destination Ports	Rules.
Agent 1	53,80,110,143	1 to 200 rules
Agent 2	23,3306,22	200 to n rules

Table I describes the parameters which are used in experiment. It shows that two agents will be used with mentioned destination ports and number of rules.

IV. EXPERIMENTAL SETUP AND RESULTS

The experiment is performed by choosing two agents with specific number of signature rules in small databases, each one is the Intel Corei3 with 4 GB RAM, Linux as operating system for sending duplicate packets and two others with windows environment. Snort is used as the signature based intrusion detection platform and BASE is used as security analyzer. All the alerts are stored in MYSQL database. To check the performance of the proposed architecture, during a period of time we used IDS wakeup [14] which is designed to test the functionality of the intrusion detection system by generating some common attacks. Two agents work in parallel to detect the attack and we can increase the number of agents according to our network traffic load. In this task we select the ports for both agents 53 for DNS server, 80 for HTTP and 110 for POP3, and for agent 2 we select the ports 3306 for MySQL, 23 for Telnet. And packets are sent to agents, selected ports are open as listed in Table II and all other ports are stopped by using firewall. Number of agents can be increased or decreased in both manual and automatic fashion. In manual alteration of number of agents, the administrator will be the sole decision maker to alter the number of agents according to the network traffic. In the second case, if we want the number of agents to be changed automatically, some algorithm should be deployed to make changes according to traffic load. Suppose for n packets there is one agent, if the number of packets increases to 2n the algorithm add a second agent and so on.

TABLE II: SIGNATURE DETECTED

Signature Name	Description	Type	Attack
Rob Nets can Host	ABB Products Stack Buffer Overflow	App	14
CHAT: AIM: FILE	AIM: Client File Receive Executable	Chat	22
DB: DB2: CONNECT-DOS	DB: IBM DB2 Database Server CONNECT Request DOS	DB	10
DDOS: DIRTJUMPER	DDOS: Dirt Jumper C&C Communication	DDOS	50
FTP:AUDIT : COMMAND FAILED	FTP: Command Failed	FTP	10
TCP: AMBIGUOUS-T OOBIG	TCP: Options Error WSF Too Big	TCP	26
TROJAN: INFECTOR: CLIENT-REQ	TROJAN:Infector: Client-Request	UDP	35
Rob Nets can Host	ABB Products Stack Buffer Overflow	App	14

To check the performance of the proposed architecture, the packets from the duplicator module are forwarded to each agent database for processing and the results are sent to the central complementary database server. We check the processing time of sending one file consists of 489856 packets, the protocols HTTP, POP3, IMAP, SMTP with telnet, MySQL database and SSH. By packet duplicator the copy of each packet is sent to agent 2 for processing. Firstly agent 1 database compares the packets signature with their small database consist of the snort rules given range of protocol and at the same time the copy of same packet is processed by the agent 2 database in similar way. Hence, the time period of comparing the packet with all the signatures in one database is 0.573100 seconds. As the comparing process is done simultaneously in both agents databases, so the maximum time to process the packet with all the signatures of two databases is 0.573100 seconds. Now if a packet matches with a signature in any database early at any time instant, then the time consumed will be less than 0.573100 seconds. Now we compare it with the traditional technique by single database that consist entire set of rules and send the same file for processing it consume the time 1.14620 seconds which is double as compare to our proposed methods. The result of signature detected show in the Table II.

V. Conclusion

Today's security infrastructure has several shortcomings when dealing with the complexity and subtleties of a new generation of cyber-attacks. In this paper we introduce a new parallel agent based model for intrusion detection by using the agents to improve the performance of signature base IDS that can be increased or decreased according to the network traffic. The experimental results proved that, by using this method we can reduce the processing time of signature database by 1/n times for n databases as compared to the conventional technique which use a single database. For future work our proposed system can be improve as more comprehensive and automated system by enhance the database updating on behalf of the frequency and appearance of the threats. It can also be investigated in the design and algorithms to improve the real time security and reduce the false alarm

Acknowledgment

The authors are grateful to Talha Akram, Sajjad Haider and Abu Bakar Sidique (PhD Scholars, Chongqing University) for their invaluable support during this research work. The authors are also thankful to all the reviewers for their kind guidance to make this work more perfect.

References

[1] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, “Network intrusion detection,” *Network*, IEEE, vol. 8, no. 3, pp. 26-41, May-June 1994.

[2] R. Srivastava and V. Richhariya, “Survey of current network intrusion detection techniques,” *Journal of Information Engineering and Applications*, vol. 3, no. 6, pp. 27-33, 2013.

[3] The Symantec Internet Security Threat Report. (2011). [Online]. Available: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=threat_report_17

[4] J. Allen, A. Christie, W. Fithen, J. Mchugh, and J. Pickle," State of the practice of intrusion detection technologies," Technical Report. CMU/SEI-99-TR-02S ESC-99-02S, Networked Systems Survivability Program, January 2000.

[5] M. Uddin, K. Khowaja, and A. A. Rehman, "DyanmicMulti layer signature based intrusion detection system using mobile agent," *International Journal of Network Security & Its Application*, vo1. 2, no. 4, pp. 129-141, October 2010.

[6] D. J. Brown, B. Suckow, and T. Wang. A survey of intrusion detection systems. Department of Computer Science, University of California, San Diego, CA, the United States. 2002. [Online]. Available: http://charlotte.ucsd.edu/classes/fa01/cse221/projects/group10.pdf.

[7] Snort-Home page. The software snort. (2013). [Online]. Available: https://www.snort.org/

[8] D. Stiawan, A. H. Abdullah, and M. Y. Idris, "The trends of intrusion prevention system network," in *Proc. 2010 2nd International Conference on Education Technology and Computer (ICETC)*, vol. 4, pp. 217-221, June 2010.

[9] I. Charitakis, K. Anagnostakis, and E. Markatos, "An active traffic splitter architecture for intrusion detection," in *Proc. 11th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer Telecommunications Systems*, MASCOTS 2003, pp. 238-241, Oct. 2003.

[10] F. I. Shiri, B. Shanmugam, and N. B. Idris, "A parallel technique for improving the performance of signature-based network intrusion detection system," in *Proc. 2011 IEEE 3rd International Conference on Communication Software and Networks* (*ICCSN*), May, 2011, pp. 692-696.

[11] P. Wheeler and E. Fulp, “A taxonomy of parallel techniques for intrusion detection,” 2007, in *Proc. the 45th Annual Southeast Regional Conference*, New York, NY, USA, pp. 278-282.

[12] D. P. Gaikwad, P. Pabshettiwar, and P. Musale, “A proposal for implementation of signature based intrusion detection system using multithreading technique,” *International Journal of Computational Engineering Research*, vol. 2, no. 7, pp. 59-65, November 2012.

[13] R. A. Wasniowski, “Multi-sensor agent-based intrusion detection system,” in *Proc. the 2nd Annual Conference on Information Security Curriculum Development* (*InfoSecCD '05*), ACM, New York, NY, USA, 2005, pp. 100-103.

[14] S. Aubert. IDSwakeup. (2000). [Online]. Available: http://www.hsc.fr/ressources/outils/idswakeup/index.html

Hafiz Gulfam Ahmad Umar was born in Pakistan, in 1984. He received the B.S and M.Sc degrees in computer science and information technology from Bahauddin Zakarya University Multan, Pakistan, in 2003 and 2005 respectively. He is currently pursuing PhD in computer science at Chongqing University, Chongqing, China.

From 2007 onwards he is serving as a lecturer in Agriculture University Faisalabad. His research interest includes data mining, information security and cloud computing.

Mr. Umar is a recipient of Chinese Government Scholarship for PhD in computer science from Chongqing University, P. R. China.

Chuandong Li was born in Shandong province, P. R. China. He received his bachelor degree in mathematics and statistics from Sichuan University China in 1992, master degree and Ph.D in mathematics research & cybernetics and computer software and theory from Chongqing University China in 2001 and 2005 respectively.

He is currently engaged as a professor of computer software and theory, control science and engineering, computational mathematics at Southwest University Chongqing, China. He is reviewer of international journal of IEEE TNN, IEEE TAC, IEEE TCAS, IEEE TSMC_B, CHAOS, IET Control Theory and Applications, International Journal of Control, Physica A, Physics Letters A, International Journal of Robust and Nonlinear Control, Neuro computing, International

Journal of Bifurcation and Chaos and served in program committee of several international conferences (WCICA'08, IJCNN 2008, ISNN2008, ICIA2008, ICWAPR2008, ICCCA2008 etc. He is the author of more than 70 SCI papers (first author: 32). His research interest includes delay system dynamics, chaos synchronization and application, theory and application of impulse control, hybrid systems, iterative learning control, and pattern recognition.

Dr. Li was awarded by Chongqing Municipal Natural Science Award, Chongqing outstanding doctoral dissertation and the Ministry of Education for New Century Excellent Talents plan in 2006.In 2007 he was nominated for The National Excellent Doctoral Dissertation Award and in April 2008, he was selected for fourth Chongqing young teacher.

Zeeshan Ahmad was born in Pakistan, in 1988. He received the B.E. degree in electrical (telecom) engineering from the Bahria University Islamabad, Pakistan, in 2011. He is currently pursuing M.E. degree in electronics and communication engineering at Chongqing University, Chongqing, China.

From 2010 to 2012 he worked in telecom sector on CMPAK SDR swap and expansion project of ZTE and on Huawei-Telenor Pakistan MS project. He is the author of one conference publication. His research interest includes array signal processing, radars, adaptive arrays, GPS and satellite navigation systems.

Mr. Ahmad was the recipient of 1st position holder award in secondary school certificate examination in 2004 and the Chinese government scholarship for M.E degree in Chongqing University, China in 2012.