International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 24 Issue 8 – MAY 2017.

DISCOVERY OF MALWARE PROPAGATION ATTACK USING MULTIVARIATE CORRELATION ANALYSIS

DEVALLA SRI MAHALAKSHMI MANIKYAMBA [#1] and R.CHANDRA SEKHAR [*2]

[#] *PG Scholar, Kakinada Institute Of Engineering & Technology Department of Computer Science & Engineering , JNTUK,A.P, India.*

[* *] *Assistant Prof, Dept of CSE, Kakinada Institute of Engineering & Technology, JNTUK, A.P, INDIA.*

***Abstract*— A recent development in enterprises is growing with high number of customized users. As the number of user's increases, the size of network channels also increases. In some scenario, the user may be normal or malicious users. Some target based attacks are performed to degrade the server's performance. Differ from traditional attacks, these sort of targeted attacks are defined by the experter's and network traces are used for detecting the attacks. In this paper, we propose multivariate correlation analysis to detect the target based attack, named malware propagation attack. The geo-positions of the users are estimated for detecting the attacks. Experimental design shows the efficiency of the system.**

***Index Terms*— Network security, malware, targeted attacks, multivariate correlation analysis and malicious users.**

I. INTRODUCTION

With the evolution in network security, the mobile devices such as mobile phones, personal digital assistants, net books and tablets are widely connected [1]. Generally, network is defined as the collection of two or more networks that are combined together. There are different kinds of networks, but computer networks are widely studied by the researchers. The computer networks are mainly used for exchanging the information. The ingress data are transformed into packets. Then these packets are transferred to the network channel. The network connections are mainly by associated wires. Computer networks differ in the transmission media used to carry their signals, the communications protocols to organize network traffic [2], the network's size, topology and organizational intent. In most cases, communications protocols are layered on (i.e. work using) other more specific or more general communications protocols, except for the physical layer that directly deals with the transmission media. Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications [3].

Presently, the malicious activities are handled using two approaches. These are categorized into features based on their malicious activities. Traditional methods [4] were designed based on signature based detection approach. Some techniques are designed by creating signatures. If doesn't meet the requirements of the malicious, then it is known as zero day attacks. If any new malicious activity is found, it is matched with instances and new signature is generated. Knowing the weakness of detection systems malware designers developed code obfuscation techniques like code reordering, garbage insertion, variable renaming to disguise their content [5].

The rest of the paper is organized as follows: Section II describes the related work; Section III discusses about the proposed work; Section IV describes the experimental results of the proposed work and at last concluded in Section V.

II. RELATED WORK

In order to detect the attacks in the medical field, various techniques have been studied. In this section, we describe about the established techniques. Let us review about the categories presented in Intrusion Detection Systems. The categories in IDS are listed as follows:

a) Host based IDS: Host based interruption identification framework is utilized on the gadget that is being checked. It comprises of operators who are dependable to recognize interruptions by checking the logs, framework calls or any changes to the record frameworks.

b) Network based IDS: This method screens the continuous activity on the system to distinguish any live aggravations or infiltration endeavors. This requires a NIC card to catch and screen all activity that passes through the system. It thus contains a sensor module fit for breaking down a positive match with any danger designs inside its database.

c) Signature based IDS: Signature based interruption location takes a shot at predefined marks. This system is proficient for assaults that is already been known and assist relies on upon ceaseless redesigning of its signature databases. The weakness

of this framework is that it purposely comes up to obscure the assaults.

d) Behavior based IDS: Behavior or Anomaly based interruption location framework is equipped for distinguishing obscure assaults and assailant designs. The real burden of such frameworks is characterizing its gadget on its host.

Shuyuan Jin et al investigated Multivariate Correlation Analysis to detect the SYN flooding attacks. It effectively identified the normal and traffic creating attacks. According to the variant intensities, the behavior pattern of unknown attacks is effectively monitored. The linear complexity of the method makes its real time detection practical. *Mihui Kim et al* presented the hybrid data mining approach to detect the DDoS attacks. The feature selection mechanism is employed to select the important attributes. Their proposed algorithms exhibited high accuracy rate in the real networks.

Aikaterini Mitrokotsa et al predicted the DDoS attacks using Self- Organizing Maps. They targeted to detect the unknown and known patterns of the traffic data. The network events are checked out and create in log events of network traffic. Extensive simulations show the effectiveness of this approach compared to previously proposed approaches regarding false alarms and detection probabilities. A Change-Point Monitoring (CPM) was invented by Haining *Wang Danlu Zhang Kang G. Shin* to detect the Denial of Service attacks. To make the detection mechanism insensitive to sites and traffic patterns, a non-parametric Cumulative Sum (CUSUM) method is applied to make the detection system robust. CPM does not require per-flow state information and only introduces a few variables to record the protocol behaviors. The statelessness and low computation overhead of CPM make it immune to any flooding attacks. As a case study, the efficacy of CPM is evaluated by detecting a SYN flooding attack. The most common DoS attack. The evaluation results show that CPM has short detection latency and high detection accuracy.

III. PROPOSED FRAMEWORK

In this section, we explain about the proposed framework used for detecting the malware propagation attacks. The system architecture is given in Fig. 3.1. The proposed framework executes in four phases. It is listed as follows:

a) Formation of networks
b) Malware propagation
c) Filtering malware detection
d) Performance evaluation

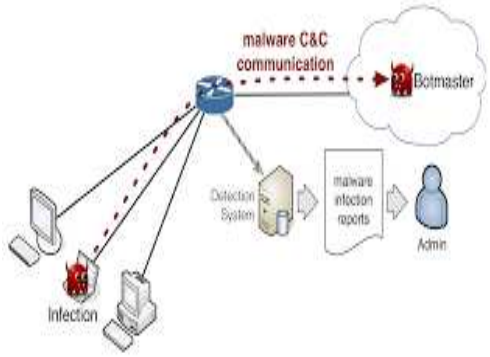

Fig.3.1 System Architecture

A. *Formation of networks*

The networks are formed by different number of hosts that follows the power law. By exploring the power law, the network size is determined for the increasing population. The greedy algorithm is used for defining the nodes in networks. The malware spreading model is designed as epidemic model to detect the malware attacks. Since our model creates malware infected nodes that simulate malware attacks by nodes. As we have claimed that this model characterizes the MMS and proximity malware spreading, we validate the malware spreading in both the proximity and MMS scenarios.

B. *Malware Propagation*

The malware propagation is injected in three stages, namely,

a) Early stage: It depicts about the malware that infects the systems at the least percentage. The propagation is done using exponential distributions.
b) Final stage: The host system is fully compromised by the malwares.
c) Late stage: It depicts the time taken by the early stage and final stage.

C. *Filtering malware detection*

The malware may occur in the networks in distributed manner. The similar networks may carry multiple malwares. The facts behind different malwares are that they produce the different vulnerabilities. So it's a necessitate one, to formulate different mathematical model for each malwares in order to avoid the collisions. The network layers contain network modeling methods.

D. *Performance evaluation*

Our experimental analysis also shows that the spreading model doesn't make use of power law. Android model is used for sharing the malware protection and to decrease the number of specific vulnerabilities.

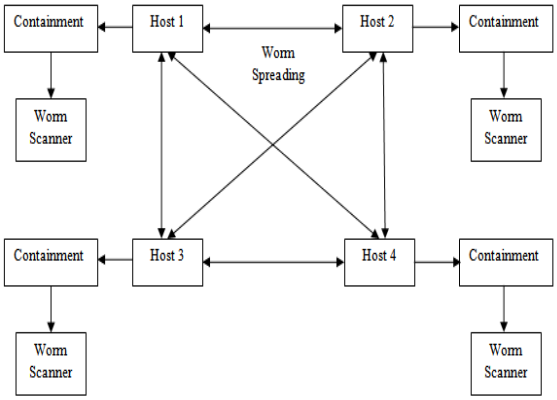

Fig.3.2 Proposed workflow

IV. EXPERIMENTAL DESIGNS

This section explains about the experimental analysis of the systems. The designs are explored as follows:

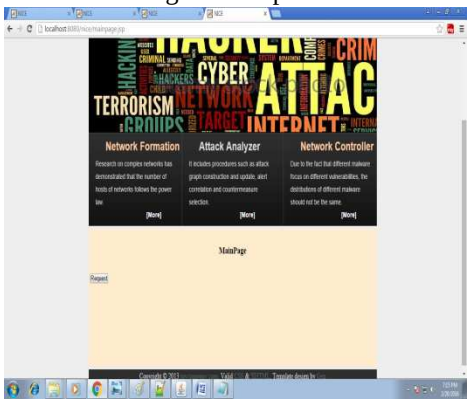

Fig. 4.3. Main Page of the proposed system

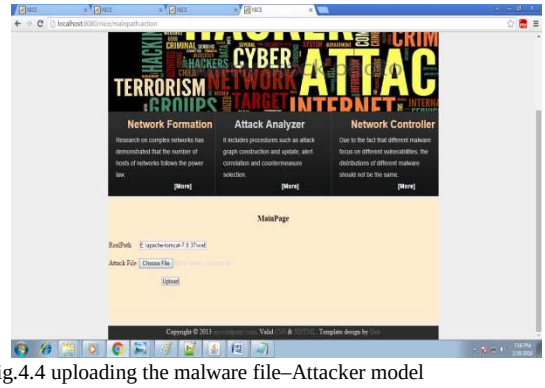

Fig.4.4 uploading the malware file–Attacker model

Fig.4.5 Malware spreading model

Fig.4.6 Viewing the malware spreading in the system

Fig.4.7 Malware attack is injected to the system

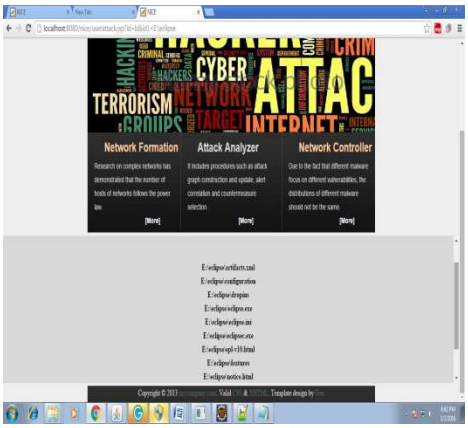

Fig.4.8 Using network analyzer tool, the drivers are analyzed

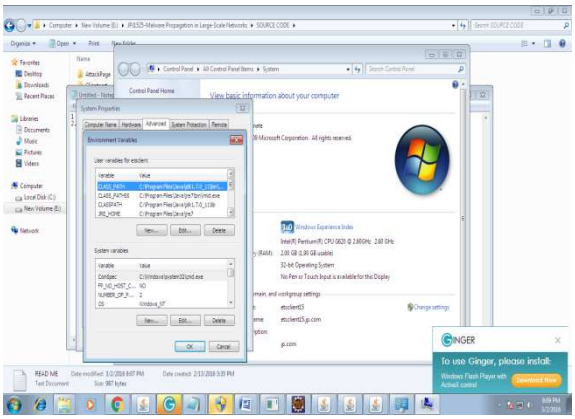

Fig.4.9 viewing the class path of the drive

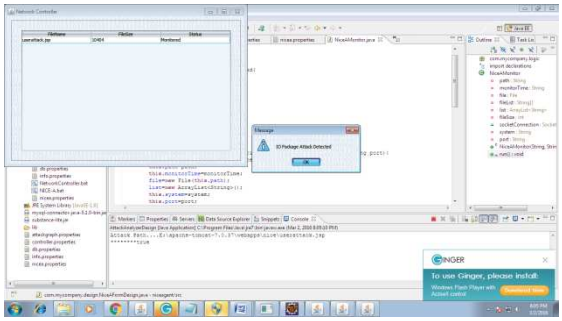

Fig.4.10 Detecting the ID based attack

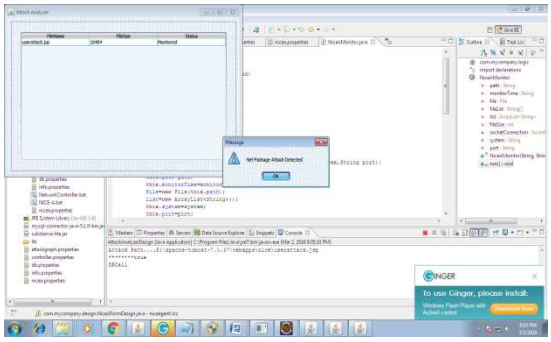

Fig.4.11 Detecting the net package attack

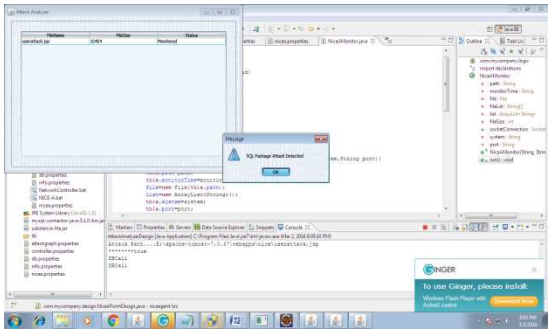

Fig.4.12 Detecting the SQL package attack

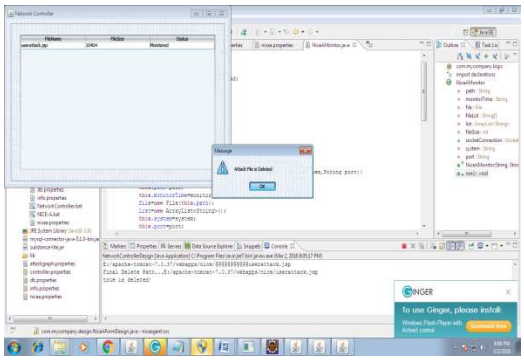

Fig.4.13 Attacked file is detected

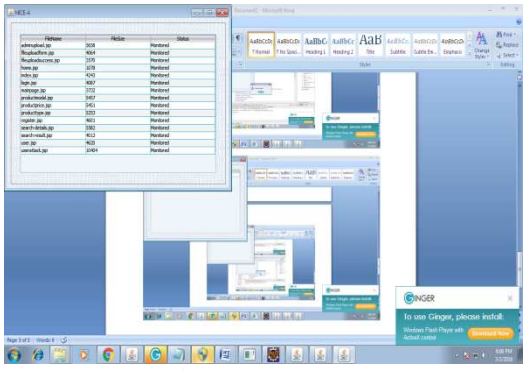

Fig.4.14. Rechecking of the drives using network analyzer tool

V. CONCLUSION

This paper explains about the malware propagation in large scale networks. Both the upper layer and lower layer in the network layer are modeled for analyzing the distributing environment. A proximity and MMS malware based propagation models are designed. The algorithm is scattered for each network layer. It acts as centralized solution. The intention of this study is to reduce the propagation attacks and enhance the efficiency of the system. Therefore, security and authentication mechanisms should be considered. From the aspect of malware, since some sophisticated malware that can bypass the signature detection would emerge with the development of the defense system, new defense mechanisms will be required.

REFERENCES

[1] Robert Mitchell, IngRay Chen, Member, IEEE, “Behavior Rule Specification-based Intrusion Detection for Safety Critical Medical Cyber Physical Systems”, IEEE Transactions on Dependable and Secure Computing, Vol: 99, 2014.

[2] H. Al-Hamadi and I. R. Chen. “Redundancy management of multipath routing for intrusion tolerance in heterogeneous wireless sensor networks”. IEEE Transactions on Network and Service Management, 10 (2):189–203, 2013.

[3] M. Aldebert, M. Ivaldi, and C. Roucolle. “Telecommunications Demand and Pricing Structure: An Econometric Analysis”, Telecommunication Systems, 25:89– 115, 2004.

[4] M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee. “Security challenges in next generation cyber physical systems. Beyond SCADA”: Networked Embedded Control for Cyber Physical Systems, 2006.

[5] B. Asfaw, D. Bekele, B. Eshete, A. Villafiorita, and K. Weldemariam, “Host-based anomaly detection for pervasive medical systems”, In Fifth International Conference on Risks and Security of Internet and Systems, 1–8, October 2010.

[6] F. Bao, I. R. Chen, M. Chang, and J. H. Cho, “Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection”. IEEE Transactions on Network and Service Management, 9(2):169–183, 2012.

[7] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. Fovino, and A. Trombetta, “A multidimensional critical state analysis for detecting intrusions in SCADA systems”. IEEE Transactions on Industrial Informatics, 7(2):179 –186, May 2011.

[8] A. C´ardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, “Challenges for securing cyber physical systems”, In First Workshop on Cyber-physical Systems Security, DHS, 2009.

[9] I. R. Chen and T. H. His, “Performance analysis of admission control algorithms based on reward optimization for real-time multimedia servers”, Performance Evaluation, 33(2):89–112, 1998.

[10] I. R. Chen, A. P. Speer, and M. Eltoweissy, “Adaptive fault tolerant QOS control algorithms for maximizing system lifetime of query-based wireless sensor networks”. IEEE Transactions on Dependable and Secure Computing, 8(2):161–176, 2011.

[11] I. R. Chen and D. C. Wang, “Analysis of replicated data with repair dependency”. The Computer Journal, 39(9):767– 779, 1996.

[12] I. R. Chen and D. C. Wang, “Analyzing Dynamic Voting using PetriNets”, In 15th IEEE Symposium on Reliable Distributed Systems, 44–53, Niagara Falls, Canada, October 1996.

[13] C.F. Tsai and C.Y. Lin, “A Triangle Area Based Nearest Neighbors Approach to Intrusion Detection, ”Pattern Recognition, vol. 43, pp. 222-229, 2010.

[14] A. Jamdagni, Z. Tan, X. He, P. Nanda, and R.P. Liu, “RePIDS: A Multi Tier Real-Time Payload-Based Intrusion Detection System,” Computer Networks, vol. 57, pp. 811-
824, 2013.

[15] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R.P. Liu, “Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis, ”Proc. Conf. Neural Information Processing, pp. 756-765, 2011.

[16] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R.P. Liu, “Triangle-Area-Based Multivariate Correlation Analysis for Effective Denial-of-Service Attack Detection,” Proc. IEEE 11th Int’l Conf. Trust, Security and Privacy in Computing and Comm., pp. 33-40, 2012.

[17] S.J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P.K. Chan, “Cost-Based Modeling for Fraud and Intrusion Detection: Results from the

JAM Project, ”Proc. DARPA Information Survivability Conf. and Exposition (DISCEX ’00),vol. 2, pp. 130-144, 2000.

[18] G.V. Moustakides, “Quickest Detection of Abrupt Changes for a Class of Random Processes, ”IEEE Trans. Information Theory, vol. 44, no. 5, pp. 1965-1968, Sept. 1998.

[19] A.A. Cardenas, J.S. Baras, and V. Ramezani, “Distributed Change Detection for Worms, DDoS and Other Network Attacks, ”Proc. The Am. Control Conf.,vol. 2, pp. 1008-1013, 2004.

[20] W. Wang, X. Zhang, S. Gombault, and S.J. Knapskog, “Attribute Normalization in Network Intrusion Detection, ”Proc. 10th Int’l Symp. Pervasive Systems, Algorithms, and Networks (ISPAN), pp. 448-453, 2009.

[21] M. Tavallaee, E. Bagheri, L. Wei, and A.A. Ghorbani, “A Detailed Analysis of the KDD Cup 99 Data Set,”Proc. IEEE Second Int’l Conf. Computational Intelligence for Security and Defense Applications, pp. 1-6, 2009.

[22] D.E. Knuth, The Art of Computer Programming Vol I: Fundamental Algorithms. Addison-Wesley, 1973.

AUTHOR PROFILE

DEVALLA SRI MAHALAKSHMI MANIKYAMBA is a student of Kakinada Institute Of Engineering & Technology affiliated to JNTUK, Kakinada pursuing M.Tech (Software Engineering). Her Area of interest includes Data Mining and its objectives in all current trends and techniques in Computer Science & Engineering.

R.CHANDRA SEKHAR *M.TECH is working as Assistant Professor, Department of Computer Science & Engineering, Kakinada Institute of Engineering & Technology, JNTUK, A.P, INDIA.*