ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st& 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Efficient Decentralized Network Control And Attack Analysis Model Using ENICS In Collaborative Protection Networks

Sakthidevi.I, Joshva Devadas.T

Assistant Professor, Department of Information Technology, Sethu Institute of Technology, Pulloor, Virudhunagar, Tamilnadu, India.

Professor, Department of Information Technology, Sethu Institute of Technology, Pulloor, Virudhunagar, Tamilnadu, India

Abstract—In wireless network environments, the chances for the vulnerability and the attacks against the data are getting higher at a gradual phase because of the various hacking and intrusion mechanisms. Lot of researches is in progress to protect the data and the associated nodes against these attacks. In comparison, the protection for the data and the nodes are reasonable for the centralized networks in defining specified architectures. But alarmingly, the security measures among the decentralized networks are very less in number and hence the need for efficient decentralized network control and attack analysis model is very high. In our work, we design a novel mechanism called Enhanced Network Intrusion Detection and Countermeasure Selection (ENICS) for detection and prevention of intrusion in the decentralized network. The control centre associated with the upstream intermediate network has three sub divisions, network controller, node profiling and attack analyzer. We analyze and detect the DDOS attacks using the control centre. Programmable network has performance enhancer and counter measure selection. This will ease the prevention control for the decentralized collaborative networks. In the simulation analysis, we measure the performance metrics, viz. CPU Utilization, Network Communication Delay, Success Analysis Rate and Throughput Analysis Rate for ENICS and compare them with the existing works based on NICE and Firecol-DGSOT using the simulation tool NS2. Results show that ENICS has better performance measure while detecting and preventing the intrusion attacks of the decentralized networks

Keywords— Collaborative networks; Counter measure selection; DDOS attacks; ENICS; Intrusion Detection; Intrusion Prevention

I. INTRODUCTION

Numerous protection mechanisms systems are there to secure the wireless networks against the vulnerable attacks [1] [2] [3]. Most of the intrusion detections deal with the centralised networks. Only limited number of researches is under process for the decentralised networks. To aim for the common goals in the intrusion based detection and prevention systems, lot of works has been established by means of individual participation and modular designs. The integration of the modular designs to build as a coherent system for protection and prevention is the need of the modern day works. Internet has emerged as a major source of active participation and storage [4] [5]. To transmit a data from the remotely located server to the local client machine and vice versa involves the passage along the contaminated route. To secure the previous data along the public runway and to prevent it from malicious attachment needs a dedicated and one to one flow all along the way which is practically impossible. To develop a tunnel virtually across the data transmission path extends to the development of new Intrusion Prevention System. If at all, any attacks are prone in the data path, the mechanism to detect it and to get rid of it is also of prime importance. [6][7][8][11]Existing anomaly based intrusion works on deviation principle in which the contaminated path is simply eliminated in the routing algorithm. [9][10] For effective and efficient data delivery, the design of the system which detects the anomaly and prevents such anomalies in the near future is necessary [12]. This should be looked into by the proposed Enhanced Network Intrusion detection based on Counter Measure Selection (ENICS) solution [11][13]by analysing the decentralized collaborative network control and attack

analysis model using quick change point detection method. Existing anomaly detection is measured by trust aware routing but ENICS provides the better security than fuzzy based trust aware routing[16],and data cleaning methods for packets counter measure [14][15] in Wifi positioning system. Our proposed method covers the collaborative network and measure the intrusion in global level.

The paper is organized as follows: Section 2 deals with the decentralized network control and detection model based on ENICS architecture. Section 3 deals with the implementation procedures for Quickset change point detection mechanism. Section 4 deals with the simulation analysis. Section 5 deals with the conclusion and the future works.

II. Decentralized Network Control And Detection Model – ENICS Architecture

ENICS model is designed as high secured one. Collaborative computation and counter measure selection are the prime factors in this model. The potential attacks shall get brief communication exchange with the vertical collaborative network. Depending on the probable attacks in the pathway and analyzing cost benefits, this ENIVS model is proposed. To reduce the countermeasures and the cost investment, greedy objective techniques are used.

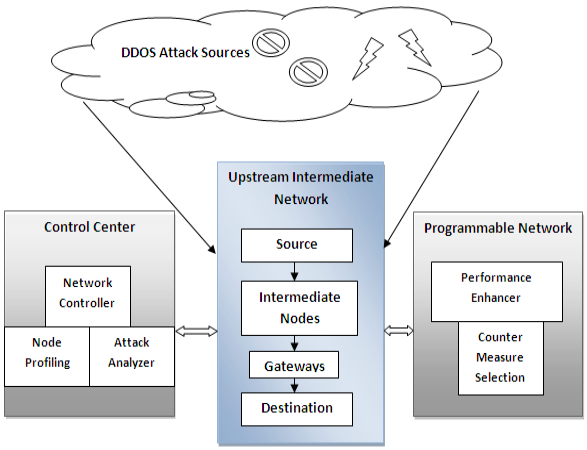

Fig. 1. ENICS in Decentralized Network Model

The decentralized network model can be divided into three sections, one with the upstream intermediate network, the other one control centre and another one, programmable network. Upstream Intermediate Network is one in which the actual data transmissions occur. The data is transmitted from the source to the destination through the intermediate nodes and gateways. During the data transmission, when the DDOS attack sources invade the network, there is a high probability of intrusion into the network. During such intrusion, control centre controls the network through network controller, node profiling and attack analyzer associated with it. The programmable network has performance enhancer and the counter measure selection to control and restore the network. Information stored in the network controller can be categorized as stable, vulnerable, exploited or zombie based on the type of susceptibility. The schematic architecture Decentralized Network model using ENICS is described in figure 1.

III. Algorithm – Counter Measure Selection

The core algorithm for the intrusion detection and prevention model is based on the counter measure selection phenomenon as illustrated in figure 2. On the reception of the counter measure selection alert in the programmable network, the data starts transmitted from the source. Considering the variation between the distance to the target and the threshold value, the value of ACG (Alert Correlation Graph) is getting updated or acknowledged for retransmission. Based on the risk probability set for the network controller and the benefits of the target node identification probability, updating of SAG (Scenario Attack Graph) and ACG (Alert Correlation Graph) are done regularly. The optimal selection of CM (Counter Measure) based on ROI (Return of Investment) is defined as final procedure in the counter measure selection algorithm.

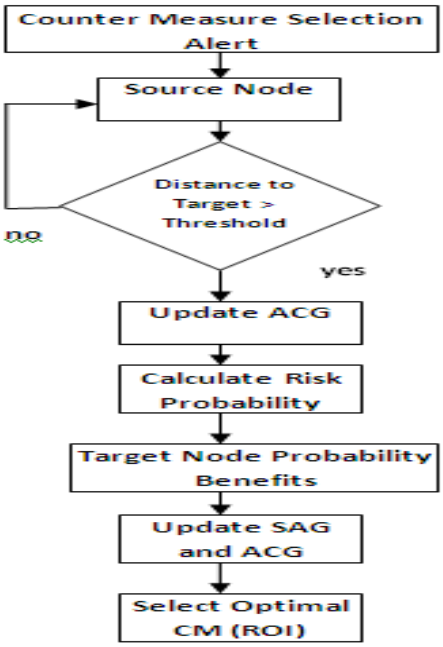

Fig. 2. Counter Measure Selection Algorithm

IV. Quickset Change point Detection

To identify the change in the state time process, Quickest change point detection mechanism is used. The computation measures such as Overall Average Delay to Detection and the Minmax function in the quickest change point detection are computed for the network detection model based on ENICS. Rapid Anomaly detection is analyzed in the study. By this mechanism,

we have formulated the multi-cyclic detection procedure based on counter measure selection

Overall Average Delay to Detection (OADTD) on the Counter Measure (CM) selection part is defined as

$$OADTD(CM) = max \{ E_T [CM-T| CM > T]\} \quad 0 \leq T < \infty \quad (1)$$

Where E_T is the entropy and T is the Time

The Minimax quickest change point detection problem based on counter measure selection is defined as the delta sum of all the overall average delay to detection probability.

$$OADTD(CM_{opt}) = \Delta\zeta \; OADTD(CM) \quad (2)$$

V. Performance Evaluation

TABLE I. Simulation Environment

Simulation parameters	Simulation values
Wireless standard	IEEE 802.11
Number of nodes	67
Base protocol	AODV
Algorithm	Counter Measure Selection
System Bandwidth	2 Mbps
Protocol Layer	Cross Layer MAC
Antenna	Omni Directional
Simulation Environment	1500 * 1500
Channel Propagation	Wireless / Two ray ground

For the performance evaluation, the following parameters are taken in the simulation environment. We design an Intrusion Detection System with better security and performance analysis in the collaborative environment. The IEEE standard for WLAN (IEEE 802.11) is taken as reference with the base protocol as Adhoc On-Demand Vector Protocol. The Implementation and the Data transmission occur in the cross layer (Medium Access Control – MAC). For the transmission, Wireless / Two ray ground – Omni Directional antenna is preferred. The Design of the simulation environment is implemented in Network Simulator (NS2) with the simulation environment size of 1500 m x 1500 m. The total number of nodes taken for simulation is 67, including the intermediate nodes and gateways.

TABLE II. Defence Mechanism against DDOS Attack

Defence Mechanism against DDOS Attack					
	Accuracy	**Scalability**	**Complexity**	**Network Delay**	**System Performance**
Centralized	Low	Low	Low	Low	Moderate
Hybrid (Decentralized)	Medium	Medium High	Medium High	Medium High	Poor Moderate
ENICS	**High**	**High**	**Medium**	**Low**	**Good**

For the Decentralized Network control and attack analysis in the collaborative systems, the parameters Accuracy, Scalability, Complexity, Network Delay and System Performance (in terms of Throughput Efficiency) are taken for consideration. For a defense mechanism against DDOS attacks in the Intrusion Detection System, three types of Networks viz. Centralized, Hybrid and ENICS are compared.

The Results listed in the following table show that ENICS system which is having a centralized as well as secured control center and programmable network is better in terms of all the parameters. In terms of accuracy and scalability, centralized network is low; hybrid network is medium where as enhanced decentralized network ENICS is high. Comparing the parameter complexity, centralized network has low complexity, whereas decentralized network has medium high complexity, but ENICS has medium complexity only. The two other parameters are included for our simulation analysis to test the network delay and the system performance. ENICS shows better results in both the parameters. The Network Delay is very much reduced and the system performance in terms of Throughput Efficiency is good while implementing the IDS system using ENICS.

With respect to the graphical analysis, the metrics are tested for three different algorithms and the comparison values are plotted in the line / column charts. The performance of the existing algorithms, NICE and Firecol-DGSOT are compared with the performance of the proposed ENICS algorithm.

The figure 3 shows the CPU utilization in percentage with reference to the traffic load in packets per second. In the simulation analysis, it is shown that the system using ENICS reduces the CPU utilization to the greater extend. The plot is drawn to demonstrate the effective utilization of the system resources in a network based intrusion detection system.

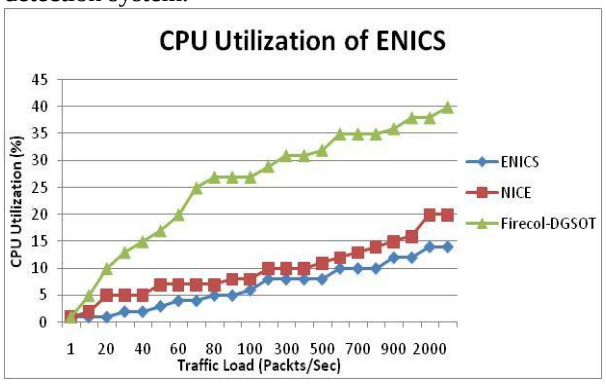

Fig. 3. CPU Utilization of ENICS.

The figure 4 shows the network communication delay with respect to different algorithms. Delay is the parameter which reduces the system performance. Lesser the communication delay better will be the system performance. In our simulation analysis, we have compared the delay performance in three different levels, one using the minimum number of nodes, another one using the maximum number of nodes and finally we have

calculated the average network communication delay of the system using three different algorithms. In the performance evaluation, it's found that the network IDS system using ENICS has lesser delay on both minimum and maximum node implementation.

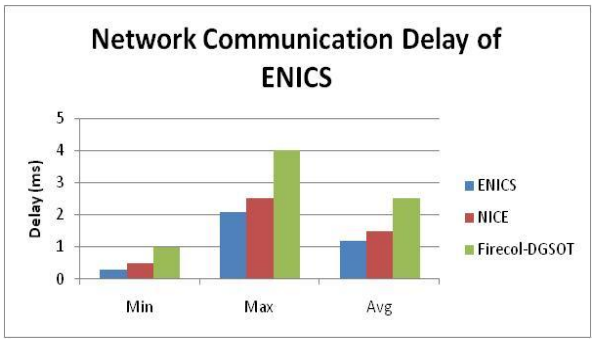

Fig. 4. Network Communication Delay of ENICS.

The success analysis rate of the data transmission with reference to the traffic load is plotted in Figure 5. The Results obtained indicate that the number of successful transmitted data is better in ENICS when compared to the other algorithms. In the real time environment, ideal success rate of 100% could never be achieved. Still increasing the success rate nearing to the good practical conditions gives better performance in the system.

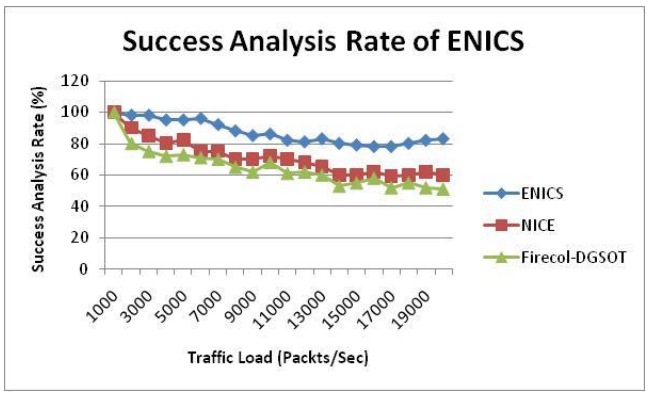

Fig. 5. Success Analysis Rate of ENICS.

Figure 6 shows the throughput analysis of the collaborative network based IDS comparing the different algorithms. The performance of the system using ENICS is better and the system gives higher throughput when using ENICS. This shows that the efficiency of the collaborative wireless network is increased using the proposed model.

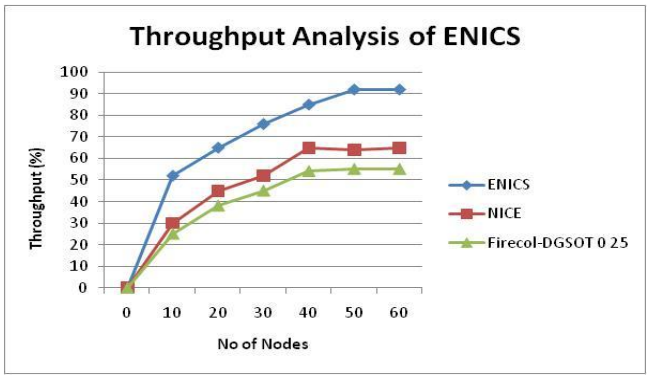

Fig. 6. Throughput Analysis of ENICS.

VI. Conclusion & Future Enhancement

The collaborative attacks in the decentralized networks and the novel method to detect and prevent the network are presented in the paper by using ENICS mechanics. Attack detection and futuristic prediction model is introduced in this paper. The solution proposed inhibits the characteristics of the real time Intrusion Detection and Prevention (IDPS) model. The experimental analysis shows that the performance metrics shows better results while implemented using the proposed model. Future works on the collaborative networks may increase the scope of the preventive measure for the system at the time of attacks using heterogeneous counter measure selection procedures.

References

[1] Alexander G. Tartakovsky, Senior Member, IEEE, Aleksey S. Polunchenko, and GrigorySokolov "Efficient Computer Network Anomaly Detection by Changepoint Detection Methods" IEEE JOURNAL OF SELECTED TOPICS IN SIGNAL PROCESSING, VOL. 7, NO. 1, FEBRUARY 2013

[2] Jonny Milliken,Member, IEEE,Valerio Selis, Kian Meng Yap,Member, IEEE, and Alan Marshall,Senior Member, IEEE, "Impact of Metric Selection on Wireless DeAuthentication DoS Attack Performance", IEEE WIRELESS COMMUNICATIONSLETTERS, VOL.2, NO. 5, OCTOBER 2013

[3] G. Thatte, U. Mitra, and J. Heidemann, "Detection of low-rate attacks in computer networks," in Proc. of the 11th IEEE Global Internet Symp., Phoenix, AZ, Apr. 2008, pp. 1–6.

[4] G. Thatte, U. Mitra, and J. Heidemann, "Parametric methods for anomaly detection in aggregate traffic," IEEE/ACM Trans. Networking, vol. 19, no. 2, pp. 512–525, Apr. 2011.

[5] A.G.Tartakovsky,B.L. Rozovskii,R.B. Blažek and H.Kim, "A novel approach to detection of intrusions in computer networks via adaptive sequential and batch-sequential change-point detection methods,"IEEE Trans. Signal Process., vol. 54, no. 9, pp. 3372–3382,Sep. 2006.

[6] A. G. Tartakovsky, B. L. Rozovskii, R. B. Blažek, and H. Kim, "Detection of intrusions in information systems by sequential changepoint methods (with discussion),"Statistical Methodology., vol. 3, no. 3, pp. 252–340,2006.

[7] A.G.Tartakovsky, B.L.Rozovskii, and K.Shah, "An on parametric multichart CUSUM test for rapid intrusion detection," inProc. Joint Statist. Meetings, Minneapolis, MN, Aug. 2005.

[8] Zhijun Wu, Zhifeng Chen, "A Three-Layer Defense Mechanism Based on WEB Servers Against Distributed Denial of Service Attacks", Communications and Networking in China, 2006. ChinaCom '06.

[9] Shui Yu, Wanlei Zhou, "Entropy-Based Collaborative Detection of DDOS Attacks on Community Networks", Pervasive Computing and Communications, 2008.PerCom 2008. Sixth Annual IEEE International Conference

[10] Chun-Jen Chung,Student Member, IEEE, PankajKhatkar, Student Member, IEEE, TianyiXing,Student Member, IEEE, Jeongkeun Lee, Member, IEEE, and DijiangHuang,Senior Member, IEEE" NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems"IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 4, JULY/AUGUST 2013

[11] Roy, D.S. Kim, and K. Trivedi, "Scalable Optimal Countermeasure Selection Using Implicit Enumeration on Attack Countermeasure Trees,"Proc. IEEE Int'l Conf. Dependable Systems Networks(DSN '12),June 2012.

[12] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs,"IEEE Trans. Dependable and Secure Computing,vol. 9, no. 1, pp. 61-74, Feb. 2012.

[13] SamanTaghaviZargar,Member, EEE,James Joshi,Member, IEEE,and David Tipper,Senior Member, IEEE" A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks"IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 4, FOURTH QUARTER 2013

[14] T. JoshvaDevadas, C. Seelammal and S. Sadasivam, 2013.On Data Cleaning with Intelligent Agents to Improve the Accuracy of Wi-Fi Positioning System using GIS. Asian Journal of Scientific Research, 6: 53-66. DOI: 10.3923/ajsr.2013.53.66

[15] T. JoshvaDevadas, R. Ganesan "Intelligent Agent Based Knowledge Management and Knowledge Discovery", International Journal of Advanced Research in Computer Science ,Vol 3, No2, Mar-Apr 2012, ISSN 0976 569

[16] I.Sakthidevi, E.srievidhyajanani "Fuzzy based Trust aware routing Framework for dynamic WSN"circuits, power computing technologies IEEE international conference on 2013 Page(s):1041 - 1046 Print ISBN: 978-1-4673-4921-5