DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5728

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

USING MULTI-AGENT SYSTEMS FOR INTRUSION DETECTION IN COMPUTER NETWORKS: A GLANCE

Harmanpreet Kaur
Department Of Computer Science & Engineering,
Guru Nanak Dev University, Regional Campus,
Gurdaspur, India

Harjot Kaur
Department Of Computer Science & Engineering,
Guru Nanak Dev University, Regional Campus,
Gurdaspur, India

Abstract: The development of Cyber attacks and information safety has become one of the important issues throughout the world. IDS (Intrusion detection systems) are one of the vital components in modern infrastructure in order to enforce various network rules and regulations. Intrusion Detection System is one of the extensively used systems which are used to diagnose malicious activities and various attacks on computer networks, but its present framework confronts a huge number of alerts and false positive alarms. Lots of work has been done to propose various MAS-based intrusion diagnostic techniques for handling the attack alerts, reducing them and for differentiating the real attacks from false positive attacks. This paper reviews various techniques used for intrusion detection in computer networks using multi-agent systems. The lack of accuracy should be improved by using various techniques like the Neural, Data mining and Threshold. Our aim will be to propose novel performance enhancement technique using multi-agent systems that will improve the lack of accuracy and false positive alarm generation problem in IDS with less processing time.

Keywords: Intrusion detection, multi-agent system, false positive rate, alert reduction, networks.

I. INTRODUCTION

According to Micheal Woolridge[14], An agent can be defined as, "A computer system that is situated in some environment, and that is capable of autonomous action in this environment in order to meet its design objectives".

According to Milan Rollo [6], Multi-agent system (MAS) can be defined as, "A collection of multiple autonomous (intelligent) agents, each acting towards its objectives while all interacting in a shared environment, being able to communicate and possibly coordinating their actions". Intrusion detection can be assumed as an autonomous platform which can be used for identifying attacks/intrusions by analyzing network traffic and monitoring various nodes in a computer network. Intrusion detection systems (IDSs) are a vital constituent of a fully-accomplished and protecting-in-depth architecture which is deployed for securing computer networks and hence they play a vital role in attack detection in the same. It can be considered one of the efficient security paradigms, which can be used for detecting, preventing and probably reacting to various types of attacks [15]. It observes various nodes for any malicious activities and gathers and examines the collected data looking for the presence of any type of intrusive behaviours. If any unsure or malicious activities are detected, it raises an alarm and prompts the network administrator to react immediately. The main purpose of IDS is to detect various types of attacks in an efficient manner. The IDS can be categorized as either an anomaly detection system or a misuse detection system [8]. The technique used by misuse detection system is to identify and compare attack signatures of various attacks which were formerly saved in the database of IDS. The major drawback of the misuse system is that IDS database should have a signature entry for each type of attack in order to compare them with various incoming packets; therefore the process of intrusion detection with misuse IDS becomes very long and cumbersome. Whereas, in anomaly detection system, an attack is identified from the fluctuated behavior of various network users and traffic. Henceforth, this system has to keep analyzing the network during a period for collecting various vital statistics about the same.

The remainder of the paper is organized as follows. The literature review associated with various intrusion detection systems using MAS is presented in section 2. Section 3 describes the problem definition, i.e., using Multi-agent Systems for Intrusion Detection in Computer Networks, section 4 explains the proposed model of MAS-IDS (multi-agent system Intrusion Detection System) also various techniques which are removed false positive alarms and section 5 presents conclusions.

II. BACKGROUND WORK

Labiod et al. [7] have focused on the new technologies which overcame the drawbacks of security issues in existing intrusion detection systems, i.e., a problem of autonomy, flexibility, adaptability etc. The researchers proposed the use of DAI (distributed artificial intelligence), based on the MAS paradigm in their proposed intrusion detection system. The work also described a multi-agent system named as DIMA (Development and Implementation of the Multi-Agent Systems) which was exploited to actualize a novel architecture called MAIDA (Multi-Agent Intrusion Detection Architecture) that supported various security management activities. In MAIDA, two types of agents were included, i.e. manager and slave agents. A hybrid agent model was selected to implement various resident agents in MAIDA (Multi-Agent Intrusion Detection Architecture). The main motive of applying intelligent agents within DIMA platform was to illuminate two particular attacks: doorknob rattling and IP spoofing. As a future research direction, the authors intended to implement

© 2015-19, IJARCS All Rights Reserved

the multi-agent framework MAIDA related to details described in their work based on DIMA platform.

Gorodetski et al. [4] have presented a software tool called MASDK (Multi-agent System Development Kit) that provides an agent-based network security system that intent on supporting various fundamental aspects of a MAS paradigm. In this work, ASACN (Agent-Based Simulator of Attacks against Computer Networks), a layered model is developed, in which every agent (malefactor) existing in lower layer enforces attacks. The attack enforcement is according to a scheme which can be presented in terms of various higher layers of the proposed model. MIDLS (Multi-Agent Intrusion Detection Learning System) has been designed in this work which makes intrusion detection decisions on the basis of a multi-level model of network traffic and host-based audit data. As a future research direction, the authors aim to expand various abilities present in multi-agent network security assurance applications using MASDK.

Hamami et al. [1] have presented the MAS for intrusion detection in complex networks (networks with many users, machines, and connections). The researchers' perspective of proposed IDS present that MAS is an appropriate solution for intrusion detection considering its various properties like distribution, cooperation etc. and comprising agents' properties like autonomy, pro-activity, as they match the entire requirements. The system designed by authors comprises two levels, i.e., external and internal levels. The external level defines the roles and relations between various agents in MAS and internal level includes functions, i.e., discovering interfacing, and discussion functions. By applying these three functions, the pace of agents for intrusion detection becomes faster with improved accuracy. But, the proposed work lacked adaption and flexibility features, as it possessed no capability to learn new attacks. As a future research direction in IDSs, the authors have suggested the use of a new theory of Adaptive Multi-Agent System (AMAS) for intrusion detection in complex networks.

Servin et al. [11] have proposed an RL (Reinforcement Learning) approach combined with sensory skills in agents to diagnose DOS (Denial of Service Attacks) for a hierarchical architecture of a Distributed IDS. In this architecture, network sensor agents learn through observations of network signals using the technique of Q-Learning and send them up to central agents (RL-IDS) at a higher level in the hierarchy of agents. The agents residing in the upper level of hierarchy learn how to depict locally collected information from these signals. The work presents solutions that enable the agents to learn an accurate policy of diagnosis and it shows that the technique can be scaled up for many agents. As a future work direction, the presented work suggests porting the conceptual network model in the direction of realistic network simulation.

Gandotra et al. [2] have presented a three-phased threat oriented security model by choosing a proactive step in risk management to eliminate various possible and potential threats to a network. In the presented model, the identification of threat is the first phase in which known threats have been diagnosed using threat modelling task. And for identifying unknown threats research honey tokens have been used along with various analytical techniques. The intelligent multi-agent system planning has been used in the second phase in which risk reduction has been evaluated with respect to both known and unknown threat sets. In the third phase, meta-agents are introduced which automatically check the accomplishment of various agents in MAS and a security checklist is conveyed by them for taking appropriate countermeasures. As a future research direction, the researchers planned to extend the presented model by making it more cost-oriented.

Jakobson et al. [5] have proposed the federated adaptable MAS for achieving cyber attack tolerant missions. The word '*federated*' in the work refers to "a specific type of distributed MAS architecture in which multiple autonomous agents (federations) were classified into a hierarchical control structure". Every agent in MAS is a modeled as BDI (Belief Desire Intention) agent with the capability of cyber-security situation awareness and adaptability. Various components of the proposed system had been prototyped and tested by researchers as well. As a future research direction, the researchers want to validate the proposed model and its architecture along with the advanced research in several directions which includes self-organizing cyber terrain and offline analysis of cyber security.

Mokarian et al. [8] have presented data mining technique which aims to reduced false positives alarms and improve accuracy in intrusion detection systems. The article incorporated two false positive reduction methodologies, i.e., the detection and the alert processing techniques. Data mining is the main technique proposed by authors for reducing alerts and false positives alarms. The presented background work was based on the problem of lack of accuracy in intrusion detection.

Ganapathy et al. [3] has proposed an intelligent (feature selection) and classification technique for development of an efficient IDS (Intrusion Detection System). Furthermore, two new algorithms have been presented by the authors i.e. Intelligent Rule based Attribute Selection algorithm and Intelligent Rule based Enhanced Multiclass Support Vector Machine (IREMSVM) respectively. The presented literature review of the work includes many classification techniques based on neural networks, decision tree, naive Bayes, fuzzy sets etc. The authors compared new classification IREMSVM algorithm with existing IAEMSVM (Intelligent agent-based enhanced multiclass support vector machine) and analyzed that IREMSVM provided security in a network in an effective manner.

Singh et al. [13] have outlined in their work that cyber-security can basically involve every part of MAS research and it is a great research opportunity in the same. After that, the authors proposed a cyber-security ecosystem, in which three main autonomous entities were involved, namely system, stakeholders and adversaries (attackers). The stakeholders and adversaries interact with each other through a system, which is made of three components, i.e., social architecture, users and technical architecture. The system is modelled in the form of a micro-society comprising various norms in the form of a social architecture and principals as users. The authors have concluded from their research that MAS can fill the void of principles which are required by cyber-security in order to become a full-fledged science in itself.

Yaseen et al. [15] have proposed a multi-agent system which aims to improve the performance of IDS with less processing time. In this work, the multi-agent system has demonstrated intrusion detection capability and also required less time to meet the appropriate objective of determinate various attacks for improved accuracy as in meantime. The proposed data mining clustering technique has been used to organize information in clusters i.e. normal or attack clusters. The researchers have proposed the architecture of MAS-IDS which comprises a set of agents that perform their roles autonomously. It includes various agents, i.e., Coordinator, Communication, and Analysis agents. As in future research, direction suggested in this work is to enforce MAS-IDS with real data networks, and the main motive of IDS used new approaches of selecting the initial centers of clusters and enhances the performance of IDS with less proceeding time.

Retnaswamy et al. [10] have presented a new ontology-based multi-agent infrastructure to recognize intrusions in the computer network. The work proposed a multi-agent framework which combined ontology and multiple agents for intrusion detection. The framework comprised of IDS broker, deputy commander, and response agents. In the presented experiment, the performance of multi-agent based intrusion detection system (MABIDS) was compared with back propagation neural network (BPNN), back propagation neural network multi-Agent (BPNN-MA) and it was proved that MABIDS provided better results in terms of detection rate, accuracy and reduced false alarm rate. As a future research direction, the researchers planned to extend the performance of their attack detection system by reducing the memory needed for data processing.

Sadhasivan et al. [12] have presented a new Adaptive Rule-Based Multi-agent Intrusion Detection System (ARMA-IDS) for a secure data transfer in a network. By using ARMA-IDS, the focus of the work was to enhance the performance of detecting attacks with an adaptive update of attack information in the ARMA-IDS's database. The ARMA-IDS was used to verify the performance of two training datasets, i.e., KDD (Knowledge Discovery and Data) cup99, SCADA (Supervisory Control and Data Acquisition) and one testing data set, i.e., real-time traffic, to show better intrusion detection rate in networks. The work used the combination of rules and responsibilities defined for various agents (sniffer, filter, anomaly-detection, rule mining and rule-based agents) in the MAS in order to efficiently determine the misuse and anomaly behavior in KDD and SCADA. ARMA-IDS detected various faults in networks and updated the existing database using a feedback loop. The performance of the proposed ARMA-IDS was analyzed using the combination of density-based clustering and rule formation. The authors using the approximate analysis of ARMA-IDS with various existing algorithms namely random forest, Jrip, AdaBoost, and mining common path algorithms proved that proposed ARMA-IDS showed better performance in SCADA and KDD datasets.

Mojumder et al.[9**]** have presented the use of the hybrid technique for developing a better network IDS, which is based on the fusion of clustering and classification data mining algorithms, to increase performance and reduce the rate of false alarms. The authors have used K-means clustering algorithm to introduce more cluster information in the form of the new set of features in the feature dataset. Five different classifiers namely SVM (Support Vector Machine), Decision Tree, Naive Bayes, Random Forest and K-Nearest Neighbour are then used classifying various types of attacks and comparing the results for the NSL-KDD dataset. After comparison with various hybrid approaches, the authors proved that the hybrid technique improves accuracy and shows a sustainable decline in false positive rates. As a future research direction, the authors suggest for enforcing intrusion avoidance ability including intrusion detection and testing it on real-life network traffic.

III. PROBLEM DEFINITION: USING MULTI-AGENT SYSTEMS FOR INTRUSION DETECTION IN COMPUTER NETWORKS

IDS (Intrusion detection systems) are a vital component in modern infrastructure in order to enforce various network rules and regulations. So far a lot of techniques using multi-agent systems have been applied for the detection of intrusions, which has been illustrated in many literature reviews regarding the same. Intrusion Detection System is one of the extensively used systems which are used to diagnose malicious activities and various attacks on computer networks, but its present framework confronts a huge number of alerts and false positive alarms. The previous work has been done to presented diagnostic techniques for handling the attack alerts, reducing them and for differentiating the real attacks from false positive attacks and improves accuracy by using various techniques like hybrid data mining, clustering, and adaptive algorithms. There are few false positive reduction techniques which may cause lack of accuracy and miss real attack alerts. In our work, the aim will be to use new methods based on multi-agent systems that will improve the lack of accuracy problem in IDS with less processing time.

IV. PROPOSED MODEL

We have envisaged a model for intrusion detection system which will help to accelerate the accuracy and decline false alerts. The model is elaborated in fig.1, showing how the above-mentioned targets would be achieved. Initially, an anomaly detection method based intrusion detection system is used in networks of agents which results in the formation of the huge amount of false alarms. To reduce the number of false alarms, incremental learning approach can be implemented by using two techniques, i.e., detection and alert processing technique. Our model is based on incremental learning technique, which is a fusion of data mining, threshold, and neural networks. Eventually, this will help to achieve the objective of less generation of false alarms and escalation inaccuracy.

© 2015-19, IJARCS All Rights Reserved

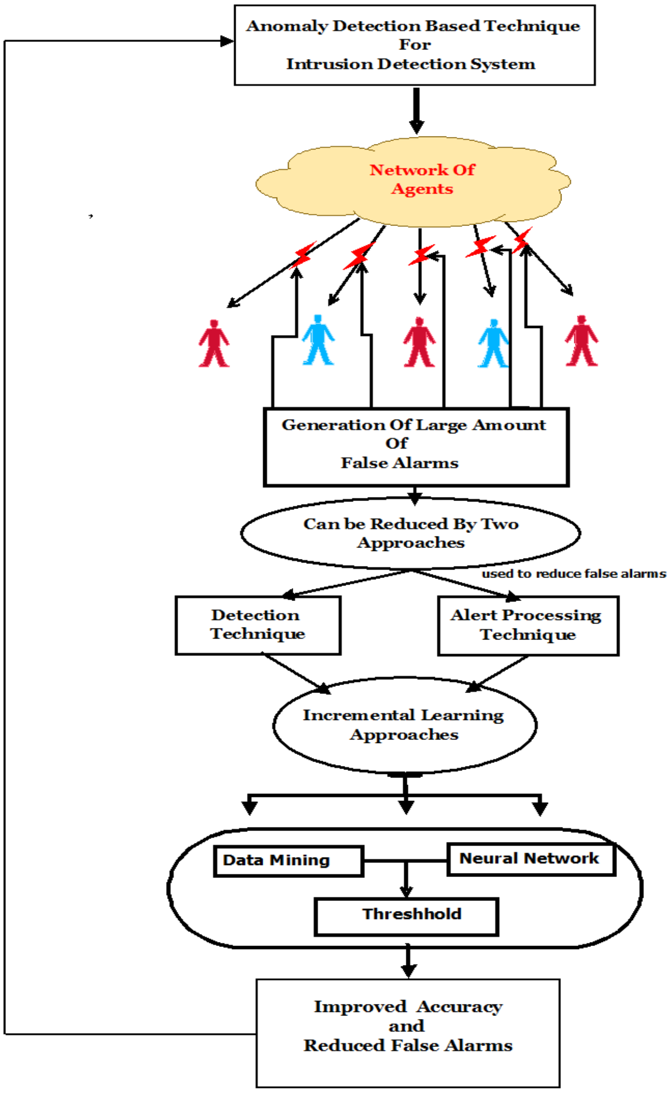
Anomaly Detection Based Technique For Intrusion Detection System
Network Of Agents
Generation Of Large Amount Of False Alarms
Can be Reduced By Two Approaches
used to reduce false alarms
Detection Technique
Alert Processing Technique
Incremental Learning Approaches
Data Mining
Neural Network
Threshhold
Improved Accuracy and Reduced False Alarms

Fig.1 Framework to reduce false alerts using incremental approach

V. CONCLUSIONS

In this work, we have examined various papers which are mainly published in indexed journals and conferences, which have visualized modern applications of detection of known and unknown attacks in computer networks. Various current studies have been reviewed with multi-agent based intrusion detection systems in networks considering step by step improvement including various techniques in order to improve accuracy and reduce a generation of false alarms. It has been systematically investigated that the generation of false alarms can be depreciated at the same time while performing network-based multi-agent intrusion detection. The summary of works that we have reviewed reveals that usage of incremental learning approach instead of data mining approach can lend a hand to make intrusion detection more accurate and can also reduce in a generation of false alarms. Thus, on the basis of this idea, we proposed a framework for intrusion detection. Our infrastructure can be considered as the first and fundamental step to enhance the performance by using networked multi-agent based intrusion detection for reduction of the amount of false alarm generation.

VI. REFERENCES

[1] Al-Hamami, A., & Hashem, S. (n.d.). A Proposed Multi-Agent System for Intrusion Detection System in a Complex Network. 2006 2nd International Conference on Information & Communication Technologies. doi:10.1109/ictta.2006.1684990.

[2] Gandotra, V., Singhal, A., & Bedi, P. (2012). Threat-Oriented Security Framework: A Proactive Approach to Threat Management. *Procedia Technology,4*, 487-494. doi:10.1016/j.protcy.2012.05.078

[3] Ganapathy, S., Kulothungan, K., Muthurajkumar, S., Vijayalakshmi, M., Yogesh, P., & Kannan, A. (2013). Intelligent feature selection and classification techniques for intrusion detection in networks: a survey. EURASIP Journal of Wireless Communications and Networking, 2013.

[4] Gorodetski V, Kotenko I, and Karsaer K**,** Multi-agent technologies for computer network security: Attack simulation, intrusion detection, and intrusion detection learning Computer Systems Science and Engineering · July 2003.

[5] Jakobson, G. (2012). Using federated adaptable multi-agent systems in achieving cyber attack tolerant missions. 2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support. doi:10.1109/cogsima.2012.6188415.

[6] Jakob. M, Rollo M, Introduction to Multi-Agent Systems, Agent Technology Center, Dept. of Computer Science and Engineering.

[7] Labiod H, Boudaoud k, and Labetoulle j, towards a new approach for intrusion detection with intelligent agents, 1998.

[8] Mokarian A., Farahani A., Delavar A, (2013) False Positives Reduction Techniques in Intrusion Detection Systems-A Review IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.10, October 2013.

[9] Mojumder, N., Shahabub, M., Afsana, M., Mehedi, M., & Shabanam, S. (2017). A Cluster-based Hybrid Framework for Network Intrusion Detection. International Journal of Computer Applications,172(1), 23-29. doi:10.5120/ijca2017915058

[10] Retnaswamy, B., & Ponniah, K. K. (2016). A new ontology-based multi-agent framework for intrusion detection. International Journal of Communication Systems,29(17), 2490-2502. doi:10.1002/dac.3189

[11] Servin, A., & Kudenko, D. (n.d.). Multi-agent Reinforcement Learning for Intrusion Detection. Adaptive Agents and Multi-Agent Systems III. Adaptation and Multi-Agent Learning Lecture Notes in Computer Science, 211-223. doi:10.1007/978-3-540-77949-0_15.

[12] Sadhasivan, D. K., & Balasubramanian, K. (2017). A Fusion of Multiagent Functionalities for Effective Intrusion Detection System. Security and Communication Networks, 2017, 1-15. doi:10.1155/2017/6216078.

[13] Singh, M.P Cybersecurity as an application domain for multi-agent systems.In: Proceedings of the 14th International Conference on Autonomous Agents and MultiAgent Systems(AAMAS), IFAAMAS,pp.1207-1212.Blue Sky Ideas Tracks, Istanbul, May 2015.

[14] Wooldridge, M. (2002). An Introduction to multiagent systems. John Wiley and Sons Ltd., Chichester, UK.

[15] Yaseen W, Othman Z, Zakree M, Nazi A,(2016) Real-Time Intrusion Detection System Using Multi-agent System, IAENG International Journal of Computer Science, 43:1, IJCS_43_1_10.

© 2015-19, IJARCS All Rights Reserved