COMPUTER AND NETWORK SECURITY: ONTOLOGICAL AND MULTI-AGENT SYSTEM FOR INTRUSION DETECTION

SAILAJA.P 1. PAMBALA NAGESWARA RAO 2, MATOORI KIRAN 3
THAMBI VINOD KUMAR, 5.G.AMIRTHAYOGAM
Assistant Professor, Department of Computer Engineering, Ellenki college of Engineering and Technonlogy, patelguda (vi), near BHEL ameenpur (m), Sangareddy Dist. Telangana 502319.

Abstract

Today the security aspect is a backbone of every computer system, particularly when this system contains sensitive information. When we use our com- puters and connect to the network or use web services, we trust that our personal and sensitive information (im- ages, passwords, credit card number …etc) are confi- dential and well secured by the used security system. Unfortunately, the hackers may succeed to gain access to the system and misuse our information. Generally, the aim of the intrusion is to find new ways to annoy, steal and harm parts of computer systems. Moreover, with the possibility of connecting several computers and networks, the necessity of protecting the whole data and machines from attackers (hackers) that try to get some confident information to use for their own benefit or just destroy or modify valuable information was born. At this point IDS appears to help users, companies or institutions to de- tect when they are getting compromised. In this paper, we develop an intrusion detection system using multi agent system, ontological techniques (IDSMAO) and misuse method.

Keywords: Intrusion Detection Systems, Computer and Net- work Security, Semantic Web, Ontology, Multi-agents System (MAS), JADE and JENA

Introduction

With the evolution of Internet and computer networks, security has become a major concern over the years. There are many systems of protection against security concerns such as firewalls that protect a network by pre- venting intrusions from the Internet and control the flow of data going in the network. But these systems cannot pre- vent all the malicious traffic and they may allow the pass- ing of an intruder. Thus, IDS (intrusion detection systems) have to provide a way to catch all kinds of malicious ac- tions. With the increasing number of attacks on computer systems through web services and applications day by day, there is a high need to protection of our computers. These attacks that occur are basically those that take an advantage of the vulnerabilities and misconfigurations on the systems. Even with the presence of firewalls and proxies, the at- tacker is successful in detecting the vulnerabilities and gaining access into the system. The objective of Intru- sion Detection Systems (IDS) is to detect and initiate a quick response when an unauthorized activity takes place. IDS prove to be an integral part of every computer sys- tem. Typically, when they are used with: security policy, vulnerability assessments, data encryption, user authen- tication, access control, and firewalls, they can greatly enhance network safety.

In this paper, we propose a new way to detect intruders. We introduce a new IDS, called IDSMAOnto(Intrusion Detection System based on Multi-Agent and Ontology). IDSMAOnto is based on the integration of the multi-agents

system technology and the ontology techniques. The basic functionality of our intrusion detection system is the security guard, it generates an alarm when it detects something suspicious and then the administrator of the network security investigates the cause of the alarm.

Our proposed system uses a set of agents that can be applied to a number of tasks, namely: data capturing, filtering the captured data, also analyze data to detect attacks and ultimately alerting the administrator (as in [4][12]). IDSMAOnto efficiently uses misuse detection strategies as in [14]. IDSMAOnto creates new ontology of the signature of the susceptible attack (collected data), then it compares this signature with the ontology of at- tacks signatures (mapping process) to decide whether it is an attack or not. Moreover, the power and utility of the ontology is realized by the fact that we can express the relationships between collected data and use those rela- tionships to deduce that the particular data represents an attack of a particular type. Ontologies provide powerfull constructs that include machine interpretable definitions of the concepts within a domain and the relations be- tween them [18][9].

The remainder of this paper is organized as follows: in the next section, we present the related works then we intro- duce the intrusion detection field by giving definitions and background on security approaches and types of IDS. Moreover, we express the advantages and the importance of using multi-agent systems in the field of IDS. In sec- tion four, we present our general modeling of the proposed approach. Section five, is dedicated to explain the de- tailed IDSMAOnto system architecture and our ontology. In the section six, we present the functioning of our sys- tem using AUML diagrams. The validation and evaluation of and the results of the developed system are shown in the next section. We finish this paper by a conclusion.

1. Related Works

Security is a focal aspect of every computer system and so the quality of these systems depends on the provided functionalities as well as the degree of security. Several works presented many approaches and methods to en- sure high degree of security.

The authors of [13] proposed the ontological model for representing intrusion detection and prevention events, over multi-agents architectures and using intelligence computing for reasoning, classification and pattern rec- ognition. The authors focused first the Intrusion Detection Messages Exchange Format (IDMEF). The aim is to en- able interoperability between heterogeneous IDS (IDMEF based on XML). To provide reasoning capability, the au- thors added Semantic Web Rule Language (SWRL) to allow writing rules expressed in OWL concepts providing reasoning capabilities. The attacks were created with test- ing tools as Metasploit, IDSWakeUP, Mucussynchro- nized with Snort. The raw data was converted to XML then processed to OWL instances; furthermore the ontology is updated via SPARQL. The use of ontology is to represents the signatures for known attacks and novel attacks, and the intelligent behavior uses the inference model and reasoning tools integrating neuronal networks in the multi-agent system.. According to the authors, the detection accuracy of the proposed ontology based IDS is superior to that obtained for traditional signature based IDS, because it provides better performance in processes such as knowledge representation, cooperation, distribu- tion, intelligence reasoning, reactivity, among others.

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-1, 2017
DOI: 10.21276/ijcesr.2017.4.1.7

The authors of [5] used intelligent combination of cluster- ing technique and an ontology to improve new multi-agents IDS. The proposed system is a new distributed intrusion detection system called OCMAS-IDS (Ontology and Clus- tering based Multi-AgentS Intrusion Detection System). This system takes the advantages of the multi-agents technology and the benefits of semantic relations as well as the high accuracy of the data mining technique. In this paper, the proposed system uses a set of agents that can be applied to a number of tasks, namely: data cap- turing process, detecting the known and unknown attack categories and ultimately alerting the administrator if any attack is detected. OCMAS-IDS expressed the advan- tages of integration of the multi-agents technology, the ontology and the clustering technique. The experiments of this system on a real-life network traffic and a set of simulated attacks, showed the effectiveness of the pro- posal in terms of (i) the scalability and (ii) the detection ability of our system.

In the paper of [21], design and implementation of ontol- ogy based knowledge representation for a peer-to-peer MultiAgent Distributed Intrusion Detection System (OntologyBased MADIDS) are introduced. The aims is to develop a distributed intrusion detection system, by tak- ing advantage of ontology technique to overcome some knowledge sharing limitations of current IDSs. The pri- mary focus of this paper is on the detection of attack tools by implementing Outbound Intrusion Detection (OID), but the aims of Ontology-Based MADIDS not only detect intrusion on a single host, but also in a distributed do- main, also with the help of P2P architecture. So if one host detects and adds a new attack to the ontology, it shares it to the other hosts. This implementation makes the framework more flexible and robust and to enable more intelligent behavior in agents. The authors cover different types of Network Attack, which are DoS, R2L, U2R and Probe, also this system is tested on the attack R2L, but never implemented in real cases.

2. Theoretical Foundations

2.1. Computer and Network Security

Nowadays computers and the Internet are used almost in every part of our lives: saving all the data, purchases, office, electronic transactions, learning …etc. With the possibility of connecting several computers and networks was born the necessity of protecting all this data and machines from attackers (hackers) [8]. Computer security is the process of preventing and detecting unautho- rized use of your computer. Prevention measures help to stop unauthorized users from accessing any part of our computer system. In addition, detection helps to deter- mine whether someone attempted to break into our sys- tem, if they were successful or not, and what they may have done [1]. Computer security infrastructure is based on the following three mains security services: confidenti- ality, integrity, and availability in a computer system. Con- fidentiality is the intruder has access to confidential infor- mation and Integrity means that information can be modi- fied or altered by the attacker. Availability means that the system gets blocked so it cannot be used normally [8].

2.2. Vulnerabilities

Vulnerabilities in network security can be summed up as the “soft spots” that are present in every network. The vulnerabilities are present in the network and individual devices that make up the network. Networks are typically plagued by one or all of three primary vulnerabilities: tech- nology weaknesses, configuration weaknesses and se- curity policy weaknesses: [2][11] (they are primary but are not just limited to these three factors).

- Technological Weaknesses: Computer and network technologies have intrinsic security weaknesses. These include TCP/IP protocol

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-1, 2017
DOI: 10.21276/ijcesr.2017.4.1.7

weaknesses, operating system weaknesses, and network equipment weaknesses.

• Configuration Weaknesses: Network administrators or network engineers need to learn what the configuration weaknesses are andcorrectly configure their computing and network devices to compensate.

• Security Policy Weaknesses: Security policy weak- nesses can create unforeseen security threats. The net- work can pose security risks to the network if users do not follow the security policy.

2.3. Intrusion Detection Systems

Several terms are associated in the security that is re- lated to Intrusion are as follows:

• Intrusion: Any set of actions that attempt to compro- mise the integrity, confidentiality, or availability of a com- puter resource [3]. An intrusion consists of a number of related steps performed by the intruder that violate a given security policy [19].

• Intrusion Detection: Intrusion detection is a set of tech- niques and methods that are used to detect suspicious activity (actions that attempt to compromise the integrity, confidentiality, or availability of a computer resource) both at the network and host level [10]. More formal definition: it relates to the problem of identifying individuals who are using, or attempting to use a computer system without authorization (crackers) and those who have legitimate access to the system but are abusing their privileges (the insider threat) [20].Intrusion Detection Systems: Intrusion detection sys- tems help computer systems to prepare and deal with attacks. They collect information from a variety of van- tage points within computer systems and networks, and analyze these information for symptoms of security prob- lems [19][6][3].

2.4. Analysis types

Intrusion detection systems must be able to distinguish between normal and abnormal activities in order to dis- cover malicious attempts in time:

• Misuse Detection: The Signature Based Detection com- pares a possible threat with the attack type already stored in the IDS. The limitation of this type of detection tech- nique is that if any new type of threat comes which is not already known to the IDS, the system becomes vulner- able to that attack [23]. Misuse detectors are very effec- tive at detecting attacks without generating an overwhelm- ing number of false alarms.

• Anomaly Detection: in this type of detection, the IDS looks for vulnerabilities based on rules set forth by the user and not on the basis of signatures already stored in the IDS. This type of detection usually uses Artificial In- telligence to distinguish between normal traffic and anoma- lous traffic [23]. IDSs based on anomaly detection detect unusual behavior and thus have the ability to detect symp- toms of attacks without specific knowledge of details. However, anomaly detection approaches usually produce a large number of false alarms due to the unpredictable behaviors of users and networks [24].

4.5. Multi-agent systems (MAS) and Ontology based IDS

Multi-agent systems (MASs) are systems consisting of more than one autonomous agent that are able to inter- act with one another.. The particular characteristic here is that in order to achieve their goal(s), these agents must coordinate their actions [7]. The multi-agent system has become an increasingly powerful tool in developing com- plex systems that take advantages of agent properties. Originally, multi-agent systems came from the field of ar- tificial intelligence (AI). At first, this field was called dis- tributed artificial intelligence (DAI) [22][17]. Moreover, Multi- Agent Systems

(MAS) is a field of very active research. It has become a new paradigm provides a very suitable ar- chitecture for a design and implementation of dynamic open system such as: Security, e-learning, Ecommerce…etc. With agent-based technologies, a support for com- plex information systems development is introduced by natural decomposition, abstraction and flexibility of man- agement for organizational structure changes. A MAS is a community of autonomous agents working together, sometimes complex ways of cooperation, coordination, competition, in order to achieve a goal: solving a complex problem. The MAS paradigm is a very appropriate plat- form for IDS and extracting relations and meaning of con- cepts using ontologies.

Ontology-based IDS solutions are becoming increasingly used in information security. Raskin in [15] developed an ontology for the data integrity of web resources and advo- cated the use of ontologies for information security. On- tology is the explicit specification of the conceptualization of a domain which captures its context. Ontological mod- els are flexible in defining, nearly any concept to the de- sired level of detail. They are also fairly easy to extend and the logical foundations of modern ontology languages allows reasoning over concepts within a knowledge base Reasoning over the instances of the data within the do- main can be used to infer new knowledge and to integrate. data. Moreover, ontological models can be easily shared, refined and reused between entities in a domain [9].

3.Modeling of the Proposed Approach

Currently, there are various kinds of intrusions and at- tacks that can damage computer security. Therefore, we focused on intrusion detection system because it is be- coming in important package in security system. Our benchmark is constituted using multi-agent system and formal ontology in order to facilitate the communication between agents.

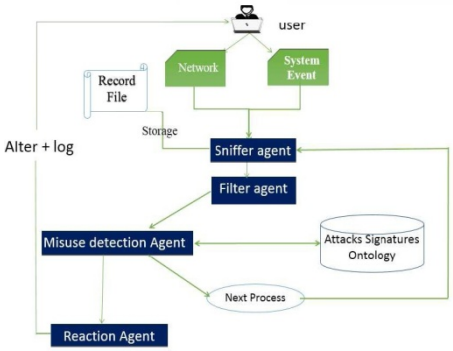


Figure 1. The proposed model of our approach

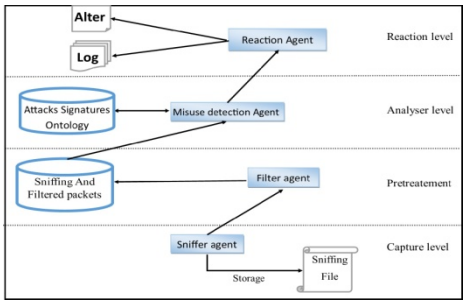


Figure 2. Detailed architecture of

IDS is composed of different cooperative, communicant and collaborative agents for collecting and analyzing mas- sive amounts of data represented in formal ontology. How- ever, the ontology is a large among of data in order to define intrusion. Thus, we propose our distributed archi- tecture that contains various agents for collecting and analyzing the data in the environment. These agents work in different levels: capture level, pre-treatment level, analy- sis level, and reaction level. The agents collect and ana- lyze the data from the environment to define the attacks exploited by the intruders. Our system contains the fol- lowing agents:

- The Sniffer Agent: It is the primer agent, that captures (catches) packets and events from the network, and sends them to other agents to be Filtered, and processed.

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-1, 2017
DOI: 10.21276/ijcesr.2017.4.1.7

• Filter Agent: It receives data from Sniffer Agent then it collects packets and filters them.

• The Misuse Detection Agent: It analyzes the collected and filtered packets, and compares the found signatures with the predefined patterns.

• Reaction Agent: It manages the events to generate reports and logs to inform the user about the intruder.

Finally, the Misuse Detection Agent sends message to sniffer agent to Process the next packet. IDSMOnto de- tects the known attacks through the intelligent agent MisuseAgent which uses ontology to enrich data intru- sions and attack signatures by semantic relationships.

4. Detailed Architecture of our Proposed System

This section describes the proposed model by making use of ontology exploited by a set of intelligent agents.

4.1. Sniffer Agent (Sniffer_A)

Sniffer Agent or capture agent records all the traffic over the network and displays them, like network connection and records all the system events such as system file operation. The sniffer agent has two-class System_Sniffer and Network_Sniffer. First, the sniffer network is respon- sible for recording all traffic that pass over the network and stores them in the memory. It records several at- tributes about network: IP address, source, and IP ad- dress of destination, whether the host has a successful connection, length of packet (the number of seconds), type of the protocol (TCP, UDP …etc.) and the port num- ber …etc. Second, system sniffer is responsible to record the events of the host system (operating system, appli- cations …etc).

Moreover, Sniffer_A can be distributed over the host (net- work and system) and duplicated to get more informa- tion. Sniffer agent gets all the list of interfaces, after that the user chooses the needed interface; then the sniffer agent opens the device (interface) and starts to sniff and get the packets from the network and sends it to Filter_AIn addition, the important work of this agent is stores these information of the network and the system in a Record File

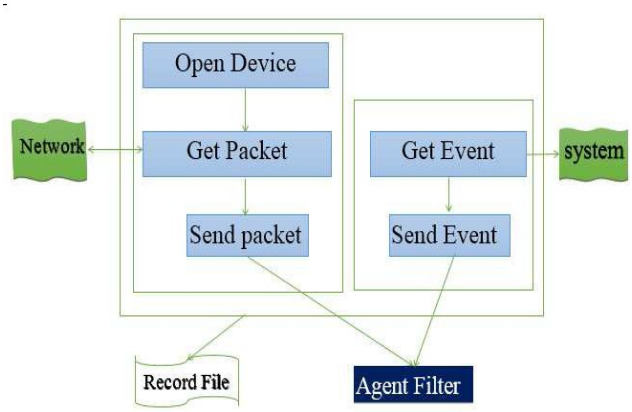


Figure 3. Sniffer agent architecture

4.2. Filter Agent (Filter_A)

The filter agent receives the data from sniffer agent or it can read it from Record File. The main role of Filter Agent is distinguishing the various types of the collected events and traffic: destination address, used protocol, packet category (TCP, UDP, ICMP, etc.); because each kind of information is concerned by a specific kind of intrusion. Thistask is important because it helps Misuse_detection_A to define the intrusion and facilitate the detection in time. The Filter_A performs its tasks as a pre-treatment phase, which precedes the analysis phase carried out by the following agent

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-1, 2017
DOI: 10.21276/ijcesr.2017.4.1.7

Figure 4. Filter agent architecture

4.3. Misuse Detection Agent (Misuse_detection_A) Misuse Detection Agent or analyzer agent, analyzes the packets captured by the Sniffer_A and then pre-processed by the Filter_A. In fact, Misuse_detection_A searches for attack signatures in these packets. When Misuse_detection_A detects an intrusion or attack, it sends a notification to Reaction Agent. This agent cannot detect the attacks without their Signatures, so the signa- ture Ontology was defined. This ontology contains many attack signatures, which are used to discover intrusions or attacks through (mapping the signatures of filtered pack- ets with the signatures ontology).

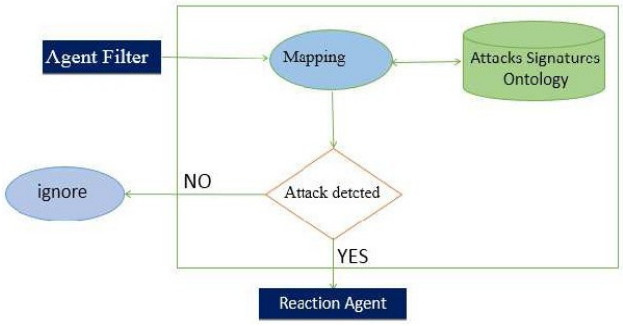
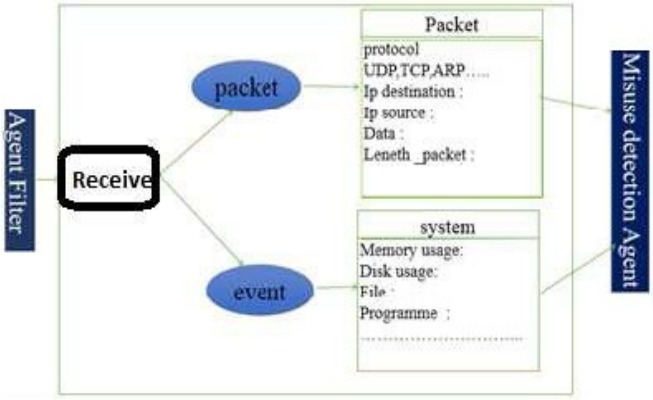


Figure 5. Misuse detection agent architecture

In the case of 100 % similarity between the events ontol- ogy and any signature attack ontology, the system alerts the user and gives the necessary information about the attack (type, addresses, port …etc). But, if there is not total similarity (100 %), we proposed the shortest path method (simple and efficient method in our case) to cal- culate semantic similarity based on the ontology hierar- chy, suggesting that the shortest path between two nodes was the simplest approach for measuring distance be- tween two terms [16]. In mathematics, the formula for the distance between two nodes by the shortest path was



denoted by, Sim(c1, c2) = 2 ☐ MAX ☐ c1 and c2 were

the compared nodes, MAX the maximum path on the hierarchy, and L the shortest path. The main advantage of this method was its low complexity in calculation. More- over, when only the is-a relationship existed in a seman- tic network, semantic relatedness and semantic distance were equivalent. However, this method was short of con- sideration for different kinds of edges as well as the se- mantic relatedness representing these edges. According to the Similarity degree, the misuse agent alerts the user by the susceptible attack and gives the degree of simi- larities with the different attacks.

4.4. Reporter (reaction) Agent

To implement passive response to security incidents, the Misuse Detection Agent report its results to the Reaction Agent. Whenever an intrusion is detected, Reaction Agent sends an alert to the system (or user). This alert can be a message popup on the screen or a message to a central- ized machine or an alert file. The result record contains the information including source IP (Source Host), type of the suspicious attack (Attack Type) ...etc. In addition, the Report_A decides the response type to implement it according to the detected event.

4.5. Ontology

Our ontology represents our database system. We adopt ontology technique to represent

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-1, 2017
DOI: 10.21276/ijcesr.2017.4.1.7

intrusion and detection knowledge (attacks signatures). Ontology has been de- veloped using the detailed description of all-important security concepts and attacks signatures. Several attacks are represented by the ontology and we use this ontology to provide detection process (mapping process) to inform the user to take the appropriate actions. The power and utility of the ontology is realized by the fact that we can express the relationships between collected data and use those relationships to deduce that the particular data rep- resents an attack of a particular type.

After collecting the information about the received packet, Misuse detection agent forms the ontology of the packet (representing this packet). Then, this agent performs the process of mapping (calculate the similarity) between the created ontology (packet ontology) and the ontologies that represent the attacks signatures as it is explained in the section 5.3.

4.5.1. Network traffic Representation

The traffic ontology (depicted in the figure 6) represents the network traffic in a variety of forms. This ontology contains the descriptions and the models of all the sus- ceptible packets, and then the system creates instances for all captured packets (ontological form). If the packet represents a TCP or UDP or ICMP packet, the system creates an instance, and then a Packet is added as an instance according to the type of the instance. From these packet instances, other new instances are created in the knowledge base using inference, which is performed by a reasoner. For example: the ICMPPacket class is a sub- class of the IPPacket class and lPPacket is subclass of Packet. When an ICMPPacket instances is created, the reasoner will use inference to create an instance in the IPPacket class because of the subclass relation. The reasoner will continue to traverse up the class tree, cre- ating instances in the parent classes. The IPPacket class hasDestMAC, hasDesCtIP, hasSrcMAC, hasSrcIP,Time and Data.

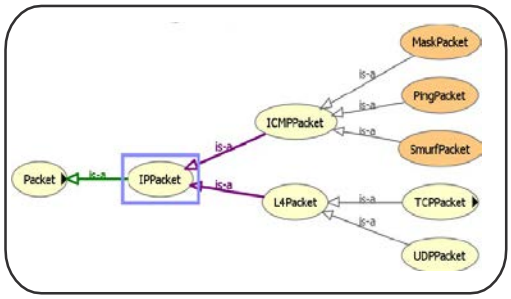


Figure 6. Packet types Ontology

Figure 7. Packet Collection Ontology

The PacketCollection class shown in the figure 7 is used to group common packet instances and classify them according to the type of the packet (PacketType class). For instance, if there were multiple ping packets to the same node within a specific time frame, an instance was created in the PacketCollection class of PacketType and PingFloodType. These instances were later used by IDSMAOnto to assist the attack identification.

4.5.2. Representation (Attacks signatures ontology) The attack ontology (Figure 8) is used to provide informa- tion about simple and complex attacks. The attack data is obtained by using inference through ontology constructs and rules. The figure 8 (attack ontology) presents a part view of our ontology. The Class thing (representing the class of all things) contains class Attackpacket has sub- class Attack. This latter class is comprised of the follow- ing subclasses:

- Recon: Refers to Reconnaissance, it means gathering information. This attack has intention to gather informa- tion by using scan technique such as: scan TCP or sniff- ing …etc.

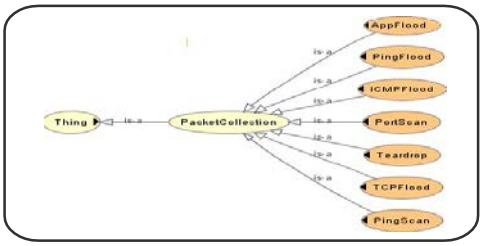
- GainAccess: Not having official permission or approval to the network. This includes the following subclasses: privilege gains or unauthorised access.

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-1, 2017
DOI: 10.21276/ijcesr.2017.4.1.7

• ViewChangeData: This class contains attributes rep- resenting malicious code that aim to change data (alter- ation).

• Availability: This class contains attributes represent- ing attack DOS and spoofing.

The figure 9 shows the Availability classes. There are two primary techniques an attacker may use to make a host or network unavailable. These two techniques are a de- nial of service or spoofing attack. An attacker gains unau- thorized access to a computer or a network by



making it appears that a malicious message has come from a trusted machine. There are two primary techniques using spoofing ARPspofing and IPspoofing.

The class DOS (figure 10) contains attributes represent- ing particular attack DOS(Denial of Service). DOS attack has two subclasses CrashNode and Resources. These classes represent more than one type of attacks. For example, a SYN flood, smurf, teardrop, ping–of–death.

Figure 11 illustrates ping of death attack using owl lan- guage, it has packetLenof 65535 and protocol is ICMP.

Our system uses another type of attack (figure 13): com- plex attack. Complex DOS has a set of attributes that represent simple attacks: a Ping scan, Node scan, and Availability attack.

The system is designed to use attack ontology and the ontology of captured traffic (calculation of similarity) to define the susceptible attacks. This allows better adapt- ability and flexibility in attack detection. The majority of the customized code was to initially populate the knowl- edge base with traffic data using a mapper program de- veloped using Java and Jena.

7. Conclusion

Using ontology with Multi-Agent System and reasoning models in the Intrusion detection systems (IDS) is a prom- ising and efficient approach. The detection architecture based on reaction rules generated by the intelligent and correlated component in our IDSMAOnto creates new reaction rules in other security components. Ontology of attacks (signatures) and communication protocols pro- vide a powerful construct for improving the detection ca- pability of the application. Various instances of attacks and corresponding vulnerabilities are tested. This work presented an ontological model integrated with multiagent system using artificial intelligence that provide better per- formance in processes such as knowledge representa- tion, cooperation, , intelligence reasoning, reactivity…etc. The use of IDSMAOnto is a valuable asset to a network manager, it allows him to understand the weaknesses in the network and take corrective action to prevent future attacks.

In future work, we aim to work on the detection of other types of attacks such as: DDoS and variants of the DoS, SQL Injection and others, and extend the number of tests and real case study.

References

[1] Ateeq, A. (2012). Type of Security Threats and It's Prevention, International journal of Computer Technology & Applications, vol. 3, no. 2, 750-752. ISSN:2229-6093.

[2] Mukesh, K. Navpreet, K. Sukhjinder, K. and Rajpal, S. (2016). Different Security Threats and its Prevention in Computer Network, International Journal of Advanced Re- search in Computer Science, vol. 7, no. 6.

[3] Vijayarani, S. and Sylviaa, S.M. (2015). Intrusion de- tection system-study, International Journal of Security, Privacy and Trust Management. (IJSPTM) Vol 4, No 1.

[4] Laftah, W. Ali Othman, Z. and Ahmad Nazri, M.Z. (2016). Real-Time Intrusion Detection System Using Multi-agent

System.IAENG International Journal of Computer Sci- ence, vol. 43, no. 1.

[5] Brahmi, I. Brahmi, H. Yahia, S. (2015). Multi-agents Intrusion Detection System Using Ontology and Cluster- ing Techniques, IFIP Advances in Information and Com- munication Technology, DOI: 10.1007/978-3- 319-19578-0_31.

[6] Gaigole, M.S. and Kalyankar, M.A. (2015). The Study of Network Security with Its Penetrating Attacks and Possible Security Mechanisms, International Journal of Com- puter Science and Mobile Computing, 4 (5).

[7] Nagwani, N.K. (2010). An Open Source Multi Agent System for Data Preprocessing of Online Software Bug Repositories, International Journal of Computer Applica- tions, 1 (8) 55-59.

[8] Soleiman, E.M. and Abdelhamid, F. (2014). Using Learning Vector Quantization (LVQ) in Intrusion Detec- tion Systems.International Journal of Innovative Research in Advanced Engineering (IJIRAE), 1 (10).

[9] Razzaq, A. Anwar, Z. Ahmad, F. Latif, K. Munir, F. (2014). Ontology for attack detection: An intelligent ap- proach to web application security. Computers &Secu- rity, V. 45, p 124-146.

[10] Rafeeq, R. (2003). Intrusion Detection Systems with Snort:Advanced IDS Techniques with Snort, Apache, MySQL, PHP. Library of Congress Cataloging-in- Publi- cation Data.

[11] Rieke, R. (2014). Security analysis of system behav- ior- From security by deign to security at runtime. PHD Dissertation, Philipps-Universität Marburg alsDisserta- tion am, Marburg.

[12] Raoui, D. Benhadou, S.andMedromi, H. (2010). Methodology for Intrusion Detection based on Multi- Agents System. Journal of Engineering and Technology Research. 2 (10) 200-206.

[13] Isaza, G. Castillo, A. Lopez, M., Castillo, L. (2010). Towards Ontology- Based Intelligent Model for Intrusion Detection and Prevention. Journal of Information Assur- ance and Security, vol 5.p 376- 383.

[14] Tripti, S. and Khomlal, S. (2011). Intrusion Detection Systems Technology.International Journal of Engineering and Advanced Technology (IJEAT), 1 (2).

[15] Raskin, V. Hempelmann, C.F. Triezenberg, K.E. Nirenburg, S.(2001). Ontology in information security: a

useful theoretical foundation and methodological tool. in: Proceedings of the 2001 Workshop on New Security Para- digms, ACM, p. 53–59.

[16] Rada, R. Mili, H. Bicknell, E. and Blettner, M. (1989). Development and application of a metric on semantic nets, IEEE Transactions on Systems, Man and Cyber- netics, vol. 19, p. 17–30.

[17] Pipattanasomporn, M. Rahman, S. Feroze, H. (2009). Multi-Agent Systems in a Distributed Smart Grid: Design and Implementation .IEEE PES Power Systems Confer- ence and Exposition (PSCE'09),Seattle, Washington, USA.p 1-8.

[18] Pinkston, J. Undercoffer, A. Joshi , and Finin T. (2004). A Target-Centric Ontology for Intrusion Detection.Univer- sity of Maryland, Baltimore County Department of Com- puter Science and Electrical Engineering.

[19] Jazayeri, M. (2003). Improving intrusion detection systems, PHD dissertation, University of Vienna. Mia.

[20] Djemaiel, Y. (2010). Tracing, detecting and tolerat- ing attacks in communication networks. PhD Thesis, tunis Engineering School of Communication SUP'COM.

[21] Dayong, Y. Quan, B. and Z. Minjie, Z. (2008). Ontol- ogy-based knowledge representation for a P2P multi-agent distributed intrusion detection system. IFIPA International Conference on Network and Parallel Computing, IEEE Computer Society, Los Alamitos, California, p. 111-118.

[22] Bousquet, F. Le Page, C. (2004). Multi-agent simu- lations and ecosystem management: a review, Ecologi- cal Modelling, 176, 313–332.

[23] Borgohain, R. (2012). FuGeIDS : Fuzzy Genetic para- digms in Intrusion Detection Systems. Int. J. Advanced Networking and Applications, 03 (06) 1409-1415.

[24] Bace, R. Mell, P. (2001). Intrusion detection systems.NIST Special Publication on Intrusion Detection Systems.