OMAIDS: A Multi-agents Intrusion Detection System Based Ontology

Imen Brahmi(✉) and Hanen Brahmi

Computer Science Department, Faculty of Sciences of Tunis,
Campus University, 1060 Tunis, Tunisia
imen.brahmi@gmail.com

Abstract. Nowadays, as a security infrastructure the *Intrusion Detection System* (IDS) have evolved significantly since their inception. Generally, most existing IDSs are plugged with various drawbacks, *e.g.*, excessive generation of false alerts, low efficiency, etc., especially when they face distributed attacks. In this respect, various new intelligent techniques have been used to improve the intrusion detection process. This paper introduces a novel intelligent IDS, which integrates the desirable features provided by the multi-agents methodology with the benefits of semantic relations. Carried out experiments showed the efficiency of our distributed IDS, that sharply outperforms other systems over real traffic and a set of simulated attacks.

Keywords: Intrusion Detection System · Multi-agents · Ontology

1 Introduction

Due to the growing threat of network attacks, the efficient detection as well as the network abuse assessment are becoming a major challenge. In this respect, the Intrusion Detection System (IDS) has been of use to monitor the network traffic thereby detect whether a system is being targeted by network attacks [2]. Even that IDSs have become a standard component in security infrastructures, they still have a number of significant drawbacks. In fact, they suffer from problems of reliability, relevance, disparity and/or incompleteness in the presentation and manipulation of knowledge as well as the complexity of attacks. This fact hampers the detection ability of IDS, since it causes the generation excessive of false alarms and decreases the detection of real intrusions [2,4].

Indeed, needless to remind that the integration of a multi-agents technology within the IDS can effectively improve the detection accuracy and enhance the system's own security. In fact, the use of multi-agents system for intrusion detection offers an appropriate alternative to the IDS with several advantages listed in literature, *e.g.*, independently and continuous running, minimal overhead, distributivity, *etc.*, [2]. Therefore, multi-agents technology makes the resilience of the system strong and thus ensures its safety [3].

In addition, the concept of ontology has emerged as a powerful method that can improve the intrusion detection features. Thus, the ontology has been shown

K. Jackowski et al. (Eds.): IDEAL 2015, LNCS 9375, pp. 156–163, 2015.
DOI: 10.1007/978-3-319-24834-9_19

to be useful in enabling a security analyst to understand, characterize and share a common conceptual understanding threats [6,9]. Besides, it provides semantic checking to design the signature rules using the SWRL (*Semantic Web Rule Language*) [5], that can solve the disparity issue of security knowledge.

In this paper, we introduce a new distributed IDS, called OMAIDS (*Ontology based Multi-Agents Intrusion Detection System*). OMAIDS stands within the crossroads of the multi-agents system and the ontology technique. Through extensive carried out experiments on a real-life network traffic and a set of simulated attacks, we show the effectiveness of our system.

The remaining of the paper is organized as follows. Section 2 sheds light on the related work. We introduce our new distributed intrusion detection system in Sect. 3. We then relate the encouraging results of the carried out experiments in Sect. 4. Finally, Sect. 5 concludes and points out avenues of future work.

2 Scrutiny of the Related Work

Recently, few approaches are dedicated to the use of semantic web within the intrusion detection field. Worth of mention that the first research in this area was done by Undercoffer *et al.* [9] in 2003. The authors developed an ontology DAML-OIL focused on the target (*centric*) and supply it within the format of the logical description language DARPA *DARPA Agent Markup Language + Ontology Inference Layer*. The proposed ontology is based on the traditional taxonomy classification migrated to semantic model. It allows modeling the domain of computer attacks and facilitates the process of reasoning to detect and overcomes the malicious intrusions.

Based on the DAML-OIL ontology [9], Mandujano [7] investigates an attack ontology, called OID (*Outbound Intrusion Detection*). The introduced ontology provides agents with a common interpretation of the environment signatures, through a FORID system. The latter detects the intrusions based on a matching strategy using a data structure based on the internals of the IDS Snort [8]. Similarly to the works done in [7], Djotio *et al.* [4] proposed a multi-agents IDS, MONI, based on an ontology model, called NIM-COM. The agents are then responsible for enabling the analysis of network traffic and the detection of malicious activities, using the Snort signatures [8]. However, the approach does not consider the secure state which is important to judge false positive alerts and successful possibility of attacks [6]. With the same preoccupation, Abdoli and Kahani [1] proposed a multi-agents IDS, called ODIDS. Based on the techniques of the semantic web, they have built an ontology for extracting semantic relationships between intrusions. The criticism of the ODIDS system is time wasting, since the system needs more time to make a connection between the agents on the network and to send and receive messages between them.

Due to its usability and importance, detecting the distributed intrusions still be a thriving and a compelling issue. In this respect, the main thrust of this paper is to propose a distributed IDS, called OMAIDS, which integrates : (*i*) a multi-agents technology and (*ii*) an ontology model. In this respect, it is shown that the use of such architecture reveals conducive to the development of IDSs [1,3,4,6,7]. The main idea behind our approach is to address limitations of centralized IDSs, by taking advantage of the multi-agents paradigm as well as the ontological representation.

3 The OMAIDS System

Agents and multi-agents systems are one of the paradigms that best fit the intrusion detection in distributed networks [2]. In fact, the multi-agents technology distributes the resources and tasks and hence each agent has its own independent functionality, so it makes the system perform work faster [3].

The distributed structure of OMAIDS is composed of different cooperative, communicant and collaborative agents for collecting and analyzing massive amounts of network traffic, called respectively: SnifferAgent, MisuseAgent and ReporterAgent. Figure 1 sketches at a glance the overall architecture of OMAIDS.

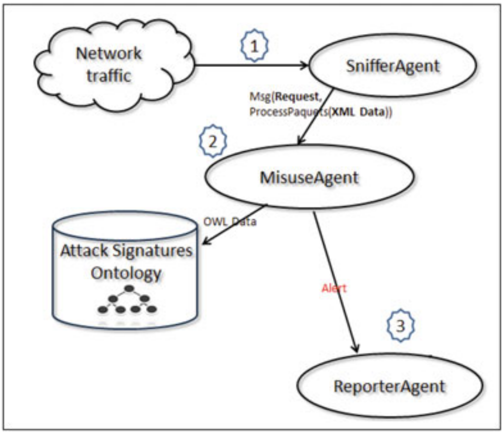


Fig. 1. The architecture of OMAIDS at a glance.

The processing steps of OMAIDS can be summarized as follows:

1. The SnifferAgent captures packets from the network. Indeed, a distributed IDS must undertake to analyze a huge volumes of events collected from different sources around the network. Consequently, the SnifferAgent permits to filter the packets already captured. Besides, it converts them to XML, using the XStream library[1]. Finally, the pre-processed packets will be sent to others agents to be analysed;

[1] Available at: http://xstream.codehaus.org/.

2. The MisuseAgent receives the packets converted to XML from the SnifferAgent. It transforms these packets to OWL format in order to be compatible with the SWRL rules stored in the ontology. Now, it is ready to analyze the OWL packets to detect those that correspond to known attacks. Indeed, the MisuseAgent searches for attack signatures[2] in these packets, by consulting the ontology ASO (*Attack Signatures Ontology*). Consequently, if there is a similarity between the OWL packets and the SWRL rules that define the attack's signatures, then the agent raises an alert to the ReporterAgent;
3. Finally, the ReporterAgent generates reports and logs.

OMAIDS detects the attacks through the intelligent agent MisuseAgent, which uses an ontology to enrich data intrusions and attack signatures by semantic relationships. In what follows, we present the proposed ontology.

3.1 The Attack Signatures Ontology (ASO)

Ontologies present an extremely promising new paradigm in computer security domain. They can be used as basic components to perform automatic and continuous analysis based on *high-level* policy defined to detect threats and attacks [6]. Moreover, they enable the IDS with improved capacity to reason over and analyze instances of data representing an intrusion [4,9]. Furthermore, the interoperability property of the ontologies is essential to adapt to the problems of the systems distribution, since the cooperation between various information systems is supported [4,6].

Within the OMAIDS system, an ontology, called ASO (*Attack Signatures based Ontology*), is implemented, in order to optimize the knowledge representation and to incorporate more intelligence in the information analysis. The ASO ontology allows the representation of the signatures basis for attacks, used with the agent MisuseAgent. Figure 2 depicts a fragment of the ontology ASO, which implements the intrusion detection knowledge. The power and usefulness of ontology, applied to the signature basis issue, provide a simple representation of the attacks expressed by the semantic relationships between intrusion data. We can also infer additional knowledge about intrusion due to the ability of the ontology to infer new behavior by reasoning about data. Therefore, this fact improves the process of decision support for an IDS [1,3,9].

The signature basis incorporates rules provided by the ASO ontology, that allows a semantic mean for reasoning and inferences. In fact, the rules are extracted using the SWRL language (*Semantic Web Rule Language*). The latter extend the ontology and enriches its semantics by the deductive reasoning capabilities [5]. It allows to handle instances with variables (?x, ?y, ?z). Thus, the SWRL rules are developed according to the scheme: *Antecedent* → *Consequent*, where both antecedent and consequent are conjunctions of atoms written $a_1 \wedge$ $...\wedge\ a_n$. Variables are indicated using the standard convention of prefixing them

[2] An attack signature is a known attack method that exploits the system vulnerabilities and causes security problem [2].

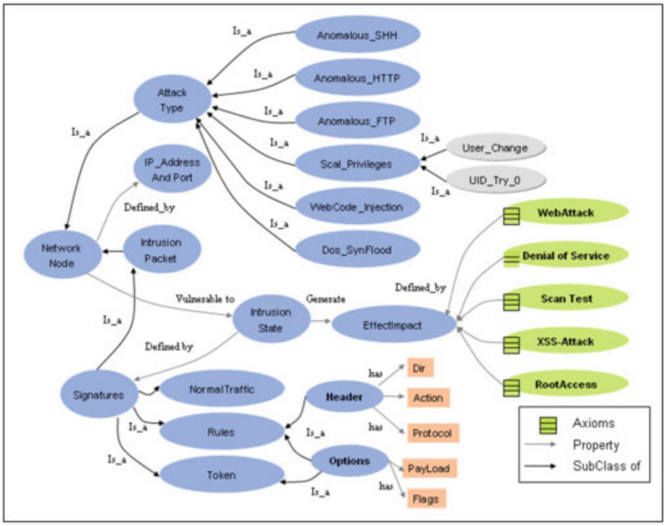


Fig. 2. The Attack Signatures based Ontology ASO.

with a question mark (*i.e.*, "?x"). The following example shows a rule represented with SWRL.

Example. NetworkHost(?z) ∧ IntrusionState(?p) ∧ GeneratedBY(?p,?z) ∧ SQLInjection(?p) ∧ Directd_To(?p,?z) → SystemSQLInjectionState(?p,?z).

Using this syntax, a rule asserting that the composition of the network host(z) and an intrusion state(p) properties implies the attack "*SQL Injection*" property.

4 Experimental Results

In order to assess the overall performance of OMAIDS in a realistic scenario, a prototype of the proposed architecture was implemented using Sun's Java Development Kit 1.4.1, the well known platform JADE[3] 3.7, the Eclipse and the JPCAP[4] 0.7. The ontology ASO is designed using PROTÉGÉ[5].

Through the carried out experiments, we have a twofold aim: (*i*) first, we focus on the assessment of the interaction between agents; (*ii*) Second, we have to stress on evaluating the performance of our system in term of detection ability.

4.1 Interaction Between Agents

Generally, within the existing centralized IDSs, the designed feature of communication and cooperation between their components are badly missing [2]. This

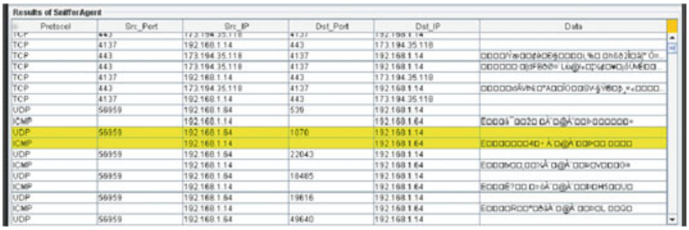
[3] Available at: http://jade.tilab.com.

[4] Available at: http://netresearch.ics.uci.edu/kfujii/jpcap/doc/.

[5] Available at: http://protege.stanford.edu/download/download.html.

latter constitutes the main hamper towards efficient detection of attacks [2]. Tacking in the account this issue, the multi-agents architecture of OMAIDS allows to facilitate the communication and the interaction between the agents that operate as the IDS components. In fact, the agents use the ACL (*Agent Communication Language*) language to communicate. Moreover, the information transmitted among agents is sent as text messages and the process complies with the FIPA (*Foundation for Intelligent Physical Agents*)[6] protocols.

The OMAIDS uses several agent's group (sniffing, filtering, analyzing, reporting). Some of these agents need high communication, with rich information, and others just need to share a reduced amount of information. Firstly, the SnifferAgent is responsible of capturing network traffic needed to carry out its task of generating and converting the packets. Figure 3 shows a SnifferAgent whenever a *TCP Connect Scan*[7] is captured and filtered.



Results of SnifferAgent

Protocol	Src_Port	Src_IP	Dst_Port	Dst_IP	Data
TCP	443	173.194.35.118	4137	192.168.1.14	
TCP	4137	192.168.1.14	443	173.194.35.118	
TCP	443	173.194.35.118	4137	192.168.1.14	[illegible]
TCP	443	173.194.35.118	4137	192.168.1.14	[illegible]
TCP	4137	192.168.1.14	443	173.194.35.118	
TCP	443	173.194.35.118	4137	192.168.1.14	[illegible]
TCP	4137	192.168.1.14	443	173.194.35.118	
UDP	56959	192.168.1.64	539	192.168.1.14	
ICMP		192.168.1.14		192.168.1.64	[illegible]
UDP	56959	192.168.1.64	1070	192.168.1.14	
ICMP		192.168.1.14		192.168.1.64	[illegible]
UDP	56959	192.168.1.64	22043	192.168.1.14	
ICMP		192.168.1.14		192.168.1.64	[illegible]
UDP	56959	192.168.1.64	18485	192.168.1.14	
ICMP		192.168.1.14		192.168.1.64	[illegible]
UDP	56959	192.168.1.64	19616	192.168.1.14	
ICMP		192.168.1.14		192.168.1.64	[illegible]
UDP	56959	192.168.1.64	49640	192.168.1.14	

Fig. 3. SnifferAgent within *TCPConnect*.

Once the captured packets are filtered and converted to XML, the SnifferAgent informs the MisuseAgent to analyze these packets. The information includes: (*i*) the protocol; (*ii*) the source IP and port; and (*iii*) the destination IP and port. Based on the signature rules stored in the knowledge base of the ontology ASO, loaded during startup, whenever the MisuseAgent perceives a similarity between a packet and a rule, then it detects an attack. Besides, it informs the ReporterAgent with the "abnormal" network status. The information includes: (*i*) an alert information indicating that an attack occurs; (*ii*) the date and the time of detection; (*iii*) the IP addresses of both attacker and victim; and (*iv*) the name of the attack.

Finally, we conclude that the agents of our system OMAIDS cooperate by using a reliable communication mechanism. This cooperation is driven by interests expressed by the agents.

4.2 The Detection Ability

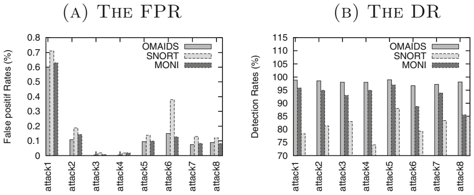
In order to evaluate the detection ability of an IDS, two interesting metrics are usually of use [2]: the *Detection Rate* (DR) and the *False Positive Rate*

[6] Available at: http://www.fipa.org.

[7] TCP Connect Scan is a scan method used by the operating system to initiate a TCP connection to a remote device. It allows to determine if a port is available.

(FPR). Indeed, the DR is the number of correctly detected intrusions. On the contrary, the FPR is the total number of normal instances that were "incorrectly" considered as attacks. In this respect, the value of the DR is expected to be as large as possible, while the value of the FPR is expected to be as small as possible.

During the evaluations, we compare the results of the OMAIDS system *vs.* that of the IDS Snort [8] and the multi-agents based ontology one MONI[8] [4]. Moreover, we simulated attacks using the well known tool *Metasploit*[9] version 3.5.1. The simulated eight different attack types are: **attack1**: DoS Smurf; **attack2**: Backdoor Back Office; **attack3**: SPYWARE-PUT Hijacker; **attack4**: Nmap TCP Scan; **attack5**: Finger User; **attack6**: RPC Linux Statd Overflow; **attack7**: DNS Zone Transfer; and **attack8**: HTTP IIS Unicode.


(a) The FPR

(b) The DR

Fig. 4. The FPR and the DR of OMAIDS *vs.* Snort and MONI.

With respect to Fig. 4(a), we can remark that the FPR of OMAIDS and MONI is significantly lower compared to that of Snort. This fact is due to the adaptive mechanisms used by the agents, enabling both systems, *i.e.*, OMAIDS and MONI, to better suit the environment. Consequently, the false alarms can be reduced correspondingly. For example, for attack3 the FPR of Snort can reach values as high as 0.019 % compared to 0.007 % of MONI and 0.005 % of OMAIDS.

Moreover, Fig. 4(b) shows that the DR of OMAIDS is higher than that of MONI. Moreover, among the three investigated IDS, Snort has the lowest DR. For instance, for attack3, whenever OMAIDS and MONI have the DR 97.9 % and 94.9 %, respectively, Snort has 74.1 % DR. This is due to his centralized architecture.

Knowing that a main challenge of existing IDSs is to decrease the false alarm rates [2], the main benefit of our system is to lower the false alarm rate, while maintaining a good detection rate.

5 Conclusion

In this paper, we focused on a distributed architecture and multi-agents analysis of intrusions detection system to tackle the mentioned above challenges within

[8] We thank Mrs. Djotio *et al.* [4] for providing us with the implementation of MONI system.

[9] Available at: http://www.metasploit.com/.

the IDSs, *i.e.*, the badly communication as well as the low detection ability. Thus, we introduced a multi-agents intrusions detection system called OMAIDS based on an efficient ontology model, called ASO. The carried out experimental results showed the effectiveness of the OMAIDS system and highlighted that our system outperforms the pioneering systems fitting in the same trend.

Worth of mention that the combination of the detection known attacks as well as the unknown ones can lead to improve the performance of the IDS and enhances its detection ability [2]. In this respect, our future work focuses on the integration of data mining techniques within the OMAIDS system.

References

1. Abdoli, F., Kahani, M.: Ontology-based distributed intrusion detection system. In: Proceedings of the 14th International CSI Computer Conference CSICC 2009, Tehran, Iran, pp. 65–70 (2009)
2. Brahmi, I., Ben Yahia, S., Aouadi, H., Poncelet, P.: Towards a multiagent-based distributed intrusion detection system using data mining approaches. In: Cao, L., Bazzan, A.L.C., Symeonidis, A.L., Gorodetsky, V.I., Weiss, G., Yu, P.S. (eds.) ADMI 2011. LNCS, vol. 7103, pp. 173–194. Springer, Heidelberg (2012)
3. Brahmkstri, K., Thomas, D., Sawant, S.T., Jadhav, A., Kshirsagar, D.D.: Ontology based multi-agent intrusion detection system for web service attacks using self learning. In: Meghanathan, N., Nagamalai, D., Rajasekaran, S. (eds.) Networks and Communications (NetCom2013), pp. 265–274. Springer, New York (2014)
4. Djotio, T.N., Tangha, C., Tchangoue, F.N., Batchakui, B.: MONI: Mobile agents ontology based for network intrusions management. Int. J. Adv. Media Commun. **2**(3), 288–307 (2008)
5. Horrocks, I., Patel-Schneider, P.F., Boley, H., Tabet, S., Grosof, B., Dean, M.: SWRL: A Semantic Web Rule Language Combining OWL and RuleML (2004). http://www.w3.org/Submission/SWRL/
6. Isaza, G.A., Castillo, A.G., López, M., Castillo, L.F.: Towards ontology-based intelligent model for intrusion detection and prevention. J. Inf. Assur. Secur. **5**, 376–383 (2010)
7. Mandujano, S., Galvan, A., Nolazco, J.A.: An ontology-based multiagent approach to outbound intrusion detection. In: Proceedings of the International Conference on Computer Systems and Applications, AICCSA 2005, Cairo, Egypt, pp. 94-I (2005)
8. Roesch, M.: Snort - lightweight intrusion detection system for networks. In: Proceedings of the 13th USENIX Conference on System Administration (LISA 1999), Seattle, Washington, pp. 229–238 (1999)
9. Undercoffer, J., Joshi, A., Pinkston, J.: Modeling computer attacks: an ontology for intrusion detection. In: Vigna, G., Kruegel, C., Jonsson, E. (eds.) RAID 2003. LNCS, vol. 2820, pp. 113–135. Springer, Heidelberg (2003)