A Multi-agent System-Based Distributed Intrusion Detection System for a Cloud Computing

Omar Achbarou(✉), My Ahmed El Kiram, Outmane Bourkoukou, and Salim Elbouanani

Computer Science Department, Laboratory ISI, Cadi Ayyad University, Marrakech, Morocco
omar.achbarou@gmail.com

Abstract. The Cloud security is one of the major obstacles to the adoption of cloud computing services. It requires some solutions such as Intrusion Detection Systems (IDSs) for protecting each user against all malicious. Existing IDS because of lower detection rate and higher false positive rate couldn't be suitable for a distributed environment such as the cloud. To tackle this problem, we propose a new distributed intrusion detection system based on a multi-agent system to identify and prevent known and unknown attacks in this environment. Carried out experiments demonstrated the performance and efficiency of our proposed system integrated with multi-agent technology.

Keywords: Cloud computing · Intrusion detection system · Distributed system Multi-agent systems

1 Introduction

Cloud computing is based on the logic of consumption of service, implying that responsibility for the deployment, control, management and maintenance of the infrastructure, platform or software is the responsibility of the cloud service provider (CSP) [1]. Despite the enormous technical and commercial benefits of the cloud environment, security and privacy concerns are the main obstacles to its widespread adoption around the world, and particular attention should be paid to security when choosing a cloud service. In view of these security concerns, the integration of an IDS can be important for detecting attacks or other activity that can be considered suspicious or illegal.

Existing IDS solutions have been developed for conventional networks and systems, but are not easily adaptable to a dynamic environment such as cloud computing. Thus, it is necessary to develop a flexible, secure solution that is adapted to the changing and complex evolution of the cloud environment. Although IDS models have been proposed in the research literature, IDS components alone are not able to parse all of the large reports generated. Thus, these proposed solutions remain limited due to their insulation; in other words, they are not able to collaborate or cooperate with each other. Their detection results are therefore isolated, and cannot be collected and

E. H. Abdelwahed et al. (Eds.): MEDI 2018 Workshops, CCIS 929, pp. 98–107, 2018.
https://doi.org/10.1007/978-3-030-02852-7_9

analyzed systematically. Thus, there is a need for IDS solutions based on the concepts of collaboration, cooperation, autonomy and dynamism; these concepts are needed to detect attacks effectively and to respond to intrusions by reducing response time.

In this work, we propose a solution that meets these requirements in the form of a multi-agent system-based distributed IDS (MAS-DIDS) that can identify and prevent all anomalies in a cloud environment. This system is based on a distributed architecture of IDSs that work in collaboration and communicate with each other, in order to adapt to the complexity of cloud networks. Each IDS is composed of a group of dynamic, responsive, and cooperating agents which work together to make the IDS more autonomous and flexible. The main objective of our research work is to implement a MAS-DIDS that combines the two techniques of signature-based and anomaly-based intrusion detection, in order to block both known and unknown attacks within a complex, dynamic and changing environment. Finally, the efficiency and performance of the proposed model are studied in terms of different metrics: detection rate (DR), false positive rate (FPR), and response time.

The rest of the paper is organized as follows. The next section presents a theoretical background, in which we describe the main concepts of cloud computing, IDS and our types, and multi-agent systems (MAS). We discuss several related works in the area of multi-agent IDSs in Sect. 3. Section 4 forms the core of this paper, and explains and describes our proposed model in detail. Section 5 presents the details of a performance evaluation and the effectiveness of our proposed model based on an experimental study. The final section summarizes the main contributions of this work.

2 Theoretical Background

2.1 Cloud Computing

Cloud Computing is a flexible, reliable and cost-effective environment that offers a set of services in the form of on-demand services, accessible from anywhere, anytime and by anyone. Cloud computing builds on established trends to reduce the cost of delivering services while increasing the speed and agility with which services are deployed regardless of the location of users or equipment [2].

Beyond the proposed definitions, NIST has defined a cloud computing model with five essential characteristics, three service models and three deployment models [2], as shown in Fig. 1.

In general, the architecture of a cloud computing can be divided into three layers: the infrastructure layer (IaaS: Infrastructure as a Service) application layer (SaaS: Software as a Service) and Platform layer (PaaS: Platform as a Service). Each layer represents a different part of the cloud computing stack [3].

- IaaS: The most basic cloud-service model is that of providers offering computing infrastructure, machines and other resources. In the case of IaaS, resources and hardware are virtualized.
- PaaS: To provide a platform allowing customers to run, develop, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application.

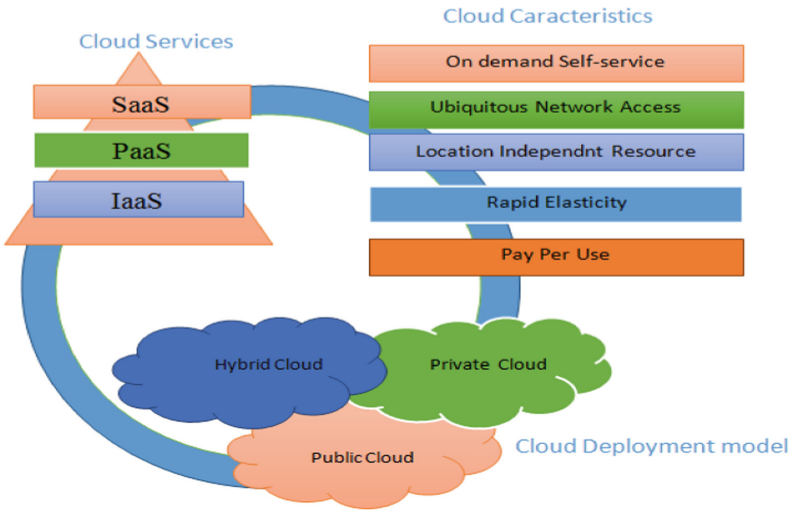

Fig. 1. Cloud computing architecture

- SaaS: To use provider software running on a cloud infrastructure and accessed from various client devices via a client interface.

There are three common deployment models to consider [4, 5]:

- The private cloud is designed for exclusive use by a single organization;
- In a public cloud, the cloud provider offers their resources as a service to the general public;
- A hybrid cloud is a combination of cloud deployment models (public and private) that attempts to address the limitations of each approach.

2.2 Intrusion Detection Systems

As detailed in previous section, there are different types of attacks in cloud environment. Intrusion Detection System is effective solution to detect and resist these attacks. IDSs are software or hardware systems that realize intrusion detection, log detected information, alert or perform predefined procedures [6]. They can be either hardware or software that includes whole observed computing entities.

An HIDS is an agent that monitors and analyzes any action, internal or external, that bypasses the system security policy, while an NIDS attempts to detect unauthorized access to a network by analyzing the network traffic for signs of malicious activity and anomalous events [7]. A distributed IDS consists of a several IDSs in the cloud network communicating with each other, or with a central point that manages that system. By distributing these cooperative IDSs on this environment to process and to analyze the collected events [8].

An IDS increases the security level of a cloud by using two main intrusion detection techniques [9]; the first is based on signatures (signature-based detection or misuse detection) and the second on behaviors (anomaly detection).

- A signature-based detection technique detects attacks by verifying that observations match known attacks. This technique therefore uses a knowledge base for the different existing attacks [10]. This principle of intrusion detection is reactive and meets several constraints; the IDS only detects attacks that have been defined.
- An anomaly detection technique is based on research on abnormal behavior, and anything that deviates from normal conditions triggers an alarm [8]. This type of detection is effective on unknown attacks but can generate a large number of false positives.

Some IDSs combine both techniques to achieve better results. This is approach used in our proposal, which incorporates both techniques.

2.3 Multi-agent Systems

A Multi-Agent system has a group of intelligent agents interacting with the environment and with themselves [11]. An agent is a computer system located in an environment that acts autonomously and flexibly to achieve the objectives for which it was designed [12]. Agents can be described with different characteristics:

- **Flexibility:** The agent is able to carry out actions in an autonomous and reflexive way in order to achieve the objectives set for it. Flexibility in this case means **reactivity** and **pro-activity**;
- **Autonomous:** The agent is able to act without any intervention, that is to say, the agent decides himself which action to undertake among those that are possible;
- **Social:** The agent must be able to interact with other agents when the situation so requires to complete his tasks or to help these agents perform their tasks.

3 Related Works

In the literature, there are many works that use an IDS with the agent approach to secure systems against attacks. However, most of these studies have developed solutions for well-defined networks and systems, and are not suitable for dynamic and complex environments such as the cloud environment. Agent-based IDS implementation is one of the new paradigms for intrusion detection in this environment, and this approach has been examined by several researchers.

In their article, Venkataramana and Padmavathamma [13] introduced a multi-agent intrusion detection and prevention system using agents for the detection of attacks in the cloud. In [14, 15], the authors proposed a trust model that used mobile agent technology. In this work, mobile agents can dynamically move across the cloud network to perform certain tasks, such as accounting and monitoring the integrity and authenticity of virtual machines. Depren et al. [16] have proposed an intelligent intrusion detection system using both anomaly and misuse detection techniques, to

enable a computer networks to handle attacks. Wang and Zhou [17] presented the concept of a cloud alliance, involving communication between agents and the exchange of mutual alerts, primarily to resist DoS and DDoS attacks. In [18], an IDS based on mobile agent technology and cryptographic mechanisms has proposed by Idrissi et al. This proposal consists on elaborating detection mechanisms, based on cryptographic traces generated by mobile agent to secure CC architecture against insider threats. Authors Seresht and Azmi [19] proposed a hybrid IDS that analyzes the network traffic in the system environment, this analysis is performed by using virtual machines. Indeed, each instance is composed by intelligent agents to perform a defined selection algorithm. These agents communicate and cooperate with others to detect anomalies. A thorough study of security solutions based on agent technology reveals IDS solutions that use the different properties of intelligent agents to detect attacks and respond to intrusions. Existing solutions are poorly suited to the growing complexity of cloud networks; they use centralized and non-collaborative IDSs and are not suitable for dynamic environments. Thus, they are not able to cooperate and communicate with each other to detect complex attacks. For example, if an IDS detects a new attack, it does not share this result with other IDSs in its environment.

In the next section, we therefore propose a secure solution that meets all these requirements in the form of a DIDS based on a multi-agent approach, which can identify and prevent all attacks in a cloud environment.

4 Proposed MAS-DIDS System

We propose a Multi-Agent System-Based Distributed Intrusion Detection System, as shown in Fig. 2, with a distribution and cooperation mode, which detects known or unknown attacks in a distributed environment. This system is composed of a group of intelligent agents with mobility and responsiveness, which can communicate and cooperate with each other in order to effectively detect coordinated and distributed attacks in this environment.

First, as the network administrator, the cloud service provider (CSP) receives the packets from different users. The CSP transfers these packets to the Management Agent (MA), which also checks and analyzes the packets before sending them to the available IDSs (IDS-1, IDS-2,…, IDS-n) in the system. The IDSs use Sniffing Agent (SA) as a network capture and analysis tool, allowing the capture results to be saved in a file entitled “ResultsFile.cap” for analysis by the Filter Agent (FA). The FA also communicates with the SA to parse and filter the list of packets using signatures (fingerprint attack). Then, the FA routes the hashed packets to a Misuse Detection Agent (MDA). This node is responsible for checking each signature in the local database, coordinating with the Basic Agent (BA). Two results are possible after checking a signature with BA: either the signature exists or it does not. When a signature exists in the local database, the MDA concludes that this is proof of an ongoing known attack, and an alert is generated to initiate a response. However, when a signature does not exist in a local database that is currently synchronized with the global database, the current packet is transmitted to the anomaly intelligent agent (AIA). The goal of the AIA is to detect anomalies through an analysis of possible abnormal behaviors; on this basis, it

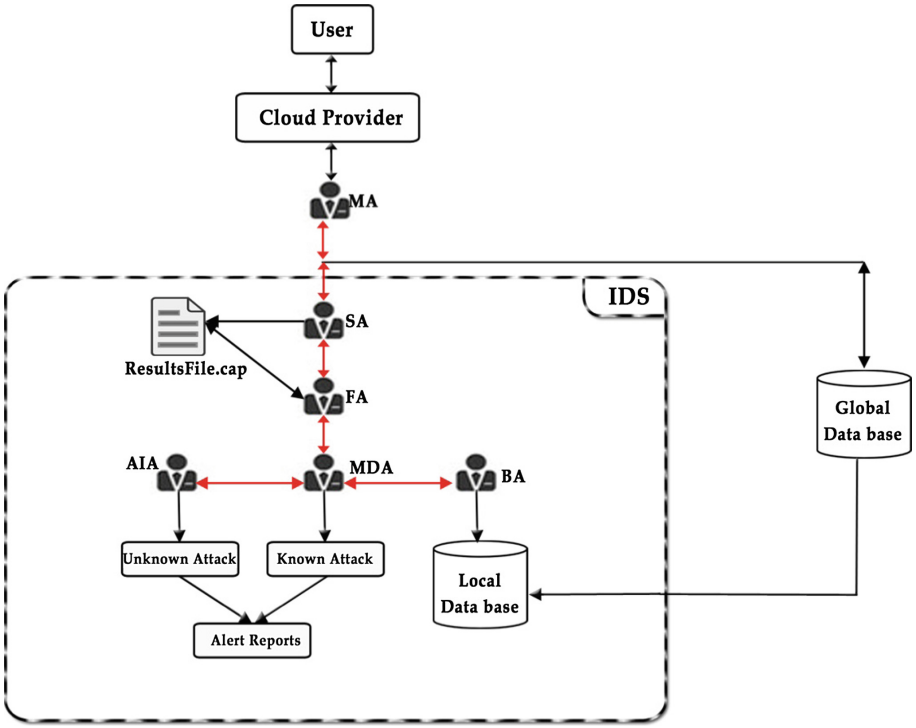

Fig. 2. Proposed MAS-DIDS architecture

can classify a current packet as an unknown attack or a false positive. In order to avoid false positives, the AIA communicates the alert triggered to the MA, which classifies the alert by applying the following formula:

$$\#number\ of\ IDSs\ sending\ the\ same\ alert / \#number\ of\ IDSs\ in\ the\ system > 0.5 \quad (1)$$

If the result is greater than 0.5, the packet is classified as a new type of attack to block. On this basis, the MA allows the rules obtained to be automatically added to the global database, and communicates the alert to the CSP via the central console, in order to block the source of the detected attack.

5 Experimental Results

In this paper, several experiments have been made to verify the performance of our approach. This Proposed model has been implemented using some tools and libraries such as the Java language, the JADE framework, the JPCAP platform and the Aglets platform that has been configured on an Eclipse IDE.

JADE (Java Agent DEvelopment Framework) is a software Framework, which simplifies the implementation of multi-agent systems [20]. The Aglets platform can be

distributed by moving agents from one machine to another one [21]. In addition, JPCAP is an open source framework for capturing and sending network packets [22]. It provides facilities to capture raw packets live from the wire and save captured packets to an off-line file [23].

Indeed, the Sniffer Agent based on the JPCAP library collects the network events using the "*CaptureTool*" class and saves them into a sniffing file.

As a matter of fact, two interesting measures were used to validate the performance of our Proposed system: false positive rate (FR) and detection rate (DR).

- DR refers to the amount of attacks detected among all detections (2);
- FR refers to the number of instances falsely detected as attacks among all detections (3).

$$DR = \frac{TP}{TP + FN} \tag{2}$$

$$FR = \frac{FP}{TN + FP} \tag{3}$$

TP: true positive
FP: false positive
FN: false negative.

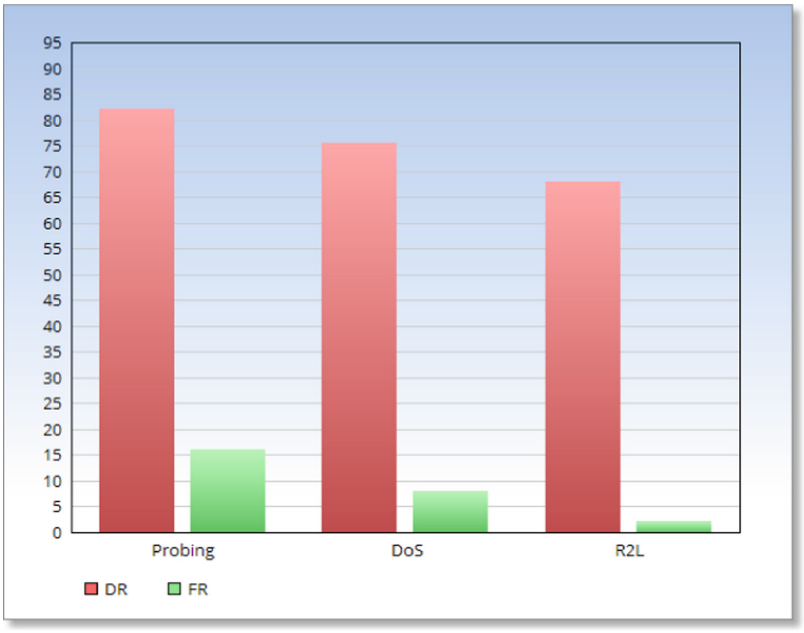

Fig. 3. Performance of MAS-DIDS.

Based on these concepts, Fig. 3 shows the detection performance of our model based on the results given in Table 1, which proves the increase in DR and the decrease in FPR in our simulated cloud environment.

Table 1. Experimental results

Attack type	DR	FR
Probing	82%	16%
DoS	75.5%	8%
R2L	68%	2.3%

The experiment results of our proposed model prove that it has a detection rate higher than 80% and a false alarm rate lower than 8% are reached. So R2L attacks have the best performance. Consequently, we can conclude that the results indicate that our proposed system provides many favorable characteristics, such as high detection rate and low false positive rate and good response time for detection.

The proposed system was compared with similar systems where there was IDS model which was not based on multi-agent systems. The results of this comparison are proved in Fig. 4 based on the data given in Table 2. It demonstrates that our proposition worked not only better in term of efficiency but also in term of response time.

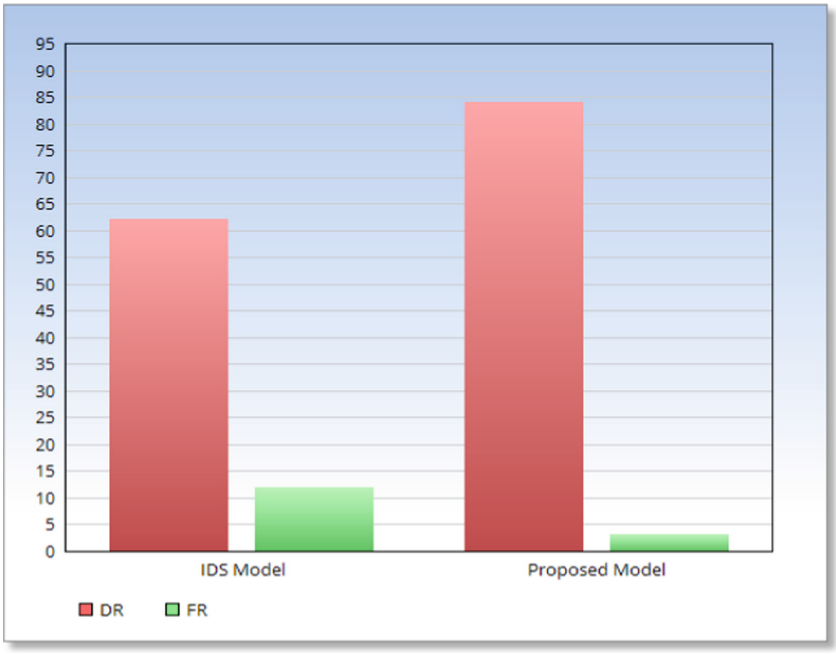

Fig. 4. Comparison between IDS model without agent and our proposed system.

Table 2. Experimental data

Simulation system	DR	FR
IDS model	62%	12%
Proposed model	84%	3.2%

6 Conclusions

Distributed IDS based on multi-agent system has been the important of research direction in the field of intrusion detection, and has the advantages of detecting distrusted attacks and balancing the load in a cloud environment. On the basis of analyzing the existing IDS models based on multi-agent system, this paper presented a new distributed IDS based on intelligent agent technology. Experiments proved that our proposal is efficient and valuable for detecting all intrusions in cloud computing. In future, we plan to experiment our proposed system in real cloud environment.

References

1. Ramachandran, M., Chang, V.: Towards performance evaluation of cloud service providers for cloud data security. Int. J. Inf. Manag. **36**(4), 618–625 (2016)
2. Mell, P., Grance, T.: The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology, vol. 145, p. 7. NIST Special Publication (2011)
3. Achbarou, O., El kiram, M.A., El Bouanani, S.: Securing cloud computing from different attacks using intrusion detection systems. Int. J. Interact. Multimed. Artif. Intell. **4**(3), 61 (2017)
4. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. **34**(1), 1–11 (2011)
5. Singh, S., Jeong, Y.S., Park, J.H.: A survey on cloud computing security: issues, threats, and solutions. J. Netw. Comput. Appl. **75**, 200–222 (2016)
6. Achbarou, O., El Kiram, M.A., Elbouanani, S.: Cloud security: a multi agent approach based intrusion detection system. Ind. J. Sci. Technol. **10**(18) (2017)
7. Patel, A., Taghavi, M., Bakhtiyari, K., Júnior, J.C.: An intrusion detection and prevention system in cloud computing: a systematic review. J. Netw. Comput. Appl. **36**(1), 25–41 (2013)
8. Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., Rajarajan, M.: A survey of intrusion detection techniques in Cloud. J. Netw. Comput. Appl. **36**(1), 42–57 (2013)
9. Liao, H.-J., Lin, C.-H.R., Lin, Y.-C., Tung, K.-Y.: Intrusion detection system: a comprehensive review. J. Netw. Comput. Appl. **36**, 16–24 (2012)
10. Keegan, N., Ji, S.-Y., Chaudhary, A., Concolato, C., Yu, B., Jeong, D.H.: A survey of cloud-based network intrusion detection analysis. Hum.-Cent. Comput. Inf. Sci. **6**(1), 19 (2016)
11. Cavalcante, R.C., Bittencourt, I.I., Da Silva, A.P., Silva, M., Costa, E., Santos, R.: A survey of security in multi-agent systems. Expert Syst. Appl. **39**(5), 4835–4846 (2012)
12. Baig, Z.A.: Multi-agent systems for protecting critical infrastructures: a survey. J. Netw. Comput. Appl. **35**(3), 1151–1161 (2012)

13. Venkataramana, K., Padmavathamma, M.: Multi-agent intrusion detection and prevention system for cloud environment. Int. J. Comput. Appl. **49**(20), 24–29 (2012)
14. Hada, P.S., Singh, R., Manmohan Meghwal, M.: Security agents: a mobile agent-based trust model for cloud computing. Int. J. Comput. Appl. **36**(12), 975–8887 (2011)
15. Saadi, C., Chaoui, H.: Cloud computing security using IDS-AM-Clust, Honeyd, Honeywall and Honeycomb. Proc. Comput. Sci. **85**, 433–442 (2016)
16. Depren, O., Topallar, M., Anarim, E., Ciliz, M.K.: An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. Expert Syst. Appl. **29**(4), 713–722 (2005)
17. Wang, H., Zhou, H., Wang, C.: Virtual machine-based intrusion detection system framework in cloud computing environment. J. Comput. **7**(10), 2397–2403 (2012)
18. Idrissi, H., Ennahbaoui, M., Souidi, E.M., El Hajji, S.: Mobile agents with cryptographic traces for intrusion detection in the cloud computing. Proc. Comput. Sci. **73**, 179–186 (2015)
19. Seresht, N.A., Azmi, R.: MAIS-IDS: a distributed intrusion detection system using multi-agent AIS approach. Eng. Appl. Artif. Intell. **35**, 286–298 (2014)
20. Bellifemine, F., Caire, G., Poggi, A., Rimassa, G.: JADE: a software framework for developing multi-agent applications. Lessons learned. Inf. Softw. Technol. **50**(1–2), 10–21 (2008)
21. Shinde, P., Parvat, T.J.: DDoS attack analyzer: using JPCAP and WinCap. Proc. Comput. Sci. **79**, 781–784 (2016)
22. Su, C.J.: Mobile multi-agent based, distributed information platform (MADIP) for wide-area e-health monitoring. Comput. Ind. **59**(1), 55–68 (2008)
23. Fortino, G., Garro, A., Russo, W.: Achieving mobile agent systems interoperability through software layering. Inf. Softw. Technol. **50**(4), 322–341 (2008)