Expert Systems With Applications 000 (2016) 1–14

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

A Biological Immune System (BIS) inspired Mobile Agent Platform (MAP) security architecture

Pallavi Bagga[a], Rahul Hans[b,*], Vipul Sharma[b]

[a] Research Scholar, Department of CSE, DAV University, Jalandhar, Punjab, India
[b] Assistant Professor, Department of CSE, DAV University, Jalandhar, Punjab, India

ARTICLE INFO

Article history:
Received 22 June 2016
Revised 21 October 2016
Accepted 31 October 2016
Available online xxx

Keywords:
Malicious mobile agent
Nonce-based authentication
Pattern matching
N-gram feature extraction
Feature selection
K-nearest neighbor classification

ABSTRACT

The proliferation of malicious entities in the distributed environment poses various serious threats to the protection of Mobile Agent Platform (MAP). Numerous researches have been proposed to ward off the inherent security risks, though these solutions are not enough to identify and remove all the vulnerabilities. In this paper, a self-adaptive IV-Phase MAP Security Architecture is proposed, which is inspired by the Biological Immune System, with the prime objective of detecting unknown malicious mobile agents. In this context, data mining methods are studied for the detection of unknown malicious executable. In particular, Boyer Moore pattern matching algorithm and N-gram feature analysis of mobile agent using a k-Nearest Neighbor Classifier, facilitate the discovery of known and unknown malicious content from incoming mobile agent in the proposed architecture, and protects against the Man In The Middle (MITM) attack, the Masquerading Attack, the Replay attack, the Repudiation attack and the Unauthorized Access Attack. The architecture is designed and implemented in IBM Aglets. A comprehensive 5-fold cross validation scheme on a large collection of malicious and non-malicious files is performed while performing Classification technique involving Feature Selection Method. The propitious experimental outcomes express that the performance (time and security) and accuracy of proposed architecture outperform the earlier known related schemes and makes the proposed architecture suitable for MAP protection in the Mobile Agent Environment (MAE). Above all, these findings exhibit wide-ranging newness, since the concept of machine learning has never been employed so far in the sphere of Mobile Agents System (MAS). Hence the proposed work is likely to be of great interest to the researchers who particularly deal with MAS security.

1. Introduction

In present era, one of the emanating paradigms for structuring applications over the Internet is Mobile Agent technology, due to its effective characteristics like autonomy, intelligence, adaptability, flexibility etc. (Aneiba & Rees, 2004). It has been engaged in many sectors from the network management exercises to the information management (Bieszczad, Pagurek, & White, 1998; Satoh, 2003). It affords an infrastructure not only for executing autonomous agents but also for dispatching them between different computers. Thus, a mobile agent is not restricted to the platform where it is written or created; rather it travels freely among different machines (Urra, Ilarri, Trillo, & Mena, 2009). Moreover, the agent defers its computations at one platform, moves to another with its state, data and code, and recommences the execution there (Eid, Artail, Kayssi, & Chehab, 2005). Autonomy and mobility are underlined as a cornerstone of the agent (Horvat, Cvetković, & Milutinović, 2001).

Despite the fact that mobile agents present many advantages to the distributed computing including network load reduction, overcoming network latency, executing dynamically, asynchronously and autonomously (Lange & Oshima, 1999); the security alone is a massive problem that shades down its global acceptance.

- The mobile agents while roving in a network bring with them the fear of viruses, Trojan horses and other invasive means or entities (Thomsen & Thomsen, 1997). This is because the attacks can be occurred when the mobile agent traverses in the communication channel and there may be some attackers overhearing the network either to gain some of the information carried by the agent (passive attack) or altering that information for their own benefits (active attack) (Oppliger, 1999).

[*] Corresponding author.
E-mail addresses: pallavibagga315@gmail.com (P. Bagga), rahulhans@gmail.com (R. Hans), vipuls85@gmail.com (V. Sharma).

http://dx.doi.org/10.1016/j.eswa.2016.10.062
0957-4174/© 2016 Elsevier Ltd. All rights reserved.

Table 1
Authors, Year, Title, publisher, and Citations of various papers containing MAP security approaches.

Authors	Year	Paper Title	Publisher / Report	# Citations	# References	Name of Approach	Type
Wahbe et al.	1994	Efficient software-based fault isolation	ACM	1369	41	Sandboxing mechanism	Prevention
Ordille	1996	When agents roam, who can you trust?	IEEE	125	9	Path histories	Detection
Farmer et al.	1996	Security for mobile agents: Authentication and state appraisal	Springer	345	17	State appraisal, Agent authentication	Detection, Prevention
Ousterhout	1997	The safe-Tcl security model	Springer	146	13	Safe code Interpretation & padded cells	Prevention
Lee et al.	1997	Self-protecting mobile agents obfuscation techniques evaluation report	Network Associates Lab. Report	18	30	Proof Carrying Code	Prevention
Sonntag et al.	2000	Mobile agent security based on payment	ACM	13	13	Payment based techniques	Prevention
Bryce	2000	A security framework for a mobile agent systems	Springer	17	26	Resource protection	Prevention
Hefeeda et al.	2001	On mobile code security	CERIAS Tech Report	8	8	Digital shrink wrap	Detection
Noordende et al.	2002	A security framework for a mobile agent system	DFKI	14	17	Mansion paradigm	Prevention
Alfalayleh et al.	2004	An overview of security issues and techniques in mobile agents	Springer	45	8	Code signing	Detection
Saxena et al.	2005	Authenticating mobile agent platforms using signature chaining without trusted third parties	IEEE	18	20	Authentication primitives	Detection
Cao et al.	2006	Path-history-based access control for mobile agents	Taylor & Francis	3	39	Path-history based access control model	Detection
Venkatesan et al.	2008	Protection of mobile agent platform through Attack Identification Scanner (AIS) by Malicious Identification Police (MIP)	IEEE	8	7	Malicious Identification Police	Detection
Venkatesan et al.	2010	Advanced mobile agent security models for code integrity and malicious availability check	Elsevier	26	29	Policy based MIP	Detection
Marikkannu et al.	2011	A secure mobile agent system against tailgating attacks	Science	2	6	Dual checkpoint analysis	Prevention
Venkatesan et al.	2013	Artificial immune system based mobile agent platform protection	Elsevier	1	9	Artificial Immune System	Detection
Idrissi et al.	2015	Security of mobile agent platforms using access control and cryptography	Springer	0	17	Access Control and Cryptography	Detection

Note: Citations are considered up to March 2016; *Prevention* - approaches preventing the attacks from malicious agents; *Detection* - approaches detecting malicious mobile agents.

- Likewise, if a mobile agent is recognized to be gentle, it can never be assured that the platform it is staying upon may be venomous to it or not and may extract sensitive information from the agent, warp it, or even exploit it for the vicious activities since agent platforms have complete control over the agents during execution (Jansen & Karygiannis, 1999).

Last decade has revealed numerous efforts from researchers as shown in Table 1, providing techniques or models to conquer security risks but malicious mobile agents still exist as a hurdle in a way to widely deploy the Mobile Agent technology in a distributed environment. In this paper, a self-adaptive IV-Phase security architecture is proposed, protecting Mobile Agent Platform (MAP) from malicious mobile agents. The architecture is inspired by the Biological Immune System (BIS) and the performance of the proposed architecture is evaluated using metrics such as “False Negatives”, “False Positives”, “True Positives”, “True Negatives”, “Sensitivity Rate”, “Specificity Rate”, “Accuracy Rate”, “Miss Rate”, “Positive Predictive Value”, “Negative Predictive Value”, “Fall-out” and “Receiver Operating Characteristic - Area Under Curve”, employing 5-fold cross validation Scheme on a large collection of non-malicious and malicious files.

1.1. Analogy to Biological Immune System

In recent years, the Biological Immune system (BIS) has been the target of considerable research interest in the area of malicious detection, aiming for better performance After examining the potent natural mechanism cautiously, many computer scientists have proposed Artificial Immune System based Computer models to solve several problems ranging from malicious detection to combinatoric optimization and to clustering or classification (Hart & Timmis, 2008; Zheng, Chen, & Zhang, 2010). An Artificial Immune System based MAP protection was earlier proposed in (Venkatesan, Baskaran, Chellappan, Vaish, & Dhavachelvan, 2013), and achieved good results. However, the time complexity is quite high. Moreover, it doesn’t prevent all the attacks.

The BIS generally begins when a “pathogen” (foreign substance) enters the biological structure (or body). The proteins on the surface of a pathogen are called “Antigens” which trigger the immune system into producing antibodies (using B-plasma cells) specific to that antigen. The immune system possesses two types of responses: primary and secondary. If the pathogen comes first time to body (primary response occurs), the macrophages ingest it and display its antigen fragment on their cell surfaces. The macrophage