INFORMATION SECURITY APPROACH IN OPEN DISTRIBUTED MULTI-AGENT VIRTUAL LEARNING ENVIRONMENT

Dr. Zahi A.M. Abu Sarhan [1] and As'ad Mahmoud As'ad Alnaser[2]

[1]Department of Computer Information Systems, Applied Science Private University, Amman, Jordan
[2]Department of Computer Science, Al-Balqa' Applied University, Ajlun University College, Ajlun, Jordan

ABSTRACT

This paper presented the main information, security problems and threats in open multi-agent distributed e-learning information systems and Proposed various approaches to solve information security attacks in virtual learning environment using service oriented architecture which based on multi-agent information systems architecture, the solution on the multi-agent learning information system implementation based on the implementation of two types of systems the first system with the centralized mobile agent information security management and the second system with decentralized mobile agents security management, and proposed the migration behaviour simulation for their active software components (software agents).

KEYWORDS

Information security, Distributed multi-agent system, Virtual learning environment. Agent migration.

1. INTRODUCTION

Relevance research in the field of distributed artificial intelligence and multi-agent systems (MAS), according to[1], on the complexity of modern organizational and technical systems, variety, tasks distribution and the huge volume information flows and critical information processing time. The theoretical researches in MAS field mainly carried out in the following areas: Agents theory, Agents collective behaviour, agents and MAS architecture; methods, languages and agents communication tools, agent's implementation languages; agents migration support tools within network. The greatest difficulty in theoretical studies and practical implementations of modern MAS are the issues related to agent's information security and information resources, which they operate in open multi-agent virtual learning environments. Providing information security is an important task that must be solved when developing MAS, focused on the usage in various fields.

Software agent is computer system, which is found in some environment and is capable of autonomous action in this environment in order to meet its design objectives [2]. Software agents have characteristics that make them suitable for complex functions. Such features include: autonomy, interaction, reactivity, activity, intelligence and mobility [3].

E-learning represents the use of electronic media and information and communication technological innovations in education and learning processes. E-learning is generally

comprehensive of all forms of academic technological innovation in study and education. E-learning contains various types of media that deliver text, sound, pictures, computer animation, and streaming video, and contains technology programs and procedures such as sound or movie record, computer-based learning, as well as regional intranet/extranet and web-based learning. Information and interaction systems, whether free-standing or depending on either regional networks or the Internet in networked learning, underlay many e-learning procedures [4].

E-learning can occur in or out of the classroom. It can be self-paced, asynchronous learning or may be instructor-led, synchronous learning. E-learning is suited to distance learning and flexible learning, but it can also be used in conjunction with face-to-face teaching, in such case the term blended learning is commonly used [4].

Virtual learning environments (VLE) have become a frequent tool in higher education organizations for supporting and assisting both study and education. They create a platform for instructors and students to access educational materials, read reports, interacts with others, send and receive assignments, get involved in conversations and group work. These days, there are plenty of commercial VLE techniques available in the market. Each of them offers its own features and performance [5].

2. PROBLEMS AND INFORMATION SECURITY THREATS IN OPEN MAS

Ensuring the information security problem in MAS can be presented in several ways. First, it is necessary to provide nodes protection against hidden attacks by malicious programs or spyware agents. Second, we need to protect agents themselves from exposure applications running on the network nodes. Third, it is necessary to ensure the protection MAS agents from attacks spyware agents, migrating between network nodes. The first problem can be successfully solved by using strong authentication methods executable agents' code; agents program code integrity monitoring and access restrictions either by software agents, or information or services that they provide. The second problem is one of the major unsolved problems today. The reason for this is the existence of a large set of malware that can unauthorized way affect the agents operation process and manipulate the confidential information, on which the agents operate. The third problem solution based is on special security protocols which create exchanging messages between agents in multi-agent environment.

Security threats in distributed MAS include: passive unauthorized message exchanging interception within communications process between agents, the integrity breach of the transmitted data over the network, unauthorized access to the data, denial of service, intercept requests with their subsequent modification and playback, the rejection of fact receiving or sending data. The decentralized nature of building distributed MAS, none single centre, the components heterogeneity, the potential communication with any node make multi-agent environment maximum vulnerable to any kind of these threats [6].

3. EXISTING INFORMATION SECURITY SOLUTIONS IN OPEN MAS

Ensuring information security under consideration class of systems can be organized as complex of famous solutions. The most efficient and flexible at present solutions for agent's information security, and MAS are:

- Agents protected states method [7];
- Mobile cryptography methods [8];
- Police Office security model [9];

- Buddy Model of security for mobile agents [10];
- Methods of the organization of self-organizing systems trusting relationship [11];
- Methods based on using algorithms for confidential communications and proxy performing, the functions and limitations of restricting access to resources and services based on the methods of identification and authentication [12].

Despite such a wide range of existing solutions, none of these approaches provided a comprehensive solution of agent's information security problems from harmful sites and spyware in open MAS.

4. MULTI-AGENT VIRTUAL LEARNING ENVIRONMENT

A virtual learning environment (VLE) is a software system designed to support teaching and learning. VLEs generally function on the World Wide Web, and, therefore, they can be utilized both on and off-campus, provided that the users are authorized and can access the Internet. This surmount over the restriction of traditional face-to-face educating, and guarantees that learning is neither limited to location nor time. VLEs become more popular and included in many college organizations all over the world. It is not only because of their versatility, but also because they provide an extensive range of tools or features, such as content distribution, evaluation, emails [13].

Based on the learning process components the representation of VLE can be presented as shown in figure 1.

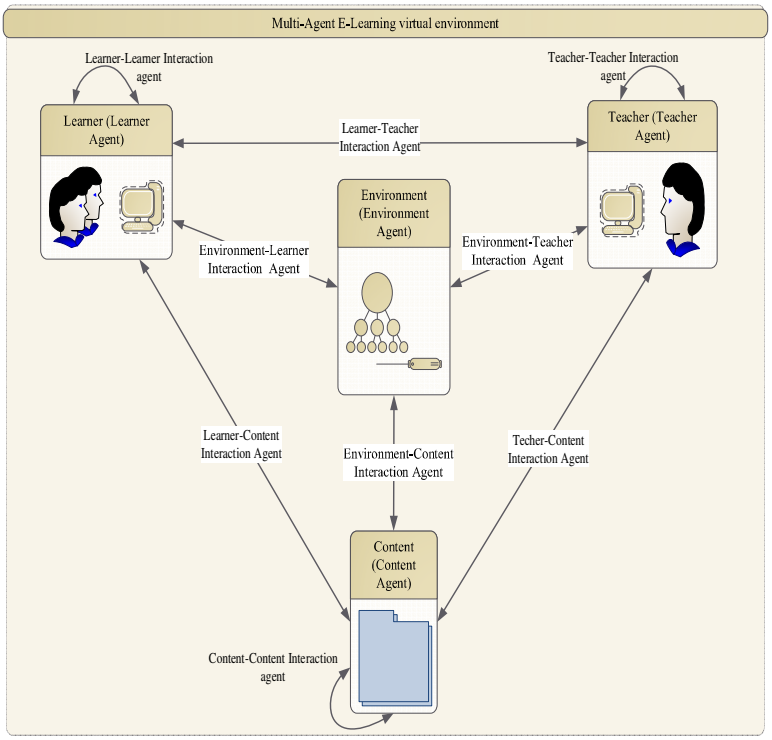

Figure1. Virtual learning environment based on multi-agents architecture.

5. OPEN MULTI-AGENT VIRTUAL LEARNING ENVIRONMENT STRUCTURE AND FORMAL REPRESENTATION

The main part of this work focuses on solving agent's information security problems. As example of ensuring information security in e-learning systems, OMAVLE (Open Multi-Agent Virtual Learning Environment).

In terms of overall functioning logic e-learning has a multi-agent realization. Agent-based orientation is expressed in the fact that in its real subject e-learning activity is represented by one or more mobile software agents that represent e-Learning-activities and implement procedures for an automated search agent partners for cooperation.

In general, the model OMAVLE can be assigned as a theoretic-set of relations and can be represented as the next set of sets [14]:

$$OMAS = \{S\} \cup \{A\} \cup \{U\} \cup \{VLP\} \cup \{IR\} \cup \{O\} \cup \{ATTR\};$$

Where $\{S\}$ - set the system users (E-Learning subjects); $\{A\}$ - set of agents in the system, representing the interests of users in a virtual learning environment; $\{U\} = \{SH\} \cup \{CH\}$ where U set of the system nodes, in which agents operate, $\{SH\}$ - multiple server hosts, $\{CH\}$ - multiple client hosts; $\{VLP\}$ - set of virtual learning-platforms (VLP), within which the combined agents of joint activities with similar interests and goals; $\{IR\}$ - set of information system resources; $\{O\}$ - relations between model objects sets; $\{ATTR\}$ - set of model objects attributes;

There are two main types of operational agents in the system $\{A\} = \{MA\} \cup \{CA\}$, where $\{MA\}$ - the migrating mobile agents between network nodes; $\{CA\}$ - the control agents (moderators), that operating within the VLP and coordinating the processes of mobile agents interaction and migration.

On the set of objects model the following relationship, that defines the structure of OMAELS, can be defined:

$$\{O\} = \{SMA\} \cup \{SHVLP\} \cup \{MAVLP\} \cup \{CAVLP\} \cup \{CAMA\};$$

Where $\{SMA\} \subset \{S\} \times \{MA\}$ - the availability relation of each virtual learning subject representative - agent; $\{SHVLP\} \subset \{SH\} \times \{MA\}$ - The existence relation of each system server node of VLP; $\{MAVLP\} \subset \{MA\} \times \{VLP\}$ - The existence relation of each VLP agents of joint activities with common interest areas; $\{CAVLP\} \subset \{CA\} \times \{VLP\}$ The membership relation of each virtual platform with its control agent (agent-moderator); $\{CAMA\} \subset \{CA\} \times \{MA\}$ - The membership relation of each control agent from agent joint activities set that it coordinates their interaction.

Each mobile agent can be described with the following parameters set:

$$\{MA\} = \{Id_{MA}, Id_{MP}\} \cup \{ST_{MA}\} \cup \{D_{MA}\} \cup \{SS\}$$

Where Id_{MA} - The mobile agent unique identifier; Id_{MP} - The server node unique identifier from which mobile agent migrates, $\{ST_{MA}\}$ - The mobile agent states set; $\{D_{MA}\}$ - data set, which mobile agent operates; $\{SS\} = \{C\} \cup \{Pk, Sk\}$ - mobile agent internal security system; $\{C\}$ - The set of data encryption cryptographic methods with open and/or private key; Pk - public key known only by mobile agent and its control agent (the public keys refresh rate determined by the control agent); Sk - private (secret) key known only by mobile agent (the secret key refresh rate determined by mobile agent).

6. PROBLEM SOLUTION FOR INFORMATION SECURITY IN OMAVLE

Novelty of what proposed in this paper is problem solving for ensuring information security in open distributed MAS which is a combination of two approaches to the OMAVLE formation [15].

The first approach is based on the concept of a closed network lies in the development of a multi-agent virtual electronic learning environment with independent agent platforms based on the technology [16], within which agents operate with other agents that have similar interests and goals (collecting agents with the similar interests private groups), and the using of agents state protection method in order to prevent hidden malware and spyware agents attacks. Formulation VLP based on agents consensus where each agent shared information with other agents with the same interest and same goals, this virtual learning platform can be collected form single node in network or from multiple nods and this VLP begins allotted platform [17] (private group of agents with the same interests, implemented on any of the nodes in the system).

The second Proposed approach, based on the idea which described in [15] which involves the implementation of an open multi-agent environment specialized software component - the mobile agents security system (MASS), providing the cryptographic techniques and mechanisms implementation to protect the system agents of various computer attacks types from malicious software, and using simulation tools for analysis, forecasting and studying the dynamic agents behaviour in the system.

As a simulation tool can be used system-dynamic complexes or agent-based models. For Extending Multi-Agent Security System (MASS) functionality integrated into MASS structure, developed specific software components, that provides support for inter-agent (between agents) interaction and agents self-organization, as well as implementing protection mechanisms that protect the system agents from various types of computer attacks as malware. These components include:

- Registry Server;
- Agents Name server;
- Public key encryption Server;
- Data encryption module;
- Special register;
- Agent Control System.

Registry Server contains information about the operated system nodes, and controls the new nodes and new agent's connections to the system. Agent Name Server collects information about all system agents.

Formation and maintenance distributed agents registry carried out on the basis of their binding to the dendritic domain conceptual models. Public key encryptions Server jointly with data encryption module are the core of agent's information security system, agents, agent's representative and system nodes. It implements agent identification and authentication procedure and information cryptographic protection methods with public key. The key server stores a set of individual public keys to encrypt the information that system agents operate within each other interaction and with running applications on the network nodes.

In this paper, as a data encryption with public key method proposed to use classical asymmetric key cryptographic encryption algorithm with RSA public key [18, 19] and its modifications [20]. For ensuring the integrity and confidentiality of their requests and to protect information about participations, the agents use electronic signature and known private key encryption methods. Special register contains full information about all VLP registered in the system, and their constituent agents coalitions. MASS integrates with agents control system, representing software components set that implement the agents operation and interaction internal logic, inter-agent communication protocols.

7. MULTI-AGENT SECURITY SYSTEM MANAGEMENT FUNCTIONING ALGORITHM.

The study proposed two embodiments of MASSM: the first system with centralized mobile agent's security management, and the second system with decentralized mobile agent's security management.

When a new learner connects to the system, the system generates for hem his virtual representative (mobile agent), this mobile agent acting as learner interest. The agent is generated by the server host and performed the following actions:

- Searching learning application and/or learning partner that satisfies given constraints in the system data base distributed heterogeneous server hosts;
- Forming the virtual learning structures (agents' coalition) to implement specific leaning task. To the agents assigned not only searching and placement information tasks, but also analysis and processing functions. The agent provides the gathered and formed information to its owner to make a decision.

After generating a new agent in the system, the information about him and his owner will be registered in the appropriate system registry. At the time of generating control agent assigned to each new mobile agent unique identifier and name that will be registered in the agents name server, and determined the public key for agents data encryption and decryption, private (secret) key generated by the agent themselves at the registration moment in the system. The public key is known only by agent manager from the native system host (node) where the mobile agent was created. Having passed the registration stage created agent starts interacting with other agents within the agent-based representation of the host where it was generated, the agent begins improve its knowledge about the system, exactly, the agent begins collect all available information about already registered agents in the system, system components and virtual learning platforms, which problem orientation coincides with the agents interests area.

In the case of systems with a centralized mobile agent's security management in an open multi-agent virtual learning platform as shown in figure 2 is implemented on a dedicated server, which functional structure shown in Figure 3.

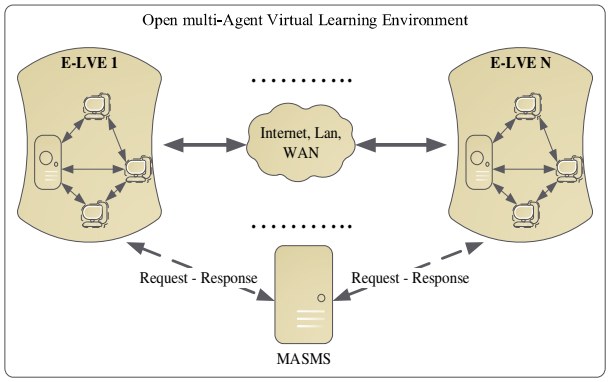

Figure 2. Open multi-agent VLE with the centralized mobile agent's security system management.

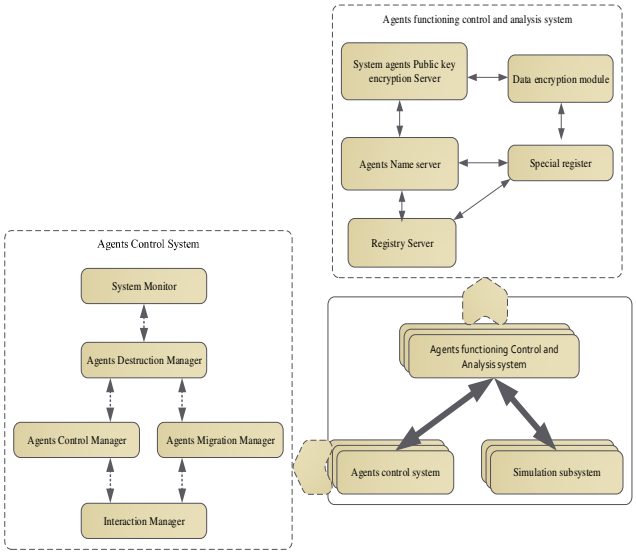

Figure 3.The functional structure of Mobile agent security server.

Security Server provides mobile agents centralized information storage about all agents in the system, accessible hosts, virtual learning platforms, agent's public keys which can access only the system control agents. In the security server must be realized data encryption and decryption module, and the system monitoring, agent's behaviour analysing and modelling in the system, which is also available for agent control in the system. Let us consider algorithm functioning the main components OMAVLS utilizing this approach to implement MASS, as in Figure 4.

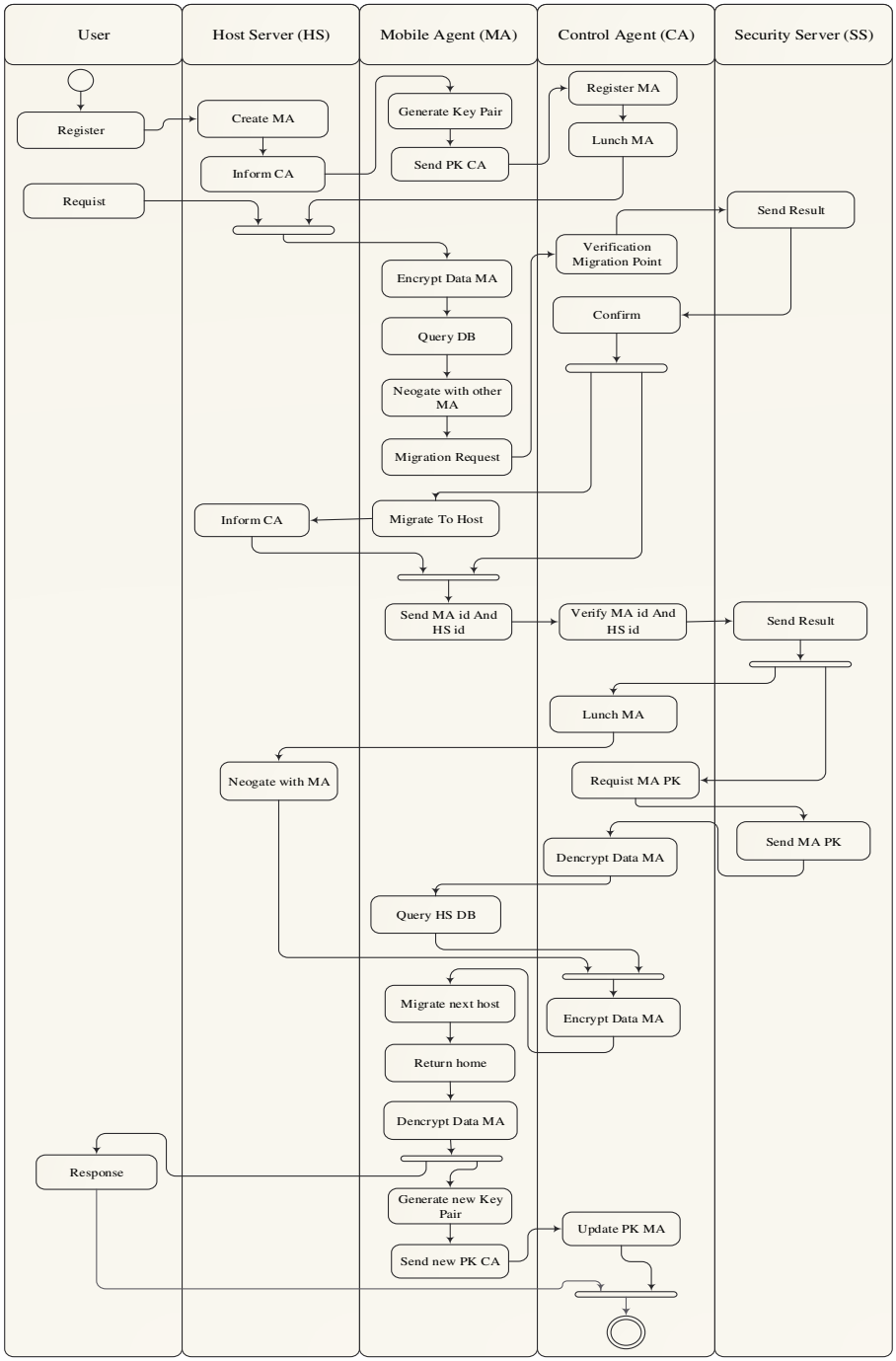

Figure 4. Algorithm interaction main components OMAVLE with centralized mobile agent security system management.

Suppose that some mobile agent MA_i plans to migrate from the virtual learning platform VLP_i, located on the host SH_i, to another virtual learning platform VLP_k, which functioning on the host SH_k. MA_i agent sends a request to its control agent CA_i to carry out migration to VLP_k on host SH_k. When the control agent CA_i received a request from the agent MA_i, accesses the mobile

agents security server (MASS) acts as the certifying canter lead, MASS requesting information to verify the existence of SH_k and VLP_k respectively. In positive response case the control agent CA_i allows the agent MA_i to carry out migration to the host SH_k and initiates an agent MA_i moving process via Agents Migration Manager. At the entrance to the agent-based representation of host SH_k, is a protected memory area (the agent-based representation environment of the receiver host), where loads the software code and migratory agent data which is accessible only by the receiver host SH_k control agents, agent MA_i imposes his certificate to the control agent CA_k on platform VLP_k, in which he wants to be member in. The certificate is an electronic document that contains an agent electronic key, agent information (The mobile agent unique identifier Id_{MA}; The server host unique identifier (address) Id_{MP} from which he migrated, etc.), countersignature certificate authority CA_i and information about the certificate validity period. The control agent CA_i platform VLP_k refers to the central mobile agent security server and checks the information contained in the agent MA_i certificate. If the agent and the host are registered in the system, and the certificate is authentic, the agent MA_i will be loaded into main memory host SH_k, and SH_k host resources within the platforms VLP_k address space become available for agent MA_i.

Agent MA_i can gather all necessary information and can negotiate with agent belonging to host VLP_k. Otherwise, the agent MA_i will be blocked, and the access to all resources SH_k host will be prohibited. However, the control agent CA_i puts the agent MA_i in "black list" and informs all known agents about presence "foreign" agent in the system.

Since all the operated data by agent MA_i which encrypted with private key and unknown to any agent within the node SH_k, the control agent CA_i accesses the mobile agent security server and requests the public key to decrypt the agent MA_i data, searching is carried out by agent ID Id_{MA}. After receiving the public key and decrypt agent MA_i data, the agent data become available to all agents in platform VLP_k. Before entering the agent MA_i into the node VLP_k The control agent CA_i provides it with needed information about all the agents operating within platform VLP_k, thereby the agent MA_i knowledge about the system already replenished. After returning agent MA_i to his "native" host, it generates a new key pair (Sk_{MA_i}, Pk_{MA_i}), and its control agent CA_i updates its public key, which is stored on the mobile agent security server.

In the case of decentralized mobile agents security system management figure 5 MASS in open multi-agent virtual learning environment was implemented on each server node of the system (portals), where users register their learning requisites [14]. With this solution, MASS is part of the agent-based representation on the server node and performs a similar function as the mobile agents security server: stores information about agents in the system, available hosts, virtual learning platforms, agents public key which can access only the system control agent, implementing procedures of agents data encryption and decryption, monitoring, analysing and modelling agents behaviour in the system. Consider the functional structure of mobile agent security host figure 6 and the main components interaction principles of OMAVLS with this implementation approach MASS figure 7.

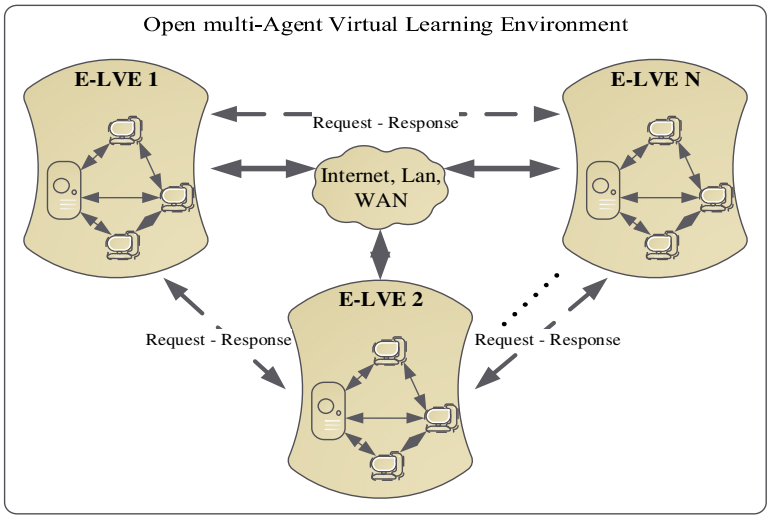

Figure 5.Open multi-agent VLE with the decentralized mobile agent's security c system.

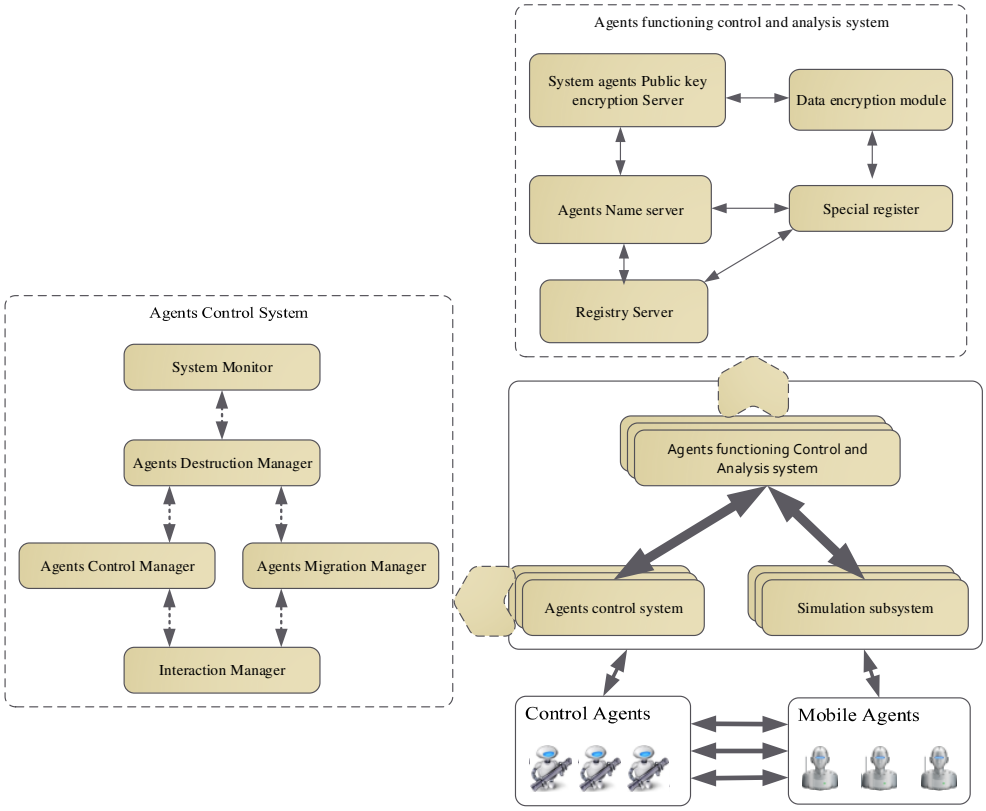

Figure 6. The functional structure of Mobile agent security host

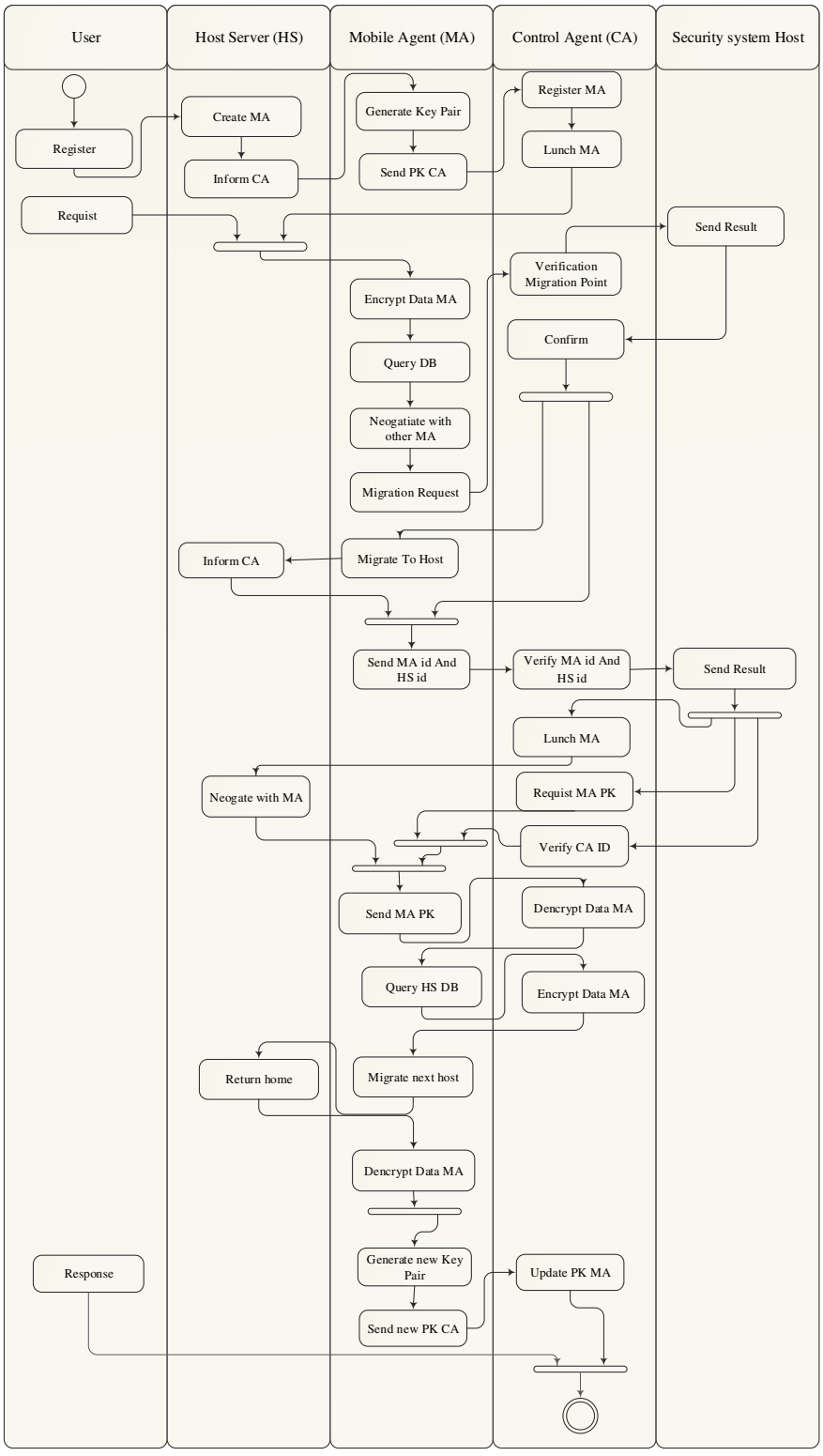

Figure 7. Algorithm interaction main components OMAVLE with decentralize mobile agent security system management.

Suppose that some mobile agent MA_i plans to migrate from the virtual learning platform VLP_i, located on the host SH_i, to another virtual learning platform VLP_k, which functioning on the host SH_k. MA_i agent sends a request to its control agent CA_i to carry out migration to VLP_k on host SH_k. When the control agent CA_i received a request from the agent MA_i, accesses the mobile agents security system in agent representation, and request information to verify the existence of SH_k and VLP_k respectively. In positive response case the control agent CA_i allows the agent MA_i to carry out migration to the host SH_k and initiates an agent MA_i moving process via Agents Migration Manager. At the entrance to the agent-based representation of host SH_k, agent MA_i imposes his certificate to the control agent CA_k on platform VLP_k, in which he wants to be member in. The control agent CA_k on platform VLP_k based on the information contained in the certificate checks the existence of node SH_i and agent MA_i in the local system register and in the MASS. If the agent and the host are registered in the system, the control agent CA_k access the control agent CA_i on the host SH_i from which migrated agent MA_i this center acts as certificate center, and prompting to confirm the existence of an agent MA_i and the fact that he was permitted to migrate to the host SH_k. If the control agent CA_i confirms the existence of agent MA_i and the fact of migration to host SH_k, the control agent CA_k, the agent MA_i will be loaded into host SH_k main memory, and gives him access to all resources within the host SH_k address space platforms VLP_k. Agent MA_i can gather all necessary information and can negotiate with agent belonging to host VLP_k. Otherwise, the agent MA_i will be blocked, and the access to all resources SH_k host will be prohibited. However, the control agent CA_i puts the agent MA_i in "black list" and informs all known agents about presence "foreign" agent in the system [14].

Since all the operated data by agent MA_i which encrypted with private key and unknown to any agent within the host SH_k, the control agent CA_k accesses the control agent CA_i and requests the public key to decrypt the agent MA_i data, control agent CA_i provides agent CA_k with public key for agent MA_i. After receiving the public key and decrypt agent MA_i data, the agent data become available to all agents in platform VLP_k. However, the control agent CA_k assigns a special label to agent MA_i and stores information about it in the agents safe registry replicated within the system. Thus the trust level in the agent MA_i by other agents increases. After returning agent MA_i to his "native" host, it generates a new key pair (Sk_{MA_i}, Pk_{MA_i}), and its control agent CA_i updates its public key, which is stored on the mobile agent security server.

Obviously, the implementation of the system OMAVLS with decentralized security management improves its reliability and resistance to internal and external information security threats, and also allows to organize effective agents and system components protection from purposeful influence malware and spyware agents. The advantages of this embodiment of the MASS, despite the relatively high communication channels loading and redundancy of stored data, are flexibility, adaptability and balancing information security load between servers, system nodes and the control agents [14].

8. CONCLUSIONS

The amid of this study is to analysed the fundamental difficulties and challenges in different types of information security issue arranged in open distributed multi-agents information frameworks. Modern methodologies aimed to solve issues related with guaranteeing agents information security and multi- agents frameworks, Develop the operation standards and the general structure of data security in OMAVLE, Proposed different information security approaches in OMAVLE based on the system implementation with centralized and decentralized security management, as well as the behaviour simulations of their active components (agents).

The proposed methodologies constitute the subsystem information security premise and actualized as an unpredictable programs within the e-learning activities educational support representing OMAVLE. Mobile software agents and proposed arrangements for information security management implemented software tools in development agents environment.

ACKNOWLEDGEMENT

The authors are grateful to the Applied Science University, Amman, Jordan, for the full financial support granted to this research.

REFERENCES

1. Bordini, R.H., A.E.F. Seghrouchni, and M. Dastani, Multi-agent programming: Languages, platforms and applications. 2009: Springer.
2. Erl, T., et al., Web service contract design and versioning for SOA. 2009: Prentice Hall.
3. Brooks Jr, F.P., The design of design: Essays from a computer scientist. 2010: Pearson Education.
4. Tavangarian, D., et al., Is e-learning the Solution for Individual Learning. Electronic Journal of E-learning, 2004. 2(2): p. 273-280.
5. Ho, W., et al., Measuring performance of virtual learning environment system in higher education. Quality Assurance in Education, 2009. 17(1): p. 6-29.
6. Bijani, S. and D. Robertson, A review of attacks and security approaches in open multi-agent systems. Artificial Intelligence Review, 2012: p. 1-30.
7. Song, H.K., et al. Application of genetic algorithm for logistics based on multi-agent system. in Information Networking (ICOIN), 2013 International Conference on. 2013. IEEE.
8. Sander, T. and C.F. Tschudin, Protecting mobile agents against malicious hosts, in Mobile agents and security. 1998, Springer. p. 44-60.
9. Guan, X., Y. Yang, and J. You. POM-a mobile agent security model against malicious hosts. in High Performance Computing in the Asia-Pacific Region, 2000. Proceedings. The Fourth International Conference/Exhibition on. 2000. IEEE.
10. Page, J., A. Zaslavsky, and M. Indrawan. A buddy model of security for mobile agent communities operating in pervasive scenarios. in ACM International Conference Proceeding Series. 2004.
11. Ramchurn, S.D., D. Huynh, and N.R. Jennings, Trust in multi-agent systems. The Knowledge Engineering Review, 2004. 19(1): p. 1-25.
12. Lin, M.-H., C.-C. Chang, and Y.-R. Chen, A fair and secure mobile agent environment based on blind signature and proxy host. Computers & Security, 2004. 23(3): p. 199-212.
13. Van Raaij, E.M. and J.J. Schepers, The acceptance and use of a virtual learning environment in China. Computers & Education, 2008. 50(3): p. 838-852.
14. МАСЛОБОЕВ, А.В. and В.А. ПУТИЛОВ, Разработка и реализация механизмов управления информационной безопасностью мобильных агентов в распределенных мультиагентных информационных системах. Вестник Мурманского государственного технического университета, 2010. 13(4-2).
15. Kannammal, A. and N. Iyengar, A Framework for Mobile Agent Security in Distributed Agent Based E-Business Systems. International Journal of Business and Information, 2008. 3(1): p. 129-143.

16. Karnik, N.M. and A.R. Tripathi, Security in the Ajanta mobile agent system. Software: Practice and Experience, 2001. 31(4): p. 301-329.
17. Wen, G., et al., Consensus in multi-agent systems with communication constraints. International Journal of Robust and Nonlinear Control, 2012. 22(2): p. 170-182.
18. Cao, Y.-y. and C. Fu. An efficient implementation of RSA digital signature algorithm. in Intelligent Computation Technology and Automation (ICICTA), 2008 International Conference on. 2008. IEEE.
19. Somani, U., K. Lakhani, and M. Mundra. Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. in Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on. 2010. IEEE.
20. Rangaswamy, A. and M. Punithkumar, New Symmetric Key Cryptographic Algorithm Using Combined Bit Manipulation And MSA Encryption Algorithm: NJJSAA Symmetric Key Algorithm. International Journal of Innovative Research and Development, 2013. 2(6).

AUTHORS

Dr. Zahi A. M. Abu Sarhan Received the M.S. and PhD degrees in Computerized Control Automated Systems and Progressive Information Technologies from Kharkov National University of Radio Electronics, Kharkov in 1998 and 2004, respectively. During 2004-2008, I was an Assistant Professor at the Economics and Administrative science/ MIS Department at Applied Science University. Since 2008, I am an Assistant Professor at the Faculty of Information technology, Applied Science University in Jordan. Research interests include: Information system reengineering, Service oriented architecture, software agents, agents theory, agents behaviour.

As'ad Mahmoud As'ad Alnaser received a Ph.D in computer engineering from National Technical University of Ukraine “Kyiv Polytechnic Institute”. I am currently an assistant professor of the Department of Computer Science at Al-Balqa' Applied University, Ajlun University College. My research areas include wireless and mobile networks, Internet protocols, and Image processing.