International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:12, No:9, 2018

An Approach to Secure Mobile Agent Communication in Multi-Agent Systems

Olumide Simeon Ogunnusi, Shukor Abd Razak, Michael Kolade Adu

***Abstract*—**Inter-agent communication manager facilitates communication among mobile agents via message passing mechanism. Until now, all Foundation for Intelligent Physical Agents (FIPA) compliant agent systems are capable of exchanging messages following the standard format of sending and receiving messages. Previous works tend to secure messages to be exchanged among a community of collaborative agents commissioned to perform specific tasks using cryptosystems. However, the approach is characterized by computational complexity due to the encryption and decryption processes required at the two ends. The proposed approach to secure agent communication allows only agents that are created by the host agent server to communicate via the agent communication channel provided by the host agent platform. These agents are assumed to be harmless. Therefore, to secure communication of legitimate agents from intrusion by external agents, a 2-phase policy enforcement system was developed. The first phase constrains the external agent to run only on the network server while the second phase confines the activities of the external agent to its execution environment. To implement the proposed policy, a controller agent was charged with the task of screening any external agent entering the local area network and preventing it from migrating to the agent execution host where the legitimate agents are running. On arrival of the external agent at the host network server, an introspector agent was charged to monitor and restrain its activities. This approach secures legitimate agent communication from Man-in-the Middle and Replay attacks.

***Keywords*—**Agent communication, introspective agent, isolation of agent, policy enforcement system.

I. Introduction

MOBILE agent communication provides great support and incredible advantages over the traditional designs of network communication [1]. The capability of mobile agents is as a result of its ability to communicate and collaborate with other entities that make up the environment of the agent system [2]. Such entities include other agents, platforms, other applications, and human users. This social ability of mobile agents empowered them to solve problems that are sometimes beyond the knowledge of the individual agent which could be solved by several entities. Mobile agents use their social ability via negotiation, collaboration, and cooperation to achieve their designed objectives. However, it is not usually easy to efficiently send message to an agent.

Based on the significance of MAS in the deployment of real applications, there is need for confidentiality protection of agent communication to facilitate hitch-free collaboration of agents and attainment of their set objective(s). This study therefore, focuses on the development of a non-cryptographic agent communication protection scheme devoid of computational complexity characterized the existing cryptographic-based schemes. The proposed scheme employs external agent migration restriction technique [3], [4] to isolate and confine external agent activities to the network server where it is believed its mission could be accomplished. The network server usually hosts the network sharable resources among which could be of interest to the visiting external agent.

In this paper, the state-of-the-art techniques for agent communication security are summarized in Section II to provide an overview of current developments. The proposed scheme and its components are delineated in Section III. Section IV presents the implementation details, while Section V concludes with a discussion of future directions.

II. Related Work

An approach to secure agent communication using Open PGP to encrypt and sign ACL messages was developed by [5]. The PGP defines standard formats for signatures, encrypted messages and certificates for public keys exchange. PGP supports secure message services including message confidentiality using symmetric and asymmetric encryption algorithms. It also uses digital signature to ensure message integrity and origin authentication. The author proposed the use of PGP to encrypt and sign the whole ACL message without altering the message envelop, while the encoding and decoding of PGP structured messages are left for the agent to handle. The encryption/decryption and signature processing are to be performed by the agent communication channel (ACC) service. An agent oriented public key infrastructure (APKI) was proposed in [6] for multi-agent system based e-service. Digital certificates were generated, stored, verified, and revoked for the purpose of satisfying different access and delegation control. The agents' certificates were used for their authentication, while attribute and authentication certificates were proposed for the authorization and delegation of agents. In [7], a security system architecture called X-security was proposed, which implements message encryption and signing to improve trust and confidentiality in mobile agent society. This approach is also used security certification authority (SCA) agent for issuance of identity certificates to the mobile agents in accordance to FIPA standard. The SCA is a standalone agent which is at the same level of the agent naming server and the directory server. Other mandatory and

Olumide Simeon Ogunnusi and Michael Kolade Adu are with the The Federal Polytechnic, Department of Computer Science, P.M.B. 5351, Ado-Ekiti, Ekiti State, Nigeria (e-mail: olu_simmy@yahoo.com, memokadu@yahoo.co.uk).

Shukor Abd Razak is with the [2]Universiti Teknologi Malaysia, Faculty of Computing, Department of Computer Science, 81310 UTM Johor Bahru, Johor, Malaysia (e-mail: shukorar@utm.my).

additional information about mobile agent (such as agent identity, public key, and validity time) are contained in the certificates. An AgentScape [8] presented a novel security policy enforcement system for multi-agent middleware systems, which also allows users to develop customized policies to suit their individual needs. AgentScape supports SSL-based communication between hosts and/or locations. It provides the basis for hosts/locations to authenticate each other and all messages transmitted between them including agent migration are encrypted to facilitate confidentiality. The drawbacks of the current information systems was analyzed in [9] which employed the idea of an information retrieval system based on mobile multi-agent (IRSMMA) to improve the performance of nowadays information retrieval system. This system however, brings some security concerns such as masqueraded malicious host, malicious mobile agent, and generation of fake information. To overcome these threats, a mobile multi-agent security architecture (MMASA) is introduced with the following policies: Authentication with X.509 certificates; Confidentiality with the use of SSL on the transport layer; IDEA algorithm to encrypt mobile agents and RSA to encrypt the key; Integrity with the use of MD5 for message digest and PKI with RSA for digital signatures; Access control with the use of java authentication and authorization service; and Reliability using audit resource of java. A multi-agent based security mechanism (MAgSeM) that is used to improve a traditional non-agent based system was proposed in [10], [11]. The authors claimed that as a result of the interactive, autonomous, extensible and mobility properties of the agents, the agents were able to perform their tasks with minimal interaction with the user. Java agent development framework (JADE) was used to develop the security mechanism while FIPA agent communication language was used to implement agent communication. Cryptographic schemes were used to secure the transfer of sensitive data. The key to decipher the information was kept with the sender. A token was sent to the receiver to sign and forward it back to the sender to receive the key to decipher the information. A secure and lightweight public key-based security scheme was presented in [3]. The scheme used mutual authentication protocol and access control based on Elliptic curve cryptography to ensure that medical data are not leaked to unauthorized person. A secure data communication with the use of digital signature was proposed in [12]. To create the digital signature, a message digest was generated by running the message to be transmitted through a hash algorithm (MD5). The generated hash value was then encrypted with the sender's private key. The encrypted hash value is then added to the end of the message before it is transmitted. A lightweight mutual authentication mechanism in order to improve PMIPv6-based network mobility scheme (LMA_IFP_NEMO) was proposed in [13]. They used authentication, authorization and accounting (AAA) servers to boost the security of IFP_NEMO protocol using only symmetric cryptography, nonces and hash operation primitives to facilitate secure two-pass authentication between mobile router and proxy mobile IPv6 domain.

III. The Proposed Policy Enforcement System

The policy is made up of two phases. The first phase is to ascertain that the execution environment of the legitimate agents is devoid of any form of interaction order than the collaboration required of them to accomplish their designed objective. In the proposed policy, an agent from a foreign security domain enters into the receiving security domain via its agent server, as illustrated in Fig. 1.

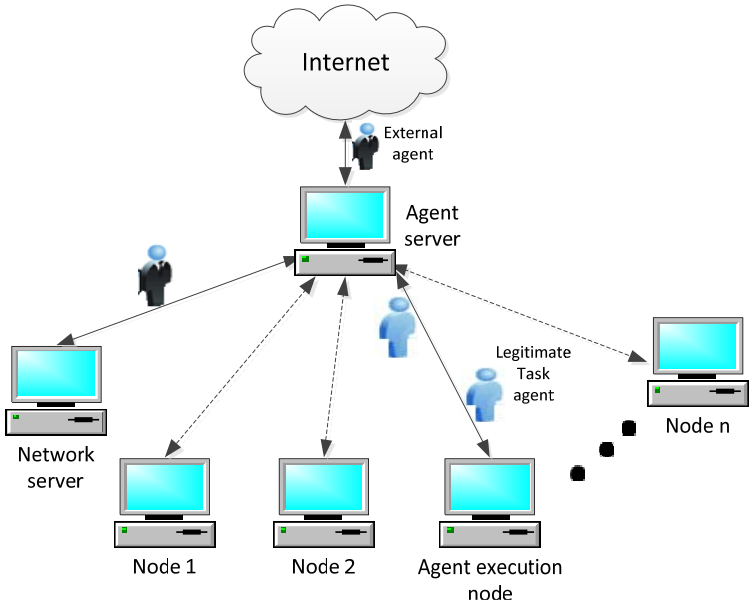

Fig. 1 Restriction of External agent to Network Server

The agent server was made to scan the external agent against any malicious tendency using Attack Identification Scanner [14], [15]. If the external agent is found to be non-malicious, the controller agent at the agent server sends a migration request to the external agent to migrate to the network server for execution. The scanning at the agent server is necessary because it is possible for an agent to be malicious due to:

i. its intelligence;
ii. its owner/originator activity;
iii. infliction of agent with malicious code along its migration path unknown to the agent owner.

The second phase of the policy ensures that the activities of the external agent are confined to the network server. To achieve this, JADE's introspector agent was equipped with additional functionality to determine whether the activity performed by the external agent is permissible or not. The introspector agent carries a table of agent's prohibited activities, as shown in Fig. 2. An activity of the external agent is censored and kept in suspense by the introspector agent while it is compared with the list of prohibited activities. Any match in the comparison pops up error message, thereby blocking the external agent from performing such an activity. The communication or connection ability of the external agent was also checked and confined to the network server. This technique has deprived the external agent from connecting to the communication channels of the legitimate agents running and collaborating at the agent execution host.

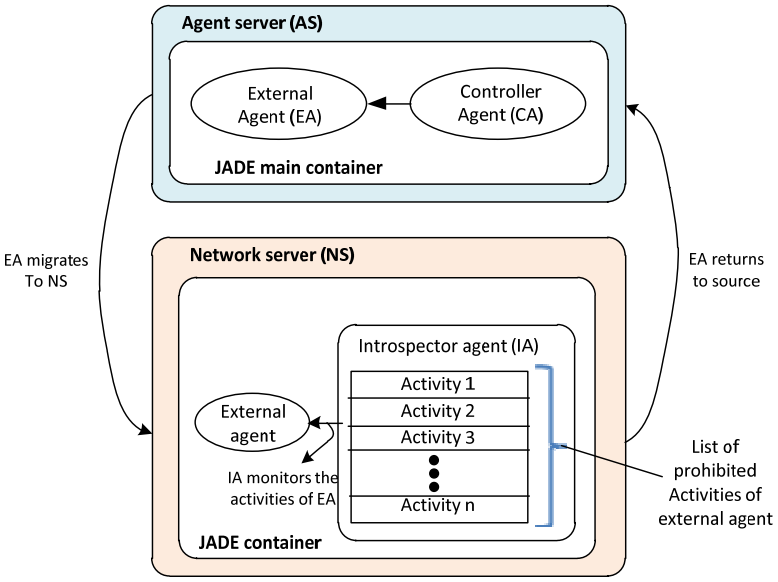

Fig. 2 Confinement of External Agent Activities to the Network Server

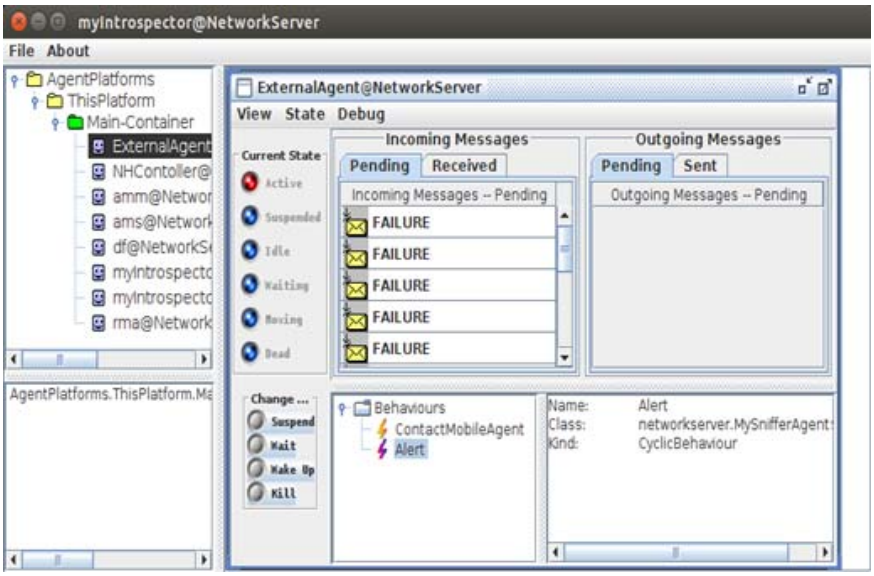

Fig. 3 Snapshot of JADE GUI showing arrival of external agent at the network server

IV. Implementation Details

On arrival of the external agent at the agent server, the controller agent sends it to the network server as shown in Fig. 3. At the network server, the external agent can perform any desired activity but strictly under watch by the Introspector Agent resident on the Network Server (acting as a watchdog). The Introspector Agent determines whether the activity performed by the external agent is permissible or not. In other words, an activity of the external agent is *blocked*, if and only if, such activity is found among the list of prohibited activities maintained by the Introspector Agent, otherwise it is permitted. The Introspector agent is an administrative tool of JADE Agent Management System (AMS) designed to monitor and control the life-cycle of agents running on the platform and their exchanged messages including the queues of sent and receiving messages [16]. In this study, the functionality of Introspector Agent was extended such that it is configured to block external agent from performing activities enlisted in a table of prohibited activities. In this study, the external agent prohibited activities stored in Introspector Agent include external agent communication capability outside its runtime environment. The external agent communication constraint is purposely to confine the external agent communication capability to its environment.

Any attempt by the external agent to execute communication activity not permitted by the Introspector Agent will trigger error message *"Error communication blocked"* as shown in Fig. 4. The inability of the external agent to have successful connection with the legitimate agent communication channel at the agent execution host foils man-in-the-middle and replay attacks by external agent on the legitimate agents' communication.

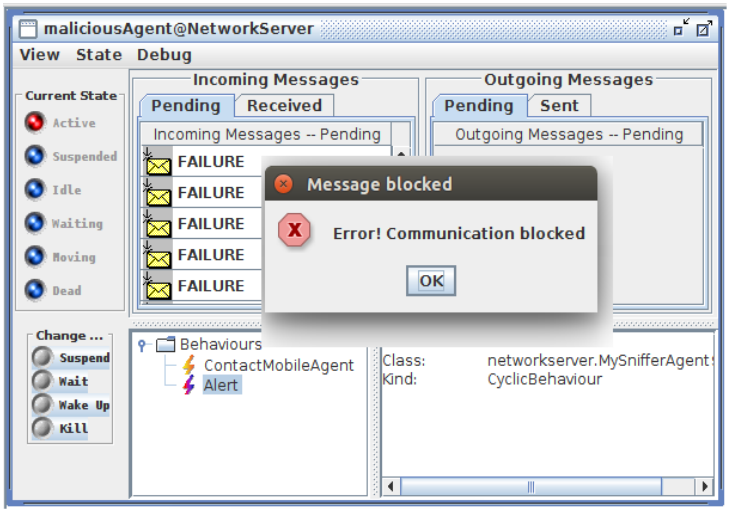

Fig. 4 Snapshot of JADE GUI showing the reaction of introspective agent to the communication activity of external agent running on the network server

V. Conclusion

This article presents a non-cryptographic technique to secure agent communication using policy enforcement system. This technique mandates the external agent to run on a desired neutral host and at the same time isolates and confines its activities to the host. The idea is to curtail its ability to communicate with the legitimate task agents running at the agent execution host. The isolation and confinement was achieved by establishing prohibited activity-space for the external agent such that none of its activities could be found in the activity-space. This was used to limit what the external agent could do, especially its communication coverage. The isolation of the external agent to the network server has helped to curtail its ability to access the communication channel through which the legitimate agents communicate with one another. Further research could focus on how the external agent running on the network server be prevented from eavesdropping the communication among the legitimate agents in the agent execution host.

References

[1] Singh, Parwinder, & Malhotra, Mrs Sheenam. (2013). Trends in Mobile Agent Communication for Mobile Networks. *International Journal, 3*(5).

[2] Cavalcante, Rodolfo Carneiro, Bittencourt, Ig Ibert, da Silva, Alan Pedro, Silva, Marlos, Costa, Evandro, & Santos, Robério. (2012). A survey of security in multi-agent systems. *Expert Systems with Applications, 39*(5), 4835-4846.

[3] Lee, Xuan Hung, Khalid, Murad, Sankar, Ravi, & Lee, Sungyoung. (2011). An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare. *Journal of Networks, 6*(3), 355-364.

[4] Kandil, Heba, & Atwan, Ahmed. (2014). *Mobile agents' authentication using a proposed light Kerberos system.* Paper presented at the 9th International Conference on Informatics and Systems (INFOS).

[5] Niklas Borselius and Chris J. Mitchell (2003). Securing FIPA agent communication. In H. R. Arabnia and Y. Mun, editors, Proceedings of the 2003 International Conference on Security and Management (SAM'03), Vol. 1, pages 135–141. CSREA Press, Nevada.

[6] Hu, Yuh-Jong, & Tang, Chao-Wei. (2003). *Agent-oriented public key infrastructure for multi-agent E-service.* Paper presented at the 7th International Conference on Knowledge-Based Intelligent Information and Engineering Systems, pp 114–136.

[7] Novak, P., Rollo, M., Hodik, J., & Vlcek, T. (2003). Communication security in multi-agent systems. *Multi-Agent Systems and Applications*

III, Proceedings, 2691, 454-463.

[8] Quillinan, Thomas B, Warnier, Martijn, Oey, Michel, Timmer, Reinier, & Brazier, Frances. (2008). *Enforcing security in the agentscape middleware.* Paper presented at the Proceedings of the 2008 workshop on Middleware security.

[9] Xiao-Long, Xu, Jing-Yi, Xiong, & Chun-Ling, Cheng. (2010). *The model and the security mechanism of the information retrieval system based on mobile multi-agent.* Paper presented at the 12th IEEE nternationalConference on Communication Techology (ICCT).

[10] Sulaiman, Rossilawati, & Sharma, Dharmendra. (2011). *Enhancing security in e-health services using agent.* Paper presented at the 2011 IEEE International Conference on Electrical Engineering and Informatics (ICEEI).

[11] Sulaiman, Rossilawati, Huang, Xu, & Sharma, Dharmendra. (2009). *E-health services with secure mobile agent.* Paper presented at the 7th Annual Communication Networks and Services Research Conference, pp 270-277.

[12] Krishnalal, G, & Babu, Jisha. (2013). *A Secure Data Transmission For Multiagent System Using Digital Signature.* Paper presented at the International Journal of Engineering Research and Technology, pp 4-7.

[13] Ben Ameur, Sirine, Zarai, Faouzi, Smaoui, Salima, Obaidat, Mohammad S, & Hsiao, KF. (2014). *A lightweight mutual authentication mechanism for improving fast PMIPV6-based network mobility scheme.* Paper presented at the 4th IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC).

[14] Venkatesan, S, & Chellappan, C. (2008). *Protection of mobile agent platform through attack identification scanner (AIS) by malicious identification police (MIP).* Paper presented at the First International Conference on Emerging Trends in Engineering and Technology, 2008. ICETET'08.

[15] Venkatesan, S, Chellappan, C, Vengattaraman, T, Dhavachelvan, P, & Vaish, Anurika. (2010). Advanced mobile agent security models for code integrity and malicious availability check. *Journal of Network and Computer Applications, 33*(6), 661-671.

[16] Bellifemine, Fabio, Caire, Giovanni, Trucco, Tiziana, Rimassa, Giovanni, & Mungenast, Roland. (2003). Jade administrator's guide. *TILab (February 2006)*.