International Journal of Soft Computing 10 (2): 99-109, 2015
ISSN: 1816-9503

Attacks and Security Solutions for Agent Communication in Multi-Agent Systems

Olumide Simeon Ogunnusi and Shukor Abd Razak
Department of Computer Science, Faculty of Computing,
Universiti of Teknologi Malaysia, 81310 Skudai, Johor Bharu, Johor, Malaysia

Abstract: Agent communication security has been a subject of much research in the recent past motivated by the need to effectively harness the social ability of agents to deploy distributed applications and conservatively utilize network bandwidth. Security of agent communication is inevitable to overcome the impediments that may hinder the performance of mobile agents to accomplish their designed objectives. Such, impediments encompass denial of service attack, man in the middle attack, eavesdropping, resource availability attack and replay attack. Researchers have made series of effort to combat these threats to agent communication using cryptographic signature, message encryption and access control to facilitate agent authentication and authorization. This study therefore, focuses on the review of the attacks and security solutions for mobile agent communication proposed by the researchers in the field of agent technology. Researchers then carried out comparative analysis of the various security mechanisms in literature and assess them using the parameters: authentication technique and network overheads.

Key words: Mobile agent, agent communication, agent communication security, inter-agent authentication, mechanisms

INTRODUCTION

Mobile agents are intelligent software agents capable of moving from one machine to another in heterogeneous computer network and carry out the task instructed by their owners (Guan *et al*., 2010). Their social property is as a result of their ability to communicate with one another and their host platform which is consequential to their ability to solve complex problems through collaboration. This communicative ability of mobile agent has really made cooperation between agents possible. There are two types of communications in multi-agent system. They are peer to peer communication and broadcasting communication. In peer to peer communication, only two agents are involved in the communication as shown in Fig. 1 while in broadcasting communication, an agent sends the same messages to several agents as illustrated in Fig. 2. However, there are threats to the communication which are very synonymous to what is being experienced in convectional computer networks (Cavalcante *et al*., 2012). These threats can be passive or active. Passive threats may be in form of attackers listening to the communication between agents while active threats may be a third party attempting to intercept and modify the exchanged data (Lu and Huang, 2006).

Mobile agent communication has provided great support and remarkable advantages over the traditional

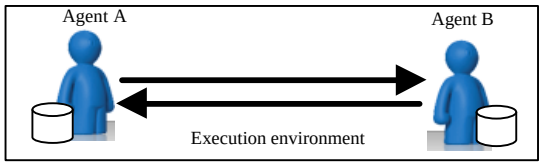

Fig. 1: Peer to peer communication of agent

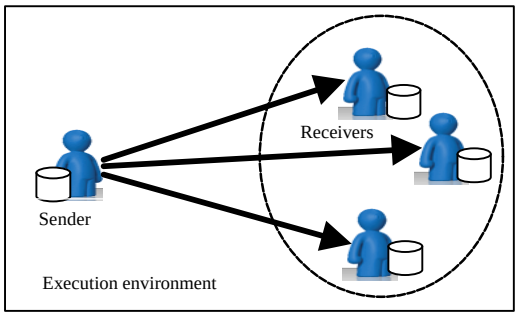

Fig. 2: Broadcast communication of agent

architectures of network communication (Singh and Malhotra, 2013) and the strength of mobile agents is derived from its ability to communicate and interact with other entities that make the agent system environment (Cavalcante *et al*., 2012). Such entities include other agents, non-agent software and human. This social ability

Corresponding Author: Olumide Simeon Ogunnusi, Department of Computer Science, Faculty of Computing, Universiti of Teknologi Malaysia, 81310 Skudai, Johor Bharu, Johor, Malaysia

of mobile agents empowered them to solve problem that is sometimes beyond individual knowledge which could be solved by several entities. Mobile agents use their social ability via negotiation, collaboration and cooperation to achieve their designed objectives which invariably raises some security concerns over the already known communication problems. Through, the social ability, agents can lie to other agents, cheat in negotiations, breach of agreements of collaboration and cooperation, formation of plots and other forms of corruption that are a notchabove the simple message exchanges (Cavalcante *et al*., 2012). Collaboration is one of the effective means to attain agents' goals in multi-agent system and doing so with malicious agents may make them deviate from achieving their goals (Jung *et al*., 2012). For example, a malicious agent may demand other agents to provide services it does need with the intention to make some community services unavailable. To get rid of such unwanted interactions, a solution to the method of controlling unauthorised collaboration is inevitable. An effective access control mechanism is required to enable secure cooperation among agents.

Security of agent communication is concerned with the verification and authentication of the identities of the agents involve in the sending and receiving messages in the course of their communication. Since, one-factor authentication technique (username and password) regarded as the first line of authenticating entities on a network is no longer adequate to secure sensitive information, the second line of authentication, referred to as two-factor or multi-factor authentication technique is widely adopted to combat the nefarious activities of unrelenting attackers called hawkers. Two-factor authentication is a security process in which an entity provides two means of identifying itself. The entities identifiers can be from: who they are what they have or what they know. In multi-agent system, the parameters usually used for the identification of mobile agents are the agents' names (who they are) and the digital signatures of their senders (what they have). In fact, authentication is a process of confirming who or what an entity declared to be. For mobile agents to have access to network resources, authentication is required and is a prerequisite to giving them authorization access to the required resources.

This study, therefore is charged with surveying of the various authentication techniques proposed by researchers to guarantee security of agent communication in a multi-agent system.

MOBILE AGENT COMMUNICATION

There is a communicating channel through which the agent communication message can pass in either direction. In peer to peer communication, there is a mailbox attached to the agent at each end and either of the agents can send and receive message. An Agent Communication Language (ACL) is a lingua francafor multi-agent system (Chopra *et al*., 2013). Agents require a communication model to capture the communications and flow of knowledge exchange within the agent community. ACL provides a set of language primitives to implement the Agent Communication Model (Li and Kokar, 2013). Agent communication is communicative and performative acts of agents and it occurs in the form of message passing among the collaborative mobile agents. Figure 3 illustrates a typical scenario of message passing between two agents.

Agent communication must be based on a standadised agent communication language or protocol (ACL) such as Knowledge Query and Manipulation Language (KQML), Foundation for Intelligent Physical Agents (FIPA). The conventional inter-process communication mechanisms like TCP, UDP, RPC, rendezvous and group multi-cast in client-server applications can be adopted by multi-agent applications but these mechanisms are particularly too low level to fully support the required communication of collaborating mobile agents (Mishra and Xie, 2003). This is primarily due to the fact that the inter-process communication mechanisms do not take agent mobility of collaborating agents into consideration. As a result of the unique mobility property of mobile agent, the actual location where agent communication is taking place and the locations where agents are executing at the time of communication play a significant role. In view of this, DaAgent System (Mishra *et al*., 1999) provides two types of inter-agent communication techniques:

- Location-dependent communication
- Location independent communication

In Location-Dependent Inter-agent Communication (LDIC) technique, mobile agents communicate with one

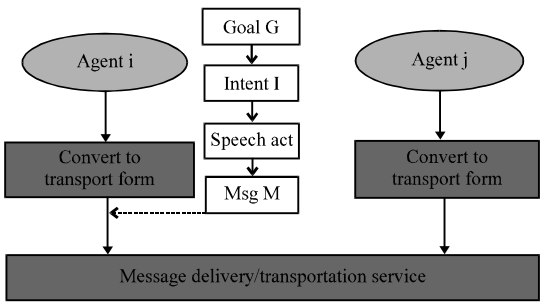

Fig. 3: Message passing between two agents (Burg, 2002)

another on a specific host in the network. All the agents to be involved in the communication (i.e., sender agents and the receiver agents) need to visit this host to communicate while in location-independent inter-agent communication, a mobile agent communicates with another agent without regard to any specific location in the network. In this case, the communicated information follows the receiver agent until the receiver agent receives it.

MOBILE AGENT COMMUNICATION SECURITY

Communication is an essential feature of Multi-Agent System (MAS). However, the social ability of mobile agents raises some security concerns over the already known communication problems. Despite the quantum of research efforts in multi-agent system, the wide acceptability of the system is still not achieved due to the security imbroglio. For example, in an agent-based intrusion detection system where each participant in the intrusion detection task is expected to collaborate and through proper coordination identify intrusive packets and send alert signal to the network administrator, there exist an unauthorised malicious agent whose mission is to sabotage the security mechanism in place by killing the legitimate agents so that the intrusive packets can have their leeway and perpetrate their nefarious act. The saboteurs or cyber criminals can easily achieve this by simple request to the agent management system (of JADE for example).

Collaboration is one of the effective means to attain agents' goals in multi-agent system and doing so with malicious agents may make them deviate from achieving their goals (Jung *et al*., 2012). An effective access control mechanism is required to enable secure cooperation among agents. Mobile agents must have a secured communication mechanism to receive messages from other agents and also exchange their views on a given task with other agents on an agent platform especially during the process of negotiation or collaboration of the agents that are on a problem-solving mission. The security mechanism must also be able to restrain an alien mobile agent from interfering, spying or eavesdropping the agent communication.

In order to effectively harness the benefits offered by the use of multi-agent technology in real applications, it is imperative to ensuresecurity, integrity and authenticity of inter-agent communication (Novak *et al*., 2003).

ATTACKS ON AGENTS COMMUNICATION

A number of attacks identified in literature (Constantinescu and Popirlan, 2011; Pozo *et al*., 2004; Oey *et al*., 2010) have severe effect on communication among mobile agents among which are:

- Man in the middle attack
- Reply attack
- Denial of Service attack (DoS)
- Eavesdropping

Both man in the middle attack and replay attack are classified as active attack because of their outright manipulation of the agent communication while eavesdropping attack and DoS are passive attacks. Figure 4 illustrate an active attack where a malicious agent MAG captures the data communicated by agents A and B, manipulate and replay the communicated data stream without the knowledge of the two agents.

Man in the middle attack: This is one of the most important attacks upon crypto system. Suppose there are two mobile agents (agent A and B) that intend to communicate. Man in the middle attack occurs when a malicious agent having impersonated agent B, receives and keep all the messages from agent A and send its own messages back. So, agent A will communicate with the malicious agent without realizing that it is not communicating with agent B. The malicious agent will use similar method to impersonate agent A and communicate with agent B.

Replay attack: This attack is concern with a malicious agent trying to authenticate itself through valid authentication steps tapped from the communication channel. The measure against this attack is that all legitimate mobile agents must be encrypted using a very strong crypto system.

Denial of service attack: Denial of Service attack (DoS) is regarded among the major threats and toughest security problem in today's internet (Karthik *et al*., 2008). In agent communication, a denial of service attack occurs when an agent community is deprived access right to the resources required for its collaboration for the accomplishment of its designed objective. For instance, DoS attack occurs if the execution environment seizes to provide the communication resource required by the agent community for effective communication among its members during collaboration.

Eavesdropping: This attack occurs when an unauthorised (malicious) agent eavesdrops on the communication between two agents by monitoring the communication. The malicious agent collects information but does not actively tampered with neither the agents nor the agent communication. This attack compromises the privacy of agent communication by observing or listening to secret

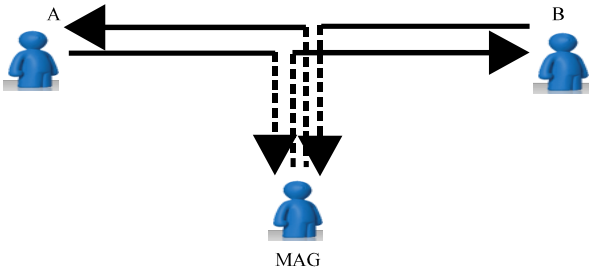

Fig. 4: Active attack

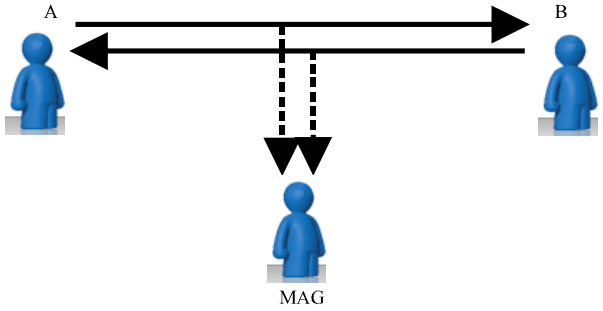

Fig. 5: Passive attack

communication among agents. The information captured by the malicious agent may be used to launch a more severe attack on the agent community. Figure 5 illustrates a passive attack where a malicious agent MAG monitors the communication between agent A and B.

EXISTING AND RELATED LITERATURE

Researchers have proposed many solutions to the confidentiality threat of agent communication using authentication and authorization mechanisms, encryption and digital signature. In (Novak *et al*., 2003), a security system architecture called X-security was proposed which implements message encryption and signing to improve trust and confidentiality among mobile agent society. This approach also used Security Certification Authority (SCA) 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 additional information about mobile agent (such as agent identity, public key, validity time) are contained in the certificates. In this architecture (Fig. 6), a security module can be positioned between the core of an agent and the communication layer such that the agents that have the module may choose to create secured messages (by encrypting or signing the messages) or unsecured messages (by passing the messages directly from the agent's core to the communication layer).

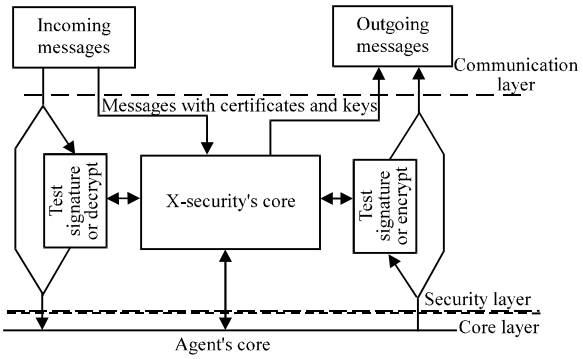

Fig. 6: Incorporation of security module with agent

The security module has several units. Each one is saddled with the provision of encryption, decryption, creation or checking signatures and connection to SCA and exchanging certificates with other agents. The security module also maintains a database of receives certificates and private keys. It also provides an interface between the agent's core and the security module.

The security approach to agent communication proposed by Novak *et al*. (2003) has some advantages. The first is the idea of having a security module that is autonomous of the core of the agent and can be imported from any library or inherited from a super class. The second advantage is the concern about the temporary inaccessibility of the certificate authority that is responsible for issuing the certificates. Here, agents are allowed to provide their certificates (once signed by the CA) to each other for inter-agent authentication. Thirdly, the system maintains the scalability because the security module is the responsibility of the agent and not the platform which allows the coexistence of safe and unsafe agents from other hosts. However, for real time application, the architecture does not provide an alternative means of securing the communication between agents in case the X-security core is attacked or breakdown and hence the architecture is deficient of fault tolerance and prone to single point of security failure. Another concern is the need for mutual authentication of the mobile agents before communication begins. Mutual authentication necessitate that each mobile agent must possess the certificates of all other agents thereby resulting to heavy weight of the agents with its consequent undesirable memory and communication overheads on the network and its resultant network degradation.

Wang *et al*. (1999) proposed a simple and lightweight multi-agent system security scheme using Asymmetric Encryption algorithm involving compressing the message, N-bit grouping, subtracting from the secret key saved in

the secret code file and ungrouping. According to the researchers, the hackers face a combinational exploitation problem in an attempt to guess the secret codes and the compression adds another security layer. However, the researchers attributed the weakness of the scheme to the weakness of the algorithm for short messages and secret key management difficulties which include producing, transferring and saving large secret files in agents especially when large number of agents is involved in the communication where each pair of communicating agents must maintain separate secret key.

Wong and Sycara (2000) used unique agent identities and Secure Socket Layer (SSL) protocol beneath their agent communication layer as a means of providing agent communication security in their proposed security infrastructure to address the security and trust of RETSINA framework. In a different research with the same approach conducted by Vila *et al*. (2007), the researchers introduced many security services for JADE framework by integrating their security mechanism (IMTP over SSL) and JADE-S security features. IMTPoverSSL uses certificate-based container to container structure to provide confidentiality, data integrity and mutual authentication. A container is a group of agents. In this framework, each container securely stores other containers' certificates and the security features are deployed using TLS/SSL protocol. Both security schemes for agent communication rely on the security of TLS (Transport Layer Security) and SSL. However, the disadvantage of the use of SSL for agent communication security is that it is a widely used existing security mechanism and various hackers from different communities (network, web) are trying to find its vulnerabilities and exploit them to lunch attack.

Borselius and Mitchell (2003) developed an approach to secure agent communication using Open PGP to encrypt and sign ACL messages. Researchers also recommended the use of XML encryption service to secure ACL messages. However, this approach is inadequate to prevent attacks that exploit information flow such as man in the middle attack.

Policy-driven security mechanisms can be used for access control, defining acceptable behavior and protect confidentiality in adversary environment (Bijani and Robertson, 2012). Wagner (1997) uses database concept of multi-level security and applied it to inter-agent communication for the protection of confidential information. Knowledge of Message Specification Language (MSL) databases and some basic inter-agent communication rules were defined. The security specifications are implemented by the communication rules while the MSL database assigns a security classification such as unclassified, confidential, secret and top secret, to every information item and allocates authorization to every user. The whole system then enables all agents to comply with the defined security policy.

Some agent development frameworks such as JADE-S (JADE Board, 2005) provide some degree of security support for agent communication at the transportation layer only. JADE-S secures agent message transportation using signature and encryption and also employ access control mechanism based on Java Authentication and Authorisation Service (JAAS). Lack of security support by FIPA and FIPA compliant JADE platform is stated by Poggi *et al*. (2001), Poslad and Calisti (2000) and Farkas and Huhns (2002).

The concern of Hu and Tang (2003) about the scalability of the system informed their proposed multi-level security architecture where agents are responsible for the certification management. The hierarchy of certification authorities eased the addition of new trusted certification authorities to the system so as to support additional agents. Researchers also recognised the necessity of a public key infrastructure exclusively for agents.

Some relevant works are proposed in order to build scalable authorization mechanisms. For example, Becerra (2003) provides a model where authorization and authentication decisions are made via the cooperation of the mobile agents whose responsibility is to manage the security on the system. In this model, a voting scheme is used to get a consensus about a decision. The main problem with this model is the high communication overhead required in order to implement the security process.

Similarly, a relevant work is proposed by Xiao *et al*. (2007) an authorization mechanism based on RBAC (Role-based Access Control) Model. The researchers believe that with the use of policies based on roles, it is possible to design a security architecture that automatically adapts to system changes. Of course, this is partly true. Assigning access policies to groups of agents with the same capability makes the system independent of the input and output of individual agents. However, human users are still required for the management of the policies assigned to roles that make up the system.

Many of the studies showing concern about the security of multi-agent community focus on authentication methods as the basis for building security infrastructure for certifying and ascertaining that agents

and their owners are reliable entities and will exercise good behaviour. Other research ideas consider authorization as the key method to add security to MAS (Wen and Mizoguchi, 2000; Xiao *et al*., 2007).

Xu *et al*. (2010) analysed the drawbacks of the current information systems and employ the idea of an Information Retrieval System Based on Mobile Multi-Agent Agents (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 which follows the policies stated:

- 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
- Reliability using audit resource of java

Sulaiman and Sharma (2011) and Sulaiman *et al*. (2009) proposed a Multi-Agent based Security Mechanism (MAgSeM) that is used to improve a traditional non-agent based system. Researchers claimed that as a result of the interactive, autonomous, extensible and mobile properties of the agents, the agents were able to perform their tasks with minimal interaction with the user. Java Agent Development (JADE) framework is used to develop the security mechanism while FIPA agent communication language is used to implement agent communication. Cryptographic schemes are used to secure the transfer of sensitive data. The key to decipher the information is kept with the sender. A token is sent to the receiver to sign and forward it back to the sender to receive the key to decipher the information. In this security mechanism, the sender is in control of the transferred information while the details of the decryption are unknown to the receiver. The proposal addresses the security of:

- Confidentiality with the use of symmetric keys AES or Blowfish
- Information using SHAI (to create hashes of the information)
- Channel using SSL
- Integrity using PKI (to encrypt via RSA)

However, researchers assume that the communicating agents exchanged certificates via a secure channel. The type of technology adopted for agent certification is not specified.

In (Subalakshmi *et al*., 2011), a model to enhance small e-Health organizations' functionalities by applying a multi-agent system using the JADE framework is proposed. The JADE framework gives the system autonomy, peer to peer characteristics, a distributed system, interaction schemes and support for the J2ME platform. Using the model patient can get the service from the system using the Patient Agent (PA). When the doctor wants to checkup the patient he/she can get all the detail of the patient and give the medicine using Doctor Agent (DA) while all the internal activity is control by Controller Agent (CA). The agents can communicate via the internet for the provision of medical care services. However, the researchers are mainly concerned with the data flow within the e-Health care organization and little consideration is given to confidentiality protection of the patient sensitive information carried by the agents using simple firewall, login and password validation. They have also failed to take cognisance of the need for the confidentiality protection of agent communication, thereby making it vulnerable to attacks.

Ahmed (2010) proposed the use of Short Message Service (SMS) to secure mobile agent system. It identifies and discusses many malicious mobile agent threats such as pilfering of sensitive data, damage to host resources, denial of service and annoyance attacks. The study therefore, advances several solutions and methods to solve the problems such as software-based fault isolation, code signing, firewalling, safe code interpretation, proof caring code, path histories and state appraisal. This system's idea is that the mobile agents are generated by a SMS written in a specific Mobile Agent Description Language (MADL) which gives them all the required information to perform their tasks. The security in the system is claimed to be anchored on the belief that the mobile agent owner is separated from the source of the mobile agent and hence, he cannot induce malicious code into the agent.

Loulou *et al*. (2006) proposes a conceptual model for secure mobile agent systems. The proposed model focuses on overcoming possible attacks on the mobile agent system considering the basic security concepts such as agent authenticity, authorization and security

policies. In this proposal, security policies are enforced to control the entities of mobile agent systems. However, only authorization policies are specified.

Dadhich *et al.* (2011) propose a different security mechanism using trust-centric approach to proffer solution to security problems of agent system with the claim that it enables better security decisions with uncertainty in the behaviour of entities. It also claim that current security systems are associated with the problems of violation of identity and intentional assumptions, lack of security hierarchy in open environments compared to closed environment and lack of behavioural evidences. The study then introduces some trust-centric solutions that overcome the conventional security problems by using authentication trust, improving itinerary composition and authorization process, integrating behavioural and cryptographic-based evidences and evaluation of evidences.

Vieira-Marques *et al.* (2006) propose and discuss an information gathering system to secure integration of distributed, inter-institutional medical data with the adoption of agent technology. The systems was designed to enhance the existing Virtual Electronic Patient Records (VEPR) System to work on networked and distributed medical systems rather than only a local medical system with its attendant novel challenges. The security mechanism of the system needs to ensure that only authorized staff can access the information and that data moving through the network are protected and safe. The proposed mobile agent system is based on JADE framework and agent communication is implemented using FIPA-ACL. Security wise, this proposal focuses at:

- Self-protection (integrity): agents protect their code and data by carrying their own protection mechanisms. This is made possible by creating a digital envelope using public key cryptography signatures, symmetric keys and code encryption
- Protection of medical information (confidentiality): this is concerned with protecting the information carried by the agents using a scheme based on hash-chains
- Access control: this consists of two modules: authentication and Role Based Access Control (RBAC). The first is achieved using X.509 certificates and Secure Assertion Markup Language (SAML). The second one uses RBAC to manage users' role policies and uses Extensible Access Control Markup Language (XAMCL) to ensure interoperability of the system access control policies

All the five agents (mobile scheduler, collector agent, remote broker, local broker and document broker) present in the system communicate using FIPA standards and interaction protocols. In this security scheme, the researchers rely on the inbuilt security of FIPA to guarantee the confidentiality protection of agent communication since no mention is made concerning their effort to secure agent communication.

ANALYSIS OF RELATED WORK

Studying all security mechanisms on mobile agent communication is too broad an area. In view of this, this study is focusing on the confidentiality protection of agent communication in multi-agent systems. Researchers have proposed many solutions to the confidentiality threat of agent communication using authentication and authorization mechanisms, encryption and digital signature which are discussed.

Memory overhead of the existing security schemes: The discussion here is based on the assessment of the volume of memory required by each agent to store the digital certificate(s) for mobile agents' authentication. It is considered as important because of its direct consequence on the performance of the network. In multi-agent systems, one of the prominent measures to secure agent communication is authentication. That is an agent should be able to verify the legitimacy of the agents it is communicating with and have knowledge of the identities of the agents involved in collaboration. In alternative, the execution environment of the agents could be able to validate the identities of the community of agents running in its environment. This technique has been adopted by researchers as a prerequisite to authorisation. However, the usual technique of validating agents by the previous researchers has been by mutual (or inter-agent) authentication.

Wen and Mizoguchi (2000), Novak *et al.* (2003), Wong and Sycara (2000), Vila *et al.* (2007), Borselius and Mitchell (2003), Wagner (1997), Becerra (2003), Xiao *et al.* (2007), Sulaiman and Sharma (2011), Vieira-Marques *et al.* (2006), Lin and Huang (2010), Usman *et al.* (2012) and Xu *et al.* (2010) have proposed various security schemes for confidentiality protection of agent communication using inter-agent authentication mechanism. This mechanism necessitates each mobile agent possessing the certificates of all other agents in the agent community. The consequence of which is that the memory of the

mobile agents must be large enough to store the certificates and hence rendered them heavy weight with its attendant high memory overhead.

Computation overhead of the existing security schemes: Low computation overhead is considered as an important functionality of a security scheme because high computation overhead can result to latency in the network. In some of the security schemes, cryptographic signatures are used to validate the source of an agent while symmetric and asymmetry cryptosystems are used to secure agent's certificate and in some schemes, agent's data. In the case of asymmetric (public/private key) cryptography, this technique involves encryption of the certificate with the public key of the execution platform before the agent migrates. At the execution platform, certificate is decrypted using the private key of the execution platform. This method of mobile agent validation is a compulsory means of protecting the confidentiality of agent communication. However, the method imposes computation overhead on the network.

The encryption and decryption processes utilise processor time that would have been dedicated to other important processes. If the time for encryption and decryption of mobile agents is excessive, it might lead to high network latency. Many of the existing proposals employed cryptographic encryption and decryption and cryptographic signatures to secure the confidentiality of agent communication which has been recognized by researchers to be central to secure communication amongst the agents within multi-agent system. Notable among them are Wang *et al*. (1999), Wong and Sycara (2000), Wen and Mizoguchi (2000), Novak *et al*. (2003), Vila *et al*. (2007), Borselius and Mitchell (2003), Becerra (2003), Sulaiman and Sharma (2011), Vieira-Marques *et al*. (2006), Lin and Huang (2010) and Usman *et al*. (2012).

The techniques adopted by the researchers for using cryptographic mechanism to protect the confidentiality of agent communication are at variance. For example Wang *et al*. (1999), Wong and Sycara (2000) and Vila *et al*. (2007) use Cryptographic algorithm for the encryption of message alone. This method has the potential to generate high computation overhead if the message for encryption is long. However, for short messages such security technique may not impact negatively on the efficiency of the network. In the case of Sulaiman and Sharma (2011), cryptographic protocols are used to secure both the data and the agent code and to sign the data. In a bid to reduce the computation overhead of security scheme, Sulaiman and Sharma (2011) device a means of ensuring that large part of the agent components are encrypted using secret key with smaller key length while the secret key itself is protected using asymmetric (public/private) cryptography.

Communication overhead of the existing schemes: Low communication overhead is another important functionality of a security scheme in order to overcome excessive utilization of the network bandwidth. Mobile agents communicate with one another through message passing using specific agent communication language and specification such as FIPA ACL and KQML. FIPA's specification for agent communication was considered a defacto standard, however without consideration for security of agent communication (Borselius and Mitchell, 2003). An agent can communicate with another agent while they are in the same execution platform and also while they are in different platforms.

In multi-agent system, it is fundamental for mobile agents to collaborate by message passing to achieve their designed objective. However, this phenomenon could be avoided for the authentication of the mobile agents. Based on the knowledge of the existing proposed schemes, it was observed by Wen and Mizoguchi (2000), Novak *et al*. (2003), Wong and Sycara (2000), Vila *et al*. (2007), Borselius and Mitchell (2003), Wagner (1997), Becerra (2003), Xiao *et al*. (2007), Sulaiman and Sharma (2011), Vieira-Marques *et al*. (2006), Lin and Huang (2010), Usman *et al*. (2012), Xu *et al*. (2010), Hu and Tang (2003), Wang *et al*. (1999) and JADE Board (2005), adopted inter-agent authentication technique which involves passing of certificates of the agents among themselves for verification and authentication. An inter-agent authentication based security scheme would definitely boost the communication overhead of the network.

To substantially reduce the communication overhead due to inter-agent communication as a technique for agent authentication, a centralised agent authentication could be a better option since it does not require mutual passing of certificates among agents. With centralised agent authentication, only an entity (platform) responsible for the agent authentication stores the certificates of all the agents for verification purpose while each agent only stores its own certificate. During authentication, one-way message (certificate) passing is required from each of the agent to the platform.

The tabular analysis of existing agent communication security schemes and their comparison with the proposed scheme for the confidentiality protection of agent communication is shown in Table 1.

Table 1: Analysis of existing agent communication security schemes

	Security mechanism						Network overheads		
Researchers	ME	DS	CA	TM	ACM	AA/AT	MO	COMPO	COMMO
Wen and Mizoguchi (2000)	Y	Y	Y	Y	Authentication	Inter-agent authentication	H	H	H
Novak *et al.* (2003)	Y	Y	Y	N	Authentication	Inter-agent authentication	H	H	H
Hu and Tang (2003)	Y	Y	Y	N	Authentication and RBAC	Inter-agent authentication	H	H	H
Wang *et al.* (1999)	Y	N	N	N	Authentication	Inter-agent authentication	H	L	H
Wong and Sycara (2000)	Y	N	N	Y	Unique agent identity	Inter-agent authentication	H	L	H
Vila *et al.* (2007)	Y	N	Y	N	Authentication	Inter-agent authentication	H	L	H
Borselius and Mitchell (2003)	Y	Y	N	N	Authentication	Inter-agent authentication	H	H	H
Wagner (1997)	N	N	N	N	Authentication based on security classification	Inter-agent authentication	H	L	H
JADE Board (2005)	Y	Y	N	N	JAAS	Inter-agent authentication	H	H	H
Xiao *et al.* (2007)	N	N	N	N	Role-based ACM	Inter-agent authentication	H	L	H
Sulaiman and Sharma (2011)	Y	Y	N	N	Authentication	Inter-agent authentication	H	H	H
Vieira-Marques *et al.* (2006)	Y	Y	N	N	Authentication and RBAC	Inter-agent authentication	H	H	H
Lin and Huang (2010)	Y	Y	N	Y	Authentication	Inter-agent authentication	H	L	H
Usman *et al.* (2012)	Y	Y	N	N	Authentication	Inter-agent authentication	L	L	H
Xu *et al.* (2010)	Y	Y	Y	N	JAAS	Inter-agent authentication	H	L	H

Y = Yes; N = No; H = High; L = Low; TM = Trust Model; ME = Message Encryption; ACM = Access Control Mechanism; DS = Digital Signature; AA/AT = Agent Authentication/Authorisation Technique; CA = Certification Authority; COMPO = Computation Overhead; MO = Memory Overhead; JAAS = Java Authentication and Authorisation Service; COMMO = Communication Overhead; RBAC = Role-Based Access Control

CONCLUSION

Mobile agents must have a secured communication mechanism to receive messages from other agents and also exchange their views on a given task with other agents on an agent platform especially during the process of negotiation or collaboration of mobile agents on a problem-solving mission. In view of this, this study has been able to explore a systematic approach to survey existing literature on agent communication security in multi-agent systems. Attacks on agent communication were identified and discussed and the existing agent communication security schemes were reviewed and analysed being the core of this study. From the analysis in Table 1, researchers can observe that almost all the existing agent communication security schemes impose high memory and communication overheads on the network except Usman *et al.* (2012) whose proposed scheme has low memory overhead as a result of its utilization of stack memory architecture which complies with Last In First Out (LIFO) memory scheme. The high network overheads characterised by the majority of the proposed agent communication security schemes have a consequential effect on the network performance.

In order to effectively harness the benefits offered by the use of multi-agent technology in real applications, it is imperative to ensure that the agent communication security mechanism must also be able to restrain an alien mobile agent from interfering, spy or eavesdropping the agents' communication. Almost all the existing security schemes exploit the capability of message encryption and digital signature while few combined them with trust management to secure agent communication. However, these techniques cannot secure agent communication against man in the middle attack whose mission is to hijack the original message transmitted by the sender by impersonating the receiver and forward its own message as response to the sender without the knowledge of the sender and intended receiver. This therefore, calls for a mechanism that can isolate potentially malicious agent to a host and deprive it permission to establish communication thread to other hosts where legitimate agents are running.

ACKNOWLEDGEMENT

The research is supported by the Universiti Teknologi Malaysia (UTM) and The Federal Polytechnic, Ado-Ekiti under Tertiary Education Trust Fund, Nigeria.

REFERENCES

Ahmed, T.M., 2010. Generate secure mobile agent by using SMS to protect Hosts. Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications, May 16-19, 2010, Hammamet, Tunisia, pp: 1-4.

Becerra, G., 2003. A security pattern for multi-agent systems. Proceedings of Agent Based Technologies and Systems, August 2003, Calgary, Canada, pp: 142-153.

Bijani, S. and D. Robertson, 2012. A review of attacks and security approaches in open multi-agent systems. Artif. Intell. Rev., 10.1007/s10462-012-9343-1.

Borselius, N. and C.J. Mitchell, 2003. Securing FIPA agent communication. Proceedings of the International Conference on Security and Management, June 23-26, 2003, Las Vegas, USA., pp: 135-141.

Burg, B., 2002. Foundation for intelligent physical agents. FIPA, Geneva, Switzerland. http://pegasus.javeriana.edu.co/~mad/Fipa%20Presentacion.pdf.

Cavalcante, R.C., I.I. Bittencourt, A.P. da Silva, M. Silva, E. Costa and R. Santos, 2012. A survey of security in multi-agent systems. Expert Syst. Appl., 39: 4835-4846.

Chopra, A.K., A. Artikis, J. Bentahar, M. Colombetti and F. Dignum *et al.*, 2013. Research directions in agent communication. ACM Trans. Intell. Syst. Technol., Vol. 4. 10.1145/2438653.2438655.

Constantinescu, N. and C.I. Popirlan, 2011. Authentication model based on multi-agent system. Ann. Univ. Craiova-Math. Comput. Sci. Ser., 38: 59-68.

Dadhich, P., K. Dutta and M.C. Govil, 2011. On the approach of combining trust and security for securing mobile agents: Trust enhanced security. Proceedings of the 2nd International Conference on Computer and Communication Technology, September 15-17, 2011, Allahabad, India, pp: 379-384.

Farkas, C. and M.N. Huhns, 2002. Making agents secure on the semantic web. IEEE Internet Comput., 6: 76-79.

Guan, H., H. Zhang, X. Meng and J. Zhang, 2010. A communication security protocol of mobile agent system. Wuhan Univ. Nat. Sci., 15: 117-120.

Hu, Y.J. and C.W. Tang, 2003. Agent-Oriented Public Key Infrastructure for Multi-Agent E-Service. In: Knowledge-Based Intelligent Information and Engineering Systems, Palade, V., R.J. Howlett and L. Jain (Eds.). Springer, Berlin, Heidelberg, ISBN-13: 9783540408031, pp: 1215-1221.

JADE Board, 2004. JADE security guide. http://jade.cselt.it/doc/tutorials/JADE_Security.pdf.

Jung, Y., M. Kim, A. Masoumzadeh and J.B. Joshi, 2012. A survey of security issue in multi-agent systems. Artif. Intell. Rev., 37: 239-260.

Karthik, S., R.M. Bhavatharini and V.P. Arunachalam, 2008. Analyzing interaction between denial of service (DOS) attacks and threats. Proceedings of the International Conference on Computing, Communication and Networking, December 18-20, 2008, Tamil Nadu, India, pp: 1-9.

Li, S. and M.M. Kokar, 2013. Agent Communication Language. In: Flexible Adaptation in Cognitive Radios, Springer, Berlin, Heidelberg, ISBN-13: 9781461409670, pp: 37-44.

Lin, D. and T. Huang, 2010. A mobile-agent security architecture. Proceedings of the 2nd International Conference on e-Business and Information System Security, May 22-23, 2010, Wuhan, China, pp: 1-4.

Loulou, M., M. Jmaiel, A. Hadj Kacem and M. Mosbah, 2006. A conceptual model for secure mobile agent systems. Proceedings of the International Conference on Computational Intelligence and Security, November 3-6, 2006, Guangzhou, China, pp: 524-527.

Lu, F. and M. Huang, 2006. Research and design of security in multi-agent system. Proceedings of the IET International Conference on Wireless Mobile and Multimedia Networks, November 6-9, 2006, Hangzhou, China.

Mishra, S. and P. Xie, 2003. Interagent communication and synchronization support in the DaAgent mobile agent-based computing system. IEEE Trans. Parallel Distrib. Syst., 14: 290-306.

Mishra, S., Y. Huang and H. Kuntur, 1999. DaAgent: A dependable mobile agent system. Proceedings of the 29th IEEE International Symposium on Fault-Tolerant Computing, June 15-18, 2009, Madison, WI., USA.

Novak, P., M Rollo, J. Hodik and T. Vlcek, 2003. Communication Security in Multi-Agent Systems. In: Multi-Agent Systems and Applications III, Springer, Berlin, Heidelberg, pp: 454-463.

Oey, M.A., M Warnier and F.M.T. Brazier, 2010. Security in large-scale open distributed multi-agent systems. Autonomous Agents, 6: 108-130.

Poggi, A., G. Rimassa and M. Tomaiuolo, 2001. Multi-user and security support for multi-agent systems. Proceedings of the joint workshop on Dagli Oggetti Agli Agenti: Tendenze Evolutive Dei Sistemi Software, September 4-5, 2001, Modena, Italy.

Poslad, S. and M. Calisti, 2000. Towards improved trust and security in FIPA agent platforms. Proceedings of the Workshop on Deception, Fraud and Trust in Agent Societies, June 3-7, 2000, Barcelona, Spain, pp: 1-6.

Pozo, S., R.M Gasca and M.T. Gomez-Lopez, 2004. Secure tunnels for mobile multi-agent systems. Proceedings of the Iberoamerican Workshop on Multi-Agent Systems, November 22-26, 2004, Puebla, Mexico.

Singh, P. and S. Malhotra, 2013. Trends in mobile agent communication for mobile networks. Int. J. Adv. Res. Comput. Sci. Software Eng., 3: 1313-1317.

Subalakshmi, R.J., A. Das and N.C.S. Iyengar, 2011. A small e-Health care information system with agent technology. Proceedings of the International Conference on Computational Intelligence and Communication Networks, October 7-9, 2011, Gwalior, India, pp: 68-72.

Sulaiman, R. and D. Sharma, 2011. Enhancing security in e-Health services using agent. Proceedings of the International Conference on Electrical Engineering and Informatics, July 17-19, 2011, Bandung, Indonesia, pp: 1-6.

Sulaiman, R., X. Huang and D. Sharma, 2009. E-health services with secure mobile agent. Proceedings of the 7th Annual Communication Networks and Services Research Conference, May 11-13, 2009, Moncton, NB., Canada, pp: 270-277.

Usman, M., V. Muthukkumarasamy, X.W. Wu and S. Khanum, 2012. Securing mobile agent based wireless sensor network applications on middleware. Proceedings of the International Symposium on Communications and Information Technologies, October 2-5, 2012, Gold Coast, Australia, pp: 707-712.

Vieira-Marques, P.M., S. Robles, J. Cucurull, R.J. Cruz-Correia, G. Navarro and R. Marti, 2006. Secure integration of distributed medical data using mobile agents. IEEE Intell. Syst., 21: 47-54.

Vila, X., A. Schuster and A. Riera, 2007. Security for a multi-agent system based on JADE. Comput. Secur., 26: 391-400.

Wagner, G., 1997. Multi-level Security in Multiagent Systems. In: Cooperative Information Agents, Kandzia, P. and M. Klusch (Eds.). Springer, Berlin, Heidelberg, ISBN-13: 9783540625919, pp: 272-285.

Wang, H., V. Varadharajan and Y. Zhang, 1999. A Secure Communication Scheme for Multiagent Systems. In: Multiagent Platforms, Ishida, T. (Ed.). Springer, Berlin, Heidelberg, ISBN-13: 9783540659679, pp: 174-185.

Wen, W. and F. Mizoguchi, 2000. An authorization-based trust model for multiagent systems. Applied Artif. Intell., 14: 909-925.

Wong, H.C. and K. Sycara, 2000. Adding security and trust to multiagent systems. Applied Artif. Intell., 14: 927-941.

Xiao, L., A. Peet, P. Lewis, S. Dashmapatra and C. Saez *et al*., 2007. An adaptive security model for multi-agent systems and application to a clinical trials environment. Proceedings of the 31st Annual International Computer Software and Applications Conference, Volume 2, July 24-27, 2007, Beijing, China, pp: 261-268.

Xu, X.L., J.Y. Xiong and C.L. Cheng, 2010. The model and the security mechanism of the information retrieval system based on mobile multi-agent. Proceedings of the 12th IEEE International Conference on Communication Technology, November 11-14, 2010, Nanjing, China, pp: 25-28.