A Secure Data Transmission For Multiagent System Using Digital Signature

Prof. Krishnalal G.
Faculty, Dept. of Computer Science
Amal Jyothi College of Engineering

Jisha Babu
PG Scholar, Computer Science
Amal Jyothi College of Engineering

ABSTRACT

Recent multi agent systems are characterized by decentralized control, autonomy and local views. The application of multiagent systems on open environment such as internet creates new challenges especially with respect to security issues such as authentication, authorization and privacy. Two very common attacks that faced by multiagent systems are man-in-the-middle attacks and replay attacks. This paper proposes an authentication approach for the solution of these attacks to some security problems in open multi-agent systems using Digital signature. Every agent in the system needs to create a key-pair. The identity of the agent can now be verified by checking whether the agent can correctly decrypt a message encrypted with public key.

KEY WORDS

Multiagent system, Digital signature, Security.

1. Introduction

In Multi agent system (MAS) agent works with other agents to communicate to accomplish some desired tasks that will provide the independence and automation in the system. Agent's interaction can be used either to provide some common goal or to achieve their own interests. MAS have their application on Peer-to-Peer [1],[2],[3],[4], Grid computing[5], Semantic Web[6], and MANETs[7]. MAS have several important characteristics [8]:

- Agent has incomplete information/capabilities for solving the problem
- No system global control
- Decentralized data
- Asynchronous computation

In open multi-agent systems agents must interact with other agents with which they are not familiar. In such environment, a security, non-repudiation and authentication technique is critically required. The following security properties should be provided [9]:

- Confidentiality: assurance that communicated information is not accessible to unauthorised parties;
- Data integrity: assurance that communicated information cannot be manipulated by unauthorised parties without being detected;

- Authentication of origin: assurance that communication originates from its claimant;
- Availability: assurance that communication reaches its intended recipient in a timely fashion;
- Non-repudiation: assurance that the originating entity can be held responsible for its communications.

An important security problems are issues relating to the identification and authentication of the sending and receiving parties. Authentication can be provided by using Digital Signature. A digital signature works by creating a message digest which ranges from between a 128-bit and a 256-bit number which is generated by running the entire message through a hash algorithm. This generated number is then encrypted with the sender's private key and added to the end of the message. The digital signature can, also, be used for verifying the integrity of a document. One of the most important digital signature scheme is Digital Signature Algorithm (DSA). In this paper, we propose a secure data transmission of multiagents using digital signature algorithm. Here we verifies message digest using MD5 (Message digest 5) algorithm.

2. Attacks on Agents Affecting Communication

There are many attacks that affect agent's communication [9],[10],[11]. In this section, the three main attacks on agent in communication between agents are described below.

1) Man in the middle attack: Man in the middle attack occurs when the malicious agent intercepts messages sent from service provider to intended recipient agent. The attacker (malicious agent) then changes message and send it to the original recipient agent. The recipient agent receives the message, sees that it came from service provider and acts on it. When the recipient agent sends a message back to service provider agent, the attacker intercepts it, alters it, and returns it to service provider agent. Service provider agent and recipient agent never know that they have been attacked.

2) *Denial of Services:* The attack which resists its users from availing any services is called Denial of Service. The agent denies its user from giving services when it is under attack. Centralized systems are more vulnerable towards denial of service attack as the attacker can overload the system by sending fake data (or updates) and request which in turn over burdens the system. This results in denial of service.

3) Reply attacks:

In a replay attack gained knowledge of data content is used to modify data content that has been transported before to acquire unauthorized information. Such a "spoofing and masquerading attack" threatens the integrity of the platform. In this paper we present a secure message transfer of agents communication using MD5 using Digital Signature.

3. Secure Agent Communication

In multi agents systems, efficiently sending messages to an agent is not simple because they move continuously from one agent platform to another.

The unauthorized manipulation of data can happen either in storage or during transmission [12]. We require each agent to have a public and private key pair. We use public key cryptography to make agents uniquely identifiable. Agents are given a public key certificate and a private key. An agent proves its identity by signing with its private key. Such a signature is valid only if the correspondent public key is certified. For communication, an agent A sign the message with its private key $P_r(A)$ along with its public key $P_u(A)$. The message that sent from the source is signed using source's private key guarantees the integrity of the message and the authenticity of the message origin. Even though agents may tamper with the data that are stored in its local database and provide false or random data when processing a search request later, other agents are able to detect whether the data is corrupted by verifying the signature and discard the data if it is corrupted. When an agent *M* wishes to communicate with agent *N*, it issues a request for agent *N*'s, including in the request its public key $P_u(M)$. A hash function is applied to the request to make a message digest. MD5 is used to obtain this message digest. Both the request and digest is sent to the receiver. At receiving side, agent *N* verifies the request. Then the receiver i.e. agent *N*, encrypts its response with M's public key $P_u(M)$, signs it with its own private key, and sends the signed encrypted response, together with its public key, to the polling agent. Upon receiving the response, agent *(M)* verifies the signature using the received public key and decrypts the message using its own private key $P_r(M)$. Figure 1 and Figure 2 illustrates the above mentioned communication. Agent *M* verifies the signature of each piece of feedback by the public key of the feedback source. The fact that the data are encrypted with the public key of the polling agent *M* protects their confidentiality.

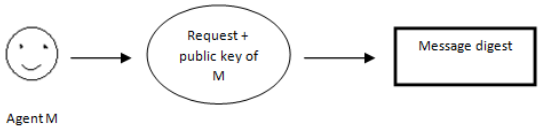

Figure 1. Agent M creates request message using digital signature

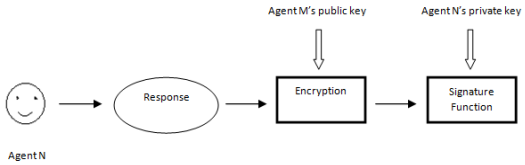

Figure 2. Agent N sent response to agent M

The fact that data are signed with the responding agent's private key allows the detection of integrity violations of the data and the authenticity of their origin.

4. Conclusion

We have presented a secure transmission for multiagents system using digital signature along with MD5. So it provides both security and confidentiality. This type of security is useful in open environment in which agents interact with other agents that are not familiar. We have mentioned some common attacks during communication. Our proposed model addresses these security issues associated with these open environments.

5. References

[1] R. Steinmetz and K. Wehrle, Peer-to-Peer Systems and Applications. Springer-Verlag, 2005
[2] Gnutella, http://www.gnutella.com, 2000.
[3] Kazaa, http://www.kazaa.com, 2011.
[4] edonkey2000, http://www.emule-project.net, 2000.
[5] I. Foster, C. Kesselman, and S. Tuecke, "The Anatomy of the Grid:Enabling Scalable Virtual Organizations," Int'l J. High Performance Computing Applications, vol. 15, no. 3, pp. 200-222, 2001.
[6] T. Berners-Lee, J. Hendler, and O. Lassila, "The Semantic Web,"Scientific Am., pp. 35-43, May 2001.
[7] Joseph P. Macker, William Chao, Ranjeev Mittu,Myriam Abramson, "Multi-Agent Systems in Mobile Ad hoc Networks" Military Communications Conference, 2005. MILCOM 2005.
[8] Niklas Borselius " Mobile agent security" Electronics & Communication Engineering Journal, IEEE 2002
[9] S. Pozo, R. M. Gasca, M. T. Gómez-López "Secure Tunnels for Mobile Multi-Agent Systems" Iberoamerican Workshop on Multi-Agent Systems (IBERAGENTS). Puebla, Mexico, 2004
[10] Nicolae Constantinescu, Claudiu Ionut Popirlan, "Authentication model based on Multi-Agent System", An. Univ. Craiova, Ser. Mat. Inf. 38, No. 2, 59-68
[11] M.A. Oey, M. Warnier , F.M.T. Brazier "Security in Large-Scale Open Distributed Multi-Agent Systems" pages 107-130, chapter 6, IN-TECH, ISBN 978-953-307-089-6, 2010
[12] L. Xiong and L. Li, "Peertrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities," IEEE Trans. Knowledge and Data Eng., vol. 16, no. 7, pp. 843-857, July 2004.