Coalition Signature Scheme in Multi-agent Systems

Yiming Ye
IBM TJ Watson Research Center
PO Box 704, Yorktown Heights, NY 10598, USA
+1 (914) 784-7460
yiming@watson.ibm.com

Xun Yi
School of Electrical and Electronic Engineering
Nanyang Technological University, Singapore 639798
+65 790-4390
exyi@ntu.edu.sg

ABSTRACT

The Internet will never reach its full potential as an electronic marketplace unless e-commerce agents, or proactive Web Programs, are used to automatically or semi-automatically perform e-commerce tasks. The dynamic and heterogeneous interactions among them and the automations brought by them will create tremendous opportunities as well as introduce the risk and vulnerability for e-commerce. In this paper, we study the security issues with respect to an important multi-agent interaction – the multi-agent coalition formation where e-commerce agents dynamically forming coalitions to exploit the benefits of grouping. We propose a coalition signature mechanism to provide a means for a coalition to bind its identity to a peace of information during its interactions within an e-commerce marketplace. The coalition signature environment includes a certificate authority, coalition representatives, and coalitions of a coalition structure. We detail the processes for certificate issuing, coalition certifying, coalition signing, coalition signature verifying, and coalition revocation. Our performance analysis results show that the proposed coalition signature scheme can be implemented efficiently.

Keywords

E-commerce agent, coalition security, coalition signature

1. INTRODUCTION

The pervasive connectivity of the Internet and the powerful architecture of World Wide Web are changing many market conventions and are creating tremendous opportunity for conducting business on Internet. Electronic commerce activities, such as on-line exchange of information services and products etc are bringing business to a whole new level of productivity and profitability. In parallel with the emergence of electronic commerce, there have been interesting developments in the area of intelligent software agents, or software entities that are capable of independent actions in open, unpredictable environments. The Internet will never reach its full potential as an electronic marketplace unless e-commerce agents, or proactive Web Programs, are used to automatically or semi-automatically perform e-commerce tasks such as negotiation, bidding, auction, transaction, and matchmaking etc. As e-commerce agent technology becomes more mature and standardized, we may envision that tens of thousands of e-commerce agents will be seamlessly embedded in everywhere of the Web. The dynamic and heterogeneous interactions among them and the automations brought by them will dramatically reduce certain types of frictional costs and time incurred in the exchange of commodities. However, before we fully enjoy the benefits brought by e-commerce agents, we must realize that the risk and vulnerability is also imminent: the ubiquitous existence of various software agents designed by all kinds of people can work, interact, and also *attack* at any time from anywhere of the "wild web", where the "distance" among them has collapsed to near zero and the transactions can be done instantly. The electronic linking, either wired or wireless, among various agents has made security an issue that must be woven into any agent-based service environment, especially when digital agents migrating through wireless or wired linkage from one network computer or device to another and sensing, executing, transacting, and interacting along the way. The security issues, we believe, that related to agents include but not limited to the following: keeping data or preference of an agent secrete from other agents except those who are authorized to access; ensuring data that belong to an agent not been altered by unauthorized

agents; identifying and authenticating agents during agent interaction; verifying the source of data received by an agent; binding information to an agent; authorization during agents interaction; validation during agent interaction; access control in agent community; agent certification; acknowledging the receiving of data or services by agents; avoiding Internet worms floods; the reputation and trust in mobile agent environment; and agent security against malicious hosts in the network, etc.

Most of the existing researches in e-commerce agent security address the security issues with respect to a single agent in mobile computing environments. Different from the traditional client/server model, the mobile agent model allows both non-executable messages and executable codes traverse the network. Thus, issues like trust for mobile agent, agent data integrity against malicious hosts and security key management must be addressed. Robles et. al. [13] propose a trust model for multi-agent marketplaces based on concentric spheres structure - physical security in the core, a security infrastructure in the middle spheres, and complex aspects of trust, such as reputation, fairness, and reliability, in the outer spheres. Tahara et. al [19] propose a tool for agent data security. A visual tool is used to specify the behaviors of an agent. A mobile program encodes these formal specifications with formal logic. During an application, the activities of the agent can thus be verified by proving the corresponding logic notation encoded in the mobile program. Chan et. al [1] introduce a public key infrastructure to protect a mobile agent during a comparison shopping process against malicious hosts that try to manipulate and execute the agent's data. The strategy requires that each host and agent in the system to possess a pair of keys for encryption and decryption. Each agent or host can encrypt or digitally sign the data items carried by the agent, thus providing security. Loureiro et.al [9] propose a protocol for secure data collection based on an original secure cryptographic technique. Their approach can maintain the integrity of the sequence of data segments such that data collected will not be modified or tempered by parties other than the real host. Yi et. al [21] propose a secure electronic transaction protocol in which a trusted agent service center is incorporated into the payment system. This payment agent is used to perform secure transactions based on customers' requests. Romao et. al [14] propose a proxy certificate mechanism in which the owner of an agent can delegate some power to the agent. Their goal is to prevent the exposure of private keys when a mobile agent has to sign documents during Internet transaction.

It is important to study the security issues for a single agent. However, it is even more important to study the security issues with respect to a group of interacting e-commerce agents. Because it is the sheer interconnectedness and dynamic interactions among these agents that will make the future web a virtual dynamic marketplace, and at the same time, make the security issues one of the top issues to be addressed. In this paper, we study the security issues with respect to a very important multi-agent activity: the dynamic multi-agent coalition.

The remainder of this paper is organized as follows. The next section details the issue of coalition security. Section 3 proposes the coalition signature scheme for e-commerce multi-agent systems. Section 4 briefly concludes the paper.

2. COALITION SECURITY

Cooperation and sharing resource by creating coalitions of agents are an important way for autonomous agents to execute tasks and to maximize payoff. For example, e-commerce agents that represent self-interested real world parties such as buyers or sellers may explore the benefits of grouping by forming coalitions. Coalition formation has been addressed by researchers from both the game theory community and the multi-agent community. Game theory emphasizes the issues of N-person games formation under different settings and the distribution of the benefits among players, without providing algorithms that agents can use to form coalitions [20][7][10]. It concentrates on the stability and fairness issues for given coalitions. Multi-agent research emphasizes the special properties of a multi-agent environment and considers the effects of communication costs and limited computation time on the coalition formation process [5][15][16][17][18].

Here we study a very important issue that has not been addressed before – the issue of coalition security. The advancement of technologies such as EDI, KQML, FIPA, bluetooth, Semantic Web, Peer-to-Peer, SOAP, Concordia, Voyager, Odyssey, Telescript, Java, and Servelet etc. will soon made the dynamic and heterogeneous interactions between tens of thousands of e-commerce agents a reality [8][15]. Under this environment, it will be a desired behavior for different agents to form coalitions for their own benefits. When coalitions are formed, securities will be an issue for agents belonging to different coalitions. Thus, how to define signatures for different coalitions will be an issue that must be addressed.

In order to make our discussions easier, we define some concepts here. Suppose that there are totally n agents: $A = \{a_1, \Lambda\ , a_n\}$. Here A is the set of the agents. The index for agent a_i is i. A coalition $C = \{a_{i_1}, \Lambda\ , a_{i_m}\}$ is a subset of A such that $\forall i_j, a_{i_j} \in A$, or in other words, $C \subseteq A$. If agent a is alone, we assume that it forms a unit coalition $\{a\}$. A coalition

structure CS at time t is the set of all the coalitions formed by agents in A, $CS(t) = \{C_1, ..., C_a\}$. Where a is the number of coalitions at time t, $a = |CS(t)|$. C_i $(1 \le i \le a)$ is a coalition formed by agents of A, $C_i \subseteq A$. The coalitions discussed in our paper are dynamic. An agent might leave its current coalition and either becomes a unit coalition or join another coalition, or an agent that belongs to a unit coalition might join another coalition.

There are three basic kinds of coalition structures. The first kind is non-overlapping coalition structure, in the sense that there is no agent that belongs to two different coalitions. This is the coalition structure in the traditional sense - partitioning the set of agents into exhaustive and disjoint coalitions. For example, suppose that $A = \{a_1, a_2, a_3\}$ is the set of agents, then $\{\{a_1\}, \{a_2, a_3\}\}$ is a non-overlapping coalition structure. A lot of research in coalition formations is related to non-overlapping coalition structure. The second kind is overlapping coalition structure, in the sense that an agent can appear in different coalitions, but no coalitions can contain another coalition. For example, $\{\{a_1, a_2\}, \{a_1, a_3\}\}$ is an overlapping coalition structure. The third kind is nested coalition structure, in the sense that partitioned coalitions can contain each other. For example, $\{\{a_1\}, \{a_1, a_2\}, \{a_3\}\}$ is a nested coalition structure. Sometimes, a coalition structure might be a combination of the above-mentioned kinds of coalition structures.

Here we present a coalition signature mechanism that can be used by any kinds of dynamically changing coalition structure $CS(t)$. A coalition signature mechanism, we believe, is fundamental in authentication, authorization, and non-repudiation for coalitions in an e-commerce multi-agent system. The purpose is to provide a means to bind identity of a multi-agent coalition to an agreement reached by the multi-agent coalition. The signature scheme for a given coalition C is based on identities of all members of C. A coalition signature $Sig_C(M)$ on message *M* is just some bits that reflect the structure of the coalition. Only a coalition itself can generate its own coalition signatures on messages. Other coalitions or parties cannot forge any coalition signature of the given coalition. The authenticity of a coalition signature can be verified by any parties. The following section presents details of our approach. The following section presents details of our approach.

3. COALITION SIGNATURE SCHEME

The coalition signature scheme is established on public key infrastructure, in which each agent has a pair of public and secret keys. The secret key of an agent is used to generate signatures on messages, while its public key is used for other agents or parties to verify its signatures. The secret key of an agent is generated by a trusted third party, the certificate authority (CA), in the beginning phase. The public key of an agent can be computed with the identity of the agent, *CA* is only activated whenever a new coalition is formed or an old coalition is dissolved. Suppose that $A = \{a_1, \Lambda\ , a_n\}$ gives the set of agents in the multi-agent system. The identity for agent a_i is ID_i. Thus the set of identities for agents in the multi-agent system are $\Omega = \{ID_1, \Lambda\ , ID_n\}$. Usually the identity for an agent can be the name of the agent or simply the index of the agent in the given multi-agent system. In Sections 3.1 - 3.4, we illustrate the process of generating and certifying signatures of a given coalition $C = \{a_{i_1}, \Lambda\ , a_{i_k}\}$. The identity information for agent a_{i_j} in C is ID_{i_j}, where $(1 \le j \le k)$. We represent the identity set of C as $\Omega_C = \{ID_{i_1}, \Lambda\ , ID_{i_k}\}$.

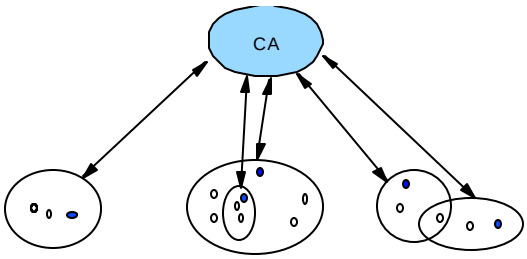

Fig. 1. *Parties involved in the coalition signature mechanism. CA is the certificate authority that has secure channel with all the agents of the multi-agent system. Agents that belong to one coalition are enclosed by a big circle. Each coalition has a representative (represented as solid circle in the figure) that helps to form the coalition signature with respect to a given message.*

The following figure gives a high level illustration of signing and verifying processes.

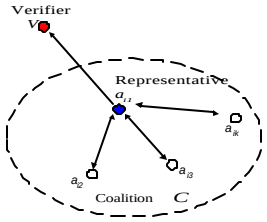

Fig. 2. *The signing process and the verifying process of the coalition signature scheme*

3.1 Certificate Issuing

In this section, we explain the procedure for CA to issue the secret certificate to individual agent.

Based on RSA [12], CA randomly chooses two distinct big primes *p* and *q* and computes *n*= *p´ q* and $\Phi(n) = (p-1)(q-1)$. Then *CA* randomly chooses its public key *e* such that $\gcd(e, \Phi(n)) = 1$ and $1 < e < \Phi(n)$ and computes its secret key *d* such that $e \times d = 1 (\mathrm{mod}\ \Phi(n))$. Finally, *CA* distributes (*e*, *n*) to all participants, but keep (*d*, *p*, *q*) secret.

The following is the process for *CA* to issue a secret certificate to an individual agent a_{i_j} in S:

Step 1: Obtain the hashed value h_{i_j} of the identity ID_{i_j} of agent a_{i_j}, $h_{i_j} = \mathrm{H}(ID_{i_j})$. Here H is a one-way hash function that hashes an arbitrary length message into 160-bit message. There exists many ways to construct the hash function H. Here we use Secure Hash Standard (SHS) [4].

Step 2: Obtain the signature s_{i_j} for agent a_{i_j} by transforming the hashed value h_{i_j} to:

$$s_{i_j} = h_{i_j}^{d} \ (\mathrm{mod}\ n) \tag{1}$$

Step 3. Issue the secret certificate (ID_{i_j}, s_{i_j}) to a_{i_j} through a secure channel. Here ID_{i_j} is the identity of a_{i_j}, and s_{i_j} is the secret key of a_{i_j} which is known only to the agent a_{i_j} besides *CA*.

3.2 Coalition Certifying

We explain the procedure for CA to certify an agent coalition when the coalition is formed as follows.

Suppose that at time T_C, a coalition $C = \{a_{i_1}, \Lambda\ , a_{i_k}\}$ is formed. The representative of C is a_{i_1} and the identity set of C is $\Omega_C = \{ID_{i_1}, \Lambda\ , ID_{i_k}\}$. CA certifies the coalition C by signing a message $I_C = \{\Omega_C = \{ID_{i_1}, \Lambda\ , ID_{i_k}\}, T_C, L_C\}$, where L_C is the lifetime of the coalition. The terms T_C and L_C together specify the group formation dynamics of the multi-agent system – when and how long a group exists.

The signature S_C of CA on the message I_C is given by

$$S_C = H(I_C)^{d} \ (\mathrm{mod}\ n) \tag{2}$$

where $H(I_C)$ stands for the hash value of I_C with *SHS*. I_C and S_C are passed to the coalition representative a_{i_1} over a public channel.

The signature S_C of CA on the message I_C can be verified with the public key e of CA by checking whether

$$S_C^e = H(I_C) \pmod n \tag{3}$$

holds or not. If so, the coalition certified by *CA* is authentic. Otherwise, it is a forged coalition.

The coalition certifying process is shown in figure 1.

3.3 Coalition Signing

Here we illustrate the procedure for the k agents in C to cooperatively sign a message M. We assume here that all the agents in C have already obtained their secret keys as described in Section 3.1.

Step 1: Each agent a_{i_j} first randomly chooses a value r_{i_j} $(0 < r_{i_j} < n)$, and then computes

$$T_{i_j} = r_{i_j}^e \pmod n \tag{4}$$

Step 2: Each agent a_{i_j} submits T_{i_j} to the representative a_{i_1} of coalition C.

Step 3: a_{i_1} computes $T = T_{i_1} \times \Lambda \times T_{i_{k-1}} \times T_{i_k} \pmod n$ on behalf of the coalition and then broadcasts T to members of the coalition.

Step 4: After receiving T, each agent a_{i_j} first computes $m = \mathrm{H}(M, T, S_C)$ and then computes

$$D_{i_j} = r_{i_j} s_{i_j}^m \pmod n \tag{5}$$

and submits D_{i_j} to a_{i_1}.

Step 3: a_{i_1} computes $D = D_{i_1} \cdot D_{i_2} \cdot \Lambda \cdot D_{i_k} \pmod n$ on behalf of the coalition C and constructs the coalition's signature $Sig_C(M)$ on M. $Sig_C(M)$ consists m, D, S_C and I_C. Or, in other words, $Sig_C(M) = \{m, S_C, D, I_C\}$.

3.4 Coalition Signature Verifying

Here we illustrate the coalition signature verification process. The coalition signature $Sig_C(M) = \{m, S_C, D, I_C\}$ on a message M can be verified by any verifier V in the following way:

Step 1: V Checks the authenticity of the coalition according to equation $S_C^e = H(I_C) \pmod n$, here e is the public key of CA.

Step 2: V Computes $h_{i_j} = \mathrm{H}(ID_{i_j})$ for all the agents a_{i_j} $(1 \le j \le k)$ that belong to S. Then computes the value of h, $h = h_{i_1} \Lambda\ h_{i_{k-1}} h_{i_k} \pmod n$.

Step 3: V Computes

$$T^* = D \cdot h^m \pmod n \tag{6}$$

Step 4: *V* computes $m^* = \mathrm{H}(M, T^*, S_C)$.

Step 5: If the above calculated value m^* equals to the value of m in the coalition signature, then the coalition signature is valid.

The processes of signature signing and verifying are shown in figure 2.

4. CONCLUSION

The pervasive connectivity of the Internet and the powerful architecture of World Wide Web will create a virtual marketplace where tens and thousands of agents can work, interact, and also attack from anywhere and at any time. The electronic linking, either wired or wireless, among various agents has made security an issue that must be woven into any agent-based service environment. In this paper, we propose a coalition signature scheme within a multi-agent environment. We show that the proposed theory is secure against forgery and that the coalition signature mechanism can be implemented efficiently. We believe that there are a lot of security issues when multiple agents interact with each other and we plan to explore more in the future.

5. REFERENCES

[1] A. Chan, T. Wong, C. Wong, M. Lyu,, SIAS: A Secure Shopping Information Agent System, The 4th Internatinal Conference on Autonomous Agents, Barcelona, Spain, une 3-7, 2000, Page 257-258

[2] D. M. Gardon, "A Survey of Fast Exponentiation Method", Journal of Algorithms, 27, 1998, pp. 129-146.

[3] L. C. Guillou and J. J. Quisqater, "A 'Paradoxical' Identity-Based Signature Scheme Resulting from Zero-Knowledge", Advances in Cryptology – CRYPTO'88, Proceedings, Springer-Verlag, 1990, pp. 216-231.

[4] http://www.itl.nist.gov/fipspubs/fip180-1.htm

[5] M. Klusch and O. Shehory Coalition formation among rational information agents, Lecture Notes in Artificial Intelligence no. 1038, Agents Breaking Away, W. Van de Velde and J. W. Perram (Eds.), pages 204-217, 1996.

[6] D. E. Knuth, "The Art of Computer Programming", Volume 2, Seminumerical Algorithms, Third Edition, 1998, Addison Wesley Longman.

[7] S. Kraus and J. Wilkenfeld. Negotiation over time in a multi-agent rnvironment: Preliminary report. In Proc. IJCAI-91, pages 56-61, Australia, 1991

[8] K. Lerman and O. Shehory, Coalition Formation for Large-Scale Electronic Markets, International Conference on Multi-agent Systems, Boston, 2000

[9] S. Loureiro, R. Molva, and A. Pannetrat, Secure Data Collection with Updates, , Electronic Commerce Research, Volume 1, Number 1-2, 2001, p119-131

[10] R. D. Luce and H. Raiffa. Games and Decisions. John Wiley and Sons, Inc. 1957

[11] J. Riordan and B. Schneier, Environmental Key Generation Towards Clueless Agents, Mobile Agents and Security, Lecture Notes in Computer Science, 1419, pp17-25.

[12] R. L. Rivest, A. Shamir, L. M. Adleman: A method for obtaining digital signatures and public key cryptosystems, Communications of ACM, 21(2)(1978) 120-126.

[13] S. Robles, J. Borrell, J. Bigham, L. Tokarchuk, L. Cuthbert, Design of a Trust Model for a Secure Multi-Agent Marketplace, The 5th Internatinal Conference on Autonomous Agents, Montreal, Canada, May 28 – June 01, 2001. Page 77-78

[14] A. Romao and M. Silva, Secure Mobile Agent Digital Signatures with Proxy Certificates, E-Commerce Agents – Marketplace Solutions, Security Issues, and Supply and Demand. LNCS-2033, 2001, page 206-220.

[15] T. Sandholm, Negotiation among self-interested computationally limited agents, Ph.D. Thesis, University of Massachusetts, Amherst, MA, 1996, USA

[16] T. Sandholm, K. Larson, M. Andersson, O. Shehory, F. Tohme, Coalition structure generation with worst case guarantees, Artificial Intelligence 111 (1999) 209-238.

[17] O. Shehory and S. Kraus Feasible Formation of Coalitions Among Autonomous Agents in Non-Super-Additive Environments, Computational Intelligence, Vol. 15(3), August 1999, pages 218-251

[18] O. Shehory, S. Kraus and O. Yadgar Emergent Cooperative Goal-Satisfaction in Large Scale Automated-Agent Systems, Artificial Intelligence Journal, Vol. 110(1), May 1999.

[19] Y. Tahara, A. Ohsuga, S. Honiden. Mobile Agent Security with the IPEditor Development Tool and the Mobile UNITY Language, The 5th Internatinal Conference on Autonomous Agents, Montreal, Canada, May 28 – June 01, 2001. Page 656-662.

[20] J. Von Neumann and O. Morgenstern. Theory of games and Economic Behavior. Princeton University Press, Princeton, NJ, 1947.

[21] X. Yi, C. Siew, Y. Miao, Agent-Mediated Secure Electronic Transaction for Online Interdependent Purcheses, E-Commerce Agents – Marketplace Solutions, Security Issues, and Supply and Demand. LNCS-2033, Springer Verlag, 2001, page 221-146.