# Efficient Trust Negotiation based on Trust Evaluations and Adaptive Policies

Bailing Liu
Department of Information and Management, Huazhong Normal University, Wuhan, China
bailing.cs@gmail.com

***Abstract*— Automated trust negotiation (ATN) is an approach that establishes mutual trust between strangers wishing to share resources or conduct business by gradually requesting and disclosing digitally signed credentials. Previous work on improving negotiation efficiency mainly focuses on using history negotiation information, which may lead to unnecessary information leakage and cannot improve the negotiation efficiency when both negotiators do not have appropriate history information. Thus in this paper, we enhance the negotiation efficiency from a new aspect, that is, adjust policies based on trust evaluations. An ATN framework is designed to enhance the negotiation efficiency. This framework can simplify the negotiation process, reduce the number of exchanged credentials and credential validations whenever possible. Furthermore, it avoids revealing unnecessary information during negotiations. This framework presents a number of innovative features, such as the support of virtual organizations and trust evaluations, and the use of fine-grained adaptive policies to adjust policies based on the trustworthiness levels. Finally, we report experimental results based on our implementation of this framework, which show that our framework can greatly enhance the negotiation efficiency whenever possible.**

***Index Term*—automated trust negotiation, access control policy, trustworthiness level, trust evaluation, efficiency**

## I. INTRODUCTION

Automated trust negotiation (ATN) is an approach establishing mutual trust between strangers wishing to share resources or conduct business by gradually requesting and disclosing digitally signed credentials. Usually, the digital credentials themselves contain sensitive information that a subject does not want to reveal to any strangers, so for each credential there is an access control policy (a policy for short) associated with it, governing the credential disclosure. Generally, a negotiation process should be organized as the following two phases, the disclosure sequence generation phase and the credential exchange phase.

The first phase can be carried out by negotiation strategies, such as eager strategy [1], parsimonious strategy [1], Prudent Negotiation Strategy (PRUNES) [2], Deterministic Finite Automaton Negotiation Strategy (DFANS) [3] and so on. For the second phase, the credentials contained in a disclosure sequence determined in the first phase should be exchanged and validated. Negotiation strategies and credential validations are both computationally expensive during negotiations. Therefore, Bertino et al. [4, 5] exploited a trust negotiation framework trust-x to enhance the negotiation efficiency by taking advantages of negotiation history information. Trust-x adopts schemes such as trust tickets and sequence predictions, which improve the negotiation efficiency even if they do not maximize the protection of the involved resources. The trust tickets support fast interactions for the negotiators who have previously completed a similar trust negotiation. The sequence prediction is used when the negotiation that is being carried on shows similarities with previously executed negotiations. Similarity is estimated based on the information collected during previous negotiations. Furthermore, we develop a trust negotiation framework [6] to improve negotiation efficiency through the use of declaration tickets and proving tickets to reduce the number of exchanged credentials and credential validations, which is also based on the negotiation history information. Previous work on negotiation efficiency enhancement mainly uses the history negotiation information, which may leak much unnecessary information and cannot improve the negotiation efficiency if both negotiators do not have appropriate history information. Thus in this paper, we propose an ATN framework that focuses on a new aspect namely adjust policies based on trust evaluations to enhance negotiation efficiency, which not only simplifies the negotiation process, reduce the number of exchanged credentials and credential validations whenever possible, but also avoid revealing unnecessary information during negotiations. This framework presents a number of innovative features, such as the support for evaluating trust by overlapping virtual organizations, and the use of fine-grained adaptive policies to adjust policies based on the trustworthiness levels. Experimental results based on our implementation of this framework are given, which show that, compared with the traditional ATN framework, our framework can greatly enhance negotiation efficiency whenever possible.

The remainder of this paper is organized as follows. Section 2 gives an overview of ATN. Section 3 proposes an ATN framework and describes its main components. Section 4 gives an example to show how the framework works, and section 5 shows our experimental results based on the implementation of the framework. We conclude the paper in section 6.


doi:10.4304/jcp.6.2.240-245

## II. OVERVIEW OF ATN

Winsborough [1] defined model of ATN as a credential disclosure sequence. Suppose *ClientCreds* is a set of client's credentials, and *ServerCreds* is a set of server's credentials. The credential disclosure sequence is defined as follow:

$\{C_i\}_{i \in [0,2n+1]} = C_0, C_1, \ldots, C_{2n+1}$, where $n \in N$, $C_{2i} \subseteq$ *ClientCreds*, $C_{2i+1} \subseteq$ *ServerCreds*.

As an example, Fig. 1 illustrates a simple trust negotiation occurring between two entities Bob and Alice. Upon requesting access to Bob's server, Bob sends the policy guarding this service to Alice, which states that she must disclose a visa card credential so that she can be billed for her service usage. Alice has this credential, but cannot be disclosed unless Bob is a member of the Better Business Bureau (BBB), so she asks Bob to reveal his BBB credential. Bob then discloses his BBB credential, which satisfies Alice's policy for her Visa card. After Alice's disclosure of her visa card, the service originally requested by Alice is granted.

## III. PROPOSED ATN FRAMEWORK

In this section, we propose an ATN framework that enhances negotiation efficiency by adjusting policies based on the evaluated trustworthiness levels. This framework not only can simplify the negotiation process, reduce the number of exchanged credentials and credential validations whenever possible, but also can avoid leaking unnecessary information during negotiations. This framework is symmetric and peer to peer, which is shown in Fig. 2. The main components of this framework are to be introduced one by one as follows.

### A. Virtual Organizations

A peer that can be trusted by all other peers would contradict the principles of a peer to peer system. However, a peer should reasonably be trusted by a limited number of peers, such as the peers in a federation, peers in reputation-based systems that rely on peers' knowledge of a limited set of other peers and so on. Thus, in this paper, suppose a peer $P_1$ trusts peers $P_2$ and $P_3$, probably because $P_1$ has successfully negotiated with these two peers, then these three peers $P_1$, $P_2$ and $P_3$ form a virtual organization (*VO* for short).

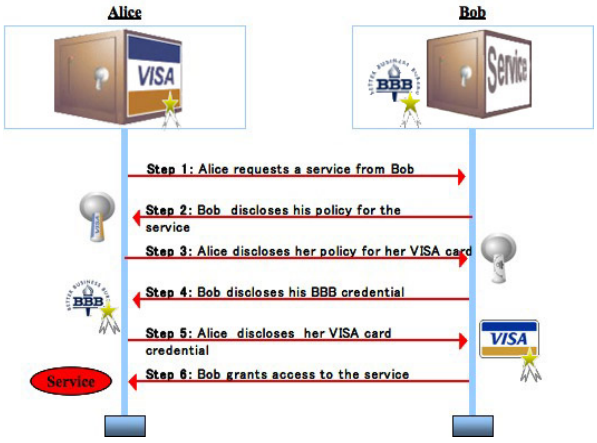



Figure 1. A simple trust negotiation scenario between Bob and Alice. (Taken from http://dais.cs.uiuc.edu/dais/security/trustb.php.)

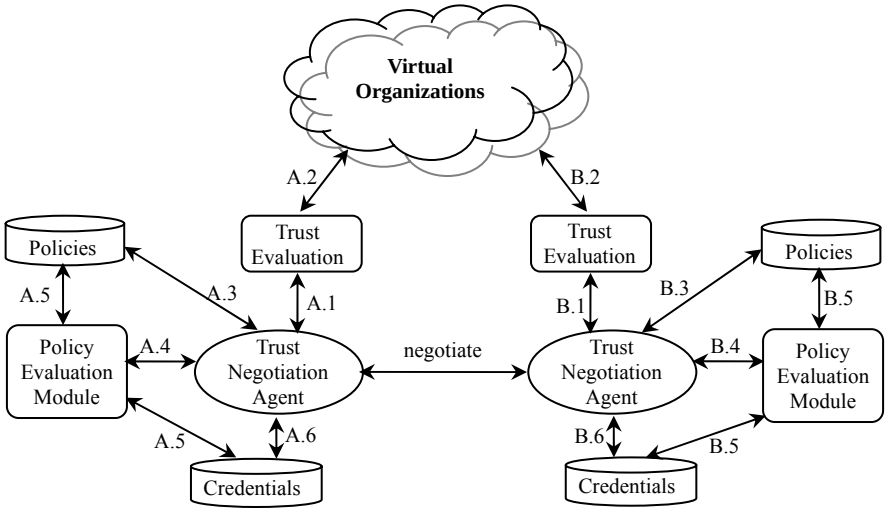



Figure 2. Proposed ATN framework

### B. Trust Evaluation Module

Trust evaluation module is responsible to evaluate trustworthiness levels of opponents by communicating with *VO*s (A.2 and B.2 in Fig. 2).

References [7] and [8] inspire us with that the evaluation of the trustworthiness levels can be achieved by overlapping *VO*s. Consider two peers $P_1$ and $P_3$. Suppose the virtual organization of $P_1$ has the following peers $P_2$, $P_4$ and $P_5$, which is represented by $VO(P_1) = \{P_1, P_2, P_4, P_5\}$, and for $P_3$, its virtual organization is represented as $VO(P_3) = \{P_2, P_3, P_6\}$. $VO(P_1) \cap VO(P_3) = \{P_2\}$, which is shown in Fig. 3. Similarly, more *VO*s can be overlapped, and the example is given in the next section.

The trustworthiness is determined by the number of

overlapping *VO*s, which has the following three levels:

- *Trust*: If two peers are in the same *VO*, then their trustworthiness levels are *trust* to each other.
- *Partial trust*: Suppose two peers $P_1$ and $P_2$ do not belong to a same *VO*. From $P_1$ to $P_2$ there is $VO(P_1) \cap \cdots \cap VO(P_2) \neq \phi$, in which the number of overlapping *VO*s is $n$ ($n$ is an integer greater than one). If $n$ is less than a threshold which is set by $P_1$, then to $P_1$, $P_2$'s trustworthiness level is *partial trust*.
- *Non-trust*: Suppose two peers $P_1$ and $P_2$ do not belong to a same *VO*. If within the threshold of the number of overlapping *VO*s, which is set by $P_1$, from $P_1$ to $P_2$, $VO(P_1) \cap \cdots \cap VO(P_2) \neq \phi$ does not hold, then to $P_1$, $P_2$ is *non-trust*.

For *partial trust*, since the trust transitivity, from one peer to another, the more overlapping *VO*s are, the lower trust level will be. Therefore, the threshold of overlapping *VO*s should not be too large, which is set according to the peer's preference. Note that, for a peer, its threshold of overlapping *VO*s for *partial-trust* is equal to the threshold of overlapping *VO*s for *non-trust*. Suppose a peer $P_1$'s threshold for *partial-trust* is set as $n$, from $P_1$ to another peer $P_2$, let $m$ be the number of overlapping *VO*s, if $1 < m \leq n$, then to $P_1$, $P_2$ is *partial-trust*; if $m > n$, then to $P_1$, $P_2$ is *non-trust*.

### C. Credential Repository and Policy Repository

The credential repository stores all the credentials that the local peer possesses. The policy repository maintains adaptive access control policies for governing the disclosure of the credentials kept in the credential repository. The policy for disclosing a local credential depends on an opponent's trustworthiness level, which is evaluated by trust evaluation module. The higher trustworthiness level is, the fewer requirements will be requested.

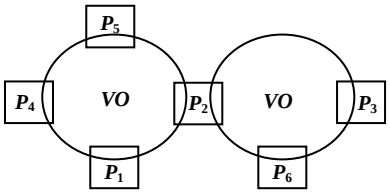



Figure 3. Two overlapping *VO*s

### D. Policy Evaluation Module

Policy evaluation module is used to determine which credentials are disclosed, when they are disclosed, which credentials are requested from an opponent according to the policies and credentials (A.5 and B.5 in Fig. 2). They can be achieved by negotiation strategies. Several negotiation strategies have been developed, such as eager strategy [1], parsimonious strategy [1], PRUNES [2], DFANS [3] disclosure tree strategy (DTS) family [9] and so on.

### E. Trust Negotiation Agent

Trust negotiation agent acts on behalf of the user to manage negotiations. In Fig. 2, when a negotiation is invoked, the trust negotiation agent firstly asks the trust evaluation module to evaluate the trustworthiness level of the opposing peer (A.1 and B.1). After obtaining the trustworthiness level responded by the trust evaluation module, the trust negotiation agent forwards the trustworthiness level to the policy repository (A.3 and B.3). Which policies are used during the negotiation correspond to this trustworthiness level (A.5 and B.5). During the negotiation, when receiving a request, the trust negotiation agent transmits the request to the policy evaluation module (A.4 and B.4). Based on the trustworthiness level, the policy evaluation module draws required credentials and policies from the repositories, and transmits a response to the trust negotiation agent who sends the response to the opponent. When a disclosure sequence leading to a successful negotiation is generated, the trust negotiation agent will exchange the credentials contained in the sequence (A.6 and B.6). If all the exchanged credentials are valid, then the originally requested resource can be granted, otherwise, it is denied. The whole negotiation process is shown in Fig. 4.

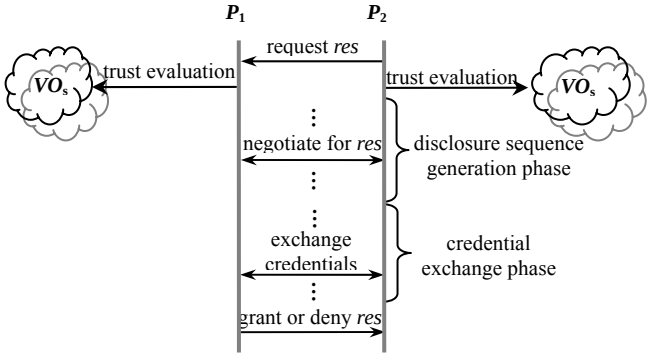



Figure 4. The negotiation process using the framework shown in Fig. 1.

## IV. AN EXAMPLE

Suppose there are two peers $P_1$ and $P_2$, $VO(P_1) = \{P_1, P_3, P_4, P_5\}$, $VO(P_2) = \{P_2, P_7\}$ and $VO(P_3) = \{P_3, P_6, P_7\}$. $P_1$ sets the threshold of the number of overlapping *VO*s as three, and $P_2$ sets the threshold as two, and their policies are shown in Fig. 5. As shown in Fig. 5, $P_1$ has three resources $S$, $S_1$ and $S_2$, and $P_2$ has two resources $C_1$ and $C_2$. Resources refer to credentials, attributes or services. For $P_1$, if an opponent's trustworthiness level is *trust*, then $P_1$ can grant $S$, $S_1$ and $S_2$ freely; if an opponent's trust level is *partial trust*, then $P_1$ can grant $S$ if the opponent has either $C_1$ or $C_2$, and the other two resources $S_1$ and $S_2$ can be disclosed freely; if an opponent's trustworthiness level is *non-trust*, then $P_1$ can grant $S$ if the opponent reveals both $C_1$ and $C_2$, $S_1$ can be disclosed if the opponent reveals $C_1$, and $S_2$ can be disclosed if the opponent reveals $C_2$. The meaning of $P_2$'s policies is similar to $P_1$'s.

Suppose that $P_2$ requests $S$ from $P_1$, and then a negotiation is invoked. Assume the policy evaluation module adopts PRUNES as the negotiation strategy. Firstly, the trustworthiness level should be evaluated.

Since $VO(P_1) \cap VO(P_3) \cap VO(P_2) = \{P_7\} \neq \phi$, which is shown in Fig.6. According to the threshold, $P_1$ considers that $P_2$ is *partial trust*, and $P_2$ considers $P_1$ is *non-trust*. The negotiation process is represented in Fig. 7.

In traditional ATN, all peers are considered as *non-trust* to each other. In this example, if using traditional ATN, the disclosure of two additional resources $C_2$ and $S_1$ needs to be negotiated, exchanged and verified. Although extra cost will be added since the evaluation of trustworthiness levels, according to our experiments, it can be neglected if the number of overlapping *VO*s is not too much.

$P_1$'s policies:

| Resources | Trustworthiness level | | |
|---|---|---|---|
| | *Trust* | *Partial trust* | *Non-trust* |
| $S$ | *true* | $C_1 \mid C_2$ | $C_1$ & $C_2$ |
| $S_1$ | *true* | *true* | $C_1$ |
| $S_2$ | *true* | *true* | $C_2$ |

$P_2$'s policies:

| Resources | Trustworthiness level | | |
|---|---|---|---|
| | *Trust* | *Partial trust* | *Non-trust* |
| $C_1$ | *true* | *true* | $S_2$ |
| $C_2$ | *true* | $S_1$ | $S_1$ & $S_2$ |

Figure 5. Policies of two peers $P_1$ and $P_2$.

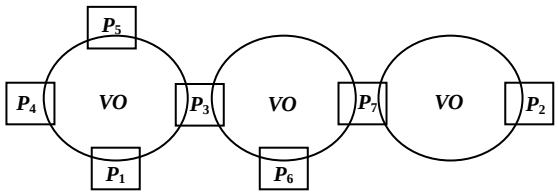



Figure 6. Three Overlapping *VO*s

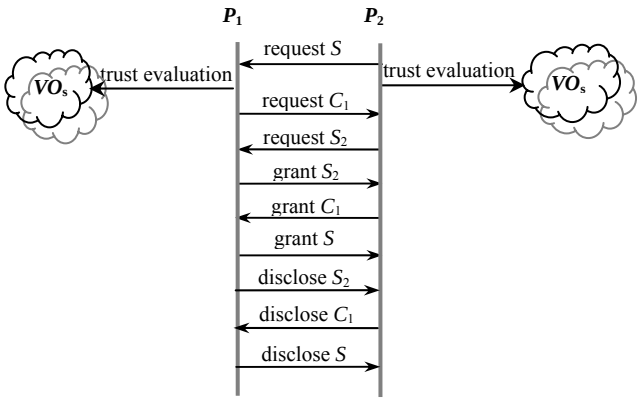



Figure 7. The negotiation process using the framework shown in Fig. 1.

## V. EXPERIMENT RESULTS

An implementation of the proposed framework shown in Fig. 2 is developed on a platform based on Java. We have conducted several experiments in a simulated P2P environment to justify our ideas about how the trust evaluation module and adaptive policies can help peers in trust negotiations. For obtaining more accurate results, the simulations were run on Celeron with 2.41 GHz processor and with 512MB of RAM, under Microsoft Windows XP. In our simulation, there are five hundred peers, and for each peer there are a unique resource and a randomly chosen number of local credentials varying between ten and fifteen. Every peer has randomly generated policies, and for each policy, there are at most three clauses, and for each clause there are at most three remote credentials. Each resource has three policies corresponding to three different trustworthiness levels, i.e. *trust, partial-trust* and *non-trust*. For a resource, the policy corresponding to *non-trust* is randomly generated first. And then, the policy corresponding to *partial-trust* is generated by removing randomly chosen number of remote credentials varying between zero and two from the policy corresponding to *non-trust*. Similarly, the policy corresponding to *trust* is generated by removing randomly chosen number of remote credentials varying between zero and two from the policy corresponding to *non-trust*. Each peer has at most two unprotected local credentials.

For each trust negotiation, two peers $P_i$ and $P_j$, $i \neq j$, are randomly chosen, and $P_i$ initiates a negotiation to $P_j$. All the peers use negotiation strategy DFANS since it can ensure negotiation success when both peers' policies are allowed. We compare the execution time of the negotiations enforced by the proposed ATN framework to the execution time of the negotiations enforced by the traditional ATN framework, that is, compare the negotiations' execution time between the circumstances that the trust evaluation module exists and the trust evaluation module does not exist in every round. For each peer, the threshold of the number of overlapping *VO*s for *partial-trust* is randomly set between two and three. One hundred negotiations are carried out, and the execution time of the first fifty successful negotiations is measured in terms of CUP time in milliseconds, which are represented in Fig. 8, Fig. 9 and Fig. 10. Note that since policies are generated randomly, not all the negotiations can be successful. According to our experiments, approximately sixty percent negotiations can succeed.

In Fig. 8, there are ten virtual organizations, and each virtual organization has one hundred peers. In Fig. 9, there are ten virtual organizations, and each virtual organization has one hundred and fifty peers. In Fig. 10, there are ten virtual organizations, and each virtual organization has two hundred peers.

From the above three figures, we can observe that the exploration of the trust evaluation module together with adaptive policies highly enhances negotiation efficiency, especially when the number of peers in each virtual organization increases.

## VI. CONCLUSION

Previous work on improving the negotiation efficiency of ATN mainly takes advantages of history negotiation information, which may lead to much unnecessary information leakage and cannot improve negotiation efficiency if both negotiators do not have appropriate history information. Hence, in this paper, we propose an ATN framework to enhance negotiation efficiency from a new aspect, that is, fine-grained adaptive policies on the basis of the trust evaluations by overlapping virtual organizations. The proposed ATN framework can simplify the negotiation process, reduce the number of exchanged credentials and credential validations whenever possible. Further, it also avoids revealing unnecessary information during negotiations. We implement the proposed ATN framework on a java platform. According to the experimental results, compared with the traditional ATN framework, the proposed ATN framework can greatly enhance the negotiation efficiency whenever possible.

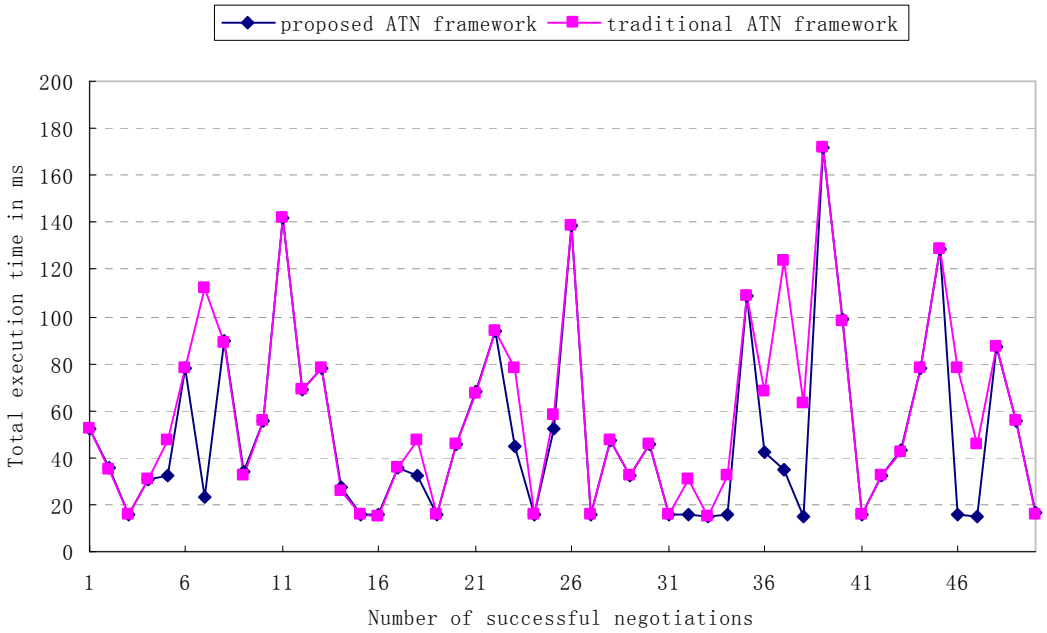



Figure 8. Comparisons of execution time between the negotiations that are carried out by proposed ATN framework and the negotiations that are carried out by traditional ATN framework (each virtual organization has one hundred peers).

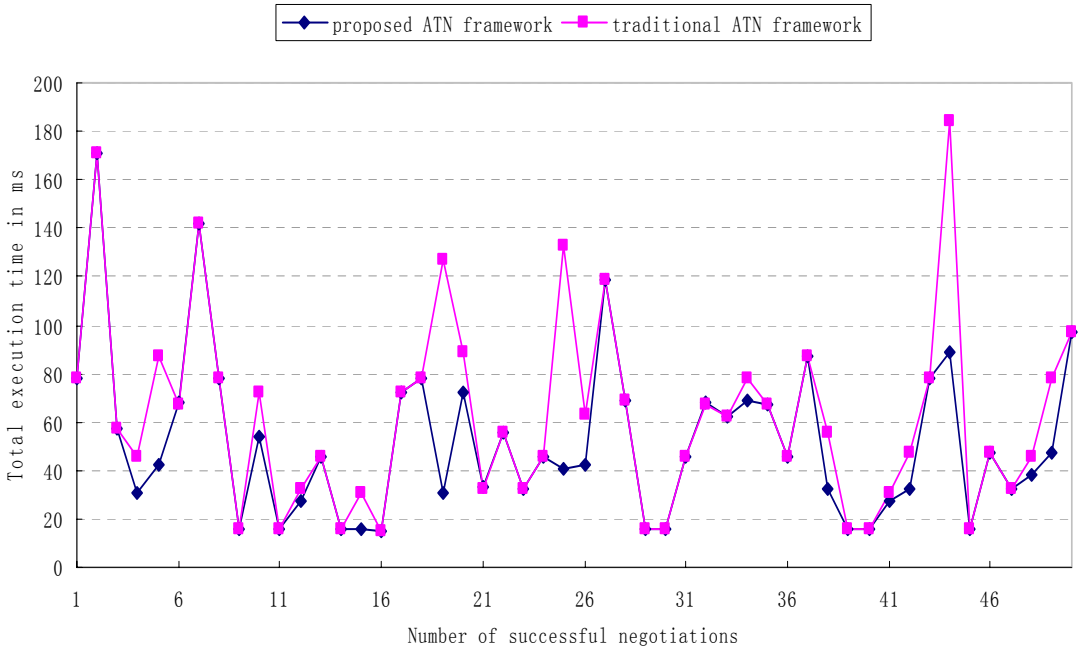



Figure 9. Comparisons of execution time between the negotiations that are carried out by proposed ATN framework and the negotiations that are carried out by traditional ATN framework (each virtual organization has one hundred and fifty peers).

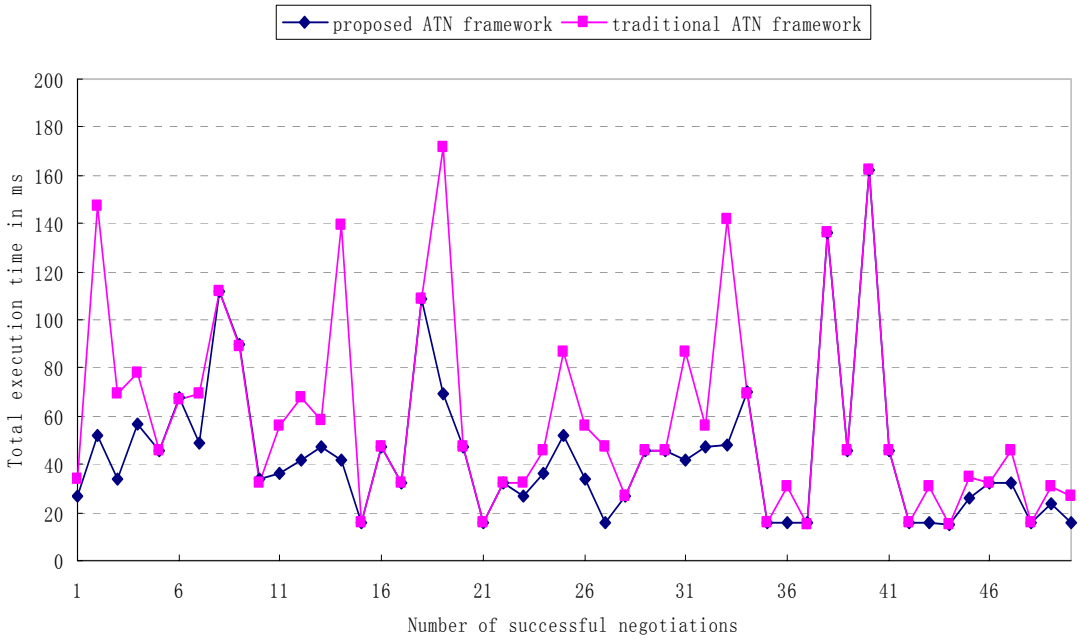



Figure 10. Comparisons of execution time between the negotiations that are carried out by proposed ATN framework and the negotiations that are carried out by traditional ATN framework (each virtual organization has two hundred peers).

## REFERENCES

[1] W. H. Winsborough, K. E. Seamons and V. E. Jones, "Automated trust negotiation," Proc. DARPA Information Survivability Conf. and Exposition, 2000, pp. 88−102.

[2] T. Yu, X. Ma, and M. Winslett, "PRUNES: an efficient and complete strategy for automated trust negotiation over the Internet," Proc. ACM Conference on Computer and Communication Security, ACM press, Nov. 2000, pp. 210-219.

[3] H. Lu and B. Liu, "DFANS: a highly efficient strategy for automated trust negotiation," J. Computers& Security, Vol. 28, No. 7, 2009, pp. 557-565.

[4] E. Bertino, E. Ferrari and A. C. Squicciarini, "Trust-X: a peer to peer framework for trust negotiations," IEEE Trans. on Knowledge and Data Engineering, vol.16, Jul. 2004, pp. 827-842.

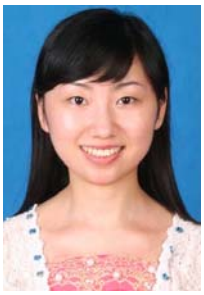
[5] A. Squicciarini, E. Bertino, E. Ferrari, F. Paci, B. Thuraisingham, "PP-Trust-X: a system for privacy preserving trust negotiation", ACM Transactions on Information and System Security, vol. 10, Jul. 2007, pp. 1-48.

[6] H. Lu and B. Liu, "A peer-to-peer framework for accelerating trust establishment". International Conference on Multimedia Information Networking and Security, Nov. 2009.

[7] O. Ajayi, R. Sinnott, and A. Stell, "Formalising dynamic trust negotiations in decentralised collaborative e-health systems. Proc. 2nd International Conference on Availability, Reliability and Security, (ARESO˜07), Vienna, Austria. IEEE Computer Society, Apr. 2007.

[8] O. Ajayi, R. Sinnott, and A. Stell, "Trust realisation in collaborative clinical trials systems," Proc. HealthCare Computing Conference HC2007, Harrogate, England, Mar. 2007.

[9] T. Yu, M. Winslett and K. Seamons, "Interoperable strategies in automated trust negotiation," Proc. ACM Conference on Computer and Communication Security, Philadelphia, 2001.



**Bailing Liu** received the PhD degree in computer science from Huazhong University of Science and Technology in 2010, China. Her research interests are in the area of information security, in particular, automated trust negotiation. In this area, Dr. Liu has published several papers in some major refereed journals, and in proceedings of international conferences.