Automated Trust Negotiation Model based on Dynamic Game of Incomplete Information

Hongwei Chen, Shuping Wang, Hui Xu, Zhiwei Ye,*Chunzhi Wang
School of Computer Science, Hubei University of Technology, Wuhan, China
Email: chw2001@sina.com

***Abstract*—This paper proposes an automated trust negotiation model based on dynamic game of incomplete information. Through the trust evaluation on the early stage of the consultation process and different processes for trust at the later stage, this paper introduces the thought of dynamic game and establishes an evaluation model based on trust relationship analysis. First of all, through the analysis and comparison, this paper combines the automatic negotiation process and the thought of game, and discusses the trust evaluation factors for the early stage of the negotiation. And then this paper quantifies the privacy value and the trust degree, provides a method of establishing automated process for trust negotiation based on the dynamic game, and finally gives the example analysis and discussion for this model.**

***Index Terms*—Automated Trust Negotiation, Dynamic Game, Trust Degree, Game Tree**

I. INTRODUCTION

In the open network environment, Automated Trust Negotiation (ATN) mechanism is suitable for processing requests of users and network services about trust issues in different security domains, including disclosure of the respective access control strategy, the certificate exchange, consultation message passing, privacy protection[1-2]. Its characteristics are as follows. First, the trust relationship between stranger entities through the attribute certificate exchange is established. Second, both consultative parties can define the access control policy, in order to regulate each other for the resource access. Third, trusted third-party participation is not required. In trust negotiation based on the attribute certificate, the focus of negotiation is to control the access to a resource, and the strategy is achieved by specific access control [3-5]. Generally, there exist two peer entities in the automated trust negotiation model, one called server which owns resources, and the other called client which requests sources. Servers and clients are in different trust domains, so the two negotiation parties don't fully trust each other. The sensitive information or service can be accessed until trust is established through negotiation.

As for negotiation strategy, William put forward the enthusiastic negotiation strategy with higher efficiency and the stingy negotiation strategy for better privacy protection. Yu thought that, controlling the access to protected resources in trust negotiation not only included the demand resources of users for final access, but also included the certificate itself [6]. Bonatt made use of the primitive predicate filter to reduce access control policy and improved the negotiation efficiency. Tian Liqin used the Bayesian network to predict user's behavior trust, and attempted to use the game theory to build trust. TrustBuilder trust system used careful negotiation strategy and attempted to synthesize the advantages of both enthusiastic and stingy negotiation strategies. Trust-X negotiation strategy used vote of confidence and trust memory, so that the negotiation efficiency was improved [7-11].

Game theory is an effective tool to analyze the interaction of both sides. Many scholars apply game theory to network trust and security. A L1-VPN fair resource sharing problem as an Adaptive Two-Stage Bargaining Process Scheme is formulated by game theory [12]. A trust evolution model for social network is established based on Logistic model and evolutionary game theory, [13]. A Game Theory-Based model which describes the relationship between security and efficiency is presented, and the existence of Nash equilibrium in this model is proved [14]. In order to prevent rational players cheating, the repeated interaction method to provide motivation so as to attract the players to cooperate in the reconstruction phase is applied. The scheme has higher safety and effectiveness, to better meet the application requirements [15].

In this paper, an automated trust negotiation model based on dynamic game of incomplete information is proposed. In section 2, we discuss trust relationships, propose an automated trust negotiation model, and give a game model for automated trust negotiation. In section 3, we establish a dynamic negotiation mechanism, including calculation of trust degree evaluation, setting of a threshold for dynamic adjustment, calculation of certificate loss, choosing of Policy, and process of dynamic game. In section 4, we provide mapping rules between negotiation sequence and game tree, and give steps for construction of the game tree. In section 5, we propose an algorithm of dynamic game for automated trust negotiation, and analyze the algorithm complexity. In section 6, we analyze the negotiation process of dynamic game in the case of incomplete information through an example. In section 7, we give our conclusion.

II. TRUST RELATIONSHIPS AND GAME ANALYSIS

A. Characteristics of Game for Interaction

doi:10.4304/jsw.8.10.2668-2674

In network environment, resource between nodes or service interaction often exhibits a game behavior [16-23]. Automated trust negotiation is a dynamic game process of incomplete information for both parties to exchange certificate or resource, select the appropriate negotiation strategy and be mutually authorized. The basis of interaction for both parties is mutual trust, and the building of trust ensures the normal service.

In the interactive process of gradually building trust between nodes, some common external behaviors can be discovered as follows.

(1) Both parties of interaction show rationality, which reflects in two aspects. First, as parties of interaction, both obtain the other party's trust realized by certificate interaction, and the trust is obtained by this kind of objective existence. Second, when both make decisions, they not only take into account the current interaction, but also consider other nodes with the same the interests for each other.

(2) Dynamic and repetitive characteristics of game. Interaction between the two parties of the game is often a dynamic game of incomplete information, and each other makes trust evaluation through some objective factors, such as interactive history, thus dynamically adjusts their strategies. Reproducibility means repeated games of certificate or resource in an interaction and role exchanges for interaction of nodes.

(3) Non-zero-sum characteristic of game. Usually, the game between nodes is a non-zero-sum game, which can achieve a win-win situation through the interaction, and is usually performed in a successful interaction that the resource demander can obtain the corresponding resource, and the resource provider can access each other's trust, ready for subsequent resource request interaction. Failure of the interaction causes negative effects for subsequent interaction due to the historical record.

B. *The Process of Trust Negotiation*

This paper considers the trust evaluation at the early stage of the consultation and different situations for the trust at the later stage, divides the automated trust negotiation process into three phases, as shown in Figure 1. Negotiation parties of both Client and Server enter into the early stage of negotiations, and first obtain the situation of each other's trust from respective local areas, called as the stage of objective trust evaluation. Then according to each other's assessment situation, select the appropriate negotiation strategy for consultation, called as the stage of dynamic negotiation. Finally, at the end of consultations, both parties of negotiations update their consultation information to record the history and provide information to other nodes, call as the stage of consultation recording.

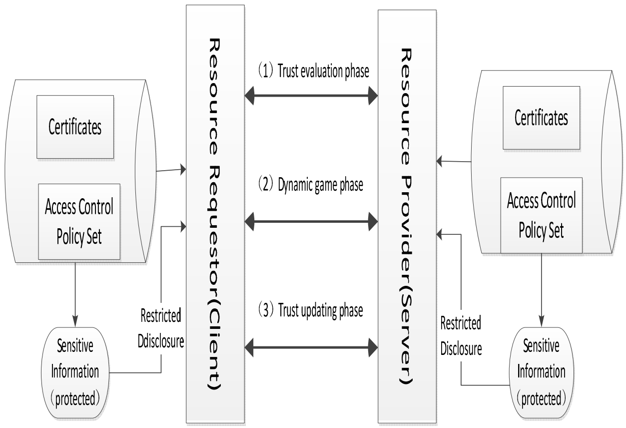


Figure 1. An Automated trust negotiation Model

C. *Game Model for Automated Trust Negotiation*

The existing negotiation strategy is the process to construct the negotiation tree. Usually, certificates are supposed as nodes, and the process of unlock-certificates are supposed as sides. This process is similar to the game with incomplete information. Both sides who participate in the game can be abstracted by decision node, and the certificate set of disclosing can be abstracted by branch. The process of negotiation is the process of constructing the game tree; via income function to calculate the participator's final effectiveness and to solve the Nash equilibrium.

In the dynamic game of incomplete information, according to the analysis above, the trust negotiation model based on dynamic game can be abstracted into quadruple form $\Gamma=(P,C,S,U)$, in which P is game participant, including both parties, the Server party and the Client party, $p\in P: P=\{Server, Client\}$, C is the collection of consultation certificates, the one for Server recorded as C_s and the one for Client noted as C_c and their correspond privacy values are respectively marked as δ_s and δ_c, $s\in S: S=\{S_s,S_c\}$, S_c is the strategy set of the Client party, non-empty set, S_s is the strategy set of the Server party, non-empty set, and U is loss (profit) function $S_c\times S_s\rightarrow U$.

III. Establishment of Dynamic Negotiation Mechanism

A. *Calculation of Trust Degree Evaluation*

Before the consultation between the two parties, reliability is collected from the network and history, which are δ_n and δ_h for hypothesis, $\delta_i\rightarrow[0,1], i\in\{n,h\}$. If $h(p)$ is recorded as historical information for interaction, and δ_h is measured by proportion of the successful number for interaction and the total number, then

$$\delta_h = \sum_{k=1}^{m} h_l(t) \bigg/ \left(\sum_{k=1}^{n} h(t) \right) + \delta_0 \quad (1)$$

in which δ_0 is the initial value when the two parties without interaction history.

Recommendation of network nodes is marked as $t(n)$, in which $t(i)$ is the current trust degrees for nodes, and $t(i) = \begin{cases} \delta_0 & Interaction \\ \delta_p & Non\text{-}interaction \end{cases}$. If δ_n is measured by the weighted average of the recommendation degree, then

$$\delta_n = \frac{1}{n} \sum_{i=1}^{n} t(i) \quad (2)$$

The objective trust value δ_p of both parties for consultation is measured by the composition of two parts δ_n and δ_h.

$$\delta_p = \lambda \alpha \delta_h + (1-\lambda) \beta \delta_n \quad (3)$$

in which α is the attenuation factor, β is uncertain factor for networks. α is used to measure certain effects on interaction caused by time in the interaction process, and β is used to measure the uncertain factors in the networks.

B. Setting a Threshold for Dynamic Adjustment

According to obtained credibility of both parties, adjust the respective initial threshold K_0.

$$K_p = (1-\delta_p) \cdot K_0 \quad (4)$$

C. Calculation of Certificate Loss

The basic value of privacy for a certificate is marked as $\varphi_p : \varphi_p \to [0,1]$. When the certificate is unlocked, the need to provide more certificates indicates that the privacy level of a certificate is higher, in other words, disclosure needs to reach the threshold. The formula of calculating the disclosure loss of a certificate is

$$U_p = \sum_{j}^{m} \sum_{i}^{n} \left| \kappa^{\tau^{n-i}} \varphi_p(c_i) - \tau^{m-j} \varphi_p(s_j) + \varphi_0 \cdot \delta_p \right| \quad (5)$$

in which κ, τ are the compensation factors. φ_0 is the basic value or loss of certificates, divided into public certificates and privacy certificates.

D. Choosing Policy

Compare the calculated value with the threshold value, in order to determine whether the next negotiation certificate achieves the conditions of interaction. The following formula is used to calculate policy $A(p)$.

$$A(p) = \begin{cases} 1 & K_p \geq Max\left\{K_p^*(c_i, s_j), U_p\right\} \\ 0 & K_p < Max\left\{K_p^*(c_i, s_j), U_p\right\} \end{cases} \quad (6)$$

in which the situation of $A(p) = 1$ means that the current certificate can continue to the next step of interaction, the value 0 means that the condition of interaction is reached, needing to re-consult.

E. Process of Dynamic Game

A complete process of consultation can be expressed as follows.

$$\Gamma = Min\left[A(p)\right] \Big| Min\left(U_p\right) \quad (7)$$

That is, each game can obtain the best interaction of certificates through the minimum utility.

IV. Process of Constructing the Game Tree

A. Mapping Rules

The actual negotiation process is very complex, and it can simplify in these condition of convention: (1)The resource requestor C and the resource provider S are both completely rational. (2) The resource requestor C and the resource provider S will pursue the maximum income for themselves in the premise of insuring to construct trust. (3) The resource requestor C and the resource provider S can obtain counterpart's access control strategy via negotiation.

As for the study of automated trust negotiation, access control rules usually use the disjunctive paradigm. In the process of dynamic game, mapping relationship should satisfy the following conditions, in order to translate the negotiation sequence into the construction of the game tree.

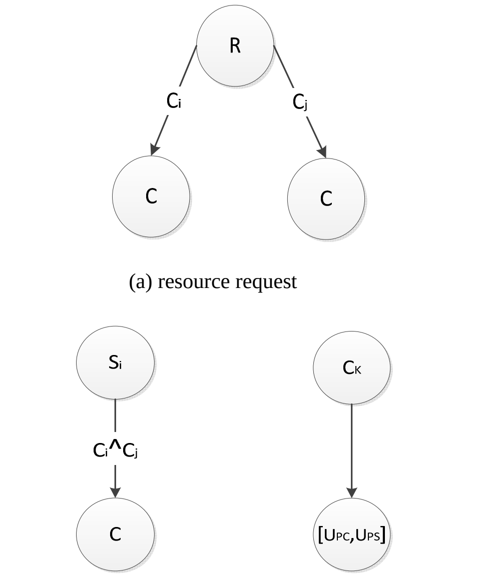
(1) The paradigm for requested resource is $R \leftarrow \cdots \{C_i\} \vee \{C_j\} \cdots$, in which R represents the requested resources, and C_i and C_j are needed disjunctive expressions of certificates by the requests, with mapping paradigm shown in Figure 2 (a).

(2) The conjunctive paradigm for certificate requirement is $S_k \leftarrow \cdots \{C_i\} \wedge \{C_j\} \cdots$, in which S_k represents conditional disclosed certificate by either party of negotiation, and C_i and C_j are needed conjunctive expressions of certificates by the requests, with mapping paradigm shown in Figure 2 (b).

(3) The paradigm to terminate negotiation is $C_k \leftarrow T$, in which C_k is unconditional disclosed certificate by either party of negotiation, usually representing the end of the negotiation.

The disjunctive method for composition is as follows.

$$S_k \leftarrow \cdots \{C_i\} \wedge \{C_j\} \cdots C_k \leftarrow T$$



(a) resource request

(b) conjunctive expression (c) negotiation termination

Figure 2. Mapping relationship between negotiation sequence and game tree

B. Construction of the Game Tree

The construction of a game tree is divided into two stages. The first stage is to construct the type of the tree, the basis and method of which is mapping rules and the thought of recursive interaction. The second stage is to calculate the corresponding loss or utility, and to assess and select appropriate consultation sequence. The steps for construction are as follows.

Step1. Initialize the tree as an empty one, denoted by T_0.

Step2. Add the requested resource R to T_0, as the root node.

Step3. Perform disjunctive decomposition of access control rules for R, and use all sub-types by the decomposition as the root nodes of the next layer of nodes for subset of access control rules, with the mapping mode $R \leftarrow \cdots \{C_i\} \vee \{C_j\} \cdots$.

Step4. Server responses to subset of access control rules for Client, and according to the mapping mode $C_k \leftarrow \cdots \{S_i\} \wedge \{S_j\} \cdots$ requests the certificate set of Client in a reversed way, with its rules as the next-layer nodes for the tree.

Step5. Client responses to subset of access control rules for R, and according to the mapping mode $S_k \leftarrow \cdots \{C_i\} \wedge \{C_j\} \cdots$ requests the certificate set of Server in a reversed way, with its rules as the next-layer nodes for the tree.

Step6. Repeat Steps (4) and (5), until the end of a cycle of access rules $C_k \leftarrow T$ or circular dependency existing for the certificate.

Step7. Calculate the profit or the loss set U_p of both parties, as the leaf nodes of the tree.

Step8. End the construction of the game tree.

V. Algorithm Of Dynamic Game For Automated Trust Negotiation

A. Algorithm of Dynamic Game for Automated Trust Negotiation

From the analysis in Section 4, the algorithm of dynamic game is summarized as follows.

Input parameters: Credentials and Strategy

// Credentials is the set of certificates of both parties, and resources are also seen as certificates here

// Strategy is the set of strategies of both parties for interaction

Output parameters: Tree and Up

// Tree is the generated game tree

// Up is the loss of utility, calculated according to the formula in Section 3

$Tree = \phi$
$Credentials = \{R, C_i, S_j\}$
$Strategy = \{p_k\}$
Select the strategy request R from Strategy
$Strategy = Strategy - \{p_R\}$
While $Strategy \neq \phi$ *do*
  For each $sub\_strategy$ *do*
    If $C_i | S_j \in Credentials$ *then*
      $Recursion(sub\_strategy, Credentials)$
        If $\exists C_i | S_j \rightarrow True$ *then*
          Create a normal branch
          Calculate U_{ps} *and* U_{pc}
        Endif
    else
      Create a blank or cycle branch
      Calculate U_{ps} *and* U_{pc}
    Endif
    $Tree = Tree \bigcup \{branch\}$
  Endfor
  $Strategy = Strategy - \{p_k\}$
Endwhile
return $OptimalStrategy(Tree, U_{ps}, U_{pc})$

B. Complexity Analysis of Algorithm

According to the analysis on dynamic game algorithm for automated trust negotiation, the worst case is circular dependency of certificates, and the time complexity for this case is $O(N^2)$, in which $N = |C|$ is the number of certificates number. And the best case is for the first time to directly create the smallest branch, and the time complexity for this case will show a linear time complexity $O(C)$. In general, mean time complexity to create and calculate the whole tree is $O(\lg N)$.

VI. Example Analysis

This section will analyze the negotiation process of dynamic game in the case of incomplete information through an example. It is assumed that the certificates and policies for both parties are shown as Table 1.

As is shown in Table 1, the representation of policies is the disjunctive paradigm. The game tree for example is shown in Figure 3. Through dynamic game, the entire game tree can be pruned, and the trust relationship can be established by calculation and selection of optimal revenue from the profits.

TABLE I.

Policies for the Example

Client		
Policy	φ_p	
C2←S2∧S3	0.3	0.6
C3←S1∨S5	0.3	0.2
C4← S5	0.3	0
C5← S2∨S4	0.4	0.2
C6←T	0.2	0
C7←S5	0.4	0.2
C8←T	0.2	0

Server		
Policy	φ_p	
R← C1∨ (C2∧C4)∨(C3∧C7) ∨(C5∧C6∧C8)	0.5	0.6
S1←C5∨C7	0.2	0.2
S2←C5	0.2	0
S3←C3∧C6	0.3	0.2
S4←T	0.2	0
S5←T	0.2	0

And trust cannot be established if the action sequence for one party cannot provide the certificate C_1. In addition, the forming of circular dependency for a certificate in the last branch also causes the trust not to be established. And there are three action sequences that can build trust, as shown in Table 2.

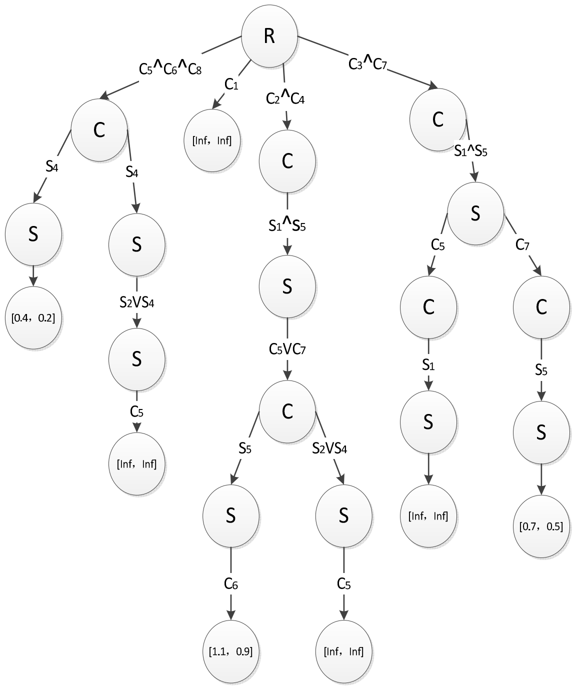


Figure 3. A game tree for example

Seen from Table 2, the sequence $C_6 | C_7 | C_8 \to S_4 \to T$ is a best sequence, and the result of the game is to build the trust relationship with as little as possible exposure of a certificate and privacy loss. In addition, the reason of sequence $C_1 \to$ Suspension is that the resource requester lacks the certificate C_1, which leads to suspension of the negotiation.

And sequences $C_2 | C_4 \to S_1 | S_5 \to C_5 | C_7 \to S_2 | S_4 \to C_5$ and $C_3 | C_7 \to S_1 | S_5 \to C_5 \to S_2 | S_4 \to C_5$ generate circular dependency of the certificate C_5, and the consultation cannot be performed.

TABLE II.

Path Analysis

Sequence of actions
$C_1 \to$ Suspension
$C_2 \| C_4 \to S_1 \| S_5 \to C_5 \| C_7 \to S_5 \to C_6 \to T$
$C_2 \| C_4 \to S_1 \| S_5 \to C_5 \| C_7 \to S_2 \| S_4 \to C_5$
$C_6 \| C_7 \| C_8 \to S_4 \to T$
$C_3 \| C_7 \to S_1 \| S_5 \to C_7 \to S_5 \to T$
$C_3 \| C_7 \to S_1 \| S_5 \to C_5 \to S_2 \| S_4 \to C_5$

Profit analysis	Successful or not	Reason
[Inf, Inf]	N	Without C_1
[1.1,0.9]	Y	
[Inf, Inf]	N	Circular dependencies
[0.4,0.2]	Y	
[0.7,0.5]	Y	
[Inf, Inf]	N	Circular dependencies

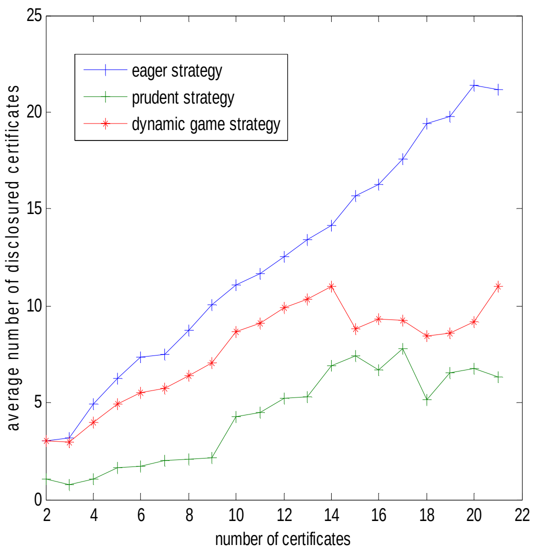


Figure 4. The comparison of simulation results

In a simulation environment, the number of certificates and access control policies and different settings of the privacy will produce different results. In order to better model the actual effect, the certificate and the strategy to obey that a certain distribution is random is reasonable. Here is a selection of the enthusiastic model and the cautious model to serve as contrast, and the average disclosed certificate number is as the comparison object, as is shown in Figure 4.

VII. Conclusion

In order to solve the privacy protection problem in the process of automated trust negotiation, this paper proposes an automated trust negotiation model based on dynamic game of incomplete information. This paper uses dynamic game for establishing dynamic game process and discusses the model through example analysis. The work of this paper can be summarized as follows.

(1) It introduces the thought of dynamic game through analysis; an automated trust negotiation model, and a game model for automated trust negotiation is proposed.

(2) It applies the process of dynamic game into establishment of automated trust negotiation. A dynamic negotiation mechanism is established, including calculation of trust degree evaluation, setting of a threshold for dynamic adjustment, calculation of certificate loss, choosing of Policy, and process of dynamic game.

(3) It provides the algorithm of establishing dynamic game process. Mapping rules between negotiation sequence and game tree, and steps for construction of the game tree are proposed. In addition, an algorithm of dynamic game for automated trust negotiation is presented, and the algorithm complexity is analyzed.

(4) It gives an example of automated trust negotiation, and the negotiation process of dynamic game in the case of incomplete information through the example is analyzed.

Acknowledgment

This work has been supported by the General Program for National Natural Science Foundation of China (No. 61170135), the National Natural Science Foundation of China for Young Scholars (No. 61202287), the Key Project for Natural Science Foundation of Hubei Province in China (No. 2010CDA011), the General Program for Natural Science Foundation of Hubei Province in China (No. 2011CDB075, No. 2012FFB00601), the Key Project for Scientific and Technological Research of Education Department of Hubei Province in China (No. D20111409, No. D20121409), the Provincial Teaching Reform Research Project of Education Department of Hubei Province in China (No. 2012273), the Key Project for Scientific and Technological Research of Wuhan City in China (No. 201210421134), and the Twilight Plan Project of Wuhan City in China (No. 201050231084).

References

[1] Bailing Liu, "Efficient Trust Negotiation based on Trust Evaluations and Adaptive Policies", Journal of Computers, vol. 6, no. 2, pp. 240-245,2011.

[2] Yu Wang, Qiuwei Yang, "Envelope Protocol for Privacy Protection", Journal of Convergence Information Technology, vol. 7, no. 1, pp. 147-155, 2012.

[3] Anna C. Squicciarini, Federica Paci, Elisa Bertino, "Trust establishment in the formation of Virtual Organizations", Computer Standards & Interfaces, vol.33, no.1, pp.13-23, 2011.

[4] Wai-Khuen Cheng, Boon-Yaik Ooi, Huah-Yong Chan, "Resource federation in grid using automated intelligent agent negotiation", Future Generation Computer Systems, vol.26, no.8, pp.1116-1126, 2010.

[5] Deqing Zou, Shangxin Du, Weide Zheng, Hai Jin, "Building Automated Trust Negotiation architecture in virtual computing environment", The Journal of Supercomputing, vol.55, no.1, pp.69-85, 2011.

[6] Zuo Chen, Qiuwei Yang, Xin Wan, Yuanyan Tu, Fei Yu, Chen Xu, "Automated Trust Negotiation with Time Behavior", Journal of Networks, vol. 6, no. 8, pp. 1091-1098, 2011.

[7] Jianxin Li, Dacheng Zhang, Jinpeng Huai, Jie Xu, "Context-aware trust negotiation in peer-to-peer service collaborations", Peer-to-Peer Networking and Applications, vol. 2, no. 2, pp. 164-177, 2009.
[8] Bailing Liu, Feng Xiao, Ke Deng, "Resolving conflicts between negotiation success and sensitive information protection in automated trust negotiation", Frontiers of Computer Science in China, vol. 5, no. 2, pp. 135-147, 2011.
[9] Antonio Maña, Hristo Koshutanski, Ernesto J. Pérez, "A trust negotiation based security framework for service provisioning in load-balancing clusters", Computers & Security, vol. 31, no.1, pp.4-25, 2012.
[10] Hongwei Lu, Bailing Liu, "DFANS: A highly efficient strategy for automated trust negotiation", Computers & Security, vol. 28, no. 7, pp.557-565, 2009.
[11] Hemalatha Chandrashekhar, Bharat Bhasker, "Quickly locating efficient, equitable deals in automated negotiations under two-sided information uncertainty", Decision Support Systems, vol. 52, no. 1, pp. 157-168, 2011.
[12] Aran Kim,Hyeopgeon Lee,Yuhwa Suh, Yongtae Shin, "Adaptive Two-Stage Bargaining Process Resource Allocation Scheme In Layer 1 VPN", International Journal of Advancements in Computing Technology, vol. 4, no. 20, pp. 285-292, 2012.
[13] Guisheng Yin, Jianguo Zhang, Yingjie Wang, "Multi-strategy Trust Evolution Model Based on Logistic Equation For Social Network", Journal of Convergence Information Technology, vol. 7, no. 17, pp. 326-332, 2012.
[14] Yichuan Wang, Jianfeng Ma, Hefeng Chen, Liumei Zhang, "Game Model of Rekeying Strategies", International Journal of Advancements in Computing Technology, vol. 4, no. 11, pp. 30-41, 2012.
[15] Jie Wang, Yong-quan Cai, "An Anti-cheating Rational Secret Sharing Scheme", International Journal of Advancements in Computing Technology, vol. 4, no. 11, pp. 77-86, 2012.
[16] Hongwei Chen, Hui Xu, Li Chen, "Incentive Mechanisms for P2P Network Nodes based on Repeated Game", Journal of Networks, vol. 7, no. 2, pp. 385-392, 2012.
[17] Cheng Zhang, Qing-sheng Zhu, Zi-yu Chen, "Credit-based Repeated Game Model Applied in Transfer Decision of Opportunistic Network", Journal of Software, vol. 6, no. 9, pp. 1649-1654, 2011.
[18] Cheng Zhang, Qing-sheng Zhu, Zi-yu Chen, "Game-based Data-Forward Decision Mechanism for Opportunistic Networks", Journal of Computers, vol. 5, no. 2, pp. 298-305,2010.
[19] Mohamed Amine M'hamdi, Jamal Bentahar, "Scheduling Reputation Maintenance in Agent-based Communities Using Game Theory", Journal of Software, vol.7, no.7, pp. 1514-1523, 2012.
[20] Guowei Wu, Zichuan Xu, Qiufen Xia, Jiankang Ren, " An Energy-Aware Multi-Core Scheduler based on Generalized Tit-For-Tat Cooperative Game", Journal of Computers, vol. 7, no. 1, pp. 106-115, 2012.
[21] Weifeng Sun, Qiufen Xia, Zichuan Xu, Mingchu Li, Zhenquan Qin, "A Game Theoretic Resource Allocation Model Based on Extended Second Price Sealed Auction in Grid Computing", Journal of Computers, vol. 7, no. 1, 65-75, 2012.
[22] Qiufen Ni, Rongbo Zhu, Zhenguo Wu, Yongli Sun, Lingyun Zhou, Bin Zhou, "Spectrum Allocation Based on Game Theory in Cognitive Radio Networks", Journal of Networks, vol. 8, no 3., pp. 712-722, 2013.
[23] Feng Zhao, Xuezhi Lv, Hongbin Chen, "A Leakage-Based Beamforming Algorithm for Cognitive MIMO Systems via Game Theory", Journal of Networks, vol. 8, no. 3, pp. 623-627, 2013.

Hongwei Chen (1975-), male, from Hubei Province, PHD, Associate Professor of Hubei University of Technology, interested in Peer-to-Peer, Cloud Computing, Grid Computing and Mobile Agent.

Shuping Wang (1988-), male, from Hubei Province, master, interested in Peer-to-Peer, Game Theory and Information Security.

Hui Xu (1983-), PHD, Lecturer of Hubei University of Technology, interested in network and service management. Since 2006, she has been a certified computer system analyst in P.R. China. In July 2008, her biography was selected for inclusion in the 26th edition (2009) of the Marquis Who's Who in the World, California, USA.

Zhiwei Ye (1978-), male, from Hubei Province, PHD, Associate Professor of Hubei University of Technology, interested in Computational Intelligence, Image Processing.

Chunzhi Wang (1963-), female, from Hubei province of China, Master's degree, Professor of Hubei University of Technology, Dean of School of Computer Science, interested in the security of network and computer network, Computer supported cooperative work. The Chairman of Wuhan of CCF Young Computer Scientists & Engineers Forum(2010).