Ordered Semiring-based Trust Establish Model with Risk Evaluating

Mingwu Zhang[1], Bo Yang[1], Shenglin Zhu[1], and Wenzheng Zhang[2]
(Corresponding author: Mingwu Zhang)

College of Informatics, South China Agricultural University[1]
No.383, Wushan Rd., Tianhe District, Guangzhou 510642, China
National Laboratory for Modern Communications, Chengdu 610041, China[2]
(Email:{zhangmw,byang, zhusl}@scau.edu.cn)
(Received May 18, 2007; revised Oct. 23, 2007; and accepted Jan. 4, 2008)

Abstract

Distributed trust management supports the provision of the required levels in a flexible and scalable manner by locally discriminating between the entities with which a principal should interact. However, there is a tension between the preservation of privacy and the controlled release of information when an entity submits credentials for establishing and verifying trust metric where it may disclose too much information of the credentials. Furthermore, trust delegation will require some levels of risk to be tolerated. In this paper, we propose a trust model with privacy protecting and risk evaluating. Our model is based on an ordered semiring framework. In proposed ordered semiring framework, credential graph is flexible enough to express trust relationship which adapts to the trust and privacy risk aggregating and concentrating in decentralized network systems. We describe a solution model to establish trust with risk evaluating with the trust opinion and privacy opinion, and also provide the minimized privacy disclosure credential search algorithm based on ordered semiring model.

Keywords: Credential graph, privacy, risk evaluation, semiring, trust management

1 Introduction

Privacy and risk are considered either through identities typically by employ policy defined incremental information release schemes to determine what is appropriate for disclosure in a given interaction, or manage numerous pseudonyms so as to disperse the information that could be attributed to a given identity. The anonymous communication problems by hiding the identity of the subject in a group of participants have been studied [7, 16]. The proposed schemes ensure that the source of a communication is unknown, but the participants may know the content. The approaches will use trusted proxies to protect privacy in a dynamic communication environments [8].

Distributed trust management [5, 8, 9] is a crucial approach to support the provision of the required levels of assurance in a flexible and scalable manner by locally discriminating between the entities with which a principal should interact. Most trust management systems assume monotonicity: additional credentials can only result in the increasing of privilege [2, 4, 6, 7, 9]. Trust is a monotonic model that $s \preceq t$ means that t denotes at least as high a trust-level as s. For scalability and efficiency considerations, trust evaluation is constrained to information provided by directly connected nodes, i.e. it is based on local interactions.

However, for information providers, incremental information release can reduce the maximally valued attribute being disclosed more frequently than desirable needs. In trust management system, a credential chain collector collects the credentials that submitted to compliance checker. In general, principal submit all their credentials to compliance checker so as to give the enough evidence that principals own the delegation or authorization. Nevertheless, the more credentials submitted, the more risk and privacy loss.

We remark a credential as a privacy value that represent multiple attributes privacy disclosure. We define privacy-protected trust model as a semiring algebra structure, which is flexible enough to express trust relation and compute trust metric based on privacy protecting. We ground our privacy model of two nodes on information-based theory. Entropy is a measure of uncertainty in a probability distribution for a discrete random variable X : $H(X) \triangleq -\sum_i p(x_i) log p(x_i)$ where $p(x_i) = P(X = x_i)$. When an adversarial gains more information, the entropy of credential privacy disclose will decrease.

The remainder of the paper is organized as follows: Section 2 presents our trust and privacy risk model in distributed trust system. A privacy protecting trust graph based ordered semiring and its search algorithm are pre-

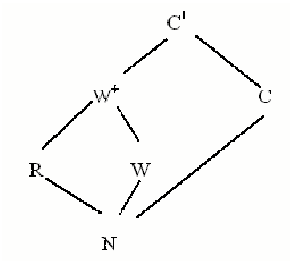

Figure 1: Example of authorization Hasse diagram

sented in Section 3. This is followed some related work that looks at privacy concerns in Section 4. And it concludes the paper in Section 5.

2 Definition

A trust authorization relationship can be taken as a delegation model with a partially ordered structure.

Definition 1. ***(Auth-stru)****. An authorization structure is denoted by* $auth = (L, \uplus, \cup, \cap)$ *where* $\uplus$ *is a partially ordered over set* L *that satisfies:*

- $\cup$ *is a greatest-lower bound operator,*
- $\cap$ *is a least-upper bound operator, and*
- *Any two elements relation in* L *has greatest-lower bound and least-upper bound.*

We consider a simple example of a file operator authorization. Consider auth $L = \{N, R, W, W^+, C, C^+\}$ with N least, R(read) and W(write) and C(create) unrelated, W^+(read/write) and greatest $C^+(W/C)$, respectively, i.e., the Hasse diagram of lattice model in Figure 1 which satisfies:

$$N \subseteq R, N \subseteq W, N \subseteq C, R \subseteq W, W \subseteq W^+$$
$$C \subseteq C^+, W^+ \subseteq C^+, \bigcup\{R, W\} = W^+$$
$$\bigcup\{R, W, C\} = \bigcup\{W^+, C\} = C^+$$

Definition 2. *A trust risk metric is defined as a complete lattice risk* $= (S_P, \preceq)$*, where* S_P *is a set of risks in privacy opinion space and* $\preceq$ *is a decidable risk order relation.*

We let $\perp$ and $\top$ denote the top and bottom elements of the lattice. The instantiation of trust risk metric also includes two associative and monotonic aggregation operator: risk aggregation $\oplus$ and risk concentration $\otimes$.

Definition 3. *Trust domain opinion as pairs* $(p, q) \in S$*, where* $S = S_T \times S_P$*,* $S_T \in [0, 1]$ *is trust opinion space and* $S_P \in [0, 1]$ *is privacy opinion space.*

A trust value pair in trust domain opinion space $(p, q) = (1, 0)$ represents full trust and no privacy loss, and $(0, 0)$ is a initialized state about a trust relation that there is not any trust value and privacy disclosure.

Definition 4. ***(Trust structure)*** *A trust structure with privacy risk metric is defined as* $T = (K, \leq, \sqsubseteq)$*, where* K *is trust lattice of auth, and two partial relation, the trust ordering* $\leq$*, and the information ordering* $\sqsubseteq$*.*

We use $\leq$ to describe the trust operator when trust evidence submits, and $\sqsubseteq$ to describe the risk value for evidence disclosure.

In order to safeguard the sensitive credential from malicious access, we use privacy entropy to describe credentials' attribute sensitivity. Before principal submit credentials, he or she expects the least privacy loss for attributes disclosure in the set of credentials.

Definition 5. ***(Attribute risk)*** *A credential* $\mathfrak{C}$ *with* i *attribute fields* X_i*, and the set* R *denotes revealed credentials that before* $\mathfrak{C}$ *is been submitted. When submitted the credential* $\mathfrak{C}$*,* X_i *privacy loss value in* $\mathfrak{C}$ *denote by* $plf_{X_i}(X_i|R)$ *is defined by:*

$$plf_{X_i}(X_i|R) = \sum_{i=1}^{n} P_i log_2 \frac{1}{P_i} - \sum_{i=1}^{n} P_i^* log_2 \frac{1}{P_i^*}, \quad (1)$$

where $P_i = Pr\{X_i \text{ is disclosed}|R\}$ *and* $P_i^* = Pr\{X_i \text{ is disclosed}|R \bigcup C\}$ *denote probability mass function that reveal credential set* R *and* $R \bigcup C$*, respectively [11].*

Definition 6. ***(Credential privacy disclosure)*** *Given* m *attributes* $X_1, \ldots, X_m$ *in a credential* $\mathfrak{C}$ *with sensitivity weight* $w_1, \ldots, w_m, (\sum_{i=1}^{m} w_i = 1)$*, each attribute with domain* $\{\{x_{11}, , x_{1n}\}, , \{x_{m1}, \ldots, x_{mn}\}\}$*. The privacy disclose entropy* H^C *is defined by:*

$$H^C = \sum_{i=1}^{m} w_i \times plf_{X_i}. \quad (2)$$

Property 1.

$$0 \leq H^C \leq mlog_2 n. \quad (3)$$

The minimum 0 of H^C is taken when all $plf_X = 0$, which means $\sum_{i=1}^{n} P_i log_2 \frac{1}{P_i} = \sum_{i=1}^{n} P_i^* log_2 \frac{1}{P_i^*}$ that credential $\mathfrak{C}$ can not disclose any privacy information. The maximum value $mlog_2 n$ is taken when $P_i = 1/n (i = 1, \ldots, n)$ and $P_1^* = \ldots = P_i^* = P_{i+1}^* = \ldots = P_n^* = 0, P_i^* = 1$ hat means it will disclose all privacy information in credential $\mathfrak{C}$ when an entity holds the credential.

When a credential is transferred from A to B, credential privacy disclosure entropy is denoted by H_{AB}^C. We assume that an entity will not disclose his confidential and privacy information deliberately. Intuitively, $H_{AA}^C = 0$. In general, the value $plf(X_i)$ of attribute X_i will be maximized by $plf(X_i) = \sum_{i=1}^{k} P_i log_2(1/P_i) = log_2 k$, because an adversary get privacy attribute value to be uniform distribution over the attribute domain when a new credential is to be assigned.

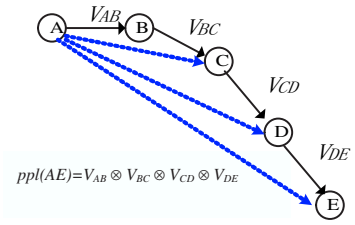

Figure 2: Privacy risk along the trust chain

Definition 7. *The privacy loss function of credential* $\mathfrak{C}$ *between two nodes A and B denoted by* $V_{AB} = 1 - H^C_{AB}/m_c log_2 k$, *where* m_c *is attribute number in credential* $\mathfrak{C}$ *and* H^C_{AB} *is privacy disclose entropy between node A and B.*

The credential privacy loss function along a chain is defined by ppl, as

$$ppl(path) = \bigotimes_{[\bar{p}\ is\ along\ the\ path]} V_{\bar{p}}. \quad (4)$$

$\otimes$ is a operator that concentrates the path, with which the property has commutative and associative. We define privacy opinion space $S_P = [0,1]$,$ppl \in S_P$.

With the increasing of trust chain, the probability of privacy loss is increasing. The operator $\otimes$ satisfies the monotonicity along a path. The *ppl* combination along a path is showed in Figure 2.

In Figure 3, when a new entity joins in, the opinion value is $(0,0)$ which means no trust information or privacy disclosure. The value $(1,0)$ represents that the trust is 1 and privacy disclosure is 0, which is excellent for building trust and balance privacy. The value $(0,1)$ is inacceptable since it has disclosed privacy but no trust be established.

The operator $\otimes$ combines opinions disclosure along a path and operator $\oplus$ combines opinions across paths. When two nodes P and Q build trust relation, the trust opinion of $P \otimes Q$ is no more than $min(P.S_T, Q.S_T)$ for that trust concentration will loss trust metric. But the privacy opinion of $P \oplus Q$ will increase because of node's disclosure risk. Furthermore, the trust opinion and privacy of $P \oplus Q$ are all no less than $max(P.S_P, Q.S_P)$.

These operators can be used in a general framework for solving path problems in graphs, provided they satisfy certain mathematical properties, i.e., form an algebraic structure called semiring.

Definition 8. *A semiring[2,5] is a system* $(K, \oplus, \otimes, \bar{0}, \bar{1})$ *such that*

- $(K, \oplus, \bar{0})$ *is a commutative monoid with* $\bar{0}$ *as the identity element for* $\oplus$,
- $(K, \otimes, \bar{1})$ *is associative, with a neutral element* $\bar{1} \in K$, *and* $\bar{0}$ *as an annihilator element for* $\otimes$: $\forall a \in K, a \otimes \bar{0} = \bar{0} \otimes a = \bar{0}$, *and*
- $\otimes$ *distributes over* $\oplus$. *For all* $a, b, c \in K$, *that* $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$, *and* $c \otimes (a \oplus b) = (c \otimes a) \oplus (c \otimes b)$.

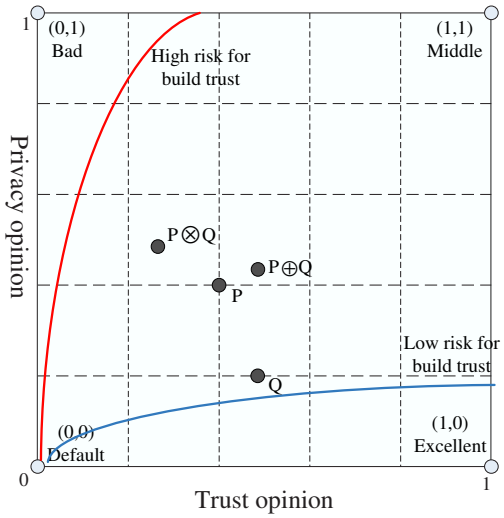

Figure 3: Privacy and trust in opinion space

An ordered semiring $(K, \otimes, \oplus)$ is a semiring with a partial order $\sqsubseteq_K$ such that the operations $\otimes$ and $\oplus$ are weakly monotonic. If $a \sqsubseteq b$ and $a' \sqsubseteq b' \Rightarrow a \oplus a' \sqsubseteq b \oplus b'$, and $a \otimes a' \sqsubseteq b \otimes b'$.

3 Semiring Trust Model

3.1 Trust Semiring

We use an ordered semiring to describe information ordering $\sqsubseteq$ in trust structure $T = (K, \leq, \sqsubseteq)$. Considering privacy concatenation along a path as $\otimes$ and aggregation of privacy across multi-paths as $\oplus$, we introduce a partial order over our semiring as an ordered semiring. Each opinion space $S = [0,1]^2$. For example, we may choose semiring $(S, \oplus, \otimes, \bar{0}, \bar{1})$ for trust opinion as Jøsang model[3], and privacy opinion that $\otimes$ operator is $+$, by which privacy loss along a path will be accumulated, and $\oplus$ operators is max. In our model, semiring is monotonic. We can verify that the neutral elements $\bar{1} = (1,0)$ and $\bar{0} = (0,0)$. So, the privacy opinion value of source node s to destination d that comprised n path in ordered semiring is

$$ppl^C(s \to d) = \bigoplus_{k=1}^{n} [\bigotimes_{[\bar{p}\ is\ a\ path\ from\ s\ to\ d]} V_{\bar{p}}]. \quad (5)$$

3.2 Ordered Monotonic Trust Graph

We will find out an optimal path that has minimum privacy disclosure along a path based our semiring when nodes will prompt trust. An important property of semirings when dealing with shortest paths problems is monotonicity. When monotonicity holds, the computation of shortest distances can be factored. We define the single-source shortest-distance problem for privacy protecting that path aggregate about privacy in trust graph G.

We consider a semiring $(K, \oplus, \otimes, \bar{0}, \bar{1})$, and a weighted directed graph G = (V, E) over K, where V represents the set of vertices of G, E for the set of edges. In that case, $\otimes$ is the operator used to calculate the weight w of a path $p = (v_0, v_1, \ldots, v_k)$ based on the weights of the path's edges that $W(p) = \bigotimes_{i \in p} w_i$.

Given an edge $e \in E$, we denote by $n[e]$ as its next vertex, by $p[e]$ as its origin or previous vertex, and by $w[e]$ its weight. Given a vertex $v \in V$, we denote by $E[v]$ as the set of edges leaving v.

In G, a trust path $\pi = e_1 e_2 \ldots e_k$ is an element of E^* with consecutive edges: $n[e_i] = p[e_{i+1}]$ for $i = 1, \ldots, k-1$. We extend n and p to paths by setting: $p[\pi] = p[e_1]$, and $n[\pi] = n[e_k]$. So a cycle is a path starting and ending at the same vertex: $n[c] = p[c]$. The weight function w can also be extended to paths by defining the weight of a path as the result of the $\otimes$-multiplication of the weights of its constituent edges:

$$w(\pi) = \bigotimes_{i=1}^{k} w[e_i], \tag{6}$$

and it can be extended to any definite set of paths by

$$w[\bigcup_{i=1}^{n} \pi_i] = \bigoplus_{i=1}^{n} w[\pi_i]. \tag{7}$$

It is rational to consider that a user will have the minimum privacy disclosure opinion about himself, i.e.$\forall i, w(i, i) = \bar{0}$, that is neutral element for $\ominus$. We expect that trust graph G is a strongly connected graph with maximum circuit weight $\bar{1}$. We use a k-closed semiring($k > 0$) to calculate path value along trust path in graph. A k-closed semiring $(K, \oplus, \otimes, \bar{0}, \bar{1})$ is closed if

- for all $a \in K$, the infinite sum $\bigoplus_{n=0}^{\infty} a^n$ is well-defined.
- *associativity, commutativity, and distributivity* apply to countable sums. Thus, for any three countable sets $(a_i)_{i \in I}$ and $(b_j)_{j \in J}$ with $A = \bigoplus_{i \in I} a_i \in K$, $B = \bigoplus_{j \in J} b_j \in K$, the following properties hold:
  - *Associativity.* for any partitioning of I in $I_k, k \in K$, $\bigoplus_{i \in I_k} a_i \in K$, and $A = \bigoplus_{k \in K} (\bigoplus_{i \in I_k})$, and a similar property holds with $\otimes$.
  - *Commutativity.* let I' be a permutation of I, then $\bigotimes_{i \in I'} a_i \in K$, and $A = \bigotimes_{i \in I'} a_i$.
  - *Distributivity.* $\bigotimes_{i \in I, j \in J} (a_i, b_j) \in K$, and $A \bigotimes B = \bigoplus_{(i,j) \in I \times J} (a_i \otimes b_j)$.

Property 2. A semiring $(K, \oplus, \otimes, \bar{0}, \bar{1})$ is k-closed if

$$\forall a \in K, \quad \bigoplus_{n=0}^{k+1} a^n = \bigoplus_{n=0}^{k} a^n. \tag{8}$$

Let well-formed decomposable path problems be defined as those for which $\oplus$ is commutative and associative, and $\otimes$ is associative and distributes over $\oplus$, formally as semiring model. These may be computed using generalized transitive closure algorithms.

Table 1: Pseudocode of construct credential graph and initialize

	INITIALIZE(G, s)
1	Procedure Initialize(G,s)
2	*GetCredentials(C)*
3	*ConstructCreditialsGraph(G, C)*
4	*For each vertex* $v \neq s$ *do*
5	$d[i] \leftarrow r[i] \leftarrow \bar{0}$
6	$d[s] \leftarrow r[s] \leftarrow \bar{1}$
7	$S \leftarrow s$

Thus far, we have assumed the graph is directed acyclic. The calculation model based algebraic structure semiring $(K, \oplus, \otimes, \bar{0}, \bar{1})$ provide appropriate framework to express the relation of trust and privacy. The aggregation over finite paths will converge.

3.3 Trust Path Search

We assume the trust graph is a simple connected graph without parallel arcs or loops, because a trust relationship is considered to be between two distinct entities and it is unique within a given trust context. S is a queue that contains the vertices to be examined next for their contribution to the shortest path weights. The vector $d[i]$ holds the current estimate of the shortest distance from s to i. The vector $r[i]$ holds the total weight added to since the last time i was extracted from S.

We present a generic algorithm to compute single-source shortest distances [11] for semirings covered by our framework. In Table 1 the pseudocode of the algorithm is presented for credential graph search based ordered semiring.

In Table 2, the function of $CalcPrivDiscloseProb(q, v, C)$ is to compute two neighbor nodes privacy disclosure value which is defined in Formula (2).

The computational complexity of this algorithm depends on the semiring used, and the actual topology of the network. The running time of this algorithm is $O(V+E)$, because each edge is visited once. The space complexity of this algorithms is $O(|V|^2)$. The more sparse the network, the more efficient for the algorithm [16].

4 Related Work

Theodorakopoulos and Baras [16] developed a novel formulation of trust computation as linear iterations based on ordered semirings, and it used edges tolerances approach to compute and analyze the attack resilience on the trust computation. Zhong and Bhargava [18] proposed a form of privacy-trust formulation to measure the quantify privacy loss. It is shown that as long as privacy

Table 2: Pseudocode of semiring path calculation

	SEMIRING-CHAIN-CALC (G, s)
1	*INITIALIZE (G, s)*
2	*While* $S \neq \Phi$
3	{ $q \leftarrow head(S)$
4	*Dequeue(S)*
5	$r' \leftarrow r[q]$
6	$r[q] \leftarrow \bar{0}$
7	*For each* $v \in Neighbour(s[q])$
8	$w[q, v] \leftarrow CalcPrivDiscloseProb(q, v, C)$
9	*If* $d[v] \neq d[v] \oplus (r' \otimes w[q, v])$
10	$d[v] \leftarrow d[v] \oplus (r' \otimes w[q, v])$
11	$r[v] \leftarrow r[v] \oplus (r' \otimes w[q, v])$
12	*If* $v \notin S$
13	$Enqueue(S; v)$
14	}
15	$d[s] \leftarrow \bar{1}$

loss is below a limit, through the use of use of properly coded credentials, it is possible to achieve arbitrarily good trust [12]. Lu et al. [10] proposed a trust-based privacy preservation method for peer-to-peer data sharing, which adopted the trust relationship between a peer and its collaborators that worked as a proxy to send the request and acquire the data. It provides a shield under which the identity of the requester and the accessed data cannot be linked. In [1], Ahmed et al. argued that statistical traceability could act as a basis for reaching a proper balance between privacy and trust. But it can't quantitate the privacy and evaluate the privacy risk when trust concentration.

Sun et al. [14] considered that trust is a measure of uncertainty with its value represented by entropy, and presented two trust models: entropy-based model and probability-based model, which based on recommendations for forwarding packets about other nodes, only applied to ad hoc networks. Yao et al. [17] proposed the notion of point-based policies for access control and gives protocols for implementing them in a disclosure-minimizing fashion. Specifically, Bob values each credential with a certain number of points and requires a minimum total threshold of points before granting access to a resource to Alice. In turn, Alice values each of her credentials with a privacy score that indicates her reluctance to reveal that credential. Bob's valuation of credentials is private and should not be revealed, as is his threshold. What Alice uses is a subset of her credentials that achieves Bob's required threshold for access, yet is of as small a value to her as possible. The author aimed at protecting service provider's security policy to protect privacy disclosure, but credential privacy has not been reinforced.

Bussard and Molva [2] use cryptographic primitive to design a privacy describing scheme based on a history of previous interactions among parties that ensure the past interactions can be proven while assuring the untraceability and anonymity. Their scheme is to aim at trust establishing with negotiation privacy [6]. In [3], Dong et al. proposed a cryptographic credential verification scheme for non-monotonic trust management systems that can correctly identify the credentials that a subject has while also protecting the subjects privacy. We introduced an algebra framework to describe trust establishing with risk disclosure evaluating when trust is propagating along a path in a monotonic trust policy environment.

5 Conclusion

We have presented an ordered semiring model that provided privacy protecting trust chain. Our scheme is based on semiring structure trust and privacy disclose calculation model, which provide an efficient way to protect credential chain minimum privacy disclosure in credential attributes when we establish the trust relationship. We also give the trust chain search algorithm based on an ordered semiring model.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grants 60573043 and 60773175, the Foundation of the Key Lab for Guangdong Electronic Commerce Application Technology(2007gdec0f002), and the Foundation of National Laboratory for Modern Communications under Grant 9140c1108010606. We would like to thank the anonymous reviewers for their valuable comments.

References

[1] M. Ahmed, D. Quercia, and S. Hailes, "A statistical matching approach to detect privacy violation for trust-based collaboration," *Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, WoWMoM 2005*, pp. 598-602, 2005.

[2] L. Bussard, and R. Molva, "Establishing trust with privac," *Security Protocols 2004*, LNCS 3957, pp. 199-209, 2006.

[3] C. Dong, G. Russello, and N. Dulay, "Privacy-preserving credential verification for non-monotonic trust management system," *MMM-ACNS 2007, CCIS 1*, pp. 171-186, 2007.

[4] S. Etalle, and W. H. Winsborough, "Integrity constraints in trust management - extended abstract," *Proceeding of 10th ACM Symposium on Access Control Models and Technologies (SACMAT)*, pp. 1-10, ACM, 2005.

[5] S. Gevers, "Privacy friendly information disclosure," *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops*, LNCS 4277, pp. 636-646, 2006.

[6] J. D. Groot, "Safeguarding privacy in trust negotiation," *3rd Twente Student Conference on IT*, pp. 1-10, Enschede, June 2005.

[7] A. Jϕsang, "Analysing topologies of transitive trust," *Proceedings of the First International Workshop on Formal Aspects in Security Trust (FAST2003)*, pp. 9-22, 2003.

[8] K. Krukow, and A. Twigg, "Distributed approximation of fixed-points in trust structures," *25th IEEE International Conference on Distributed Computing Systems*, pp. 805-814, 2005.

[9] K. Krukow, and M. Nielsen, "Trust structures: denotational and operational semantics," *International journal of Information Security*, vol. 6, pp. 153-181, 2007.

[10] Y. Lu, W. Wang, D. Xu, and B. Bhargava, "Trust-based privacy preservation for peer-to-peer data sharing," *IEEE Transactions on Systems, Man, Cybernetics, Part A*, vol. 36, no. 3, pp. 498-502, 2006.

[11] M. Mohri, "Semiring frameworks and algorithms for shortest-distance problems," *Journal of Automata, Languages and Combinatorics*, vol. 3, pp. 321-350, 2002.

[12] G. R. Murthy, "Fundamental limits on a model of privacy-trust tradeoff: information theoretic approach," *International Journal of Network Security*, vol. 3, no. 2, pp. 183-187, 2006.

[13] J. M. Signeur, and C. D. Jensen, "Trading privacy for trust," *2nd International Conference on Trust Management*, vol. 2995, pp. 93-107, 2004.

[14] Y. L. Sun, W. Yu, and Z. Han, "Information theoretic framework of trust modelling and evaluation for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 305-317, 2006.

[15] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression," *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, vol. 10, no. 5, pp. 571-588, 2002.

[16] G. Theodorakopoulos, and J. S. Baras, "On trust models and trust evaluation metrics for Ad hoc networks," *Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 318-328, 2006.

[17] D. Yao, K. B. Frikken, M. J. Atallah, and R. Tamassia, "Point-based trust: define how much privacy is worth," *ICICS 2006*, LNCS 4307, pp. 190-209, Springer-Verlag, 2006.

[18] Y. Zhong, and B. Bhargava, "Using entropy to trade privacy for Trust," *Proceedings of Security and Knowledge Management(SKM)*, pp. 76-84, 2004.

Mingwu Zhang is a Ph.D. candidate at South China Agricultural University. He received his M.S. degree in computer science and engineering from Hubei Polytechnic University, China, 2000. He is a senior member of Chinese Computer Federation (CCF), and a member of IEEE Computer Society. His research interests include network and information security, embedded computing, and trusted computing (E-mail: zhangmw@scau.edu.cn).

Bo Yang received the B. S. degree from Peking University in 1986, and the M. S. and Ph. D. degrees from Xidian University in 1993 and 1999, respectively. From July 1986 to July 2005 he had been at Xidian University, from 2002, he had been a professor of National Key Lab. of ISN in Xidian University, supervisor of Ph.D. In May 2005, he had served as a Program Chair for the fourth China Conference on Information and Communications Security (CCICS 2005). He is currently a professor and supervisor of Ph.D. at College of Information, South China Agricultural University. He is a senior member of Chinese Institute of Electronics (CIE), a member of specialist group on information security in Ministry of Information Industry of P.R.China and a member of specialist group on computer network and information security in Shanxi Province. His research interests include information theory and cryptography (E-mail: byang@scau.edu.cn)

Shenglin Zhu is a Ph.D. candidate at South China Agricultral University. His research interests include cryptography and information security, distributed network and trust model.(E-mail: zhusl@scau.edu.cn).

Wenzheng Zhang is a senior research fellow in National Laboratory for Modern Communications, China. He is a senior member of Chinese Computer Federation (CCF). His research interests include distributed network and information security, and trusted computing (E-mail: wzzhang@163.com).