http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 8 (6): 887-894, 2009
ISSN 1812-5638

Fair Blind Signature Based Authentication for Super Peer P2P Network

Xiaoliang Wang and Xingming Sun
School of Computer and Communication, Hunan University, Changsha, 410082, China

Abstract: Anonymity has received increasing attention in the literature due to the users' awareness of their privacy nowadays. While, anonymity related issues have been extensively studied in Peer-to-Peer (P2P) systems, numerous concerns have been raised about the issue of providing authentic partners in P2P systems. In addition, the network authority requires controlled anonymity, so that misbehaving entities in the network remain traceable. We are working on seeking novel and more effective methods to control anonymity, authentication and traceability. In this study, we propose a security architecture to ensure anonymity and authentication for honest users and keep traceability for misbehaving users in P2P systems. We use Fair Blind Signature Trust (FBST) to resolve the conflicts among anonymity, authentication and traceability. Signature scheme that has information about identity ensures authentication. At the same time, use of blind signature and additional anonymous scheme provides anonymity. Moreover, traceability is achieved due to the fairness of fair blind signature. Security analysis shows that the FBST can perfectly solve tradeoff between anonymity, authentication and traceability.

Key words: P2P, anonymity, authentication, traceability, fair blind signature

INTRODUCTION

As an emerging model of communication and computation, Peer-to-Peer (P2P) networking has recently gained significant attention.

Numerous concerns have been raised about the issue of providing authentic partners in P2P systems. To guarantee authentic responders, some researchers have built trust models to help peers verify the validity of other entities. A number of approaches have been proposed to provide reliable authentication in the P2P systems. Some use reputations or web of trust as authentication access. Such as Eigen trust (Kamvar *et al*., 2003) provides each peer in the network a unique global trust value based on the peer's history of uploads and thus aims to reduce the number of unauthentic files in a P2P network. The NICE (Lee *et al*., 2003) provides a platform to implement distributed cooperative applications. Based on trust chains, NICE computes a user reputation in a PGP-like model. By employing an asymmetric cryptographic algorithm, it requires peers to encrypt cookies to help others compute their reputations. Other researchers have adopted cryptography to attain security authentication (Akleylek *et al*., 2005; Lua, 2007; Narasimha *et al*., 2003). For example, Lua (2007) proposed a hybrid security protocol by unifying the ID-based cryptography and online secret sharing schemes. His scheme can verify the peers' identities by easily obtaining the ID-based public signature verification key of every other peer from the peer identifier in the P2P overlay networks.

At the same time, privacy is an important issue in current P2P systems. Taking Gnutella as an example, the identity of a requesting peer can only be hidden to further peers, but visible to all his neighbors. The identity of a peer, who responds with query results is exposed to every peer in the returning path. Privacy is demanded in P2P systems. Hence, a number of methods have been proposed to provide anonymity such as P5 (Sherwood *et al*., 2002) and APFS (Scarlata *et al*., 2001), Tarzan (Freedman and Morris, 2002) and MorphMix (Rennhard and Plattner, 2002). Most, if not all of them, deliver messages via., non-traceable paths comprised of several anonymous proxies or middle agent peers or adopt onion router technique (Syverson, 1998). For example, in APFS (Scarlata *et al*., 2001), peers construct an anonymous path with tail peers using an onion technique, providing complete and mutual anonymity for peers. However, failure to support authentication makes these approaches vulnerable to impersonation and man-in-middle attacks.

In addition, we must be concerned about anonymous abuse problem. That is, how to make anonymity controlled and traceable. Now anonymity abuse is severe. For example, some malicious peers use anonymity

Corresponding Author: Xingming Sun, School of computer and Communication, Hunan University, Changsha, 410082, China
Tel: 86-731-8821341 Fax: 86-731-8821341

systems to send a large number of packets to a certain peer. This behavior will lead to network congestion so that the peer is single point of failure in P2P communication. Some peers send anonymously malicious messages in P2P reputation systems to slander other peers. In P2P resource share, some attacking peers can use anonymity systems to create and spread virus or polluted resource.

These three considerations lead to the conclusion that P2P systems must have some methods that can satisfy not only anonymity but also authentication and traceability. However, for one peer to authenticate and trace others, he needs to know the identity of the other peers, which affects anonymity. Thus, there exists an inherent contradiction between anonymity and trust or traceability in P2P systems. To the best of our knowledge, there is no existing P2P protocol that provides anonymity as well as authentication and traceability.

How to design an anonymity, authentication and traceability protocol in P2P systems?

Some researches use zero knowledge authentication to tradeoff anonymity and authentication in P2P systems (Lai-Cheng, 2008; Lu *et al*., 2008; Wierzbicki *et al*., 2005). To protect real identities, in the these papers, each peer is required to generate a pseudonym. They are able to verify these pseudo identities are not fake, but fail to tell who these pseudonyms are in some special situations. That is to say, authority has no way to trace peers of anonymity abuse. With the help of pseudonyms, some peers still can misuse anonymity.

In this study, we propose a fair blind signature authentication scheme called Fair Blind Signature Trust (FBST) for super-peer based P2P systems, where each peer, instead of using its real identity, owns an unforgeable and verifiable identity signature. The identity signature is signed by super peer through a fair blind signature method. Compared with above proposals, our scheme can, not only solve the posed traceability problem effectively but also provide defense against playback, eavesdropping and man-in-middle attacks. We also design a novel scheme based on Shamir threshold secret share to solve the peer compromise problem.

The key idea of our proposed protocol follows. A lightweight signature from a super peer is used to authenticate local peers. The signature of super peer, which can be verified by other super peers, is used as normal peer's real identity in P2P systems. At the same time, the blinding process of signature breaks the linkage between signature and identity. Additional anonymous methods also are proposed to enhance communication anonymity. Finally, the blind signature has fairness characteristic which retains traceability. To the best of our knowledge, the proposed approach is the first one that can achieve simultaneously the features of anonymity, authentication and traceability. Present security analysis shows that Fair Blind Signature Trust (FBST) is effective.

NETWORK ARCHITECTURE AND DESIGN GOALS

Network architecture: Present unstructured P2P systems often adopt super peer structure (Yang and Garcia-Molina, 2003), such as KaZaA (Liang *et al*., 2004), Gnutella2 (gnutella). As shown in Fig. 1, peers are partitioned into a set of logical groups called

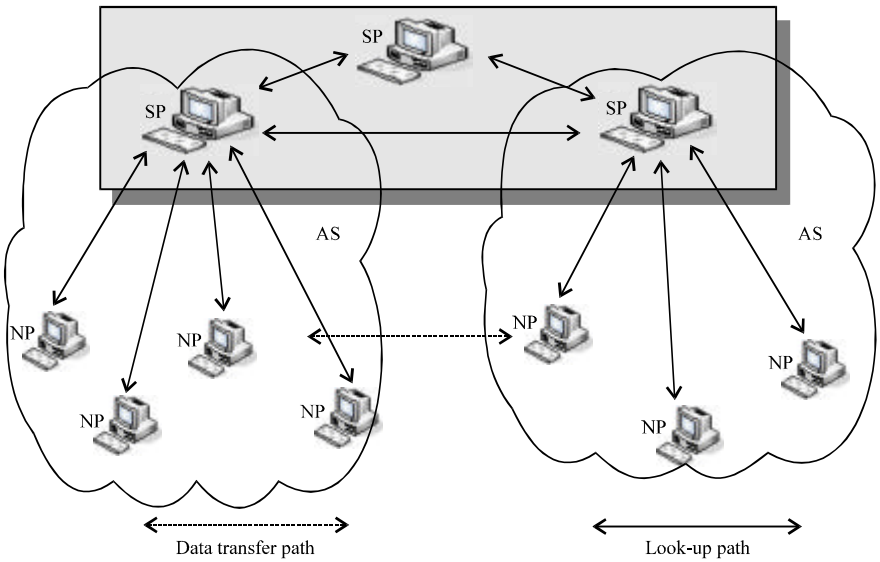

Fig. 1: Network architecture

Autonomous System (AS) by partitioning algorithms. Each AS selects a peer which has more capability of performance such as CPU processing, memory, bandwidth as the Super Peer (SP). The other peers are called Normal Peer (NP). The super peers save the information of the normal peer in the same AS. Normal peers discover and get the information of other peers through the super peers, then communicate with others directly. Super peers mode has a lot of remarkable advantages, such as Reduced time and bandwidth for search, autonomous units, manageability, load balancing and so on (Oh *et al*., 2008). Present proposed FBST is applicable on super-peer based peer-to-peer network.

Design goals: Fair Blind Signature Trust (FBST) is designed with the following goals:

- **Identity authenticity:** Intruders shall not be able to impersonate any innocent peer to send out a message without being detected
- **Traceability:** After a peer misuses anonymity, victim cooperating with authority can trace the malicious peer. This way, malicious behavior can be traceable
- **Resilience to a large number of peer compromises:** Even if a large number of peers, less than a certain threshold value, have been compromised, these peers shall have very low probability to threaten our proposed message authentication protocols
- **Privacy protection:** A sender of a message shall be able to protect its real identity if they keep legal behavior. Note that the protocol just considers protect senders' privacy, i.e., initiator anonymity and communication anonymity

CRYPTOGRAPHIC PRIMITIVES

Present scheme involves two cryptographic primitives: fair blind signature and Shamir threshold secret sharing. We describe them shortly below.

Fair blind signature: Blind signature (Chaum, 1983) is a protocol for obtaining a signature from a signer such that the signer's view of the protocol cannot be linked to the resulting message-signature pair. Blind signature schemes are used in anonymous digital payment systems. Since the existing proposals of blind signature schemes provide perfect unlinkability, criminals could misuse such payment systems. So, Stadler *et al.* (1995) has proposed a new type of blind signature schemes, called fair blind signature scheme. The scheme has the additional property that it is possible to link a message-signature pair and the corresponding protocol view of the signer.

Shamir secret sharing: Shamir (1979) showed how to divide data D into n pieces in such a way that D is easily reconstructable from any k pieces, but even complete knowledge of k−1 pieces reveals absolutely no information about D. This technique is based on polynomial interpolation: given k points in the 2-dimensional plane $(x, y)...(x_k, y_k)$ with distinct x_i's, there is one and only one polynomial q(x) of degree k−1 such that $q(x_i) = y_i$ for all i. Without loss of generality, we assume that the data D is (or can be made) a number. To divide it into pieces D_i, we pick a random k−1 degree polynomial $q(x) = a+a_1x^1+...+a_kx^k$ in which $a_0 = D$ and evaluate: $D_1 = q(1)$, ...,$D_i = q(i)$,..., $D_n = q(n)$. Given any subset of k of these D_i values (together with their identifying indices), we can find the coefficients of q(x) by interpolation and then evaluate D = q(0). Knowledge of just k−1 of these values, on the other hand, does not suffice in order to calculate D.

PROPOSAL: FAIR BLIND SIGNATURE TRUST SCHEME

The real challenge that underlies the tradeoff among authentication anonymity and traceability is that, on one hand, all existing P2P trust systems attempt to prove that anonym is an authorized entity while on the other hand; anonym does not want to reveal his real identity during communication transactions. This is where our proposed FBST design enters the picture. Instead of using their real identities in a P2P society, can a peer use a pseudonym signature to interact with others and accumulate his reputations? Clearly, if we attempt to adopt such a mechanism, we need to guarantee that an anonym has a unique signature from relative trusted entity before he begins to communicate with others. Here, we choose super peers as relative trusted entities due to super peers are often the best authentic peers elected by normal peers according to the present P2P reputation system (Karame *et al*., 2008). If the anonym misuses anonymity, collaborating with super peers and others group members, victim can trace the malicious peer.

Phase 1: Initialization: Initially, peers are partitioned into a set of logical groups called Autonomous System (AS) by partitioning algorithms (Ramaswamy *et al*., 2005). In every AS, peers elect the best authentic peer to act as the Super Peer (SP) according to SOBIE (Liu *et al*., 2008). We assume system is secure in the initialization phase. In this scheme, the Super Peer (SP) computes public modulus n = pq, where p, q are RSA-like primes and then generates a pair of RSA-like keys: a public e and a private one d. The following equation has to be true:

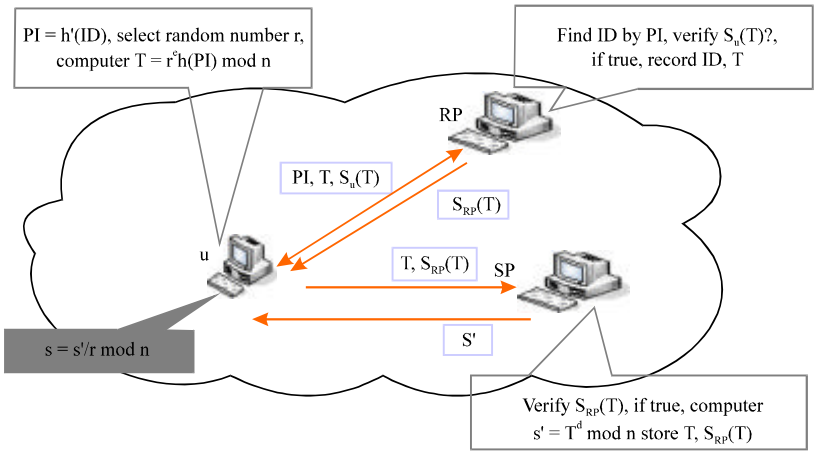

Fig. 2: Local signatures

$$e \times d = 1 \ (\mathrm{mod}(p-1).(q-1))$$

The pair (e, n) is made public. Besides, SP chooses a secure hash function h(•) and publish the h(•).

At the same time, in every AS, system designs a special trustworthy peers as the Registry Peer (RP). RP chooses a normal signature algorithm $S_{RP}(\bullet)$, then publishes it and corresponding public key for verification. In addition, RP creates some SHA-1 hash functions h_1', h_2'... and distributes different hash function to every normal peer by a secure connection. After this, RP records identity (ID) of every peer and hash function which is allocated to the peer.

Every Normal Peer (NP) in the AS also generates a normal signature algorithm $S_{NP}(\bullet)$ and publishes it.

Phase 2: Local signature: The five steps of local signature are outlined in Fig. 2.

NP logins at RP: A normal peer, called u, uses a hash function h' to compute his pseudo identity. This h' is obtained from RP in the initial phase. We assume the pseudonym is called PI_u, Piu = $h'(ID_u)$. ID_u can be user's network IP and port or other thing that can delegate identity. Then, u selects a random r, 1<r<n and computes $T = r^e h(PI_u) \bmod n$. Then, u sends Pi_u, T and $S_u(T)$ to RP through a secure channel.

$$U \rightarrow RP: Pi_u \| T \| Su(T)$$

RP verifies and signs: Since, RP has recorded identity (ID) of every peer and hash function which is allocated to the peer, he can deduce ID_u according to PI_u Then RP verifies whether $S_u(T)$ is consistent with the signature of T. If success, he records the pair (ID_u, T) and then sends $S_{RP}(T)$ to u. Otherwise the RP inform u of a failure message and the local signature process is aborted.

$$RP \rightarrow u: S_{RP}(T)$$

u authenticates message: In this step, u verifies whether T is consistent with $S_{RP}(T)$. If success, this proves that RP hasn't changed PI and then sends (T, $S_{RP}(T)$) to SP. In order to ensure anonymity, here, u use an anonymous method, called share flooding in SSMP (Han *et al*., 2005), to send (T, $S_{RP}(T)$) to SP.

$$u \rightarrow SP: \ S_{RP}(T) \| T$$

SP verifies and signs: Super Peer (SP) authenticates whether T is consistent with $S_{RP}(T)$. If success, SP computes $s' = T^d \bmod n$ and then send s' to u. Finishing this, SP keeps (T, $S_{RP}(T)$). A timestamp t_u, which is encrypted by e, is also included in the message from SP to u. It aims to prevent the message replay attack.

$$SP \rightarrow u: T^d \| e(t_u)$$

u computes and gets credential: u computes s = s'/r and gets signature. He preserves s and $e(t_u)$ as credential to communicate with strange peers. These strangers include peers not only in the same AS but also in the different AS.

Phase 3: Threshold pair sharing: In order to solve single point of failure of RP, in this case, RP should not maintain every pair (ID_u, T), but only a designated subset of neighbor peers have to do so. The RP may divide the pair into pieces and send each piece to a peer, who has a high reputation relationship. A lot of (t, n) threshold schemes have been proposed (Blakley, 1979; Shamir, 1979). In

FBST, we adopt shamir threshold secret sharing to design a secure scheme for the pair (ID_u, T) decentralization. A designated subset of peers would be chosen after the signing process. Creditable peers subset can be selected according to EigenTrust (Kamvar *et al.*, 2003). Sharing secret, i.e., pairs (ID_u, T), involves the following steps:

- According to EigenTrust, every peer can gain a unique global trust value. The SP selects n peers having good global trust value. We use $P_1, P_2,...,P_n$ to denote the n peers and call them witness peers
- The RP prepares to divide the pairs (ID_u, T) into n peers, respectively. We use S to denote binary series of pair (ID_u, T). To share secret s among n entities and ensure that no less than t participants are required to recover the secret, RP creates randomly a polynomial f(x) of degree t−1 in a finite field GF(p):

$$f(x) = a_0+a_1x+....+a_{k-1}x^{k-1}$$

The coefficient a_0 is the secret S. p is a large prime number which is 10^{200} magnitude and fulfills p = 1 (mod 8).

- RP chooses n random distinct evaluation points: x_i and secretly distributes the $S_i = (x_i, f(x_i))$, i = 1...n
- RP distributes $S_1, S_2,...,S_n$ to $P_1, P_2,...,P_n$, respectively

At last, the RP should erase all the correlated information from its memory or, after completion of this process, RP will not participate in other sub-protocols. It keeps itself offline, but awake periodically in order to deal with above register apply from newer peers. At the same time, those peers that have overdue signatures also renew their login at RP and get updated signature. If only more than t peers cooperate, the pair (ID_u, T) can be retrieved.

Phase 4: Anonymous and authentication communication: After u has gotten blind signature from SP, when he want to request resource of other peers anonymously, he use anonymous multicast (Grosch, 2000) to connect with SP. Because anonymity of multicast, the SP can not know which one is the u, but he can recognize the blind signature. There are two cases: local anonymous access and multi-domain anonymous access.

Local anonymous access: If the resource requested by u is in the local AS, since, SP has saved the information of the normal peer in his AS, he verifies the blind signature. In case of success, a normal query is sent to the peer who has the resource. Then, the peer utilize anonymous multicast to send resource to the anonym, i.e., u.

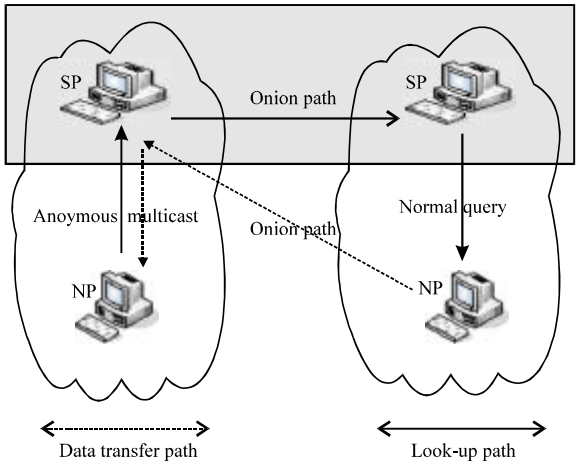

Fig. 3: Anonymous and authentication communication

Multi-domain anonymous access: The steps of multi-domain anonymous access are shown in Fig. 3.

If the local SP has not information about resource that u requested, he will use onion router to connect with other SP to transmit look-up query of u. Onion router protects communication anonymity. Other selections of anonymous protocols are possible, but such changes are out of the scope of this discussion. In order to make opposite SP know the other SP s' signatures, some extra mechanisms must be provided to ensure this. Some kind of PKI in the P2P systems have been proposed (Chen *et al.*, 2008; Pathak and Iftode, 2006). We can use them establish PKI in our FBST system, so super peers can verify each other's signatures. If the look-up message in possession of a blind signature and a timestamp has passed the verification of the opposite SP, the SP will normally transmit the message to local normal peer who has the resource. The opposite normal peer has created a SP-Table. In this Table, information about some super peers in other AS is recorded. Once the opposite normal peer receives a query, it compares query with its local SP-Table. If the information belongs to an existing record, it uses onion path to connect with opposite SP anonymously. Eventually the opposite SP implements anonymous multicast to send the resource to u.

Phase 5: Trace malicious peer: If some anonymity misuse appears, for example the malicious peer is u, SP can cooperate with RP to retrieve the signing protocol view and associated identity of the initiator corresponding to the signature. The process follows:

- When RP is on line, SP sends the signature that u use as access credential in communication to RP

- RP collects witness peers who have preserved the fragment of pair (ID_u, T) and cooperates with WPS to resume ID_u. Use S to denote binary series of pair (ID_u, T)

In order to recover S, RP must first recover f(x) using polynomial interpolation and then compute S = f(0). This operation requires at least t distinct shares. RP chooses t peers from n witness peers and then utilizes the t-share subset to reconstruct the secret pair. Using Lagrange formula, given t points (x_i, y_i), i = 1...t, RP have:

$$f(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{x - x_j}{x_i - x_j} \pmod p$$

Thus:

$$S = f(0) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{-x_j}{x_i - x_j} \pmod p$$

The complexity of Lagrange interpolation is $o(t \log_2 t)$.

SECURITY ANALYSIS

Fundamental security objectives: It is distinct to show that our security architecture satisfies the security requirements for authentication, confidentiality, which follows directly from the employment of the standard cryptographic primitives, namely, digital signature, onion router, in this system. It can defend following attacks:

Impersonate: The data which u sends to RP includes pseudo identity of u. So, other peers can't impersonate the user in the register process since they do not pass RP's verification. The difficulty of other users impersonating u is equal to attack SHA-1 hash algorithm. Even Wang *et al.* (2005) has found collisions in the full SHA-1, it is also difficult to attack it in practical situation.

Tamper: The data, which RP send to u, can't be changed by RP. Otherwise, (T, $S_{RP}(T)$) phase 2 can't pass u's verification. If RP change PI to PI`, it must select additional r` which fulfill $T = (r`)^e h(PI`) \bmod n$. This is equal to attack RSA system. On the other hand, the data which u sends to SP is signed by RP. So, u can't modify blind message. The difficulty of changing message is equal to attack RP's signature algorithm $S_{RP}(\bullet)$.

Peer compromise: As specified in phase 3, present protocol aims to protect the RP from being compromised. By distributing the secret pair (ID_u, T) to t peers who have good reputations, we alleviate the need to trust RP. In our protocol, t peers participate in the computation and keep (ID_u, T) value of others. As a consequence, to get real identity, this operation requires at least t distinct shares. There is a t−1 degree polynomial that pass through t−1 points. Thus, t−1 compromised peers cannot guess anything about secret. Note that the sink may tolerate up to p−t nonresponding peers and still be able to recover secret. Therefore, this scheme provides confidentiality and robustness against peer compromise attacks even in the presence of a few compromised peers.

Anonymity: First of all, it can be easily shown that local SP can not link a legitimate network access activity to the real identity. Because the u communicates with SP by anonymous multicast and signature is generated by the local SP using a blind signature, SP solution for the real identity from the signature is equivalent to solving the RSA algorithm. Furthermore, Man-in-the-Middle can not compromise anonymity due to onion path. Due to the use of signatures in authentication, which reveals no information about the real identity, distant super peers can only verify the signature without knowing anything about the identity of the u. At the same time, distant super peers trust u only due to introduce of local SP. Every one cannot deduce the identity of u solely.

Traceability (conditional anonymity): Any practical authentication mechanism must allow for identity revocation. In the design of FBST, authority might intend to revoke a peer's identity because the peer in possession of blind signature as credential is compromised or misbehaving. The proof follows from fairness of fair blind signature (Stadler *et al.*, 1995), since the adopted fair blind signature scheme in our security architecture achieves restrictiveness. In other words, before blind signature, in the process of register, peer's real identity is linkable to our system. This linkable information is brought to its signature. No matter how he behaves anonymously, the information is distributed and kept in some witness peers' hand. If necessary, authority can trace the peer identity. The detailed proof of fairness of fair blind signature can be referred to (Stadler *et al.*, 1995).

CONCLUSION AND FUTURE WORK

We propose an anonymous fair blind signature authentication protocol in this study, called fair blind signature trust. In this design, a fair blind signature based authentication scheme is designed to support trust management in anonymous P2P systems, so that peers may use unforgeable and verifiable signature instead of their real identities in P2P communities. Maybe, some

papers have considered trust or anonymity or traceability. However, none of them has focused on such three aspects at the same time.

We prove that the probability of a successful impersonation is computationally infeasible. We also manage to address peer compromise attacks in the FBST design. The result of security analysis shows that FBST has perfect scalability in P2P environments. We believe that wide deployment of Fair Blind Signature Trust will provide better privacy and security for P2P users.

However, We do not consider performance in practical P2P environments. Response time and traffic overhead will be addressed by experiments. At the same time, PKI assumption between super peers could be substituted for identity-based signature (Cui *et al*., 2008; Elkamchouchi and Abouelseoud, 2007; Hongzhen and Qiaoyan, 2007). Enhancing such aspects using our FBST scheme is the subject of future work.

ACKNOWLEDGMENTS

This study is supported by the National Grand Fundamental Research 973 Program of China (Grant No. 2006CB303000), the National Natural Science Foundation of China (NSFC No.60736016 and 60702065), Hunan Provincial National Natural Science Foundation of China (Grant No. 09JJ4033), National Basic Research Program 973 (Grant No. 2009CB326202), Science and Technology Program of Hunan Province (Grant No.2008FJ4221).

REFERENCES

Akleylek, S., L. Emmungil and U. Nuriyev, 2007. A modified algorithm for peer-to-peer security. Appl. Comput. Math., 6: 258-264.

Blakley, G.R., 1979. Safeguarding cryptographic keys. Proc. Natl. Comput. Conf. AFIPS., 48: 313-317.

Chaum, D., 1983. Blind Signatures for Untraceable Payments, Advances in Cryptology-Crypto '82. Springer-Verlag, Santa Barbara, CA, USA., pp: 199-203.

Chen, R., W. Guo, L. Tang, J. Hu and Z. Chen, 2008. Scalable byzantine fault tolerant public key authentication for peer-to-peer networks. Proceedings of the 14th International Euro-Par Conference on Parallel Processing Las Palmas de Gran Canaria, Spain, Aug. 26-29, Springer-Verlag, Berlin, Heidelberg, pp: 601-610.

Cui, W., Y. Xin, Y.X. Yang and X.X. Niu, 2008. Practical hierarchical identity based signature in the standard model. Proceedings of IEEE International Conference Neural Networks and Signal Processing, Jun. 7-11, Zhenjiang, China, Inst. of Elec. and Elec. Eng. Computer Society, pp: 416-421.

Elkamchouchi, H. and Y. Abouelseoud, 2007. A new blind identity-based signature scheme. Proceedings of the International Conference on Computer Engineering and Systems, No. 27-29, Cairo, Egypt, pp: 114-119.

Freedman, M.J. and R. Morris, 2002. Tarzan: A peer-to-peer anonymizing network layer. Proceedings of the 9th ACM Conference on Computer and Communications Security, Nov. 18-22, Association for Computing Machinery, Washington, DC, USA., pp: 193-206.

Grosch, C., 2000. Anonymisation services for IP multicast. Proceedings of the 25th Annual IEEE Conference on Local Computer Networks, Nov. 8-10, Tampa, FL, USA, pp: 2-9.

Han, J., Y. Liu, L. Xiao, R. Xiao and L.M. Ni, 2005. A mutual anonymous peer-to-peer protocol design. Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, Apr. 04-08, IEEE Computer Society, Denver, Colorado, USA., pp: 68-77.

Hongzhen, D. and W. Qiaoyan, 2007. An efficient identity-based short signature scheme from bilinear pairings. Proceedings of International Conference on Computational Intelligence and Security, Dec. 15-19, Harbin, Heilongjiang, China, Inst. of Elec. and Elec. Eng. Computer Society, pp: 725-729.

Kamvar, S.D., M.T. Schlosser and H. Garcia-Molina, 2003. The eigentrust algorithm for reputation management in p2p networks. Proceedings of the 12th International Conference on World Wide Web, Budapest, Hungary, May 20-24, ACM, New York, USA., pp: 640-651.

Karame, G., I.T. Christou and T. Dimitriou, 2008. A secure hybrid reputation management system for Super-Peer networks. Proceedings of the 5th IEEE Consumer Communications and Networking Conference, Jan. 10-12, Inst. of Elec. and Electronics Engineering Computer Society, Las Vegas, NV, USA., pp: 495-499.

Lai-Cheng, C., 2008. Heightening security of P2P networks by neighborhood key method. Proceedings of the 1st International Conference on Intelligent Networks and Intelligent Systems, Nov. 1-3, Wuhan, China, Institute of Elec. and Electronics Engineering Computer Society, pp: 201-204.

Lee, S., R. Sherwood and B. Bhattacharjee, 2003. Cooperative peer groups in NICE. Proceedings of IEEE INFOCOM, April, 2003, Institute of Electrical and Electronics Engineers Inc., San Francisco, CA, USA., pp: 1272-1282.

Liang, J., R. Kumar and K.W. Ross, 2004. The KaZaA overlay: A measurement study. Proceedings of the 19th IEEE Annual Computer Communications Workshop, Sept. 15, Florida, USA, pp: 1678-1685.

Liu, J., Z. Chen, D. Li and H. Liu, 2008. Towards a self-adaptive super-node P2P overlay based on information exchange. Proceedings of the 9th International Conference for Young Computer Scientists, Nov. 18-21, Zhang Jia Jie, Hunan, China, Inst. of Elec. and Elec. Eng. Computer Society, pp: 410-415.

Lu, L., J. Han, Y. Liu, L. Hu, J.P. Huai, L. Ni and J. Ma, 2008. Pseudo trust: Zero-knowledge authentication in anonymous P2Ps. IEEE Trans. Parallel Distributed Syst., 19: 1325-1337.

Lua, E.K., 2007. Securing peer-to-peer overlay networks from Sybil attack. Proceedings of International Symposium on Communication and Information Technology, Oct. 17-19, IEEE, Sydney, Australia, pp: 1213-1218.

Narasimha, M., G. Tsudik and J.H. Yi, 2003. On the utility of distributed cryptography in P2P and MANETs: the case of membership control. Proceedings of 11th IEEE International Conference on Network Protocols, Nov. 04-07, IEEE Computer Society Washington, DC, USA., pp: 336-345.

Oh, B.T., S.B. Lee and H.J. Park, 2008. A peer mutual authentication method on super peer based peer-to-peer network. Proceedings of the International Symposium on Consumer Electronics, Apr. 14-16, Institute of Electrical and Electronics Engineers Inc., Vilamoura, Portugal, pp: 487-490.

Pathak, V. and L. Iftode, 2006. Byzantine fault tolerant public key authentication in peer-to-peer systems. Comput. Networks, 50: 579-596.

Ramaswamy, L., B. Gedik and L. Liu, 2005. A distributed approach to node clustering in decentralized peer-to-peer networks. Proc. IEEE Transactions Parallel Distributed Systems, 16: 814-829.

Rennhard, M. and B. Plattner, 2002. Introducing MorphMix: Peer-to-peer based anonymous internet usage with collusion detection. Proceedings of the ACM Conference on Computer and Communications Security, Nov. 21, Association for Computing Machinery, Washington, DC, USA., pp: 91-102.

Scarlata, V., B.N. Levine and C. Shields, 2001. Responder anonymity and anonymous peer-to-peer file sharing. Proceedings of the 9th International Conference on Network Protocols, Nov. 11-14, Riverside, CA, United states, Institute of Electrical and Electronics Engineers Computer Society, pp: 272-280.

Shamir, A., 1979. How to share a secret. Commun. ACM, 22: 612-613.

Sherwood, R., B. Bhattacharjee and A. Srinivasan, 2002. P^5: A protocol for scalable anonymous communication. Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, May 12-15, Institute of Electrical and Electronics Engineers Inc., Berkeley, CA, USA., pp: 58-70.

Stadler, M., J.M. Piveteau and J. Camenisch, 1995. Fair blind signatures. Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, 1995, Saint-Malo, France, Springer-Verlag GmbH and Company KG, pp: 209-219.

Syverson, P.F., 1998. Anonymous connections and onion routing. IEEE J. Selected Areas Commun., 16: 482-494.

Wang, X., Y.L. Yin and H. Yu, 2005. Finding Collisions in the Full SHA-1. In: Advances in Cryptology-CRYPTO 2005, Shoup, V. (Ed.). Springer Verlag, New York, ISBN: 978-3-540-28114-6, pp: 17-36.

Wierzbicki, A., A. Zwierko and Z. Kotulski, 2005. Authentication with Controlled Anonymity in P2P Systems. In: Parallel and Distributed Computing, Applications and Technologies. Dalian, China, 2005. Institute of Electrical and Electronics Engineers Computer Society, Washington, DC, USA., ISBN:0-7695-2405-2, pp: 871-875.

Yang, B. and H. Garcia-Molina, 2003. Designing a super-peer network. Proceedings of the 19th International Conference on Data Engineering, Mar. 5-8, Institute of Electrical and Electronics Engineers Computer Society, Bangalore, India, pp: 49-60.