International Journal of Multimedia and Ubiquitous Engineering
Vol.9, No.2 (2014), pp.141-152
http://dx.doi.org/10.14257/ijmue.2014.9.2.14

A Reputation System Preserving the Privacy of Feedback Providers and Resisting Sybil Attacks

Keli Zhang[1], Zhongxian Li[1,2] and Yixian Yang[1]

[1]*Information Security Center, Beijing University of Posts and Telecommunications, 100876, Beijing, China*
[2]*Nation Cybernet Security Limited, 100080, Beijing, China*

kelicybergirl@163.com

Abstract

Users hesitate to submit negative feedback in reputation systems due to the fear of retaliation from the recipient user. A Preserving reputation system which does not require continuous online communication with a trusted third party is proposed, Peers in this trust model use a verifiable random function, non-interactive zero-knowledge and ratee's transaction identities, to generate evaluation tags, so as to anonymously evaluate the transaction objects and hide the identity of the transaction process. Analysis shows the scheme guarantees the privacy of feedback providers resists the inherent Sybil attacks in preserving reputation system and evidently improves the accuracy of trust accumulated value compared with existing trust models.

Keywords: *privacy, anonymity, pseudonym, Sybil attack, reputation*

1. Introduction

Reputation system is introduced into the security field as a concept of sociology. It can dynamically describe the trust relationships between peers, and judge whether the counterparts are credible according to the reputation value. However, the accumulation of reputation value mainly depends on the evaluation values of other nodes. Therefore, to obtain the authentic accumulated reputation value, the reputation evaluation values must be guaranteed to be real and reliable. However, in current reputation system, many users are reluctant to provide real reputation evaluation value, especially the negative evaluation value due to the fear of retaliation from the recipient user [1]. Meanwhile, as the evaluation information records all transactions of the users, some malicious users or unlawful people will connect all the transaction data of users to conduct systematic analysis and completely expose the activities and hobbies of all users, which will produce serious threats to the privacy of users.

To preserve privacy of interest, some anonymizating techniques can be used to conceal the real identities of network nodes which can be practically implemented by existing anonymous credentials that rely on pseudonymization. For instance, in one system under the distributed environment, a peer's reliability is calculated based on Secure multiple computation (SMC) [2]-4], this system ensures that honest users can provide real evaluation information, but it cannot identify the anonymous raters who provide false evaluation information. Game theory can be relied on to ensure that the two transaction parties provide fair evaluation information [5]-[6]; this system can resist slandering attacks, but not collusive attacks, Sybil Attacks [7]. In another reputation system, users

ISSN: 1975-0080 IJMUE

perform transaction and evaluation in connectionless Pseudonyms [9], but the complete anonymity of identities is also easy to cause the reputation system to be lack of controllability and to suffer watershed, ballot-stuffing, bad mouthing and Sybil attacks. Moreover, frequent pseudonym updates may lead to extra overhead. More seriously, a sophisticated attacker can associate the changes of pseudonym of a particular node with its reputation updates and further trace back the historic behavior. In addition, the anonymity of identities also does not comply with some business specifications.

This indicates that an implicit trade-off exists between node anonymity and reputation, and it must be examined and balanced to an appropriate extent for attaining secure, dependable, and effective reputation management. This paper proposes a privacy-preserving reputation system. The nodes use the real identities for transaction. The trust information used to evaluate the reputation of users is associated to rater's evaluation tags based on non-interactive zero-knowledge, verifiable random function (VRF) and identities of ratees, evaluation tags are not connected to the real identities of raters, which can protect the real identities of raters and the privacy of ratees. Without requiring continuous online availability of a trusted third party, each peer may be randomly assigned a number of trust value management peers. The trust management peers and the managed nodes are mutual anonymous so as to guarantee the two peers are not connected. In addition, applying special public key encryption of trust management peers can ensure the trust value will not be intercepted by ratees as well as some more malicious peers in its transmission process. Moreover, the presented scheme provides inherent detection and mitigation of Sybil attacks.

2. Related Work

There are many papers on reputation systems for peer-to-peer networks. Most focus on building distributed reputation systems, rather than worrying about privacy; [9]is typical. Recently, a number of papers have addressed the issue of reputation and privacy. A typical approach is typified by [10], who incorporate privacy into their scheme. However, their system does not provide unlinkability. It also requires a trusted "observer" module for full functionality. Recently a new cryptographic primitive called *signatures of reputation* was proposed in [11] for supporting monotonic measures of reputation while keeping anonymous. But this scheme is built from the scratch and cannot be generally applied to other reputation systems. Another work is Voss [12] and Steinbrecher [13]. In both of the systems, peers interact with each other through pseudonyms, and reputation is strongly connected to identities. In [13] reputation points are implemented as coins, which may have positive or negative value. However, these systems either rely on TTPs or centralized constructs to ensure unlinkability between identities and pseudonyms, such as the \bank". In contrast, our reputation protocols are decentralized. The work by Omar Hasan [2] is close to ours, However, the system in[2] differs from ours in two notable ways. First, it hides the reputation scores of the rater and computes reputation in a privacy preserving manner. Second, it cannot identify and resist Sybil attack.

3. Preliminaries

3.1. Bilinear Maps

Let G_1, G_2, G is a cyclic group of prime order q, g_1 is a generator of G_1, g_2 is a generator of G_2, γ is an efficiently computable isomorphism from G_1, G_2 ,with $\gamma(g_2) = g_1, \gamma(h_2) = h_1$; e is an efficiently computable bilinear map $e: G_1 \times G_2 \to G$ such that

1) (Bilinear) for all $g_1 \in G_1, g_2 \in G_2,$ and $a,b \in Z_q, e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$;
2) (Non-degenerate) if g_1 is a generator of G_1, g_2 is a generator of G_2 then $e(g_1, g_2)$ generates G.

3.2. Strong RSA Assumption

Given an RSA modulus n and a random element $g \in Z_n^*$,it is hard to compute $h \in Z_n^*$ and integer e > 1 such that $h^e \equiv g \bmod n$. The modulus n is of a special form pq, where $p = 2p'+1$ and $q = 2q'+1$ are safe primes.

3.3. CL Signatures

Camenisch and Lysyanskaya [14] came up with a secure signature scheme with two protocols: (1) An efficient protocol for a user to obtain a signature on the value in a Pedersen (or Fujisaki-Okamoto) commitment without the signer learning anything about the message. (2) An efficient proof of knowledge of a signature protocol between a user and a verifier. These signatures are secure under the strong RSA assumption. Using bilinear maps, we can use other signature schemes for shorter signatures.

3.4. DY Pseudorandom Function

Let $G =< g >$ be a group of prime order q, $s \in Z_q$. Dodis and Yampolskiy recently proposed a pseudorandom function $F_{g,s}^{DY}(x) = g^{1/(x+s+1)}$, $x \in Z_q^*$. This construction is secure under the *y*-DDHI.

3.5. Pedersen commitment

Pedersen proposed a perfectly-hiding, computationally-binding commitment scheme based on the discrete logarithm assumption, in which the public parameters are a group of prime order q, and generators $(g_0, ..., g_m)$,in order to commit to the values $(v_1, ..., v_m) \in Z_q^m$,set $C = PedCom(v_1, ..., v_m; r) = g_0^r \prod_{i=1}^m g_i^{v^i}$, $r \in Z_q$.

3.6. Non-Interactive zero- Knowledge Proof

Camenisch and Stadler give Based on discrete logarithms zero-knowledge proof identification, set $PK\{(\partial, \beta, \gamma) : y = g^{\partial} h^{\beta} \wedge y = g^{\partial} h^{\beta}\}$, represents the zero-knowledge proof integer, We can apply the Fiat-Shamir heuristic to turn such proofs of knowledge into signature proofs of knowledge on some message m,set $SPK\{(\alpha) : y = g^{\partial}\}(m)$.

4. Protocol Description

We now detail the solution that we propose to design an accurate and privacy-preserving reputation mechanism.

4.1. Protocol Overview

Our schemes are based on the signature schemes with protocols due to Camenisch and

Lysyanskaya [14]. These schemes allow a user to efficiently obtain a signature on committed messages from the signer. They further allow the user to convince a verifier that she possesses a signature by the signer on a committed message. Both of these protocols rely on the Pedersen commitment scheme.

Before joining in the system, each peer obtains a trust evaluation container based on a CL signature [14], from a trusted Third party (TTP).the container is comprised of seed s for the VRF, the peer's private key S_i and the TTP's signature $\sigma_{TTP}(S_i, s)$.

Whenever peer i contracts a bootstrap server [15] for joining the network, the bootstrap server will assign a number of trust value management peers and generate the special public-private key pairs for the trust value management peers.

After two peers interacts in real identity, the two peers mutual give anonymous proof-of-interaction. rater submit the trust value associated to raters' evaluation tags which is generated by the seed s, ratee's ID and VRF function to the TVM peers. Then the TVM peers verify the trust value.

On receiving a trust query for peer i, its TVM peer can generate a reply and forward it back to the network. Querying peer can take a majority vote amongst them and selects that value.

4.2. Protocol outline

The important steps of the protocol are outlined below:

1) Initialization

a) At first, we assume that each peer who wants to participate in the network owns a unique, initial identifier ID and is equipped with two coups of public-private pairs $< P_i, S_i >$ and $< P_i', S'_i >$. $< P_i, S_i >$ is used as the container for signature, encryption and decryption as well as obtaining evaluation certificates container. $< P_i', S'_i >$ is used as the trust value management peer for other peers in the network. P_i and P_i' stand for public key while S_i and S'_i refer to private key.

b) Peer i need to obtain the container for trust evaluation from a trusted Third party (TTP) that is trusted by all involved parties before joining the network. The implementation of protocols is based on CL signature. The details protocol are as below:

- Peer i identifies himself to the TTP by proving knowledge of S_i.
- In this step, the peer and TTP negotiate a commitment value *C*: The peer selects a random $s' \in Z_q$ and computes $C' = PedCom(SK_u, s', r)$. Then peer sends C' to TTP to verify the legitimacy of C' formation. On the other hand, TTP sends a random $r' \in Z_q$, the peer and TTP locally calculate $C = C' g_T^{r'} = PedCom(S_i, s'+r'; r) = PedCom(S_i, s; r)$, and then the peer compute $s = (s'+r') \bmod q$
- The peer and TTP run CL signature protocol for obtaining TTP's signature on committed values contained in Commitment *C*,As a result,peer i obtains $\sigma_{TTP}(S_i, s)$. As it is based on CL signature protocol, TTP is unable to know the value of S_i, s.
- Peer i saves the certificate container $W = (S_i, s, \sigma_{TTP}(S_i, s))$, where *s* is evaluating certificate container secret and $\sigma_{TTP}(S_i, s)$ is the TTP's signature.

2) Trust value management peer Select

In distributed environment, there is no trusted third party which stores trust values for peers. If nodes are allowed to calculate and store trust value by themselves, peers can randomly forge trust value. Eigenrep [16] presented an alternative approach to manager and store the trust values of the peers. In Eigenrep, every node has a set of mother peers that hold the trust values for the node. The mother peers are based on a DHT based mechanism like CAN [17] or Chord [18] hashing the ID of the node using different hashes. However, the kind of approach is easy to suffers from a number of attacks: 1) man-in-the-middle attack; 2) No anonymity. Mother peers are easy to be exposed and become the attack targets to prevent them from sending the trust values by malicious node. 3) The mother nodes are easy to be connected with the mapped node to obtain the evaluation records and identities of evaluators.

The model introduces a bootstrap like Trustme [15]which randomly distributes trust value management (TVM) peers to each node in the network. The bootstrap is equipped with a couple of public-private key pair $< P_{BS}, S_{BS} >$, P_{BS} stands for the public key and S_{BS} refers to the private key. The bootstrap sever assigns a trust value management identifier to the peer i denoted by VID_x, $VID_x = P_{BS}("ValidNode" | P'_i)$ .Any node can verify VID_x but does not compromise the real identity of peer. So the identifies of TVM peers are unknown to all nodes. Any peer j that interested in querying for the trust value of peer i can broadcast information for getting trust value. The TVM peers reply the trust value. After a transaction, peer j can securely submit the peer i' trust value to the TVM peers of the peer i. The TVM peers can compute the trust rating of peer i. To provide security and reliability, model uses smart public key cryptography mechanisms.

3) Peer join

a) Whenever Peer i contacts the bootstrap server to for joining the network, firstly it generates the tag of $\mathrm{Tag_s} = F_{g,s}^{DY}(H(\mathrm{ID})) = g^{1/s+H(\mathrm{ID})+1}$ to resist the Sybil attack based on the secret key *s* of evaluation certificate container and its own ID.

b) The peer i broadcast $<\mathrm{ID_i}, \mathrm{Tag_s}, \phi>$ in the network. Node only need to verify the legitimacy of the $\mathrm{Tag_s}$, If they become the peer i's TVM peers. Otherwise other nodes saves $<\mathrm{ID_i}, \mathrm{Tag_s}, \phi>$ in the database and temporarily do not have to verify the legitimacy of $\mathrm{Tag_s}$.

c) The bootstrap generate a private-public pair $< MP_i, MS_i >$ for peer i, which does not represent identities but is regarded as authentication mechanism. These nodes who own private key MS_i stand for the trust value management nodes of peer *i*. The bootstrap gives MP_i to node i. The bootstrap server select a number of peers that will serve as the TVM peer for peer i and generates a TVM message for the TVM peer x: $TH_{BS}(i) = VID_x \mid P_{BS}(VID_x \mid P'_x(ID_i \mid P_i \mid MP_i \mid MS_i))$ .The message is broadcasted to the network and be given to peer i. Node x receives the message and update its local database. The message can be read by peer x who only know the S_i' .When other nodes submit trust evaluation value for i, they encrypt the trust value with MP_i so as to guarantee the secure transmission of trust value while ensuring only the trust value management node of node *i* can obtain the trust information.

4) Anonymous Proof-of-Interaction

Whenever two nodes (node i and node j) interact with the real identities, they need to exchange the proof of interaction with each other. Node i obtain a blind signature σ_{Bj} from node j.Peer j gets a blind signature σ_{Bi} from node i. The proof of interaction is to prevent that the malicious peers randomly rate the other peers. Another important use of the interaction message is that if a group of co-operating peers are attempting to boost each other's ratings, they will need to exchange such messages every time, thus making them pay for every malicious attempt. The blind signature is used to prevent the peer's TVM peers from inferring the real identity of the rater.

5) Trust value generation

After two nodes (node i and node j) interact, peer will generates trust value V for i, according to its satisfaction with i. The generation process of trust value is as follows:

1) j calculates $R = H(ID_i)$ and $V = H(r_i \| T_i)$; where H is collision-free one-way hash function, r_i is trust value, and T_i is time;

2) j generates evaluation tag: $Tag = F_{g,s}^{DY}(R)$

3) j generates a ZKPOK of $(S_j, s, \sigma_{TTP}(S_j, s))$ such that:

- $R = H(ID_i)$;
- $Tag = F_{g,s}^{DY}(R)$;
- $VerifySig(pk_{TTP}, (S_j, s), \sigma_{TTP}(S_j, s)) = true$

4) Let $B = PedCom(s)$, proves the commitment value of B is the CL signature of TTP;

5) Prove $Tag = F_{g,s}^{DY}(R) = g^{1/s+R+1}$.

More formally, this proof is the following proof of knowledge:

$$PK\{(\alpha, \beta) : g_T = B^{\delta} h_1^{\beta} \wedge Tag = g^{\delta} g^{R}\}$$

Use the Fiat-Shamir heuristic to turn all the proofs above into one signature of knowledge on the values (Tag, B, R, g_T, g). Call the resulting signature ϕ.

6) Trust value verifying and identifying Sybil Attacks

After peer j generates trust value V for i. It broadcast the V to the network. The only the TVM peer can read the message and that only a peer which actually interacted with i can generate and send the trust value .The trust value V is of the form:

$$ID_i \,|\, MP_i(ID_i, Tag_i, \sigma_{Bi}, \phi, r_i, T_i, (r_i, T_i)_{sig})$$

The TVM peers need to verify t legitimacy of the trust value. The detailed verification process is as follows:

a) TVM peers firstly verify whether the trust evaluation tag Tag_i is the same with peer i's resist Sybil attack Tag_s. If they are the same, directly implement 3); if not,

implement 2);

b) TVM peers need to verify the legitimacy of Tag_i .only if the TVM peer has stored legal Tag_i , directly execute 3);

c) TVM peers verify $(r_i, T_i)_{sig} = sign(1/s + R + 1, V)$. To ensure the non-repudiation, counterfeiting and resistance of replay attacks, evaluators need to run verifiable signature for trust value. The signature secret key is $1/s + R + 1$ and the verifiable secret key is $Tag = g^{1/s+R+1}$.

d) TVM peers verify whether σ_{Bi} has been used and whether it is the signature of *i*;

e) After trust value is verified, TVM peers deal with the trust value according to the verification results:

- If Tag_i is the same with Tag_s and $(r_i, T_i)_{sig}$ is legal, it can be judged as Sybil attack and *i* will be punished;
- If Tag_i is the same with Tag_s and $(r_i, T_i)_{sig}$ is illegal, it can be judged as illegal trust value and M_i will abandon this trust value;
- If Tag_i is different from Tag_s and $(r_i, T_i)_{sig}$ is legal, M_i can store this trust value;
- If Tag_i is different from Tag_s and either Tag_i or $(r_i, T_i)_{sig}$ is illegal, it can be judged as illegal trust value and M_i will abandon this trust value.

7) Trust value calculation

To prevent bad-mouthing attacks, unfair ratings are filtered. A method to filter "unfair ratings" in [19].their algorithm regroups a peer's feedback to compute a local score with these feedback. The local score is then compared with the global one, or if the 95^{th} percentile is lower than the mean, the rater's feedback is filtered. This method is very accurate. In this reputation, evaluation tags can classify feedbacks the same rater to the ratee. To obtain the more accurate trust value of the peer, TVM peers can run the filter algorithm to calculate the accumulated trust values.

8) Trust value Relay

Whenever a TVM peer x receives a trust value query of his own management peer i. he generates a reply and forwards it back to the network.

$R = ID_i \mid MP_i \mid MS_i(T_i \mid r_i \mid VID_x \mid S_x(T_i))$. There are a number of points to note:

- The ID_i shows that the reply message contains the trust value for peer i. The MP_i key is used to decrypt the encrypted part.
- The use of encryption with MS_i indicates that the reply comes from the TVM peers. This avoids any peer to randomly send a value.
- VID_x ensures that a valid TVM peer is replying and accountability.

- T_i prevents replay attacks. $S_x(T_i)$ ensures that no node can use another peer's VID_x ,in which P_i can decrypt the $S_x(T_i)$,any node has no the key S_x .

9) Peer leave

Before exiting, TVM peer i contacts the bootstrap sever and the bootstrap check the number of the TVM peers for peer r (According to the assignment mechanism, every peer is assigned M TVM peers, whereas using information from only K (M>K)at every step.) If the number of the TVM peers is lower than K, the bootstrap will assign a new TVM peer and take place. The data at the TVM peer only maintains a time stamp, if the data is not accessed for a long enough time; Peer i just deletes it from its database.

5. Security Analysis

This section we demonstrate how our proposal ensures the security and privacy properties. We also discuss how our protocol deals with the various attacks of the malicious TVM peers.

5.1. Security Analysis

This system is under the random language machine model. Therefore, if the CL signature cannot be forged, the evaluation tags and evaluation certificates container will not be forged as well.

1) Anonymity

The trust information used to evaluate the reputation of users is associated to raters' evaluation tags instead of the real identifies of the raters. The evaluation tag is generated on the basis of verifiable random function (VRF), which guarantees the randomness of tags. As ϕ is zero-knowledge proof, the information related to rater identity will not be disclosed.

2) Legitimacy of the anonymous evaluation

The anonymity of traders' identities does not comply with the legal requirements of some commercial transactions. In this model, peers can use their real identities for transaction and after transaction they will obtain a blind signature evaluation permit σ_{Bi} as the trading evidence for submitting trust evaluation value. Which preserves the privacy of the raters, but also prevents the random evaluations from the malicious raters.

3) Unlinkability

The evaluation tags are not the same for different ratee by the same rater. If attacker wants to connect the two evaluation tags, they must judge if the $Tag_1 = g^{1/s+R_1+1}$ and $Tag_2 = g^{1/s+R_2+1}$ are generated by the same s. This is the Diffie-Hellman problem, which is considered unsolvable in polynomial time. Therefore, evaluation tags cannot connect the evaluations of the same evaluator to different users, which ensures its unlinkability.

4) Reputation Unforgeability

Whenever raters submit trust value, they need to run verifiable signature for the trust values. $1/S+R+1$ can be used as signature secret key and $Tag = g^{1/s+R+1}$ as

verifiable secret key. Only the rater with evaluation certificate container knows the evaluation tag s and other users cannot calculate $1/S+R+1$. Consequently, even malicious users intercept the tag of evaluators; they cannot sign the reputation value or forge reputation evaluation value.

5.2. Sybil-Proof property

If peer wants to attack Sybil attack, the Tag in his submitted reputation evaluation information of $\{ID_i, Tag, \phi, r_i, T_i, (r_i, T)_{sig}, \sigma\}$ must be the same with the Sybil attack-resisting tag of Tag_s, for the $H(ID)$ of the two tags is the same and the secret key s of the evaluation certificate container is also the same. If the TVM peer verifies the legitimacy of $(r_i, T)_{sig}$, and the TVM peer will identify that it is the Sybil attack.

5) No Central Trusted Authority (CTA)

It is important to notice that the bootstrap server does not act a CTA .It is rather a form of a certification authority. All the trust mechanisms are within the network and the bootstrap server does not participate in it.

5.3. Malicious TVM peers

A malicious TVM peer may do the following:

1) Refuse to participate in the protocol

If a TVM peer i refuses to participate in the protocol, it has no effect on the protocol since bootstrap assigns a number of the TVM peers for a single peer.

2) Provide incorrect trust value

If a TVM peer provides incorrect trust value, it has no effect on the condition that a peer is assigned a number of TVM peers. Then the querying peer can take a majority vote amongst them and selects trust value. Also the protocol presents a possibility to punish such a malicious peer. The replay of the trust value $R = ID_i \mid MP_i \mid MS_i(T_i \mid r_i \mid VID_x \mid S_x(T_i))$ includes the VID_x, which stands for the identity of the TVM peer.

3) Get a VID_x of another TVM peer

If a TVM get a VID_x of another TVM peer and sends a wrong trust value, it has no effect on the condition that the use of P' in VID_x and $S_x(T_i)$ can prevent the attack.

6. Efficiency Analysis

As a rater, peer need to generate evaluation tags for every new transaction object and execute the sign algorithm for every trust value. It takes $T_E + 3T_M$ times (T_E represents single-base modular exponentiation, T_M refers to multi-base modular exponentiation) to generate a evaluation tag and T_E times to sign the $(r_i, T_i)_{sig}$. The rater only need to generate a evaluation tag for the same transaction object. So, the primary costs are linear in the size of new transaction objects with respect to generating the new evaluation tags.

As a TVM peer, peer need to verify the validity of the trust value. It takes $T_E + 3T_M$ times

to verify an evaluation tag and T_E times to verify the signature $(r_i, T_i)_{sig}$. If tags submitted are the same as the tags in the database, TVM peers only need to verify the signature of trusts value to judge whether they are legal. To a TVM peer, the main costs are linear in the size of new evaluation tags.

7. Conclusion

In this paper, we presented a reputation system preserving the privacy of the feedback provider and resisting Sybil Attack. This model does not need continuous online third-party trusted center; each peer will be distributed randomly to anonymous TVM nodes. Based on evaluation tags instead of the transaction identities, Raters will anonymously submit encrypted trust values to ratee's TVM nodes. TVM nodes will verify, identify, store and calculate the trust values and safely reply the trust values of managed nodes to other nodes. Moreover, in this model Sybil attack can be automatically identified and resisted According to the security analysis, this model has desirable features of anonymity, unlinkability, unforgeability and ensures the accuracy accumulated trust value.

Acknowledgements

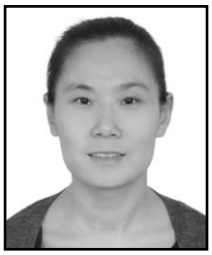
This work is supported by National Key Technology R&D Program (2012BAH37B05).

References

[1] P. Resnick and R. Zeckhauser, "Trust among strangers in internet transactions", Advances in Applied Microeconomics, vol. 11, (**2002**), pp. 127-157.
[2] O. Hasan, L. Brunie and E. Bertino, "Preserving privacy of feedback providers in decentralized reputation systems", Computers & Security, (**2011**), http://dx.doi.org/10.1016/j.cose.2011.12.003.
[3] O. Hasan, L. Brunie and E. Bertino, "A Decentralized Privacy Preserving Reputation Protocol for the Malicious Adversarial Model", Rapport de recherche RR-LIRIS-2012-008, (**2012**).
[4] T. Dimitriou and A. Michalas, "Multi-Party Trust Computation in Decentralized Environments", New Technologies, Mobility and Se(NTMS), (**2012**), pp. 1-5.
[5] M. T. Goodrich and F. Kerschbaum, "Privacy-enhanced reputation-feedback methods to reduce feedback extortion in online auctions", CODASPY '11 Proceedings of the first ACM conference on Data and application security and privacy, **(2011)**, pp. 273-282.
[6] S. Schiffner, S. Clauß and S. Steinbrecher, "Privacy, liveliness and fairness for reputation", In: SOFSEM. vol. 6543 of LNCS, Springer, (**2011**).
[7] K. Hoffman, D. Zage and C. Nita-Rotaru, "A Survey of Attack and Defense Techniques for Reputation Systems (to appear)", ACM Computing Surveys, vol. 42, no. 1, **(2009)** December.
[8] L. A. Martucci, S. Ries and M. Mühlhäuser, "Sybil-Free Pseudonyms, Privacy and Trust: Identity Management in the Internet of Services", Journal of Information Processing, vol. 19, no. 1, (**2011**), pp. 1–15.
[9] M. Gupta, P. Judge and M. Ammar, "A reputation system for peer-to-peer networks", In NOSSDAV, (**2003**).
[10] M. Voss, A. Heinemann and M. Muhlhauser, "A privacy preserving reputation system for mobile information dissemination networks", In SECURECOMM '05: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), Washington, DC, USA, (**2005**), pp. 171–181, IEEE Computer Society.
[11] J. Bethencourt, E. Shi and D. Song, "Signatures of Reputation: Towards Trust without Identity", In: Sion, R. (ed.) FC 2010, LNCS, vol. 6052, (**2010**), pp. 400–407. Springer, Heidelberg.
[12] M. Voss, "Privacy preserving online reputation systems", In International Information Security Workshops, (**2004**), pp. 245–260.
[13] S. Steinbrecher, "Design options for privacy-respecting reputation systems within centralised internet communities", In SEC, (**2006**), pp. 123–134.
[14] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols", In Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, editors, Security in Communication Networks '02, volume 2576 of LNCS, Springer Verlag, (**2002**), pp. 268–289.
[15] A. Singh and L. Liu, "Trustme: anonymous management of trust relationships in decentralized p2p systems",

in Third International Conference on Peer-to-Peer Computing, **(2003)** September, pp. 142-149.
[16] S. Kamvar, M. Schlosser and H. Garcia-Molina, "Eigenrep:Reputation management in p2p networks", In Twelvth International World Wide Web Conference, **(2003)**.
[17] S. Ratnasamy, P. Francis, M. Handley, R. Karp and S. Shenker, "A scalable content addressable network", In Proceedings of ACM SIGCOMM 2001, (**2001**).
[18] E. Sit and R. Morris, "Security considerations for peer-to-peer distributed hash tables", In IPTPS02 Workshop, Cambridge,MA (USA), **(2002)** March.
[19] A. Whitby, A .Jøsang and J. Indulska, "Filtering out unfair ratings in Bayesian reputation systems", in Proc. 7th Int. Workshop on Trust in Agent Societies, (**2004**).

Authors



Keli Zhang

She received his M.Sc. in Information Security (2008). Now She is a PhD candidate in Cryptography in Beijing University of Posts and Telecommunications University. Her current research interests include trust model, privacy and information security.

Zhongxian Li

He received his M.Sc. in Mathematics (1986) and PhD in Cryptography (1999) from Beijing University of Posts and Telecommunications University. Now he is part-time professor in Information Security Center, Beijing University of Posts and Telecommunications University. His current research interests include Cryptography, network security and trust model.

Yixian Yang

He received his M.Sc. in Mathematics (1986) and PhD in Cryptography (1988) from Beijing University of Posts and Telecommunications University. Now he is full professor in Information Security Center, Beijing University of Posts and Telecommunications University. He is Yangtze river scholars Distinguished Professor from 1999 to 2004.His current research interests include Cryptography, network security and trust model and so on.