Private Reputation Schemes for P2P Systems

Roslan Ismail[1], Colin Boyd[1], Audun Josang[2], and Selwyn Russell[1]

[1] Information Security Research Centre, Queensland University of Technology, Brisbane, QLD 4001 Australia
[2] Distributed Systems Technology Centre, University of Queensland, Brisbane, QLD 4072 Australia

Abstract. The risks from participating in P2P transactions are relatively high. To mitigate such risk a reputation scheme could be applied. Reputation schemes have emerged as a promising means for enabling electronic transactions with strangers. In order to gain optimal results from the reputation scheme, the privacy of feedback provider should be correctly addressed. The feedback provider should be allowed to leave a feedback without fear of retaliation. Unlike in centralized schemes, privacy seems impractical for P2P systems especially when accountability of feedback is also required. This paper considers how privacy can still be provided within the accountability requirement.

1 Introduction

Peer-to-peer (P2P) systems are becoming a popular medium for e-commerce. Intuitively, these systems offer several advantages compared to centralized systems such as being cheaper, more convenient, faster, and also allowing expanded scalability of the systems. Nevertheless, the risks from participating in P2P transactions are relatively high. It is easy to create a phantom transaction and based on such a transaction feedback is given and calculated to produce the reputation rating. Typically this happens because there is no trusted authority to monitor a transaction conducted between a peer and its counterpart.

In contrast, in a centralized system for example, eBay[3], each transaction is monitored by an authority. This measure ensures that the submitted feedback is based on completed transactions. P2P systems commonly have different requirements compared to centralized systems. In the context of reputation schemes, P2P systems require peers themselves to calculate and manage their reputation value on their own. P2P systems may be roughly divided into two categories. The first category is *pure* P2P systems while the second is *mediated* P2P systems. The former operates without involvement of an authority while in the latter the authority participates in certain tasks. In terms of practicality the mediated systems are preferred as it is easy to cheat in the pure P2P systems. In addition, use of unaudited information makes pure P2P unsuitable for formal e-commerce.

It is vital to monitor each transaction that takes place in the P2P systems to prevent false feedback. Recently, Fahrenholtz and Lamersdorf [5] proposed a

[3] http:www.ebay.com

Ismail R., Boyd C., Josang A. and Russell S. (2004).
Private Reputation Schemes for P2P Systems.
In *Proceedings of the 2nd International Workshop on Security in Information Systems*, pages 196-206
DOI: 10.5220/0002674201960206

hybrid solution (known as the FL scheme hereafter) which combines centralized and distributed methods to monitor transaction activities. There is an authority known as a *portal* to monitor the feedback process conducted between a peer and its counterparts. Unlike the centralized system, the reputation scheme in the FL scheme is managed by a peer itself. Although the FL scheme seems promising against a false feedback it lacks privacy. No privacy is provided for the feedback provider while submitting feedback. As a result the link between the feedback provider and the submitted feedback is available to the recipient.

Privacy is a vital topic in many electronic systems such as e-voting, e-cash and e-auction. This is equally true for reputation systems. In fact, privacy can help to solve the problem of collecting sufficient negative feedbacks. The feedback providers are usually reluctant to leave negative feedback, even when it is appropriate, for fear of retaliation. Unlike the centralized systems where privacy may not be difficult to implement privacy seems hard for P2P systems.

Another vital property of reputation scheme for P2P systems is accountability. Accountability here means that each feedback should be legitimate. To achieve this property each feedback needs to be signed by the feedback provider. However, by signing the feedback the identity of the feedback provider can easily be traced. Therefore, privacy and accountability seem to contradict one another. This conflict has motivated us to explore a novel way of providing sufficient privacy while at the same time ensuring that accountability of the feedback is not compromised.

In this paper a reputation scheme for P2P systems is applied in which peers calculate and store their reputation on their own without any involvement from an authority. The authority functions as an entity to monitor the process of delivering feedback to appropriate participants. This is vital to ensure privacy is preserved and at the same ensuring feedback is based on a legitimate transaction.

Contribution. The contributions of the paper are twofold: analyzing the security of the Fahrenholtz and Lamersdorf scheme and introducing *privacy* to the scheme.

Organisation of the paper. The remainder of the paper is structured as follows. Section 2 lists related work. Section 3 reviews the Fahrenholtz and Lamersdorf scheme. Section 4 presents our proposal. Finally section 5 discusses several issues and then concludes the paper.

2 Related Work

To understand the implementation of privacy in the reputation scheme, consider a scenario of evaluating the performance of a lecturer in a University. At the end of a semester registered students will be given an evaluation form so that they can leave feedback on the performance of lecturers. To protect the privacy of the students, they are not required to write their names on the evaluation form. By doing so the link between the feedback and students is untraceable. Usually a trusted party ensures that only enrolled students can give feedback and each student can only complete one evaluation form. In the context of e-commerce, the feedback providers are the registered students, the feedback targets are the lecturers and finally the authority refers to the university authority.

Recently, a number of reputation schemes for P2P systems have been proposed for various purposes [3–7]. Gupta et al. [6], for example, proposed a scheme to calculate peers' reputation with the help of an authority known as a centralized reputation calculation agent (CRCA). CRCA is used to maintain consistency in calculating the submitted feedback to produce reputation for peers. In addition, it also can prevent manipulation of the reputation. Since the scheme is aimed at P2P systems the reputation is returned to peers to manage. The scheme is also concerned with protecting the submitted feedbacks from being manipulated by requiring the feedback provider to encrypt and sign the feedback before sending it to CRCA.

Cornelli et al. [3] and Damiani et al. [4] have proposed two schemes (the basic and advanced schemes) to seek a reputable 'servent' (a combination of client and server) for downloading files in P2P systems. Both the schemes employ voting mechanisms to evaluate recommendations collected from others in searching for a reliable servent. An entity receiving the higher vote is a reputable entity. The basic scheme provides partial privacy as it hides the identity of the feedback provider but IP address is in clear form. The IP address is required to verify the vote's origin. The advanced scheme, on the other hand, discloses the identity of voter so that the voter credibility can be assessed. Integrity and non-repudiation of the feedback are assured via encryption and signature mechanisms.

Liau et al. [7] proposed a reputation scheme for P2P systems based on certificate mechanisms. This scheme is a pure P2P reputation scheme; a peer itself is in charge on the management of reputation. This improves the storage and integrity of the reputation rating. The reputation certificate is propagated and evaluated before it can be accepted as a reputation reference. The checking of the reputation certificate is conducted by contacting the recent preceding rater. In a case where the preceding rater is not available the next predecessor rater should be contacted and so on until an available preceding rater is found. To preserve the integrity of the reputation certificate the rater signs the updated certificate.

In all the schemes above the privacy of the feedback provider is not given a fair treatment. Rather the schemes are focussed on how to provide integrity of the feedback. However, we argue that to collect a sufficient amount of feedbacks, especially negative feedback, privacy should be seriously taken into account. Otherwise the problem of eliciting negative feedback remains unsolved. Privacy in fact empowers participants to leave negative feedback when appropriate without fear of possible retaliation. Table 1 presents properties hold by the reviewed schemes. The • denotes a full feature is available while ⋆ denotes a partial feature is provided. Out of three schemes reviewed, we choose to improve the scheme due to Fahrenholtz and Lamersdorf because it has two suitable features for P2P systems. The first feature is a monitor mechanism to check that transactions

Table 1. Summary of properties in several reputation schemes

	Integrity	Non-Repudiation	Privacy	Monitoring
Liau et al. scheme	●	●		
Cornelli et al. scheme	●	●	⋆	
Damiani et al. scheme	●	●	⋆	
Gupta et al. scheme	●	●		
Fahrenholtz and Lamersdorf scheme	●	●		●

have been conducted by the peers. By doing so a feedback is assured to be based on a legitimate transaction. The second feature is a mechanism which prevents peers from discarding unfavorable feedback collected by them.

3 Fahrenholtz and Lamersdorf Scheme

Fahrenholtz and Lamersdorf [5] proposed a distributed reputation scheme for P2P networks. In the FL scheme an entity called a portal is used to monitor transactions conducted between peers. The portal also records the number of transactions conducted, as well as the number of feedbacks obtained by each peer. This is achieved via the use of ticket and nonce. The ticket typically contains identification of a peer and its counterpart, and the nonce. The nonce is extracted from the transaction ticket and it needs to be submitted alone with the questionnaire form. These mechanisms can prevent peers from discarding unfavorable feedbacks collected. To achieve integrity and non-repudiation of the feedback each one will be encrypted and signed before sending it one to another.

3.1 Outline of FL Scheme

Figure 1 shows the entities in the scheme and their interactions. There are two types of entities in the scheme; a trusted third party (TTP) known as a portal and the peers. The peers are required to register with the portal before commencing with a transaction. Each peer is required to create a key pair (private, public) when completing the registration. The scheme contains five phases; authentication of reputation management system subjects, service location for a context-specific transaction partner, selection of transaction partner, domain dependent transaction and rating partner. For simplicity we only review phase 2 and 5 (for further details consult [5]).

- **System Setup.** Let U_1 and U_2 be two peers who want to transact one to another, and A be an authority. The identities of U_1 and U_2 are denoted by

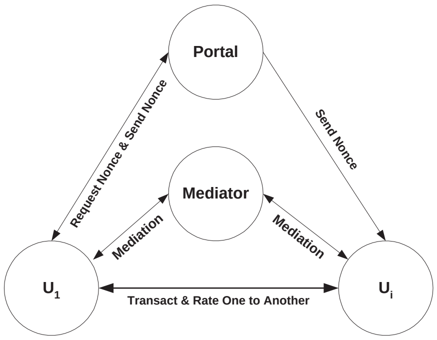

Fig. 1. Abstract View of FL scheme

id_{U_1} and id_{U_2}, respectively. $S_X(m)$ denotes that m is signed by X, $E_{Y,Z}(m)$ denotes m is encrypted using a shared key between Y and Z, and transaction tickets for U_1 and U_2 are denoted by d_{A,U_1}=$(id_{U_1}, id_{U_2}, r_{A,U_2})$ and d_{A,U_2}=$(id_{U_1}, id_{U_2}, r_{A,U_1})$, respectively. The notations r_{A,U_1} and r_{A,U_2} represent the nonce issued by an authority A for user U_1 and U_2, respectively.

- **Transaction Partner Selection.** Identification of a suitable partner must take place before a transaction begins and it is assumed that this process has already taken place beforehand. Rather we continue to the next step where U_1 requests the authority A to issue transaction tickets to itself and its counterpart. Upon receiving this request, two tickets d_{A,U_1}, d_{A,U_2} are issued and signed by A where d_{A,U_1} is for the transaction ticket for U_1 and d_{A,U_2} is for U_2. To ensure confidentiality and integrity of these tickets, they are encrypted with the key shared between A and U_1, and A and U_2, respectively. The following are the protocol messages sent by A.

  1. $A \rightarrow U_1 : E_{A,U_1}(d_{A,U_1}, S_A(d_{A,U_1}))$
  2. $A \rightarrow U_2 : E_{A,U_2}(d_{A,U_2}, S_A(d_{A,U_2}))$

- **Rating of Partner.** Upon completing the transaction, U_1 and U_2 can start to rate the performance one to another. U_1 sends the $Q'naire_{Cxt,U_1}$ along with the nonce to U_2, and vice versa. Upon receiving the $Q'naire_{Cxt,A}$, U_1 and U_2 can start to fill it with a feedback before sending it to one another. To protect the integrity of the $Q'naire$, it is encrypted with the key shared between U_1 and U_2. To confirm that the completed $Q'naire$ has already been submitted to one another U_1 and U_2 send the nonce to A. The nonce can be extracted from the transaction ticket. Upon receiving the nonces A sends an acknowledgement to both U_1 and U_2 to indicate the status of the sending nonce: either it is fine or an error is reported. The nonce functions as a means to prevent U_1 and U_2 from discarding unfavorable feedbacks. The protocol executed is described as follows.

  1. $U_1 \rightarrow U_2 : E_{U_1,U_2}(Q'naire_{Cxt}, S_{U_1}(Q'naire_{Cxt,U_2}), r_{A,U_2})$

2. $U_2 \rightarrow U_1 : E_{U_1,U_2}(Q'naire_{Cxt,U_1}, S_{U_2}(Q'naire_{Cxt,U_1}), r_{A,U_1})$
3. $U_1 \rightarrow A : E_{A,U_1}(r_{A,U_1})$
4. $U_2 \rightarrow A : E_{A,U_2}(r_{A,U_2})$

3.2 Analysis of the FL Scheme

Notation. Let N_U be the number of transactions carried out by user, F_A denotes the number of nonces received by the authority, F_U denotes the number of feedbacks obtained and recorded by the user.

The behavior of the relying party depends on the relative sizes of N_U, F_A and F_U. We consider several different cases.

1. $\mathbf{N_U = F_A = F_U}$.
   This outcome means that the number of transactions made by a user U is equal to the number of feedbacks for the user recorded by the authority and the user. This is an ideal case where all the participants follow the protocol honestly. Typically in this case the reputation rating of the user is accepted.
2. $\mathbf{F_U = F_A}$ and $\mathbf{F_U < N_U}$.
   This outcome means that the number of feedbacks recorded by user U is equal to the number of feedback recorded by authority but it is less than the number of transactions recorded by the authority. There are occasions when some feedback providers may not return their feedback after completing the transactions. This could be quite common especially when there is no reward for submitting a feedback. In addition, fear of the consequences due to the given feedback is another factor which causes lack of interest to leave a feedback. In this case the reputation of the peer is commonly accepted.
3. $\mathbf{F_U > F_A}$ and $\mathbf{F_A = N_U}$
   This outcome means that the number of feedbacks recorded by user U is greater than the number of feedbacks and transactions made and recorded by the authority. The user may create some phantom feedbacks in order to boost his reputation. Thus, in this case the reputation of the user is not accepted.
4. $\mathbf{F_U < F_A}$ and $\mathbf{F_A = N_U}$
   This outcome means that the number of feedbacks recorded by a user U is less than the number of feedbacks and transactions made recorded by the authority. The user may have discarded some of unfavorable feedbacks submitted for him. The reputation of the peer is not accepted.
5. $\mathbf{F_U > F_A}$ and $\mathbf{F_U < N_U}$
   This outcome means that the number of feedbacks recorded by a user U is greater than the number of feedbacks recorded by the authority but less than the number of transactions made. Some feedback providers may choose not to return their nonces to A. As a result A's record on the number of nonce received will be less than the number of feedback record by the user. The reputation of the user could be accepted depending on a proof provided by the user.

Although the FL scheme provides sufficient protection from the outsider attacks it is exposed to attacks by the internal players. For simplicity the communication line is assumed reliable. The nonce is always reached to the authority. In the FL scheme the portal is a trusted party. However, this may not be valid in some cases. We would like to point out some important facts regarding the above outcomes. For example, in case 2 an attack could be launched by the dishonest portal. The portal may learn the number of transactions conducted by U_1, as well as the number of feedbacks collected by U_1 from the returned nonce. With this knowledge a phantom nonce can be added to U's account. As a result U_1's reputation could be rejected as there is discrepancy in the record of the authority and U_1.

A major restriction the FL scheme possesses is that the feedback target may learn the link between the feedback provider and the feedback because it is in clear form. As a result the feedback providers may be reluctant to leave honest feedback especially in the case of negative feedback due to the consequences they may suffer later. In a real e-commerce environment negative feedback is needed to counterbalance positive feedback so that the produced reputation can reflect true behavior of users.

4 Improved Scheme

We propose an improvement of the FL scheme by introducing privacy as the major concern. The players and processes are similar to the FL scheme. To ensure that privacy can be achieved the number of a peer's counterparts should be more than one, and preferably a large number. This requirement is essential to allow unlinkability. The importance of unlinkability to maintain privacy is discussed by Maitland et al. [8]. Without sufficient number of players privacy seems impossible to implement. Another vital consideration is the timing of delivering of the feedback. If the feedback is sent immediately after the transaction is completed then the link between the feedback and the feedback provider can easily be formed. To avoid such undesirable outcome delay of the delivery of the feedback to a certain time later could be undertaken. This could either be a randomised delay, or delivery of feedbacks could be batched after a threshold number of feedbacks has been received.

Unlike the FL scheme, our proposal does not use shared keys. Instead the peers use their counterpart's public key to encrypt the feedback. However, we follow the practice of FL scheme in managing the administrative task. The authority is still responsible for issuing a nonce to each peer. The nonce must to be obtained before a transaction can take place. Besides issuing the nonce, the authority also maintains a record of the returned nonces.

There are six phases in our proposal; requesting nonce, preparing and sending token, signing and sending legitimate token, submitting feedback, calculating feedback and showing reputation. In our improved scheme, registration of participants is not required. Thus, each participant is assumed to have a valid certificate issued by the certificate authority CA.

There are several options can be taken to construct our improved scheme. One can construct a scheme based on ring signature schemes [9]. Ring signatures allow the identity of the signer to be hidden from recipients while retaining the important advantage of enabling accountability of feedback to be achieved. Thus the two characteristics we require for reputation schemes are provided. However, this option does not seem very practical to be implemented as it requires vastly more computation to verify the signatures. There are two types of computation required. The first is to verify signature of the n members in a ring signature for a feedback provider. The second is to verify each of the d feedback providers. As a result there are $d \times n$ computations are required. A second option is to implement a scheme based on a bilinear ring signature scheme. This scheme reduces the inefficiency faced by the first option but like the first scheme it is still too inefficient to be really practical. To overcome this inefficiency, a token based scheme is proposed. Since our scheme follows the same process as the FL scheme where a nonce is required to be obtained before starting a transaction this phase is not considered in the following protocol.

4.1 Protocol of the Scheme

The following protocol uses several notations as follows: ID_{FP} denotes an identification of the feedback provider, E_X denotes encryption using X's public key and Sig_X denotes signing using X's private key.

Preparing and Sending Token. FP prepares the transaction particulars m. The content of m can be the date of transaction, the feedback target's identification, the amount of transactions and the given feedback. To ensure integrity is achieved a pair (ID_{FP}, m) is encrypted using TTP's public key before sending it to TTP for signing. In a variant of this procedure the token could be created using electronic cash technology [2]. A coin is issued by the TTP for a particular transaction and when submitting feedback the coin payment protocol is used. The advantage of this option is that the feedback value can be hidden from the TTP, but there is an extra computational cost. We do not consider this option further in this paper.

$FP \rightarrow TTP : E_{TTP}(ID_{FP}, m)$

Signing and Sending Legitimate Token. Upon receiving the pair (ID_{FP}, m) from FP, TTP decrypts it and then verifies the correctness of m against a database of transactions maintained by TTP itself. If the verification is successful m is signed by TTP and then encrypted using the FP's public key. To complete the phase, TTP sends m to the feedback provider. The signed m is considered a legitimate token. Only the legitimate token can be used for submitting a feedback. Without using the legitimate token the feedback will not be counted for calculation of reputation. A nonce is also issued by TTP and then submitted to FP.

$TTP \rightarrow FP : E_{FP}(Sig_{TTP}(m), nonce)$

Submitting Feedback. FP sends to FT the legitimate token m which consists of the feedback. To protect integrity of the legitimate token, m is encrypted using the feedback target's public key. FP also send the nonce to FT.

$FP \rightarrow FT : E_{FT}(Sig_{TTP}(m), nonce)$

Calculating Feedback. Upon receiving m, FT decrypts and then verifies the TTP's signature on m. If the verification is successful the legitimate token is accepted otherwise it is rejected. The accepted token is then used to calculate the reputation of the feedback target. FT sends the nonce to TTP to confirm the feedback is received from the feedback provider. However, FT does not who is the feedback provider.

TTP sends a signed list n to the feedback target. The list n consists of number of the legitimate tokens issued by TTP for the feedback target. n is important to prevent the feedback target from discarding the submitted legitimate tokens. In addition, n also acts a means to convince the relying party that the calculated reputation is based on the submitted feedback.

$A \rightarrow FT : E_{FT}(Sig_{TTP}(n))$

Showing Reputation. Before a transaction can commence, FT sends the calculate reputation and n to the relying party so that the relying party can evaluate the validity of reputation. Due to a possibility of having huge number of tokens to be verified the relying party could batch them. The scheme proposed by Bellare et al. [1] can be employed which save the computation of verification. The relying party has to verify two signatures: the TTP's signature on the tokens and the TTP's signature on the list n.

5 Analysis

Privacy. The improved scheme achieves conditional privacy where the feedback provider is hidden from public except TTP. However, it requires trust to be placed on the trusted third party not to reveal the identity of the feedback provider otherwise the privacy of the feedback provider is compromised. In other words TTP is assumed honest in performing its task. However, in a case where this assumption is difficult to implement, for example, in the presence of the dishonest TTP then threshold schemes could be implemented. This means a number of TTP is required in which each individual TTP shares a portion of identity of the feedback provider. Without sufficient number of TTP to form the identity of the feedback provider, the privacy of the feedback provider is preserved.

6 Conclusion

An analysis conducted on the scheme of Fahrenholtz and Lamersdorf reveals a few security concerns. We have proposed an improved reputation scheme which is based on the FL scheme. The improved scheme provides privacy for feedback providers while submitting a feedback. With this property the feedback providers can leave negative feedback without fear of retaliation from the other parties. The token based solution is suitable to provide a simple privacy protection and furthermore it is efficient in terms of computation required to verify signatures.

References

1. Mihir Bellare, Juan A. Garay, and Tal Rabin. Fast batch verification for modular exponentiation and digital signatures. In K. Nyberg, editor, *EUROCRYPT '98*, volume LNCS 1403, pages 236–250. Springer-Verlag Heidelberg, 1998.
2. Stefan Brands. Untraceable off-line cash in wallets with observers, In D. R. Stinson, editor, *Advances in Cryptology - Crypto '93*, pages 302–318, Springer-Verlag, 1993.
3. Fabrizio Cornelli, Ernesto Damiani, Sabrina De Capitani di Vimercati, Stefano Paraboschi, and Pierangela Samarati. Choosing Reputable Servents in a P2P Network. In *Proceedings of the eleventh international conference on World Wide Web*, pages 376–386. ACM Press, 2002.
4. Ernesto Damiani, Sabrine De Capitani di Vimercati, Stefano Paraboschi, Pierangela Samarati, and Fabio Violante. A reputation-based approach for choosing reliable resources in Peer-to-Peer networks. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 207–216. ACM Press, 2002.
5. D. Fahrenholtz and W. Lamersdorf. Transactional security for a distributed reputation management system. In K. Bauknecht, A. Min Tjoa, and G. Quirchmayr, editors, *Proceedings of the 3rd International Conference on Electronic Commerce and Web Technologies*, volume 2455 of *Lecture Notes in Computer Science*, pages 214–223. Springer-Verlag, 8 2002.
6. Minaxi Gupta, Paul Judge, and Mostafa Ammar. A reputation system for Peer-to-Peer networks. In *ACM 13th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2003)*, pages 144–152. ACM Press, June 1-3 2003.
7. Chu Yee Liau, Xuan Zhou, Stephane Bressan, and Kian-Lee Tan. Efficient distributed reputation scheme for Peer-to-Peer systems. In *The 2nd International Human.Society@Internet Conference*, volume LNCS 2713, pages 54–63. Springer-Verlag, 2003.
8. Greg Maitland, Jason Reid, Ernest Foo, Colin Boyd, and Ed Dawson. Linkability in Practical Electronic Cash Design. In *Proceedings of Information Security Workshop (ISW 2000)*, volume LNCS 1975, pages 149–163. Springer-Verlag, 2000.
9. Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In C. Boyd, editor, *ASIACRYPT 2001*, volume LNCS 2248, pages 552–565. Springer-Verlag, 2001.