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 12 (17): 3976-3980, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.3976.3980

A Reputation Storage Scheme Based on Secret Sharing in P2P Networks

[1]Sun Hua, [1]Yu Jiong, [2]Li Li, [2]Ying Chang-Tian and [2]Liao Bin
[1]School of Software, Xinjiang University, Urumqi, Xinjiang 830008, China
[2]School of Information Science and Engineering, Xinjiang University,
Urumqi, Xinjiang 830046, China

Abstract: A storage scheme of reputation based on RSA threshold secret sharing and one-way function is proposed in Peer-to-Peer networks. In this scheme, reputation information is divided into n shares and distributed to n participants. Any t or more than t participants can reconstruct reputation information base on RSA threshold secret sharing. The validation share corresponding to the secret share is also distributed to every participant for verifying the integrity of secret share and any cheat behavior will be detected no matter who is from rightful participant or unlawful participant. The scheme is secure unless RSA cryptography and one-way function can be break through. This scheme can also defend collusion and man-in-the-middle attack.

Key words: Reputation, threshold secret sharing, one-way function, peer-to-peer network

INTRODUCTION

All kinds of the technologies are applying to P2P environments with its exponentially growing rapid, like distributed computing, file sharing and exchange protocol, e-commerce technology and so on. The peers in the P2P network can interact with others conveniently. But there are great uncertainty and risk in the online world. The peers rarely interact with the same party and most occasions they must face the strangers, especially in large distributed P2P environments. There are very few practical methods to protect the quality and the reliability of the peers in these online systems (Josang, 2007). How could peers make a decision to rely on the resources or the parties that they don't know whether they are safe enough to interact with? Reputation is a available measures to solve this problem. Before decide to use a service or have a transaction with a party, the peers can evaluate the trustworthiness of the service or the party through reputation information. The essential role of reputation systems is to record the behavior of partners after transaction and make it available to potential transaction partners for decision making purposes (Josang *et al*., 2007).

In the trust and reputation systems (Deng *et al*., 2008; Eymann *et al*., 2008;Malik and Bouguettaya, 2009), reputation scores or trust measures are important for peers to measure the trustworthiness of the other peers. Some systems take reputation information stored in the third parties or the appointed peers (Kamvar *et al*., 2003). Some take the values stored in local (Hao *et al*., 2009) or in the transaction partners. No matter where to store reputation information, they must insure the integrity of the information. Reputation information stored in other peers must protect them from tampering by the holders and avoid them to offer false feedback (Jin *et al*., 2007). Ma and Qin *et al*. (2008) proposed a encryption-free reputation sharing protocol, it divides the reputation information into some segments and uses different routes to transmit them to the initiator peer.

In this study, a reputation storage scheme based on RSA threshold secret sharing and one-way function is proposed in P2P environments. The scheme uses RSA threshold secret sharing theory and one-way function to insure security and integrity of reputation information.

THRESHOLD SECRET SHARING SCHEME BASED ON RSA AND ONE-WAY FUNCTION

Threshold secret sharing: The threshold secret sharing scheme is respectively proposed by (Shamir, 1979) and (Blakley, 1979). In the secret sharing scheme, the secret is divided into n shares and distributed to n participants. Any t or more of the participants can reconstruct the secret and this can't be done by fewer than t participants. This scheme is claimed as (t, n) threshold secret sharing. After the development of more than 30 years, it has received much attention and become mature and the threshold secret sharing scheme based on RSA cryptography has become one of the research directions (Fei and Wang, 2003).

One-way function: One-way function is a function that it is easy to generate a code given a message but virtually

Corresponding Author: Sun Hua, School of software, Xinjiang University, Urumqi, Xinjiang 830008, China

impossible to generate a message given a code (Stallings, 2005). One-way function implies three meanings:

- For any given message x, it is computationally infeasible to find a message y such that x = H(y)
- For any given message x, it is computationally infeasible to find a message y such that H(x) = H(y)
- It is computationally infeasible to find any pair (x, y) such that H(x) = H(y)

Threshold secret sharing scheme based on RSA and one-way function: The process of the threshold secret sharing scheme based on RSA and one-way function includes four steps: Division of the secret, distribution of the shares, validation of the shares and reconstruction of the secret.

Division of the secret: The secret will be divided into n shares. Before division, we need illustrate some public information and secret information at first. Public information includes: a big prime number r (where r>n), a finite field GF(r) and its primitive element β. Secret information is a positive integer m and m = pq, where p and q are two big prime number.

The detail process of the division is as follows:

- Secretly choose a (t-1)th power polynomial:

$$f(x) = b_{t-1}x^{t-1} + b_{t-2}x^{t-2} \ldots + b_1x + k \bmod r$$

where, b_{t-1}, b_{t-2}, ..., b_1 and f(x) all belong to the finite field GF(r):

- Arbitrarily choose one integer number e and it is relatively prime with Euler function φ(m), where m = pq and φ(m) = (p-1)(q-1) and take this number available by public
- Compute $d = e^{-1} \bmod \varphi(m)$ and d is the secret information
- Respectively compute $S_i = f(\beta^i)$ and:

$$W_i = H(S_i)^d \bmod m$$

where, S_i is the ith secret share and W_i is validation share corresponding to the ith secret share.

Distribution of the shares: After division of the secret, the dealer will distribute the secret shares and validation shares to different participants. The dealer respectively distributes secret share S_i and validation share W_i to participant P_i (where i = 1, 2, … , n). So, every participant has a secret share and a validation share corresponding to the secret share. The role of validation share is to verify the validity of the secret share.

Validation of the shares: The secret shares can be validated by the validation shares held by the same participants. For secret participant P_i, the secret share and the validation share held by him are respectively S_i and W_i (where, i = 1, 2, … , n), through computing one-way function $H(S_i)$ and W^e_i, if equation $W^e_i = H(S_i)$ comes into existence, the participant offers the right secret share, otherwise he is an unlawful participant or the rightful participant offering wrong share.

Let us suppose that the unlawful participant is P_i^*, S_i^* and W_i^* are, respectively the secret share and validation share supported by him. If he don't want to be found by anyone that he is not the secret participant, he must compute W_i^* and make the equation $W^{e^*}_i = H(S_i^*)$ come into existence. But this is computationally infeasible for him, as the difficulty of the one-way function and RSA cryptography.

If the rightful participant P_i deliberately offers the wrong validation share W_i^*, he must find S_i^* such that the equation $H(S_i^*) = W^{e^*}_i \bmod m$ can be setup. This is also computationally infeasible for him to do so for the same reason.

In the process of the validation, as the security of RSA and one-way function, if the malicious participants want to use false secret share to reconstruct the secret, this is computationally infeasible. After validation, if the number of the participants gets to the threshold, we can reconstruct the secret.

Reconstruction of the secret: The process of the reconstruction is shown as Fig. 1.

The peer chooses t participant from n at first. After validation of the secret shares (suppose t secret shares respectively are S_1, S_2, … , S_t), we can obtain t interpolations: (β^1, S_1), (β^2, S_2), … , (β^t, S_t), where β is the primitive element of the finite field GF(r) and build a (t-1)th power polynomial $f(x) = b_{t-1}x^{t-1} + b_{t-2}x^{t-2} \ldots + b_1x + k \bmod r$. Make $S_t = f(\beta^t)$. After compute, we get k = f(0). The detail expression is:

$$k = \sum_{i=1}^{t} S_i \prod_{j=1, j\neq i}^{t} \frac{-\beta^j}{\beta^i - \beta^j} \bmod r$$

If any participant can't pass validation, he won't be chosen to reconstruct the secret and his secret share won't be taken into the reconstruction. This can guarantee that the output secret is the integrated one.

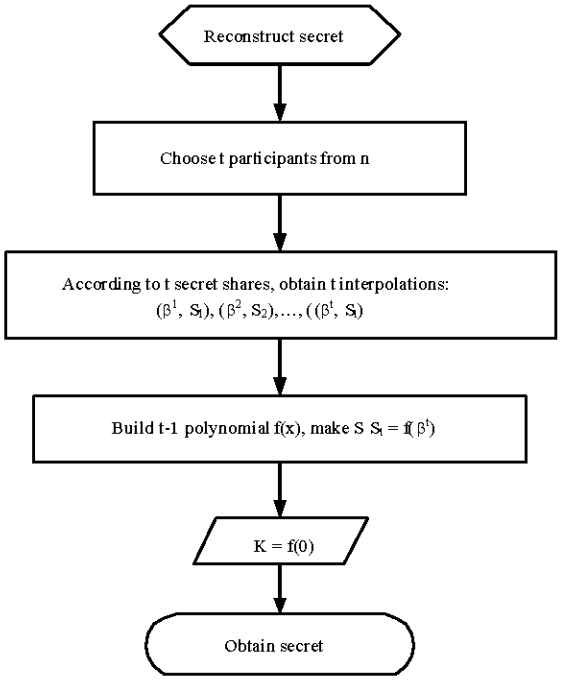

Fig. 1: Reconstruction of the secret

REPUTATION STORAGE SCHEME BASED ON RSA THRESHOLD SECRET SHARING AND ONE-WAY FUNCTION

In trust and reputation management systems, the peers will give a rating each other after every transaction. That is to say, the ratings of a peer are evaluation estimated by other peers who have had transaction with it. All of the ratings compose reputation. Every time the peers finish transaction, both of the transaction partners will store partner's reputation information to some peers. Firstly, each of them will divide reputation information independently into n shares and distributes them to n participants. When peers want to have transaction, they both query reputation of the potential partners. When query peer broadcasts query message, the participants who store corresponding reputation information will respond query message. The whole process include: Query reputation, response query, validation of the shares and reconstruction of reputation information, transaction evaluation and distribution of reputation.

Process of reputation query: The query peer broadcasts query message about some peer's reputation. The message will be transmitted according to the broadcast specification of the P2P network. Many of the peers including the malicious peers and other normal peers will all receive query message. They will look over whether they have reputation information of the queried peer. If the peer is just the participant peer who holds the queried reputation information, he will respond the query message; otherwise he will ignore the message.

Process of query response: When the participant peers receive query message, they will transmit the secret shares and the validation shares to query peer directly. Because the malicious peers also receive query message when the query peer queries reputation, they will track the message and monitor response message. But every malicious peer only obtains one secret share and validation share and they can't gain their ends through modifying secret share and validation share unless they can break through RSA cryptography. Even if several malicious peers collude, they just posses several secret shares and validation shares. As long as the amount of the malicious peers is not more than the thresholds of the secret sharing, they can do nothing.

Validation and reconstruction of reputation information: After query peer acquires many response messages and the number is up to the threshold to reconstruct, he will validate the secret shares.

If S_i and W_i are respectively the secret share and the validation share offered by participant P_i, the query peer can verify them through Eq: $W_i = H(S_i)^d$ modm. For the security of the RSA threshold secret sharing and one-way function, the query peer can clearly aware whether the secret share is the right one or not.

After receive t (threshold) right secret shares, query peer can reconstruct reputation information. Using Lagrange interpolation, he can reconstruct (t-1)th power polynomial f(x). After compute, he can get k = f(0). The secret is the reputation information.

Transaction evaluation and distribution of reputation information: After the potential transaction partners get enough reputation information each other and reputation scores get to the conditions of transaction, they have a transaction.

When the partners finish transaction, both of them will evaluate the opposing parties. They divide reputation information into some shares and transmit them to some participants to store. Although, some malicious peers will also receive the shares, they can't modify the secret shares and validation shares to realize their purposes because RSA cryptography beyond breaking through. If malicious peers use false shares to respond, as the modified share can't pass through verification and the

Table 1: Comparison among some schemes

Parameters	Server	Communication load	Secure aspect	Prevent inside cheat	Validate method	Validate content	Validation times
Scheme in Namin *et al.* (2005)	Need	Much	Storage	Yes	Hash function	Whole reputation	Only once
Scheme in Ma and Qin (2008)	Not need	Much	Transmission	No	Reputation sharing protocol	Whole reputation	Need once
Our scheme	Not need	Much	Storage and transmission	Yes	Threshold secret sharing	Secret shadow	Need t

query peer will not employ the false share to reconstruct. Therefore, the malicious peers can't destroy whole reputation information.

PERFORMANCE ANALYSIS

Properties: The scheme has some properties:

- Reputation information in this scheme is integrated and secure
- The scheme can defend collusion attack and man-in-the-middle attack
- The scheme can guard against the cheat behavior of the malicious peers
- The participants can share multi-secret.

Comparison: There are some other research works using cryptography to settle the integrated problem of reputation in Peer-to-Peer networks. Table 1 shows the main different aspects of the storage and distribution between our scheme and scheme in literature (Ma and Qin, 2008). In our scheme, the dealer peer distributes secret shares to n secret participants. And many of the secret participants transmit shares to query peer. Our scheme can defend man in the middle attack and it also can attack collude among secret participants. In the scheme of literature (Ma and Qin, 2008), the polling peers send some shares to network and the shares are transmitted to initiator peer with different routes. It can defend man in the middle attack, but if the polling peer is malicious and sends the wrong ratings, it's difficult for the query peer to detect. Only the process of the transmission is secure.

CONCLUSION

According to threshold secret sharing scheme and one-way function, we propose a reputation storage scheme. Reputation information is divided into n shares and distributed to n participants to store. Every participant will also receive a validation share corresponding to the secret share. The scheme can detect the false share unless the participant can break through RSA cryptography and one-way function.

ACKNOWLEDGMENT

The study was supported by the phD Startup Fund of Xinjiang University under grants No. BS120134, Project of Xinjiang Province Higher Educational Science and Technology Program under grant No. XJEDU2013S08.

REFERENCES

Blakley, G.R., 1979. Safeguarding cryptographic keys. Proceedings of the National Computer Conference, June 4-7, 1979, New York, USA., pp: 313-317.

Deng, L., Y. He and Z. Xu, 2008. Trusted Reputation Management Service for Peer-to-Peer Collaboration. In: On the Move to Meamingful Internet System, Meersman, R. and Z. Tari (Eds.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-88872-7, pp: 1069-1086.

Eymann, T., S. Konig and R. Matros, 2008. A framework for trust and reputation in grid environments. J. Grid Comput., 6: 225-237.

Fei, R.C. and L.N. Wang, 2003. Cheat proof Secret sharing schemes based on RSA and one-way fnction. J. Software, 14: 146-150.

Hao, L., S. Lu, J. Tang and S. Yang, 2009. An Efficient and robust self-storage P2P reputation system. Int. J. Distrib. Sensor Networks, 1: 81-88.

Jin, Y., Z.M. Gu, J.G. Gu and H.W. Zhao, 2007. A new reputation-based trust management mechanism against false feedbacks in peer-to-peer systems. Proceedings of the 8th International Conference on Web Information Systems Engineering, December 3-7, 2007, Nancy, France, pp: 62-73.

Josang, A., 2007. Trust and Reputation Systems. In: Foundations of Security Analysis and Design: FOSAD 2006/2007 Turtorial Lectures, Aldini, A. and ?R. Gorrieri (Eds.). Vol. 4. Springer-Verlag, Berlin, Heidelberg, pp: 209-245.

Josang, A., R. Ismail and C. Boyd, 2007. A survey of trust and reputation systems for online service provision. Decision Support Syst., 43: 618-644.

Kamvar, S.D., M.T. Schlosser and H. Garcia-Molina, 2003. EigenRep: Reputation management in P2P networks. Proceedings of the 12th International World Wide Web Conference, May 20-23, 2003, Budapest, Hungary, pp: 123-134.

Ma, X.X. and Z.G. Qin, 2008. Partition and multi-path transmission: An encryption-free reputation sharing protocol in Gnutella-like peer-to-peer network. Comput. Commun., 14: 3059-3063.

Malik, Z. and A. Bouguettaya, 2009. RATEWeb: Reputation assessment for trust establishment among web services. VLDB J., 18: 885-911.

Namin, A.S., R.Z. Wei, W.M. Shen and H. Ghenniwa, 2005. Applying secret sharing schemes to service reputation. Proceedings of the 9th International Conference on Computer Supported Cooperative Work in Design, Volume 2, May 24-26, 2005, Coventry, UK., pp: 696-703.

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

Stallings, W., 2005. Cryptography and Network Security Principles and Practices. 4th Edn., Prentice Hall, USA.