TELKOMNIKA, Vol. 11, No. 10, October 2013, pp. 6187 ~ 6192
ISSN: 2302-4046

A New P2P Identity Authentication Method Based on Zero-Knowledge Under Hybrid P2P Network

Xiyu Pang*[1], Cheng Wang[1], Yuhong Zhang[2]
[1]Department of Information Technology and Electric Engineering, Shandong Jiao Tong University, Jinan, 250357, China, Ph./Fax: +86-531—80687920
Email: xiyupang@126.com
[2]Department of Computer Technology, Wu Xun High School Liao Cheng, China, +86-635—7321046
*Corresponding author, e-mail: xiyupang@126.com

Abstract

On the basis of analyzing the shortcomings of traditional authentication mechanism synthetically, the paper presents a new kind of P2P identity authentication model. In the new P2P Identity authentication model, it authenticates the identity of nodes by using a new Zero-Knowledge proof identification scheme which combines the advantage of RSA. Besides, during the process of validating nodes' identity, CA (Center Authentication) doesn't need to participate in. At last, Simulation results show that the new P2P identity authentication method can improve the safety of network effectively.

Keywords: *Zero-Knowledge,Identity Authentication, CA, RSA*

1. Introduction

P2P has been widely applied in the fields such as distributed computing, file sharing and swapping, instant messaging, network-attached storage, web searching, network caching, etc.. By far, the most successful application of P2P has been the file sharing and swapping as evidenced by the P2P tools like Napster, Gnutella, BitTorrent and eDonkey which have become the main sources of internet traffic. However, accompanied with the great success of these tools, many new problems have arisen, which are mostly caused by the lack of trust, such as the malicious nodes that deliberately spread the unauthorized, tampered or even virus files.

In P2P system, each entity gets involved in the internet randomly and voluntarily and each entity varies in its capacity and reliability. The relationship among entities is more similar to the complicated social relationship [1]-[3]. The peer-to-peer network lacks centralized monitoring mechanism and the recognized credible third party authority, so the conventional centralized security infrastructure (for example, PKI and Kerberos) is no longer suitable for use, which makes it difficult to realize the trust management in the peer-to-peer network.

The reputation system is a solution to the problem of the lack of trust and it can help to achieve the following two objectives:

1. With the reward or penalty of reputation as the incentive, most nodes which intend to seriously transact are compelled to examine their own behaviors and they are inclined to choose a fixed identity, which will reduce the difficulty in identity management;

2. When the nodes in the system are in need for help, they can resort to the trust system in choosing a credible strange node as a transaction object, which will expand the trust relationship network.

However, the trust system can only help users select more credible nodes, but it fails to provide a mechanism which can enable users to verify that their transaction object is the selected node. Therefore, in addition to the trust system, it is necessary to provide a suitable identity verification mechanism for the security management in the peer-to-peer network.

The fundamental concept of zero knowledge is that one party (the prover) attempts to convince the other party (the verifier) that a statement is true, without providing the verifier any useful information.

Feige-Fiat-Shamir algorithm is the first one that is based on the zero-knowledge proof [7], [8] and its fundamental concept is that P (the prover) initially sends a number X to V (the verifier), V sends back P a random number, then P sends V a number Y encrypted by the P's

Received April 19, 2013; Revised July 15, 2013; Accepted July 25, 2013

private key and the random number, and the verifier identifies the prover by checking whether X and y satisfy a certain formula. Its security is in proportion to 2-kt ,but it has the following defects:

1. If a malicious node tampers the information of P's identity certificate and replaces V's public key with its public key, its private key will be used in computing Y and y can pass the verification of V. In this way, the malicious node can compass its illegal purpose.

2. If a malicious node intercepts the number X sent by P to V, it may derive y according to the final formula, so that the malicious node can impersonate P to gain some interests.

Because the external information exchange is time-consuming, this algorithm is not ideal for the applications like smart card. DaeHun Nyang and JooSeck Song proposed an identification scheme based on the zero-knowledge proof and the scheme requires less communication traffic and computation, which is suitable for smart card system. Because the algorithm is simple, the security of the scheme has yet to be improved.

Therefore, this paper propose a new interactive identification scheme under the P2P network based on the existing zero-knowledge identification, which security is based on the difficulty in the factorization of large numbers and cracking RSA.

2. The Frame of New Identity Authentication Based On Zero-Knowledge

The current P2P framework falls into three categories: the centralized structure, the complete distributed pattern and the presently popular semi-centralized and semi-distributed pattern. The semi-centralized and semi-distributed pattern integrates the advantages of the centralized P2P quick search and the complete distribution of pure P2P. Therefore, the existing P2P applications mostly adopt semi-centralized and semi-distributed pattern, such as Kazaa model, Skype, etc. Besides the registry management center, there is no centralized server. The security model proposed in this paper is under the semi-centralized and semi-distributed P2P network.

The new interactive identity authentication scheme includes two phases: the preprocessing before authentication and the phase of identity authentication:

1. The phase of preprocessing before authentication. During the early stage of establishing the system, each node goes to the management center for registration and the management center will allocate to each node a unique identity, public key and private key and so on.;

2. The phase of identity authentication. It is the process of identity authentication among nodes by using the new zero-knowledge identity authentication method. During this process, the management center is not required to be involved.

2.1. Preprocessing before Authentication

During the early stage of system operation, each node firstly goes to the management center for registration during which the management center entitles each node with a unique ID used to solely represent each user.

Then, the management center uses a one-to-one function h(x) to calculate the node's public key, e:

$$h(ID) = e \quad (1)$$

For each unique ID, there is only one corresponding public key,e.

After computing the public key of the node, according to the Demytko deterministic method of big prime generation, the management center first generates two big primes: p and q, then computes their product according to the formula.

$$n=p*q,\ \varphi(n)=(p-1)*(q-1) \quad (2)$$

Then, it calculates the private key, s, according to the following formula:

$$s^2=e^{-1} mod\ \varphi(n) \quad (3)$$

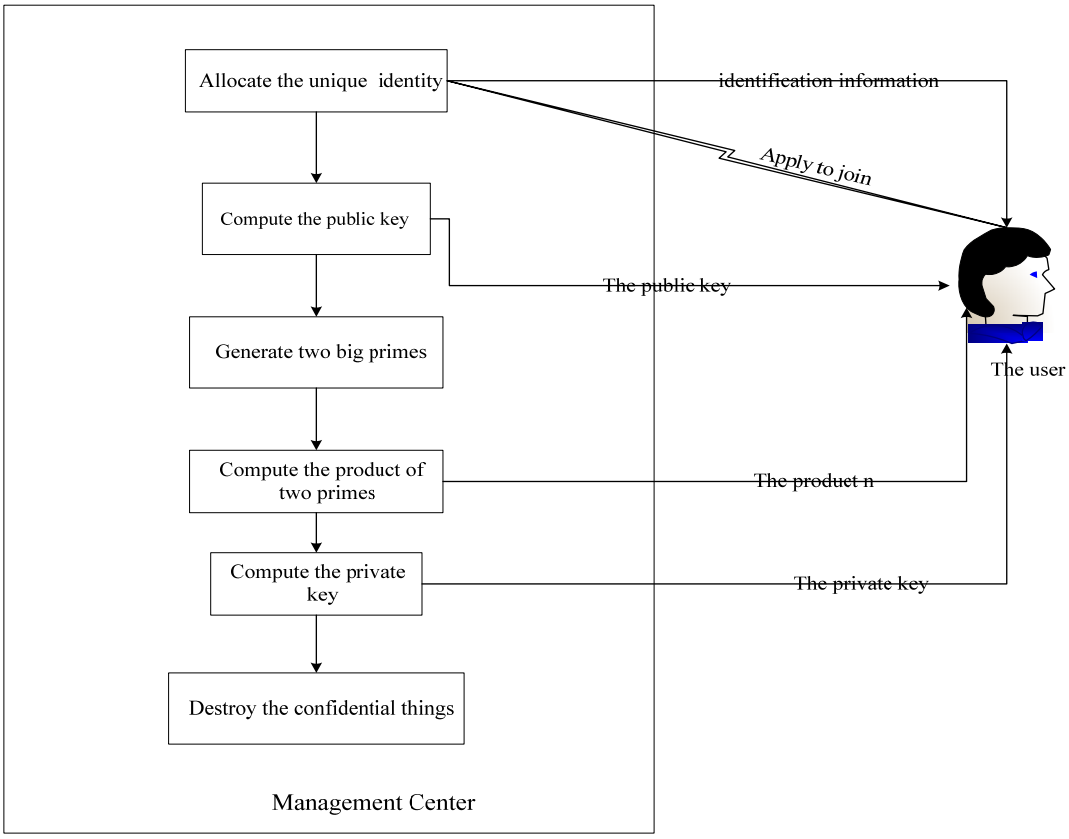

Figure 1. System Establishment Process

Finally, the server sends the ID, the public key (e), the private key (s) and the product (n) of the two big primes to the node, then publicizes the one-to-one function h(x). Because the two primes (p and q) and $\phi(n)$ are prohibited from disclosing, it is recommended to destroy them, then the management center doesn't involve the next process. During the next process of authentication, the management center is not required to be involved. The specific preprocess before authentication is as shown in the Figure 1.

2.2. Identity Authentication Process

Assuming that P and V is performing identity authentication with V as the verifier and P as the requester, the process is as shown in the Figure 2:

(1) P sends V its ID, the public key (e) and the product (n).

(2) V checks the ID and the public key (e) sent by P according to the one-to-one function. If they are one-to-one correspondence, then save the ID, the public key (e) and the product (n). If the identity conforms, then continue, otherwise go to 9.

(3) P randomly chooses an integer (r),1<r<n ,then calculates X according to formula(4), and sends the result to V.

$$X=r^{e} \bmod n \tag{4}$$

(4)V saves X and randomly chooses an integer, $b, b \in \{1,2,\cdots,n\}\ (n \to \infty)$ and secretly sends it to P.

(5)P calculates y according to formula (5) and V's random number sequence, then sends y to V.

$$y = r \times b^{s^2} \bmod n \tag{5}$$

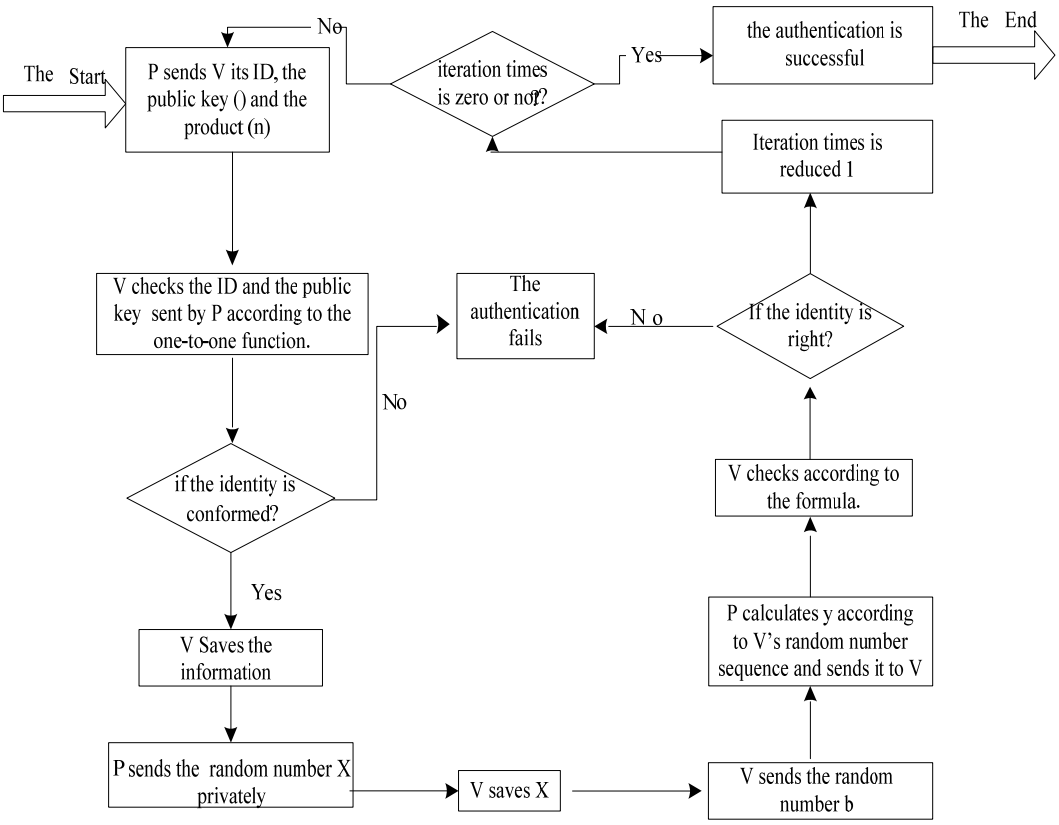

Figure 2. Identity Authentication Process

(6) V checks whether X and y means the formula (6). If it means, then continue, otherwise go to 9.

$$X = y^e \times b^{-1} \bmod n \tag{6}$$

(7) Subtract 1 from the number of iterations and if it becomes zero, then the authentication is successful, otherwise continue.

(8) Repeat step 1 to 9.

(9)The authentication fails and the access is denied.

3. Simulation

To verify the improved zero-knowledge identity authentication algorithm proposed in this paper, several simulation environments are established.

In the simulation, the nodes not only include the common nodes but also a certain number of malicious nodes which play evil roles in identity authentication. At the beginning of the test, there are 100 nodes in the network including about 10% malicious nodes. In the testing simulation environment, the distribution of shared data conforms with Zipf law and the Zipf index is valued between [0.62, 1.25]. In the test, the shared data are defined in the form of files and all files fall into 50 categories with a total number of 60. The 50 different kinds of files are labeled 1, 2… …, 50. Among them, the file with label 1 is the most popular one in the P2P system, the label 2 is less popular and so on. Therefore, in the P2P system, there are most copies of the file with label 1, the label 2 has less copies and so on. Randomly place the 60 files on 10 nodes and make sure each node at least has one file.

In the simulation, each node averagely completes 50 transactions and each transaction makes a node download a file locally. During the transacting process, a node firstly performs the

identity authentication of the node to transact and verifies that if the node is the one it wants to transact. The node randomly sends request for the shared file and when finishing downloading, the copy of the file is saved locally. In the first test, the nodes perform identity authentication by using the Feige-Fiat-Shamir algorithm and in the second test, the nodes adopt the improved zero-knowledge identity authentication algorithm proposed in this paper. After the comparison between the two tests, the result is as shown in the Figure 3.

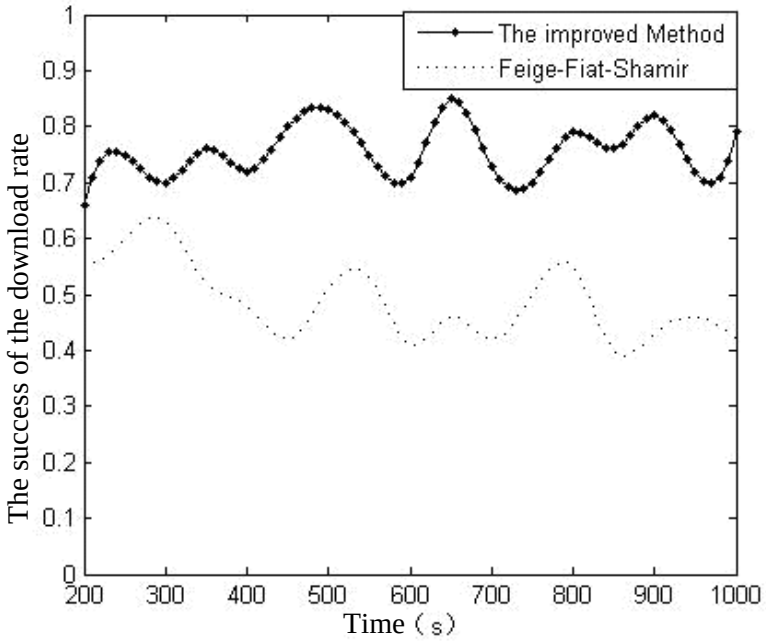

Figure 3. The Result of Simulation

In the figure 3, the horizontal axis is time and the vertical one is successful rate of downloading. As shown in the figure 3, the security performance of the algorithm proposed in this paper is better than that of Feige-Fiat-Shamir algorithm. The reason is that the model proposed in this paper adopts the authentication scheme based on zero knowledge, so if a malicious node impersonates the prover, it cannot know the private key (s) of the prover and there is not enough time for him to figure out the private key (s) by calculating the product (n) and the public key (e), so it cannot work out y in the fifth step and finally it cannot satisfy the condition in the sixth step and fails to pass the verification.

In the simulation, some malicious nodes invent a method against the above circumstances. They send the verifier the ID of the prover and their own public keys. In this way, they can use their private keys to calculate y in the fifth step and pass the verification in the sixth step. However, the proposed algorithm will verify the information sent by the prover to the verifier according to the one-to-one function and those who do not correspond will be denied, so the malicious nodes will fail. To cheat successfully, the malicious nodes must find the X and y which mean the conditions in the sixth step. According to the algorithm, if it wants to find the proper X and y, it must know the random number (b) sent by the verifier (V) to the prover (P) because the final formula requires the random number (b). Supposing the malicious node has intercepted the random number (b), it needs to work out y according to formula (6), which can be regarded as a RSA cracking problem, of which Xb can be seen as the ciphertext obtained by RSA encrypting y via using the public key (n, e), so that the problem turns into the solution of the plaintext corresponding to the ciphertext under the RSA encrypting system without knowing the private key (s), it is contradictory to the supposition.

Assuming the malicious node can predict the random number (b), it can firstly randomly choose a number y, computes X according to formula(6), then send X to the verifier and thus it

can pass the authentication, but the probability of predicting b is 1/m ($m \to \infty$)and after t times of loops, the probability will become1 /mt. Therefore, the new scheme has high reliability and safety.

4. Conclusions

The paper present a new P2P identity authentication based on Zero-Knowledge. In the new scheme, the calculation formula of y in the identity authentication is simpler than the formula used in the Feige-Fiat-Shamir algorithm. The calculation formula of X is not only simpler than the verifying formula in the Feige-Fiat-Shamir algorithm but also safer than that in Feige-Fiat-Shamir algorithm. Because in the new scheme, even if when X and b are known, y cannot be calculated.

The calculation formula of private key in the new scheme is more complicated so its safety is better. In addition, the final verifying formula of the new scheme is simpler than other algorithm.

Acknowledgements

This paper is supported by JiNan Technology Development Planning Project (201221140, 201221141), Shan Dong Jiao Tong University Project (Z201215).

References

[1] Chen K, Hwang K, Chen G.Heuristic discovery of role-based trust chains in peer-to-peer networks. *IEEE Transactions on Parallel and Distributed Systems.* 2009; 41(2): 1600-1604.
[2] WY Lai, CM Chen, B Jeng. *Information exchange mechanism based on reputation in mobile P2P networks*. Proceedings of the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing. 2007; 2: 200-204.
[3] Li Xiong, Ling Liu. PeerTrust: Supporting Reputaion-Based Trust for Peer-to-Peer Electronic Communities. *IEEE Transactions of Knowledge and Data Engineering*. 2004; 16(7): 843-857.
[4] Resnick P, Zeckhauser R, Friedman E, etal. Reputation Systems. *Journal: Communications of ACM*. 2000; 43(12): 45-48
[5] R Zhou, K Hwang, M Cai.GossipTrust for fast reputation aggregation in peer-to-peer networks. *IEEE Transactions on Knowledge and Data Engineering*. 2008; 38(2): 894-899.
[6] Jianming Fu et al. "PerformTrust: Trust model integrated past and current performance in P2P file sharing systems". on Computer Systems and Applications, 2008. AICCSA 2008. *IEEE/ACS International Conference* on . 2008; 1: 36-42.
[7] Zheng Y. *A Conceptual Architecture of a Trusted Mobile Environment*. Proc.of the Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing. 2006; 1: 100-106.
[8] Esther Palomr, Juan ME. *Dealing with Sporadic Strangers, or the (Un) Suitability of Trust for Mobile P2P Security, Tapiador.* 18th International Workshop on Database and Expert Systems Applications. 2007; 1: 45-50.
[9] Wang Cheng. *The Study of P2P Security Model Based on Identity Authentication and Trust mechanism.* Nan Jing Post and Telecommunications. 2007.
[10] Zhao Z, Wei B, Dong X. *Detecting wormhole attacks in wireless sensor networks with statistical analysis.* Proceedings of the International Conference on Information Engineering. 2010: 251-254.