

# An Anonymity Scheme Based on Pseudonym in P2P Networks<sup>\*</sup>

Hao Peng<sup>1</sup>, Songnian Lu<sup>1</sup>, Jianhua Li<sup>1</sup>, Aixin Zhang<sup>2</sup>, and Dandan Zhao<sup>1</sup>

<sup>1</sup>Electrical Engineering Department

<sup>2</sup>Information Security Institute

Shanghai Jiao Tong University, Shanghai, China

{penghao2007, snlu, lijh888, axzhang, zhaodandan}@sjtu.edu.cn

**Abstract.** One of the fundamental challenges in P2P (Peer to Peer) networks is to protect peers' identity privacy. Adopting anonymity scheme is a good choice in most of networks such as the Internet, computer and communication networks. In this paper, we proposed an anonymity scheme based on pseudonym in which peers are motivated not to share their identity. Compared with precious anonymous scheme such as RuP (Reputation using Pseudonyms), our scheme can reduce the overhead and minimize the trusted center's involvement.

**Keywords:** anonymous, P2P networks, pseudonym.

## 1 Introduction

P2P networks are increasingly gaining acceptance on the internet as they provide an infrastructure in which the desired information and products can be located and traded. However, the open nature of the P2P networks also makes them vulnerable to malicious users trying to infect the network. In this case, peers' privacy requirements have become increasing urgent. However, the anonymity issues in P2P networks have not yet been fully addressed.

Current P2P networks achieve a certain degree of anonymity [1] [2] [3], which are mainly based on the following observations:

First, a peer's identity is exposed to all its neighbors. Some malicious peers can acquire information easily by monitoring packet flows, distinguishing packet types [4]. In this case, peers are not anonymous to their neighbors and then P2P networks fail to provide anonymity in each peer's local environment.

Second, in the communication transfer path, there are high risks that the identities of peers are exposed [5] [6]. In an open P2P network, when the files are transferred in a plain text model, the contents of the files also help the attackers on the path guess the identities of the communication parties.

Therefore, current P2P networks cannot provide anonymity guarantees. In this letter, utilizing pseudonym and aiming at providing all the peers' anonymity in P2P

---

<sup>\*</sup> This work was supported by the Opening Project of Key Lab of Information Network Security of Ministry of Public Security under Grant No. C09607.

networks, we propose a new anonymity scheme. It can achieve all the peers' anonymity by changing pseudonym the contributions of our work are summarized as follows. 1) Our scheme reduces the server's cost by more than half in terms of numbers of RSA encryption operations. 2) The deficiency in the RuP protocol is avoided.

## 2 The Proposed Anonymity Scheme

Let  $S$  be the trusted third party server. It has a RSA key pair  $(K_s, k_s)$ . Each peer  $P$  is identified by a self-generated and  $S$ -signed public key as its pseudonym. Each peer can change its  $S$ -signed current pseudonym to an  $S$ -signed new pseudonym to achieve anonymity. Let  $(K_p, k_p)$  and  $(K'_p, k'_p)$  denote the current and new RSA key pairs of peer  $P$ . Respectively  $K\{M\}$  denote encrypting the message  $M$  with the public key  $K$  and  $k\{M\}$  denote signing the message  $M$  with the private key  $k$ . We define  $A$  denote an AES (Advanced Encryption Standard) key.  $H(\cdot)$  denotes a one-way hash function and "||" denotes the conventional binary string concatenation operation.  $v_p$  denote the macro value to be bound to  $U$ 's new pseudonym.

### 2.1 Overview

The main focus of this letter is the design of an anonymity scheme to achieve all the peers' anonymity in P2P networks by changing pseudonym with the help of a trusted server. From the design options provided in [7], we summarize two main challenges.

**Linkage between Pseudonyms.** Because each peer achieves anonymity by contacting the third trusted server to change its current pseudonym to a new pseudonym, the linkage of a peer's current and new pseudonyms should not be disclosed to the server and other peers.

**Linked by the Rating Values.** In P2P networks, each pseudonym is bound with one or more rating values. When a peer changes its pseudonym, its current and new pseudonyms may be linked by the rating values. If a requester changes its pseudonym and the rating values bound to the new pseudonym is unique to that of other peers, the requester's current and new pseudonyms can be linked by its unique rating values.

### 2.2 Review of the RuP Protocol

Here we assume peer  $P$  would like to change its pseudonym from  $K_p$  to  $k_p$  and  $S$ 's RSA key pair be  $(e, d)$  with modulo  $n$ . The pseudonym changing process of the RuP protocol includes two steps: anonymity step and translation step. In the former step,  $S$  first detaches the requester's rating values from the requester's current pseudonym and then binds a macro value to a blinded sequence number selected by the requester. In the latter step,  $S$  transfers the macro value from the unblinded sequence number to the requester's new pseudonym. Blind signature scheme is used to prevent the linkage between the requester's current and new pseudonyms from being disclosed to  $S$ . The details of the RuP protocol are shown below.

Step 1:  $P$  generates a new RSA key pair  $(K_p, k_p)$ , selects a random number  $r \in Z_n^*$ .

$$m = r^e \bmod n. \tag{1}$$

Then  $P \rightarrow S: k_p \{ K_p \parallel m \}$ .

Step 2:  $S$  uses  $P$ 's public key  $K_p$  to verify whether the signature is valid. If it is valid,  $S$  computes  $P$ 's macro value  $v_p$  and blindly signs  $m * H(v_p)$ .

$$m_b = (m * H(v_p))^d \bmod n. \tag{2}$$

Then  $S$  sends  $\{ m_b \parallel v_p \}$  to  $P$  and revokes  $P$ 's current pseudonym  $K_p$ . Then  $S \rightarrow P: \{ m_b \parallel v_p \}$ .

Step 3:  $P$  obtains  $S$ 's signature  $q * H(v_p)$  as follows:

$$(q * H(v_p))^d \bmod n = m_b * r^{-1} = (r^e * H(v_p))^d r^{-1}. \tag{3}$$

Then  $P \rightarrow S: K_s \{ m_b * r^{-1} \parallel v_p \parallel K_p \}$ .

Step 4:  $S$  verifies whether the blind signature is valid. Then  $S$  generates a signature on  $U$ 's new pseudonym  $K_u$ .

Then  $S \rightarrow P: k_s \{ K_p \parallel H(v_p) \}$ .

In this way,  $P$  obtains its new pseudonym  $K_p$  bound with a macro value  $v_p$  signed by  $S$ .

### 2.3 Our Proposed Anonymity Scheme

Firstly, the trusted server  $S$  selects a set of peers which need to communicate with each other to build a path. Secondly,  $S$  sends each peer on the path its next hop individually and directs each peer's new pseudonym through the path. Finally,  $S$  obtains all the new pseudonyms of the peers on the path at one time. Thus,  $S$  and other peers can not find out the linkage of the current and new pseudonyms of any peer who falls in the requester set.

We define each peer  $P_i$  would like to change its pseudonym from  $K_{P_i}$  to  $K_{P_i}$ . Our proposed scheme is described below.

Step 1: Each peer  $P_i$  sends a request to  $S$ . The request includes the current pseudonym  $K_{P_i}$  of  $P_i$  and an AES key  $A_i$  to be shared between  $S$  and  $P_i$ .

$$P_i \rightarrow S: K_s \{ k_{P_i} \{ K_{P_i} \} \parallel A_i \}. \tag{4}$$

*Step 2:*  $S$  first uses its private key  $k_S$  to decrypt the message to obtain  $P_i$ 's current pseudonym  $K_{P_i}$  and the shared AES key  $A_i$ . Here we assume that  $P_1$  is the first peer on the path and  $P_t$  is the last peer. An AES key  $A$  is also generated by  $S$  which is used to encrypt the new pseudonym of each peer on the path. Finally it sends each peer on the path a message. The message sent to  $P_i$  ( $0 < i < t$ ) includes the address of its next hop  $P_{i+1}$  on the path and the AES key  $A$  encrypted with the AES key  $A_i$ . The message sent to  $P_t$  includes the AES key  $A$  encrypted with the AES key  $A_t$  shared between  $P_t$  and  $S$ .

$$S \rightarrow P_i \ (0 < i < t): A_i \{P_{i+1} \| A\}. \quad (5)$$

$$S \rightarrow P_t: A_t \{A\}. \quad (6)$$

*Step 3:* For the first peer  $P_1$  on the path, it obtains  $P_2$ 's address and  $A$  by decrypting the message  $A_1 \{P_2 \| A\}$  sent from  $S$ . Then it generates a new RSA (public, private) key pair  $(K_{P_1}, k_{P_1})$  and encrypts its new pseudonym  $K_{P_1}$  with  $A$ .

*Step 4:*  $P_2$  obtains  $P_3$ 's address and  $A$  by decrypting the message  $A_2 \{A_3 \| A\}$  sent from  $S$ , using the AES key  $A_2$  shared with  $S$ ; it uses  $A$  to decrypt  $K_{P_1}$ . We use  $[K_{P_1} \| K_{P_2} \| \dots \| K_{P_t}]$  to represent any permutations of pseudonyms  $K_{P_1}, K_{P_2}, \dots, K_{P_t}$ . Then it generates a new RSA (public, private) key pair  $(K_{P_2}, k_{P_2})$ , encrypts  $P_1$ 's new pseudonym and its new pseudonym together with  $A$  and sends a message to  $P_3$ . Here the order of the encrypted new pseudonyms is permuted randomly, such that  $S$  can not find out each requester's new pseudonym.

$$P_2 \rightarrow P_3: A \{[K_{P_1} \| K_{P_t}]\}. \quad (7)$$

*Step 5:* The last requester  $P_t$  obtains  $A$  using the AES key  $A_t$  to decrypt  $A_t \{A\}$  sent from  $S$ , using the AES key  $A_t$  shared with  $S$ . After it receives the message  $A \{[K_{P_1} \| K_{P_2} \| \dots \| K_{P_{t-1}}]\}$  sent from  $P_{t-1}$ , it uses  $A$  to decrypt the message. Then it generates a new RSA (public, private) key pair  $(K_{P_t}, k_{P_t})$ , encrypts  $\{[K_{P_1} \| K_{P_2} \| \dots \| K_{P_t}]\}$  with the AES key  $A_t$  and sends a message to  $S$ .

$$P_t \rightarrow S: A_t \{[K_{P_1} \| K_{P_2} \| \dots \| K_{P_t}] \| H(v_P)\}. \quad (8)$$

*Step 6:*  $S$  obtains the new pseudonyms of  $P_1, P_2 \dots P_t$  using the AES key  $A_t$  shared with  $P_t$ . It generates a signature on all the new pseudonyms using its private key and revokes all the current pseudonyms of  $P_1, P_2 \dots P_t$  and sends the signature to  $P_1, P_2 \dots P_t$ . Finally, each requester  $P_i$  obtains its new pseudonym bound signed by  $S$  and its macro value  $v_P$ .

We omitted how  $P_1$  knows that it is the first requester on the path. In step 2 of our scheme,  $S$  can encrypt a flag in the message sent to  $P_1$ . In our design,  $S$  selects several peers who have the same requester peer to build a path. In fact,  $S$  does not need to produce the path beforehand; it can select it when needed. Compared with the RuP

protocol where  $S$  signs each requester a new pseudonym, in our anonymous scheme,  $S$  needs to generate a signature for a set of requesters who have the same request. In this way,  $S$ 's cost is reduced.

### 2.4 The Macro Value

Let  $R_+(K_A, K_B)$  and  $R_-(K_A, K_B)$  denote the sum of positive rating values and the sum of negative rating values given by  $A$  to  $A$ . Respectively  $K_A$  and  $K_B$  are the current pseudonyms of peer  $A$  and peer  $B$ . Then we assume the positive rating ratio  $R(K_A, K_B)$  represents a ratio of total number of positive rating values  $A$  gives to  $B$ . This process can be defined as follows:

$$R(K_A, K_B) = \frac{R_+(K_A, K_B)}{R_+(K_A, K_B) + R_-(K_A, K_B)} \tag{9}$$

A macro value computed every time when its pseudonym changes. We assume the current macro value bound to peer  $A$ 's current pseudonym  $K_A$  is  $v_A$ . Then its new macro value  $v_a$  bound to its new pseudonym  $K_a$  can be computed as follows:

$$v_a = \alpha * \frac{\sum_i R(K_A, K_i)}{t} + (1 - \alpha) * v_A \tag{10}$$

In the formula (10),  $K_i$  is the current pseudonym of the peer  $i$  and  $t$  denotes the size of the set of peers. The parameter  $\alpha$  is used to assign different weights to the average positive rating values ratio and current macro value according to anonymous needs.

## 3 Anonymity Analysis

We will describe how our proposed scheme can achieve anonymity and reduce cost in this section.

**Proposition 1:** Our proposed scheme can achieve anonymity

*Proof:* In our proposed scheme, each peer's anonymity degree is defined as the probability that a peer's pseudonyms are not linked by attackers in the time interval  $T_i$ . If we assume the anonymous have  $n$  peers on the path and a peer's pseudonym changes  $f$  times. For each peer, it does not know other peers' current pseudonyms. The probability for a peer to make a correct linkage of current and new pseudonyms of a peer on the path with  $t$  peers is no more than  $1/n$ . Hence each peer's anonymity degree is  $a_p$ .

$$a_p \geq 1 - \prod_{i=1}^t \frac{1}{n} \tag{11}$$

Therefore in a certain time interval, the higher the frequency change pseudonyms and the larger anonymous set of peers on the path, the better anonymous degree.

**Proposition 2:** Our proposed scheme can reduce cost

*Proof:* For our scheme,  $S$  performs  $t$  RSA encryption operations which is the same as that of the RuP protocol. However,  $S$  performs only  $t+2$  RSA decryption operations, while in the RuP protocol  $S$  needs  $3t$  decryption operations. Because RSA decryption is much slower than RSA encryption, the operation cost of the trusted server is reduced in our scheme.

In Table 1, we can see that our scheme introduces AES encryption and decryption operations compared with the RuP protocol. On the other hand, our protocol does not use blind signature, therefore no additional operation is involved. Compared with the RuP protocol, our protocol does not increase the message overhead.

**Table 1.** Cost comparison ( $t$ : number of peer set)

	Number of operations			
	AES (Enc., Dec.)		RSA (Enc., Dec.)	
	Set	Server	Set	Server
RuP	0	0	$(t, t)$	$(3t, 3t)$
Mine	$(t, 2t-1)$	$(t, 1)$	$(t, t)$	$(t+2, t+2)$

Our scheme is designed to provide anonymity guarantees even in the face of a large-scale attack by a coordinated set of malicious nodes. If the ultimate destination of the message is not part of the coordinated attack, the anonymity scheme still preserves beyond suspicion with respect to the destination.

## 4 Conclusions

In this letter, we discuss an anonymity scheme in P2P networks. The main contribution of this letter is that we present an anonymity scheme based on pseudonym which can provide all the peers' anonymity with the reduced overhead. The analysis has shown that the anonymity issue in our designed scheme can be solved in a very simple way.

## References

1. Cohen, E., Shenker, S.: Replication Strategies in Unstructured Peer-to-peer Networks. In: Proceedings of ACM SIGCOMM (2002)
2. Freedman, M., Morris, R.: Tarzan: A Peer-to-Peer Anonymizing Network Layer. In: Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS) (2002)
3. Liu, Y., Xiao, L., Liu, X., Ni, L.M., Zhang, X.: Location Awareness in Unstructured Peer-to-Peer Systems. IEEE Transactions on Parallel and Distributed Systems (TPDS) (2005)
4. Jøsang, A., Ismail, R., Boyd, C.A.: Survey of trust and reputation for online service provision. Decision Support Systems 43(2), 618–644 (2007)

5. Hao, L., Yang, S., Lu, S., Chen, G.: A dynamic anonymous P2P reputation system based on Trusted Computing technology. In: Proceedings of the IEEE Global Telecommunications Conference, Washington, DC USA (2007)
6. Miranda, H., Rodrigues, L.: A framework to provide anonymity in reputation systems. In: Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems: Networks and Services, San Jose, California (2006)
7. Lua, E.K., Crowcroft, J., Pias, M., Sharma, R., Lim, S.: A survey and comparison of peer-to-peer overlay network schemes. *IEEE Commun. Survey and Tutorial* 7(2), 72–93 (2005)