International Journal of Security and Its Applications
Vol.9, No.8 (2015), pp.397-408
http://dx.doi.org/10.14257/ijsia.2015.9.8.35

Leveraging Certificate-less Public Key Cryptosystem for Node ID Assignment in Structured P2P Systems

Dengqi Yang*, Jian Yang and Benhui Chen

School of Mathematics and Computer Science, Dali University, Dali 671003, China
dengqiyang@163.com; sbjc1215@126.com; bhchen_dali@163.com

Abstract

The security of node ID assignment scheme is the foundation of solving security problems in structured P2P systems. However, existing researches on the node ID assignment mechanism present one or more following problems: (1) Schemes just only focused on individual attack, but did not comprehensively analyze the security requirements of node ID assignment mechanism. (2) Schemes needed complex certificate management or met key escrow problem. (3) Almost all existing schemes required a trusted center to act as the single signer of node IDs, but it is very hard to find an absolutely trusted node in structured P2P system. As a result, none of existing schemes can prevent the single signer from being compromised or launching active attack. This paper firstly designs a threshold signature scheme based on secret sharing and certificateless public key cryptosystem without paring (CL-PKC-without-P). Based on that, it proposes a node ID assignment protocol which eliminates the three problems listed above. Using secret sharing technology, this protocol is able to resist the active attacks launching by less than t *signer, where* t *is the threshold value. The results of analysis and simulation show that this protocol is more secure, efficient and scalable.*

Keywords: *Secret sharing without relier, Certificateless signature, node ID assignment*

1. Introduction

Structured P2P network becomes more and more popular because it shows many advantages, such as better scalability, robustness and self-organization characters and so on. It can easily achieve large-scale, low-cost resource sharing. In structured P2P systems, a node represents an instance of a participant in the systems, which means that a single physical IP host may host one or more nodes. Each participating node is assigned a unique identifier, called node ID, which is the base to achieve self-organization and self-management of resources and to achieve the connectivity among nodes in structured P2P overlay network. However, many attacks related to node ID have been detected in structured P2P systems, such as nodes insertion attack [1], Sybil attack [2], Eclipse attack [3] and so on. To construct secure structured P2P systems, it is necessary to find a security and reliable node ID assignment and to check mechanism for structured P2P systems. On the other hand, node ID is the necessary element to implement other security mechanisms, such as key management, digital signature, identity authentication, in structured P2P systems. Therefore, the assignment of node ID has a great significance for constructing secure structured P2P systems.

Existing node ID assignment schemes for structured P2P systems mainly aim to defense the Sybil attack. For example, based on computational puzzles, Rowaihy [4] and Borisov [5] presented ID assignment schemes which could efficiently defense Sybil attack, but they did not discuss the cryptographic technologies adopted in their work.

ISSN: 1738-9976 IJSIA

Nguyen [6] and Lesueur [7] proposed ID assignment schemes using public key certificate technology, but their schemes required complex certificate management. Based on Identity-Based Cryptography [8], Butler [9] and Ryu [10] designed ID assignment schemes, however, their schemes met the key escrow problem and required the trusted third party, which cannot be adopted for usual structured P2P systems.

In 2012, YANG *et al*. [11] presented a reliable ID assignment scheme, which based on certificateless public key cryptosystem without pairing, for structured P2P systems. This scheme eliminated the key escrow problem and the bilinear pairings operation which was usually considered to be expensive. This scheme was able to defend most of attacks related to node ID. Unfortunately, the ID of new arrival node is assigned by a single signer in this scheme, so it cannot prevent the single signer from being compromised and launching active attack. In fact, it is very hard to find an absolutely honest node, which can act as the signer, in structured P2P system.

This paper firstly determines the goals of secure node ID assignment scheme, and then designs a certificateless (t,n) threshold signature scheme based on secret sharing technology and certificateless cryptography without paring [12]. As far as we know, this is the first certificateless threshold signature scheme without pairing. Based on the scheme, this paper presents a secure node ID assignment protocol, which does not require the trusted third party, for structured P2P systems. This ID assignment protocol avoids the complicated certificate management, key escrow problem and bilinear pairing operation. What is more, it is able to prevent the active attacks launched by less than t signers, who have been compromised, because that each valid ID is signed by t ($1<t<n$) signers together. Analysis shows that this protocol is scalable, security and efficient.

2. Preliminary

In a certificateless public key cryptosystem (CL-PKC), it is assumed that each user is assigned a unique and public identity, called ID. Based on the user's identity ID, in CL-PKC, every user's private key is composed of a secret value independently generated by the user itself and a user partial private key issued by a Key Generation Center (KGC). A user can only perform some cryptographic operations if and only if he/she knows both the user's partial private key and the user's secret value. Adversary knows only one of them should not be able to carry out any of the cryptographic operations as the valid user.

In our previous work on P2P security architecture [11, 13], we presented the definition of reliable node ID. This work focuses on the secure assignment and validation of node ID in structured P2P systems. To enhance the security of ID assignment, we modify the goals of ID assignment scheme which was defined in literature [11], the new goals of ID assignment protocol are described as follows.

- *Uniqueness*: A node in a P2P system can only be mapped to one ID in the ID space, and vice versa.
- *Non-customization*: Users can not designate desired IDs for their nodes.
- *Limitation*: The number of simultaneous IDs a node can acquire should be bounded by the system.
- *Non-forgeability*: (1) The validity of each node ID can be verified by other nodes in P2P system. This prevents a node from designating expected ID for itself. (2) Each ID should be assigned by at least t nodes (signers) together. This prevents one or a small number of nodes (signers) from forging specific IDs for the new arrival nodes.
- *Scalability*. The reliable ID assignment scheme should show good scalability.
- *Efficiency*. The reliable ID assignment scheme should be efficient.

This paper assume that the communication environment is not secure: the attacks can spoof any source IP address. Attackers may eavesdrop and modify any packet on the communication link. But it explicitly does not assume that an attack can hijack arbitrary

IP addresses. The number of adversarial or compromised nodes does not be restricted in system. An individual adversary is assumed to have limited access to computational resources and available IP addresses. It is also assumed that the absolutely honest nodes, which can independently keep the master key of system and never be compromised, do not exist in structured P2P system.

Analysis showed that a new node has to get in contact with more than one old node, called bootstrap nodes (BN), for joining the structured P2P network, such as Chord, Pastry, KAD, etc. These BNs have joined in the structured P2P network. Some BNs are provided by the organization or ownership of the P2P systems. Some BNs are selected by trust management mechanism in P2P systems. Both these BNs are relatively reliable nodes, but it does not assure that none of them may be compromised at some times. Generally, the IDs of bootstrap nodes are public and well-known.

3. Reliable ID Assignment Protocol

3.1 Threshold Signature Scheme based on CL-PKC-without-P

As described above, there are some relative reliable BNs in structured P2P systems. We firstly select *n* BNs from them to act as the signature service providers and negotiate the system parameters. These *n* BNs notated BN_i ($i=1,2,...,n$), and their ID notated ID_{BN_i}. We design certificateless threshold signature scheme as following.

In this signature scheme, any message should be signed by at least *t* BNs together. Each BN can only generate a sub-signature. A whole and valid signature can be constructed, according to threshold method, while gathering at least t sub-signature on the same message. In this case, only at least t BNs conspiracy can maliciously generate a valid signature. The details of signature scheme are described as follows.

i. BN Initialization

In the initial phase, these *n* BNs negotiate the system parameters $<p,q,G,P,P_0,H_1,H_2>$, where p,q are two primes such that $q|p-1$; G is a cyclic additive group on secure elliptic curve. P is a generator of G, and q is the order of P; $H_1:\{0,1\}^* \times G \times G \mid\rightarrow Z_q^*$, $H_2:\{0,1\}^* \mid\rightarrow Z_q^*$ are two hash functions; $P_0 = sP$ is the system public parameter, where 's' is the system private key. P_0 must be negotiated by *n* BNs together from the following factors.

1) BN_i ($i=1,2,...,n$)randomly generates a secret $b_i \in GF(p)$ and a polynomial $f_i(x)$ with degree $t-1$: $f_i(x) = a_{i,0} + a_{i,1}x + \cdots + a_{i,t-1}x^{t-1} \bmod p$, $a_{i,j} \in GF(p)(j=0,1,...,t-1)$, s.t. $f_i(0)=a_{i,0}=b_i$, and then broadcasts $B_{i,k}=a_{i,k}P(k=0,1,...,t-1)$ to all other $n-1$ BNs.
2) BN_i computes $f_i(ID_{BN_j})$ for other n-1 BNs, and then transmits $f_i(ID_{BN_j})$ to BN_j (j=1,2,…,n, $j \neq i$) by secure channel.
3) After BN_j received $f_i(ID_{BN_j})$ from BN_i (i=1,2,…,n), it verifies its validity by (1) :

$$f_i(ID_{BN_j}) \cdot P = \sum_{k=0}^{t-1} B_{i,k}(ID_{BN_j})^k \bmod q \quad (1)$$

If (1) holds, then $f_i(ID_{BN_j})$ is valid; otherwise, it is invalid.

4) After BN_i (i=1,2,…,n) received all $f_j(ID_{BN_i})$ (j=1,2,…,n, $j \neq i$)from other n-1 BNs and verified their validity, it computes $\sum_{j=1}^{n} f_j(ID_{BN_i}) \cdot P$ and broadcasts it to other n-1 BNs. (i=1,2,…,n).
5) After BN_i (i=1,2,…,n) received all $\sum_{k=1}^{n} f_k(ID_{BN_j}) \cdot P$ (j=1,2,…,n, $j \neq i$) from other n-1 BNs, it computes:

$$P_0 = \sum_{i=1}^{t} \sum_{j=1}^{n} f_j(ID_{BN_i}) \cdot P \cdot L_i = \sum_{i=1}^{n} f_i(0) \cdot L_i \cdot P = \sum_{i=1}^{n} b_i \cdot P,$$

where $L_i = \prod_{k=1,k\neq i}^{t} \frac{ID_{BN_k}}{ID_{BN_k} - ID_{BN_i}}, (i = 1,2,\cdots,n)$. Let $s = \sum_{i=1}^{t}\sum_{j=1}^{n} f_j(ID_{BN_i}) \cdot L_i$, then s is the system master key. $P_0=sP$ is the system public key. Let $s_i = \sum_{j=1}^{n} f_j(ID_{BN_i})$, then s_i is sub-key of s, called sub-master-key, which should be secretly kept by BN_i (i=1,2,…,n).

ii. Key generation for BN

In this phase, BN_i (i=1,2,…,n) chooses its secret value and computes its public key.

1) BN_i (i=1,2,…,n) randomly chooses $x_i \in Z_q^*$, $r_i \in Z_q^*$, and computes public key $X_i=x_iP$, $R_i=r_iL_iP$, then broadcasts $< ID_{BN_i}, R_i, X_i >$ to BN_j (j=1,2,…,n, $j\neq i$). BN_i saves BN_j's public keys.
2) BN_i (i=1,2,…,n) sets its public key $PK_{BN_i} =< X_i, R_i >$ and private key $SK_{BN_i} =< x_i, \perp >$, where $\perp$ denotes the partial private key, which means that it is not been computed temporarily.

iii. Signature and Verification

(1) Signature

When user A asks BNs to sign message m, it firstly selects t BNs from structured P2P system. Without loss of generality, we assume that user A has selected $BN_1,BN_2,\ldots,BN_t$. Then user A builds the set $I = \{ID_{BN_1}, ID_{BN_2}, \cdots, ID_{BN_t}\}$ and sends I to $BN_1,BN_2,\ldots,BN_t$, which makes them know that who are selected by user A to sign message m. After BN_i ($i=1,2,\ldots,t$) received A's signature request on message m, it does the following steps.

1) BN_i randomly chooses $\alpha_i \in Z_q^*, \alpha_i \neq 0$, and computes $T_i=\alpha_iP$, and then sends $< ID_{BN_i}, T_i, X_i, R_i >$ to BN_j ($j=1,2,\ldots,t, j\neq i$).
2) After BN_i received all $< ID_{BN_j}, T_j, X_j, R_j >$ from BN_j ($j=1,2,\ldots,t$, $j\neq i$), it computes $ID = ID_{BN_1} \| ID_{BN_2} \| \cdots \| ID_{BN_t}$, $T = \sum_{j=1}^{t} T_j$, $R = \sum_{j=1}^{t} R_j$, $X = \sum_{j=1}^{t} X_j$, $D_i=r_i+s_i \cdot H_1(ID,R,X)$, $\gamma=H_1(ID,T,X)$, $e=H_2(ID||m)$, $\sigma_i = \alpha_i e+\gamma(x_i+D_iL_i)$, then generates sub-signature (σ_i, γ,T_i) and sends it to A. (BNs can preprocess the public parameters R and X, which can improve the signature efficiency) .

(2) Verification

After A received all (σ_i, γ,T_i) from BN_i (i=1,2,…,t), it computes $Q_i = \sigma_i e^{-1} \cdot P - \gamma X_i e^{-1} - \gamma R_i e^{-1} - \gamma H_1(ID,R,X) e^{-1} L_i \cdot P_i$, and verifies $Q_i = T_i$, if it holds, then accepts σ_i; otherwise, refuses σ_i and requests re-signing.

Verification correctness proof:

$$
\begin{aligned}
Q_i &= \sigma_i e^{-1} \cdot P - \gamma X_i e^{-1} - \gamma R_i e^{-1} - \gamma H_1(ID,R,X) e^{-1} L_i \cdot P_i \\
&= [\alpha_i e + \gamma(x_i + D_i L_i)] e^{-1} \cdot P - \gamma X_i e^{-1} - \gamma R_i e^{-1} - \gamma H_1(ID,R,X) e^{-1} L_i \cdot P_i \\
&= \alpha_i P + \gamma x_i e^{-1} \cdot P + \gamma(r_i + s_i H_1(ID,R,X)) L_i e^{-1} \cdot P \\
&\quad - \gamma X_i e^{-1} - \gamma R_i e^{-1} - \gamma H_1(ID,R,X) e^{-1} L_i \cdot P_i \\
&= T_i + \gamma X_i e^{-1} + \gamma R_i e^{-1} + \gamma H_1(ID,R,X) L_i e^{-1} \cdot P_i \\
&\quad - \gamma X_i e^{-1} - \gamma R_i e^{-1} - \gamma H_1(ID,R,X) e^{-1} L_i \cdot P_i = T_i
\end{aligned}
$$

If all σ_i ($i=1,2,\ldots,t$) are correct, then user A computes $\sigma = \sum_{i=1}^{t} \sigma_i$ which is the whole and valid signature on message m. It is generated by $BN_1,BN_2,\ldots,BN_t$ together.

Another user called B can verify the validity of σ by computing:

$Q = \sigma e^{-1} \cdot P - \gamma X e^{-1} - \gamma \mathrm{Re}^{-1} - \gamma H_1(ID, R, X) e^{-1} \cdot P_0$, and verifying $H_1(ID, Q, X) = \gamma$.

If it holds, then accepts signature σ; otherwise, it refuses it.

Verification process correctness proof:

$$Q = \sigma e^{-1} \cdot P - \gamma X e^{-1} - \gamma \mathrm{Re}^{-1} - \gamma H_1(ID, R, X) e^{-1} \cdot P_0$$

$$= \sum_{i=1}^{t} \sigma_i e^{-1} \cdot P - \gamma X e^{-1} - \gamma \mathrm{Re}^{-1} - \gamma H_1(ID, R, X) e^{-1} \cdot P_0$$

$$= \sum_{i=1}^{t} [\alpha_i P + \gamma x_i e^{-1} \cdot P + \gamma (r_i + s_i H_1(ID, R, X) L_i e^{-1} \cdot P] - \gamma X e^{-1} - \gamma \mathrm{Re}^{-1} - \gamma H_1(ID, R, X) e^{-1} \cdot P_0$$

$$= \sum_{i=1}^{t} [T_i + \gamma X_i e^{-1} + \gamma R_i e^{-1} + \gamma H_1(ID, R, X) s_i L_i e^{-1} \cdot P] - \gamma X e^{-1} - \gamma \mathrm{Re}^{-1} - \gamma H_1(ID, R, X) e^{-1} \cdot P_0$$

$$= T + \gamma X e^{-1} + \gamma \mathrm{Re}^{-1} + \gamma H_1(ID, R, X) e^{-1} \cdot P_0$$

$$-\gamma X e^{-1} - \gamma \mathrm{Re}^{-1} - \gamma H_1(ID, R, X) e^{-1} \cdot P_0 = T$$

Thus, $H_1(ID, Q, X) = H_1(ID, T, X) = \gamma$

3.2 Node ID Assignment Protocol

To avoid single BN maliciously signs and assigns ID when it is compromised or launched active attack. We design the reliable ID assignment protocol based on the threshold signature scheme proposed in section 3.1. This protocol requires that each node ID is signed by at least t BNs together. If there is less than t BNs, it is impossible to issue a valid ID for joining node. Therefore, it largely reduces the probability of maliciously signing and assigning ID by single or a few BNs.

When a new arrival node notated N_{New} hopes to join structured P2P system, it firstly contacts t BNs which are notated with $BN_1, BN_2, \ldots, BN_t$, and sends ID assignment request to them. After some necessary checking, a vaild ID will be signed and assigned to N_{New} by $BN_1, BN_2, \ldots, BN_t$ together. Because we assume that attackers can spoof any source IP address. To test the reachability of each joining node's IP address, each joining node is weakly authenticated via callback: all responses to requests are transmitted through a BN-initiated TCP connection. To implement the *limited* goal of ID assignment, BN requires each joining node to solve a computational puzzle to control the time-cost of ID acquiring for joining nodes. The details of ID assignment protocol are shown in Fig.1.

i. System Setup

In the system setup phase, the BNs firstly establish secure channel via a Diffie-Hellman key exchange for transmitting the secure parameters. Secondly, the BNs negotiate a master key *s*, the system parameters $params=\{p,q,G,P,P_0,H_1,H_2\}$, and their sub-master-key s_i. Thirdly, the BNs generate their public and private key. The specific operational details, please refer to section 3.1.

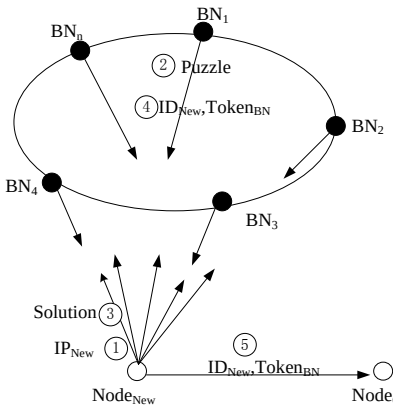

Figure 1. Node ID Assignment Protocol

ii. Node Join

N_{New} contacts the BN_i ($i=1,2,...,t$) and sends $< IP_{New}, ID_{BN_1}, ID_{BN_2}, \cdots, ID_{BN_t} >$ to BN_i. After a weakly authenticating on the identity of N_{New}, BNs negotiate a hash computational puzzle and transmits it to N_{New}. The N_{New} solves the puzzle and sends the solution to BN_i. After verifying the correctness of solution, *BNs* negotiate a common time stamp TS_{New}, and generate an identity ID_{New} according to IP_{New}, then sign the ID_{New} using their private key and sub-master-key. A more formal expression of the protocol is as follows:

1. $\text{Node}_{New} \rightarrow \text{BN}_i$: IP_{New}, $\text{ID}_{\text{BN}_1}, \text{ID}_{\text{BN}_2}, \cdots, \text{ID}_{\text{BN}_t}$
2. $\text{BN}_1, \text{BN}_2, \cdots, \text{BN}_t$ negotiate puzzle Q and TS_{New}
3. $\text{BN}_i \rightarrow \text{Node}_{New}$: $\text{TS}_{New}, \text{h}(\text{IP}_{New}, \text{TS}_{New}, Q)$ (puzzle)
   $\text{Sign}(\text{IP}_{New}||\text{TS}_{New}||Q, SK_{BN_i})$
4. $\text{Node}_{New} \rightarrow \text{BN}_i$: $\text{IP}_{New}, \text{Q}, \text{TS}_{New}, \text{Sign}(\text{IP}_{New}||\text{TS}_{New}||Q, SK_{BN_i})$ (solution)
5. $\text{BN}_i \rightarrow \text{Node}_{New}$:
   $\text{ID}_{New}, \text{TS}_{New}, \sigma_i = \text{Sign}(\text{ID}_{New}||\text{ID}_{\text{BN}_1}||\text{ID}_{\text{BN}_2}||\cdots||\text{ID}_{\text{BN}_t}||\text{TS}_1\}, SK_{BN_i})$ (token)

Where ID_{New}=SHA-1($\text{IP}_{New}||\text{Port}_{New}||\text{TS}_{New}$)。

After N_{New} received all σ_i and verified t validity, it computes $\sigma = \sum_{i=1}^{t} \sigma_i$ which is the signature on ID_{New} by t BNs. Thus far, N_{New} acquires the token for joining the structured P2P system. In ID assignment protocol, the computational puzzle Q is negotiated by $BN_1, BN_2, \ldots, BN_t$ together, which can improve the security of protocol. TS_{New} can defense the replay attack. In this protocol, we can improve system scalability by increasing the number of BNs.

iii. Add BNs

With the expansion of the system scale, this protocol can increase the number of BNs to assure its efficiency. Assuming that BN_{New} has already acquired a valid ID denoted $ID_{BN_{New}}$. BN_{New} then generates its sub-master-key and computes its public/private key, which is described as follows.

1) BN_{New} sends $< ID_{BN_{New}}$, *sub-master request*$>$ to BN_i ($i=1,2,...,n$).
2) BN_i ($i=1,2,\ldots,n$) computes $f_i(ID_{BN_{New}})$, transmits it to BN_{New} through secure channel, then sends $B_{i,k} = a_{i,k} P (k = 0,1,\cdots,t-1)$ and $\sum_{j=1}^{n} f_j(ID_{BN_i}) \cdot P$ to BN_{New} through public channel.
3) After BN_{New} received $f_i(ID_{BN_{New}})$ from BN_i ($i=1,2,...,n$), it verifies its validity by (3) :

$$f_i(ID_{BN_{New}}) \cdot P = \sum_{k=0}^{t-1} B_{i,k} (ID_{BN_{New}})^k \bmod q \quad (3)$$

If (3) holds, then $f_i(ID_{BN_{New}})$ is valid; otherwise, it is invalid.

4) After BN_{New} successfully checks the validity of $f_i(ID_{BN_{New}})$ ($i=1,2,\ldots,n$), it computes and judges whether $P_0 = \sum_{i=1}^{t-1} \sum_{j=1}^{n} f_j(ID_{BN_i}) \cdot P \cdot L_i + \sum_{j=1}^{n} f_j(ID_{BN_{New}}) \cdot P \cdot L_{New}$ is established. If it is established, then BN_{New} secretly keeps the $f_i(ID_{BN_{New}})(i=1,2,\cdots,n)$ and sets $s_{New} = \sum_{j=1}^{n} f_j(ID_{BN_{New}})$ as its sub-master-key which should be secret.
5) BN_{New} executes the key generation procedure showed as section 3.1 to generate its public key $PK_{BN_{New}} =< X_{New}, R_{New} >$ and private key $SK_{BN_{New}} =< x_{New}, \perp >$.

After finished the above four steps, BN_{New} has been added to the structured P2P system without changing the system master key. It can improve the efficiency of reliable ID assignment and make the system become more scalable by adding more signers to protocol.

4. Security, Goals and Performance

4.1 Security Analysis

In our protocol, the reliable ID is unforgeable if and only if the signature schemes are secure. So the security of reliable assignment protocol depends on the security of certificateless signature scheme proposed in section 3.1. Due to the space constraint, we do not give the proof process of the unforgeablity of our signature scheme here, but just do some brief analysis.

Two adversary attack models are consided in the CL-PKC. The first adversary attack model is the public key replacement attack, notated A_I. In attack model A_I, the adversary is able to replace any user's public key, but it can not access the system master *s*. The second adversary attack model is master key attack, notated A_{II}. In which, the adversary is able to access the system master *s*, but it can not replace the public key of target user or inquire the secret value of target user.

In our signature scheme, BN_i's public key is $PK_{BN_i} =< X_i, R_i >$ and its private key is $SK_{BN_i} =< x_i, D_i >$ (i=1, 2,…,n), where $D_i=r_i+s_i \cdot H_1(ID,R,X)$ and $ID = ID_{BN_1} \| ID_{BN_2} \| \cdots \| ID_{BN_t}$.

1) Public Key Replace Attack

Obviously, user's public key is bound by both user ID and the secret value seclected by user itself in CL-PKC. User's private key is ralated to the secret value x_i and the partial private key D_i. And the partial private key D_i is related to the sub-master-key s_i. The sub-master-key s_i contained in the partial private key D_i is the foundation to resist to public key replacement attack in CL-PKC. BN_i ($i=1,2,...,t$) generates the sub-signature σ_i on ID_A using its private key SK_{BN_i} and sends message $< ID_{BN_i}, PK_{BN_i}, ID_A, \sigma_i >$ to node A. After node A received t sub-signature σ_i, it verifies σ_i using public key PK_{BN_i}. If each σ_i is valid, then node A computes the whole signatue σ on ID_A. If adversary B attempts personate BN_i to generate the sub-signature σ_i', it can choose a secret value x_i' and a ramdom r_i', then it computes $X_i' = x_i' \cdot P, R_i' = r_i' \cdot P$, and replaces BN_i's public key PK_{BN_i} with $PK'_{BN_i} =< X_i', R_i' >$. Finally, adversary B sends $< ID_{BN_i}, PK'_{BN_i}, ID_A, \sigma_i' >$ to node A. Assuming that the signature algorithm used is unforgeable. If Adversay B attemps to forge a sub-signature σ_i' which can be verified by the new pbulic PK'_{BN_i}, it must know the private key SK'_{BN_i} which corresponds to PK'_{BN_i}. Howerver, the partial private key $D_i=r_i+s_i \cdot H_1(ID,R,X)$ contained in private key SK'_{BN_i}. Adversary B can compute D_i if and only if it knows the sub-master-key s_i. As described above, adversary B can not access sub-master-key s_i in A_I. Thus, it can not forge a valid sub-signature.

2) Master Key Attack

Situation is similar when adversary B attempts personate BN_i to generate the sub-signature σ_i' in A_{II}. Because adversary B knows the sub-master-key s_i, it can choose a ramdom r_i', then it computes $R_i' = r_i' \cdot P$, $D_i' = r_i' + s_i \cdot H_1(ID, R', X)$ and sends $< ID_{BN_i}, PK'_{BN_i}, ID_A, \sigma_i' >$ to node A. It is assumed that the signature algorithm used is unforgeable. If Adversary B attempts to forge a sub-signature σ_i' which can be verified by the new pbulic PK'_{BN_i}, it must know the private key SK'_{BN_i} corresponding to PK'_{BN_i}. However, BN_i's secret value x_i contained in the private key SK'_{BN_i}. As described above, adversary B cannot replace or inquire the secret value x_i in A_{II}. Thus, it cannot forge a valid sub-signature.

3) Anti- KGC Active Attack

As AlRiyami [12] said, there was only one single node acting as the KGC in CL-PKC. It kept the system master key *s*. Thus the KGC is able to perfonate any user and carry out any cryptography operation, if it launches active attack. In this case, the security of signature scheme depends on the reliability and honesty of KGC.

Based on the secret sharing technology, the selected *n* BNs adopt the Lagrange interpolating polynomials $f_i(x)$ with degree *t-1* to negotiate and compute the sub-master-key s_i in our signature scheme, which implicitly determinates the system master key *s*. Each BN can be considered as a sub-KGC, so there are *n* sub-KGCs in our scheme. None single BN is able to sign a whole signature, which greatly reduces the security dependence on single signer. For a polynomial of degree *t-1*, it is impossible to reconstruct the polynomial while someone knows less than *t* (*ID*,*f*(*ID*)) pairs. Thus, they cannot forge a whole and valid signature while the number of collusive or compromised BN is less than *t*. Given that the possibility for each BN being compromised is equally assumed as *p*, then the probability of no less than *t* BNs compromised probability is (4)

$$p_{Collusion} = \sum_{i=t}^{n} C_n^i p^i (1-p)^{n-i} \quad (0 \le p < 1) \tag{4}$$

4.2 The Goals Achievement of ID Assignment

This protocol achieves the goals of reliable ID assignment defined in section II. It can be easily found that this protocol satisfies the *uniqueness* and *non-customization* goals because of the properties of SHA-1. The *limited* goal has achieved because of the callback behavior and computational puzzle. The *nonforgeability* goal is achieved because that each ID has been signed by more than t BNs, which cannot be forged if the attacker does not know the private key of BN_i and the corresponding sub-master-key. The *scalability* goal can be achieved by adding the number of BN into structured P2P systems. This protocol can noticeably reduce cost and system complexity because that it requires neither certificates management nor bilinear pairings operation. So it is *efficiency*.

4.3 Performance

1) Signature scheme performance comparison

The performance of our ID assignment protocol depends on the efficiency of signature scheme. So we analyze the efficiency of our signature scheme and give a comparison between our scheme and existing certificateless threshold signature schemes in table 1. In Table 1, P denotes bilinear parings operation, E denotes exponentiation operation, S denotes scalar multiplication on elliptic curve, and H denotes Hash operation. n_u and n_m denote the length of user identities and messages, respectively.

Table 1. Comparison of Performance

Schemes	Signature	Verification
Scheme in[16]	4tP+2E+(t-1)S	6P+2E
Scheme in[17]	6(t-1)P+(n_m+3)S	3P+(n_u+n_m)S
Scheme in[18]	t(4S+2H+2P)	2S+3H+2P
Scheme in[19]	(3t+2)E+3P	3P
Our Scheme	t(1S+2H)	4S+1H

Chen [14] showed that the costs of one bilinear pairing operation, exponential operation and hash operation were at least 21 times, 3 times and 1 times of the costs of one scalar multiplication operation on elliptic curve, respectively.

2) Performance of ID assignment protocol

In our ID assignment protocol, to generate a valid signature, each BN_i need 1 time scalar multiplication on elliptic curve and 2 times hash operations when it computes $T_i=\alpha_i P$ and D_i, γ, respectively. To verify the validity of signature, each new arrival node need $4(t+1)$ times scalar multiplication on elliptic curve and $(t+1)$ times hash operation when it checks the correctness of σ_i and σ.

In ID assignment protocol, one of the goals for reliable ID assignment is to limit the time-costs that a new node acquires its valid ID. This time should not be too short in order to prevent the Sybil's attack. So we just need consider the cost for signature on the BNs. Using the probability formula, we can get the average signature times of BN_i ($i=1,2,\ldots,n$), when m new arrival nodes join systems, as (5).

$$\frac{C_{n-1}^{t-1}}{C_n^t} \cdot m = \frac{tm}{n} \tag{5}$$

We evaluated the costs of ID assignment protocol using elliptic curve-256 on a PC whose CPU frequency is 2.60 GHz and RAM is 2GB. The system parameters are shown in Figure 2.

```
                System params
P-256 curve: y^2=x^3+Ax+B
Coefficient A:
 14615016373309029182036848327162830196537850593 24.
Coefficient B:
 16323579130616811054660491940327157953054834 5413.
Base Point P:
 X: 42582623172388835044654159270140906591363556 8770.
 Y: 20352011416290410787399145795734689202798264 1970.
Subgroup Order q:
 14615016373309029182036871976068267798846434924 39.
Hash H1, H2:
 Both use SHA-256.
```

Figure 2. Simulation System Parameters

Given that the possibility of each BN selected to provide ID assignment service is the same. Then Figure 3 shows the cost of BN_i to sign valid IDs for m new joining nodes when the value of t is different.

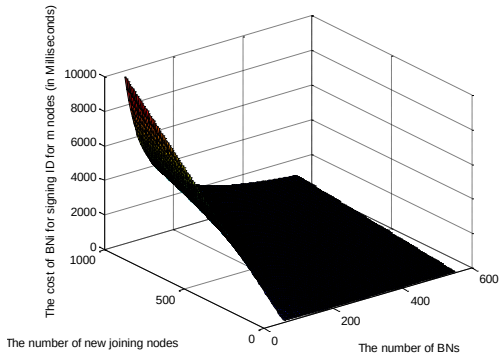

Figure 3(a). BN_i's Cost, t=30

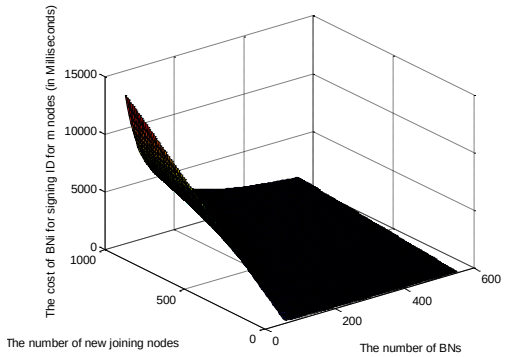

Figure 3 (b). BN_i's Cost, t=40

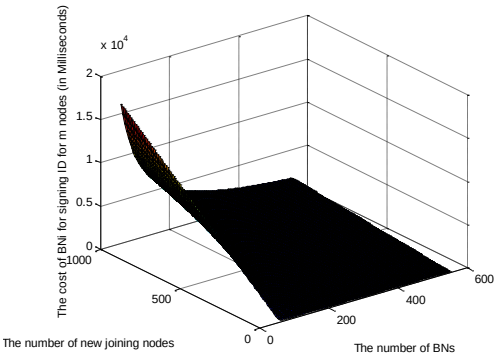

Figure 3 (c). BN_i's Cost, t=50

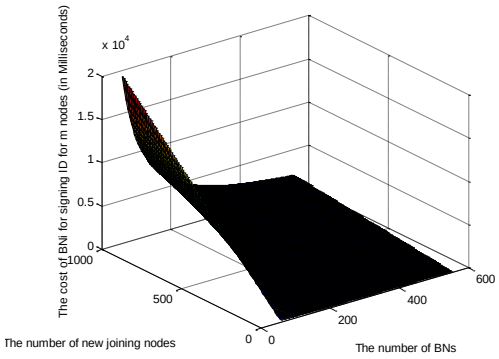

Figure 3 (d). BN_i's Cost, t=60

In the worst case, a few BN_i may always be selected. In this case, they need sign *m* valid IDs when *m* new nodes join system. The cost of BN_i, corresponding to the worst case, showed in Figure 4.

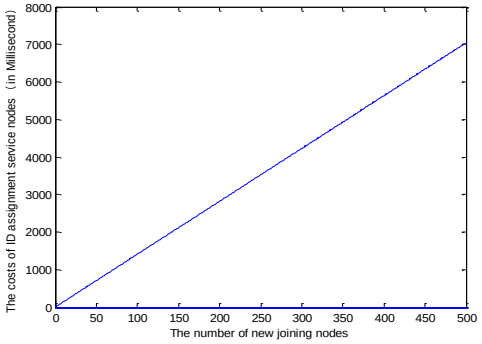

Figure 4. BN's Costs for Signing ID in Protocol in Worst Case

5. Conclusions

Based on secret sharing and certificateless signature technology, this paper designs a threshold signature scheme. As far as we know, it is the first certificateless threshold signature scheme without pairing, and it shows well efficiency and security. After that, this paper designs a reliable ID assignment protocol, which can defense attacks related to node ID and prevent single BN from being compromised or launched active attack. Analysis shows that this protocol is secure, efficient and scalable, which is able to provide reliable ID assignment service to structure P2P systems.

Acknowledgements

This work was partly supported by National Natural Science Foundation of China under Grant No.61462003, Doctor Foundation of Dali University under Grant No.KYBS201213.

References

[1] J. Yu, C. Fang, J. Xu, et al,ID Repetition in Kad. Proceedings of Peer-to-Peer Computing.**(2009)** September 9-11;USA,IEEE,pp. 111-120.
[2] Jyothi B. S.; Janakiram D..SyMon: A practical approach to defend large structured P2P systems against Sybil Attack. peer-to-peer networking and applications, 4,3,**(2011).**pp. 289-308.
[3] XiaowenYue,XiaofengQiu, P2P attack taxonomy and relationship analysis. International Conference on Advanced Communication Technology,**(2009)** July 1-3;Korea,IEEE,pp.1207-1210.
[4] Rowaihy,H., Enck,W.,McDanie,P., et al,Limiting Sybil Attacks in Structured P2P Networks, IEEE International Conference on Computer Communications,**(2007)** May 6-12;USA,IEEE,pp. 2596-2600.

[5] Borisov, N.,Computational Puzzles as Sybil Defenses.IEEE International Conference on Peer-to-Peer Computing, **(2006)** September 6-8; United Kingdom,IEEE,pp. 171-176.
[6] Nguyen Tran, Jinyang Li, Optimal Sybil-resilient node admission control. Proceedings of IEEE INFOCOM,**(2011)** April 10-15; Shanghai, China.IEEE, pp.3218-3226.
[7] Lesueur,F.,Me,L.,Tong,V., A Sybil-Resistant Admission Control Coupling SybilGuard with Distributed Certification. Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises,**(2008**) June 23-25; Rome, Italy,pp. 105-110.
[8] D. Boneh, M.K. Franklin, Identity-Based Encryption from the Weil Pairing. Int'l Cryptology Conf. Advances in Cryptology,**(2001)** August 19–23; California, USA, pp. 213-229.
[9] Butler, K., Ryu, S.,Traynor, P., et al, Leveraging Identity-Based Cryptography for Node ID Assignment in Structured P2P Systems,IEEE Transactions on Parallel and Distributed Systems.20,12, **(2009)**.pp. 1803-1815.
[10] Ryu, S.,Butler, K., Traynor, P., et al,Leveraging Identity-Based Cryptography for Node ID Assignment in Structured P2P Systems.International Conference on Advanced Information Networking and Applications Workshop, **(2007)** May 21-23; Canada,pp. 519-524.
[11] Dengqi YANG, Xingshu CHEN, Guochao ZUO, Reliable ID assignment for distributed strcutured P2P systems. Journal of Sichuan University(Engineering Science Edition) (in Chinese),44,4,**(2012)**.pp.129-134.
[12] S.S. Al-Riyami and K. Paterson. Certificateless Public Key Cryptography. In C. S. Laih, editor, Advances in Cryptology–Asiacrypt'03, Lecture Notes in Computer Science. Springer-Verlag, vol2894**,(2003)**.pp.452-473.
[13] DengqiYang,Xingshu Chen, Jian Wang, Security architecture for peer to peer applications, Journal of Digital Content Technology and its Applications,5,11,**(2011)**.pp.351-358.
[14] Chen L,ChengZ, Smart N P. Identity-based key agreement protocols from Pairings. Int.J.Inf.Secur,6,4,**(2007)**.pp. 213-241.
[15] ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) [S]**(1999)**
[16] L.C. Wang, Z.F. Chao, X.X. Li, H.F. Qian, Simulatability and security of certificateless threshold signatures, Information Sciences, 177,6,**(2007)**.pp. 1382–1394.
[17] Hu Xiong, Fagen Li, Zhiguang Qin,Certificateless threshold signature secure in the standard model,Information Sciences,16,8,**(2010)**.
[18] Hong Yuan, Futai Zhang, Xinyi Huang et al. Certificateless threshold signature scheme from bilinear maps, Information Sciences ,180,23,**(2010)**.pp.4714-4728.
[19] Piyi Yang, Zhenfu Cao, and Xiaolei Dong, Certificateless Threshold Signature for Data Report Authentication in Mobile Ad-Hoc Network, Third International Conference on Network and System Security,**(2009)** September 1-3 ,Mulbourne, Australia,pp.143-150.

Authors

Dengqi Yang, he received the B.E. degree in Information and Computing Science from Yunnan University, China in 2003, the M.Sc. degree in Computational Mathematics from Yunnan University, China in 2006, and the Ph.D. degree in Computer Science from Sichuan University, China in 2012. He worked, as an Associate Professor, at Dali University, China. His research interests mainly focus on network architecture and information security.

Jian Yang, he received the B.E. degree in Computer Science from Central South University, China in 1999, the M.Sc. degree in Computer Science from Kunming University of Science and Technology, China in 2005, and the Ph.D. degree in Computer Science from Tongji University, China in 2013. He worked, as an Associate Professor, at Dali University, China. His research interests mainly focus on Cloud Computing and Information security.

Benhui Chen, he received the B.E. degree in Computer Science from Yunnan University, China in 1999, the M.Sc. degree in Fundamental Mathematics from Yunnan Normal University, China in 2005, and the Ph.D. degree in Computer Science from Waseda University, Japan in 2011. From 1999 to 2011, he worked as a Research Associate, Lecturer and Associate Professor, and since August 2011, he has been a Professor at Dali University, China. His research interests include Computational Intelligence, Bioinformatics, Computer Networks, and so on.