A new security architecture for SIP based P2P computer networks

Yongfeng, H, Tang, S and Yip, YJ

Journal of
Computer Science, Informatics & Electrical Engineering
Volume 2, Issue 1, 2008

A New Security Architecture for SIP Based P2P Computer Networks

Huang Yongfeng, Professor, Tsinghua University, yfhuang@tsinghua.edu.cn
Shanyu Tang, Dr & Senior Lecturer, London Metropolitan University, s.tang@londonmet.ac.uk
Yau Jim Yip, Professor & Dean, University of Huddersfield, j.yip@hud.ac.uk

Abstract

Many applications are transferred from C/S (Client/Server) mode to P2P (Peer-to-Peer) mode such as VoIP (Voice over IP). This paper presents a new security architecture, i.e. a trustworthy authentication algorithm of peers, for Session Initialize Protocol (SIP) based P2P computer networks. A mechanism for node authentication using a cryptographic primitive called one-way accumulator is proposed to secure the P2P SIP computer networks. It leverages the distributed nature of P2P to allow for distributed resource discovery and rendezvous in a SIP network, thus eliminating (or at least reducing) the need for centralized servers. The distributed node authentication algorithm is established for the P2P SIP computer networks. The corresponding protocol has been implemented in our P2P SIP experiment platform successfully. The performance study has verified the proposed distributed node authentication algorithm for SIP based P2P computer networks.

Introduction

Peer-to-Peer (P2P) is one of the important topics in the research of next generation networks. P2P brings significant changes to the Internet. P2P applications have gained increasing popularity over recent years, particularly for those using Session Initialisation Protocol (SIP). It is regarded as the core control protocol for the next generation network, and is evolving from its original C/S (Client/Server) mode to P2P mode (Rosenberg & Schulzrinne & Camarillo & Johnston & Peterson & Sparks & Handley & Schooler, 2002).

SIP was initially published in 2001 for establishing, changing and terminating sessions in IP networks. Recently, SIP has widened its applications and been used in multimedia conferencing, long-distance white board and instance message. SIP was used to simplify the connection of IPSec VPN and to combine conventional multimedia services with other services, such as directory information, web browsing, searching and tracking. As an application layer protocol, SIP is independent upon the actual network. Hence any types of participants in IP networks can be connected using SIP. For instance, SIP can provide a seamless connection between PSTN and GSM. This functionality would become more and more important with the deployment of 3G mobile networks across the world.

With the expansion of SIP based applications, the C/S mode appears to have drawbacks that are hard to overcome. To address these problems, the SIPPING working group of IETF has conducted a series of research on P2P distributed mode for SIP computer networks. Since 2005 the group has proposed several protocols; the latest two are “An Architecture for Peer-to-Peer Session Initiation Protocol” (IETF SIPPING, 2005) and “A P2P Approach to SIP Registration and Resource Location” (IETF SIPPING, 2005).

The latest two protocols proposed by the SIPPING group have two different P2P SIP architectures. The first protocol suggests a distributed SIP server to be deployed, i.e. the information about participants is distributed to every server in P2P mode. These servers communicate with each other using Distributed Hash Table (DHT) algorithms and all participants share and query resources in the same mode. The second draft takes advantage of a P2P structure, leading to the elimination of the SIP server with all the SIP nodes being associated in some way. The differences between the two P2P SIP architectures are that the former still retains some characteristics of C/S mode, but has a manageable advantage. The latter is a pure P2P structure as each node in the structure maintains its neighbour’s information and the scalability and management of the structure needs to be explored further. Although both protocols suggested their own P2P SIP architectures and application algorithms, the security problems of the architectures are still remained unsolved.

The security of SIP based computer networks becomes a serious problem after transferring from C/S mode to P2P distributed mode (Singh & Schulzrinne, 2004). The centralized control method might solve most of security problems with the C/S network. However, there are more security issues to be considered in the P2P distributed environment, not only existing security threats to the centralized C/S network, but also encountering new ones in the P2P networks where nodes join and leave dynamically. Due to the lack of a centralized management, the P2P networks need extra safety approaches to ensure itself to run smoothly (Milojicic & et al, 2002).

The security of the P2P SIP network involves many aspects. They are routing security, saving and accessing security, malicious destroy, intentional deception, user and peer authentication, encryption and decryption, application security and personal privacy. The major security problem of the P2P SIP network is peer trustworthy authentication when nodes join the network.

This work focuses on peer trustworthy authentication (namely node authentication). A peer authentication solution based on a one-way accumulator is suggested in this paper for P2P SIP computer networks. The authentication method is adapted to P2P mode, and can be used to ensure the authenticity of the identity of the SIP node that is added to the P2P SIP network, preventing forged ones from being added to the network. A cryptographic primitive called one-way accumulator is also presented. The corresponding node authentication algorithms are established based on the accumulator and a node authentication protocol according to the specific characteristics of the P2P SIP application. Finally, the performance of the proposed node authentication protocol is verified in our P2P SIP experiment platform.

Authentication for P2P SIP Computer Networks

Due to the essential differences between P2P mode and C/S mode, the authentication technologies suited to C/S mode cannot be directly applied to P2P computer networks (Nowell & Balakrishnan & Karger, 2002). Hence new authentication methods capable of adapting to the P2P networks are sought.

There is no explicit difference between peer authentication and user authentication for SIP networks in C/S mode. Both adopt the HTTPS DEGEST authentication method (Rosenberg & et al, 2002). In contrast, for SIP networks in P2P mode user authentication is different from node authentication. User authentication performs at the application layer, verifying the participating user's identity in a special SIP application and ultimately confirming whether the user has right to access the resource. Node authentication is used to ensure the reliability and security of nodes and to testify the authenticity and validity of the participants. In terms of the objects being encrypted, the two authentication methods have some similarity. For example, both run in the same way that one part (or multiple parts) validates the identity of the other part (or other multiple parts). As existing methods can be directly adopted to solve the security problems associated with the user authentication for P2P SIP networks, this study is mainly focused on node authentication for the networks.

One approach to node authentication is the legal node identification technology using the global list of the legal nodes in P2P SIP networks. When a node needs to validate the identity of its peer, the identification list of legal nodes can be queried (Nowell & Balakrishnan & Karger, 2002; Lennox & Schulzrinne, 2003; Xiong & Liu, 2004). The shortcomings of this centralized authentication method include complex management, un-scalability, and single node's failure.

Node authentication based on the encryption technology has more virtues than the legal node identification technology mentioned above (Xiong & Liu, 2004). The digital signature using encryption is the major method of implementing node authentication. The basic idea is to validate the node's identity through its digital certificate issued by the authorized organization. This can be achieved on the Internet. The node participating safe communication applies a digital certificate from the authorized organization, e.g. Certificate Authority (CA), which is responsible for issuing digital certificates. The credibility of the node can then be ensured by the authorized organization. In the communication process, the node provides its own certificate when its identity needs to be validated making its peer to know its identity.

The node authentication using digital certificates has derived from the centralized CA technology. It is convenient to inosculate with the existing information security technology. It can be used for small- or medium-scale P2P networks. However it is not appropriate for large-scale P2P computer networks (Camenish & Lysyanskaya, 2002). On the one hand, there should not be a central controlling node in

the P2P networks. On the other hand, the centralized CA does not conform to the distributing character of the P2P networks.

The distributed CA technology, attempting to divide the function of the traditional centralized CA into several distributed nodes, was proposed to solve the single node's failure problem with the traditional CA technology (Lennox & Schulzrinne, 2003; Xiong & Liu, 2004). With the technology all nodes collaborate on issuing the user's certificate with their own shares of the CA private key. The users applying for certificates receive only the fragments of the digital certificates issued by these nodes, and the whole certificates can then be obtained through computing (the computing is performed by the node itself or with the help of the third party). The distributed CA technology not only needs the correlative infrastructure of key management (e.g. key distributing and key deleting) but also involves the management of certificates such as certificate withdrawing, certificate renewing etc.

A new node authentication method is proposed based on a one-way accumulator for P2P SIP networks, leveraging the distributed nature of P2P to allow for distributed resource discovery and rendezvous in a SIP network, and eliminating (or at least reducing) the need for centralized servers.

Proposed Node Authentication Based on a One-way Accumulator

The main objective of this study is to propose a new mechanism for node authentication using a cryptographic primitive called one-way accumulator. This section is to detail how to construct the one-way accumulator and the basic ideas of the node authentication.

Basic Principle

According to the correlative theory of cryptology, the one-way Hash function that meets the half-exchange law has the following characteristics (Bnaloh & Dde Mare, 1994):

- The one-way characteristic of the Hash function signifies that it is easy to compute in a certain way but it is very difficult to compute in other ways.
- Half-exchange law means, on condition seeds being given, the result of the accumulator keeps invariable when it is computed in different orders.

On the basis of the two characteristics, a one-way accumulator is suggested in this study to validate whether an appointed value belongs to the corresponding set of nodes, and a special authentication scheme is designed to meet the requirements of node authentication for P2P SIP computer networks. The basic principle is summarized below.

Firstly, each node in P2P SIP networks is assigned a number i and a uniquely correlated private key y_i. All nodes should submit their own values of (i, y_i) to an appointed authentication node, i.e. a bootstrap node in the P2P SIP networks.

Secondly, having received all nodes' values of (i, y_i), the appointed node, i.e. the bootstrap node, takes use of the one-way accumulator to calculate the total accumulative value z for all the nodes and the corresponding partial accumulative values of (i, z_i) for each node. The appointed node then sends the partial accumulative values to the corresponding nodes, and distributes / publishes the total accumulative value z to all the nodes in the networks.

Thirdly, the node j is used to validate the identity of its peer, e.g. the node i that intends to establish a connection with it. After the peer node i submitting its own value of (y_i, z_i) to the node j, the node j then calculates the Hash value $z' = h(y_i, z_i)$ and determines whether z' equals the total accumulative value z. If z' is equal to z, the node i passes validation; otherwise, the node i fails authentication.

The characteristics of the one-way accumulator determine the security and credibility of node authentication, so constructing the one-way accumulator is the core step in the design of the authentication protocol. The one-way accumulator should not only ensure the simplicity of validation computing, but also guarantee there is no contradiction between the final results.

The unique identity of the node in P2P SIP networks described by the value (i, y_i) is the warrant of the node's routing communication. So the most important aspect of the node authentication algorithm is to ensure the uniqueness of the legal node's identity. This can be achieved by using the private key distribution method, which is discussed in details in another paper.

The anti-forgery of authentication information requires that nodes in P2P SIP networks cannot forge other nodes' authentication information, and cannot destroy the uniqueness of the nodes. It could prevent nodes from spoofing credentials or repaying attacks. Thus a Challenge-Response mechanism based on a random number will be introduced in the proposed node authentication algorithm to prevent forging (Maricn & Piftzmann, 1997).

One-way Accumulator Based Node Authentication Algorithm

Constructing a one-way accumulator is the major task of designing the node authentication algorithm for P2P SIP networks. Equation (1) is proposed as a one-way accumulator based on an exponent. It has been proved to be the one-way function that has the characteristics of accumulators (Michael & Goodrich & Tamaassia & Hasic, 2002; Mukherjee, 2006).

$$z = x^{y} \bmod n \rightarrow z = x^{y_1 \cdot y_2 \cdots y_i} \bmod n, \left(y_i \in Y, i = 1,2,...n\right) \quad (1)$$

where *n* is an integer.

To establish the node authentication algorithm based on equation (1), the following procedures are performed:

Step 1: a random integer generator *RANDOM*() generates an integer *m*;

Step 2: the function *PRIME*(*m*) capable of selecting a prime number is used to choose a big enough prime number *n* from the set of [1 ,…, *m*] as follows:

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

where $\varphi(n)$ is the Euler number, *p* and *q* are prime numbers, and *p* != *q*.

Step 3: the accumulative value *z* is calculated by using equation (3).

$$z = x^{y_1 \cdot y_2 \cdots y_i} \bmod n, \left(y_i \in Y, i = 1,2,...n\right) = x^{\prod y \in Y^{y}} \bmod n \quad (3)$$

Step 4: the partial accumulative value of the node *j* is calculated by using equation (4). In fact, each node can compute its partial accumulative value z_j after receiving the accumulative value *z*.

$$\begin{aligned} z_j &= x^{y_1 \cdot y_2 \cdots y_i} \bmod n, \left(y_i \in Y, i = 1,2,...m, \forall i \neq j\right) \\ &= x^{\prod y \in Y - \{y_j\}^{y}} \bmod n = z^{y_j^{-1} \bmod \varphi(n)} \bmod n \end{aligned} \quad (4)$$

Step 5: equation (5) is used for node authentication. If *p* equals 1, the node *j* is legal and passes authentication; otherwise, node authentication fails.

$$p = \left(z == z_j^{\,y_j} \bmod n \; ? \; 1 : 0\right) \quad (5)$$

To reduce the expense of calculating the accumulative value *z*, equation (6) is then suggested to compute the accumulative value *z* when a new node *j* is added to the P2P SIP network.

$$z = z_j^{\,y_j} \bmod n \quad (6)$$

P2P SIP computer networks are dynamical and self-organized networks in which nodes can join and leave randomly. When a node is added or deleted, the boot node must update the corresponding information about all the nodes in the networks, such as re-calculating the accumulative value *z* and the partial accumulative values z_i for each node. So the node authentication protocol based on the one-way accumulator suggested above should include four stages, protocol initiation, node adding, node deleting and node authentication. The details are discussed in the next section.

Design of a Node Authentication Protocol for P2P SIP Computer Networks

Based on the one-way accumulator constructed by the method presented above, a node authentication protocol is then suggested in this section for P2P SIP computer networks.

Architecture of P2P SIP Computer Networks

According to a draft, “A P2P Approach to SIP Registration and Resource Location” suggested by SIPPING (IETF SIPPING, 2005), a hierarchical P2P SIP architecture is proposed here, as shown in Figure 1.

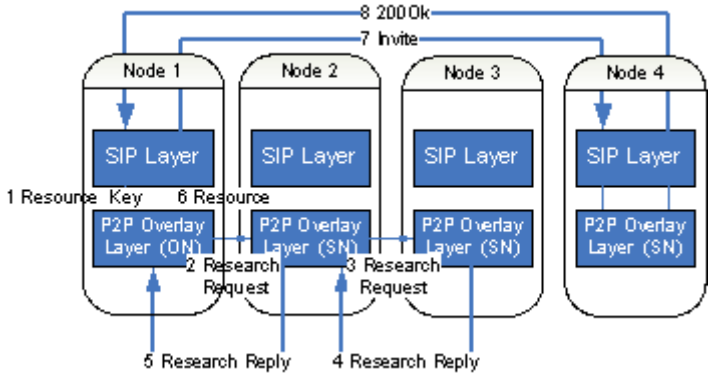

Fig. 1: The architecture of a P2P SIP network

In this architecture, the whole P2P SIP network is divided into many groups. Within a group, a super node (SN), e.g. node 2 in Figure 1, is used to store the routing information of other ordinary nodes (ONs), and the ordinary nodes query their neighbours through the SN. This is the first layer of the hierarchical architecture. The second layer consists of all the SN groups in the network. Between groups, a super node routes a message to another SN using P2P algorithms called Distributed Hash Tables (DHTs) that support efficient search mechanisms when resource names are precisely known. The proposed hierarchical architecture for P2P SIP computer networks has a number of advantages, including:

- It would reduce significantly the average number of hops in a lookup, particularly when nodes are heterogeneous.
- It would cut down the lookup latency when the peers in the same group are topologically close and cooperative caching is used within the group.
- It facilitates the large-scale deployment of the P2P lookup.

The key feature of the P2P SIP architecture (Fig. 1) compared with SIP in C/S mode is that it has no dedicated server or proxy (IETF SIPPING, 2005). The nodes participating in the overlay not only act as traditional SIP User Agents (UA), allowing their users to place and receive calls, but also play the roles of registrars and proxies in SIP networks when being viewed collectively with other peers. These roles include resource location, maintaining information, and call routing.

```
REGISTER sip:10.7.8.129 SIP/2.0
To: <sip:463ac4b449@10.4.1.2;user=node>
From: <sip:463ac4b449@10.4.1.2;user=node>
Contact: <sip:463ac4b449@10.4.1.2;user=node>
Expires: 600
DHT-NodeID: <sip:463ac4b449@10.4.1.2;user=node>;algorithm=sha1;
                overlay=chat;expires=600
Require: dht
Supported: dht
Key:yi zi
Supported:owa
```

Fig. 2: Extension to the node REGISTER messaging

The semantics of standard SIP messaging is preserved to a great extent as possible in order to implement the node authentication protocol on P2P SIP networks. All the messages that maintain DHTs and are required to query information are implemented using SIP messaging. The SIP REGISTER messaging is extended here to look up resources. It includes maintaining DHTs, such as the messages that are joined or left the overlay network, and information transferred between nodes. So the extended REGISTER messaging has two functions, one is to accomplish node registration and validate newly joined nodes (see Figure 2 for the REGISTER message format in this situation);

another function is to implement the resource registration before the session is invited, and the REGISTER messaging has no contact information, but resource IDs.

A new header parameter, Key, is introduced in the node REGISTER messaging as shown in Figure 2. It is used to inform the peer about its authentication number y_i (private) and the partial accumulative value z_i with both parameters being encrypted.

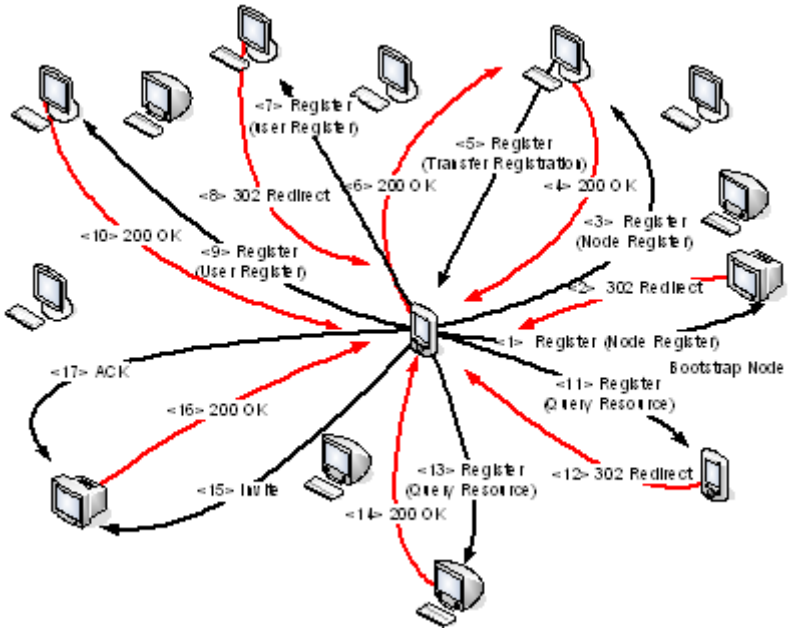

Fig. 3: The signalling process of a P2P SIP network

Consequently, the REGISTER messaging has various functions at different states for P2P SIP networks, and the whole signalling process of the P2P SIP networks is shown in Figure 3. The first REGISTER message is used to accomplish node registration; similarly, the second and the third are also used for node registration. But the seventh and ninth REGISTER messages are used to perform user registration. Having completed user registration, a node sends an INVITE message, e.g. the 15th message, to initiate a session with its peer. Among these messages, the node registration message, REGISTER, has the information of node authentication.

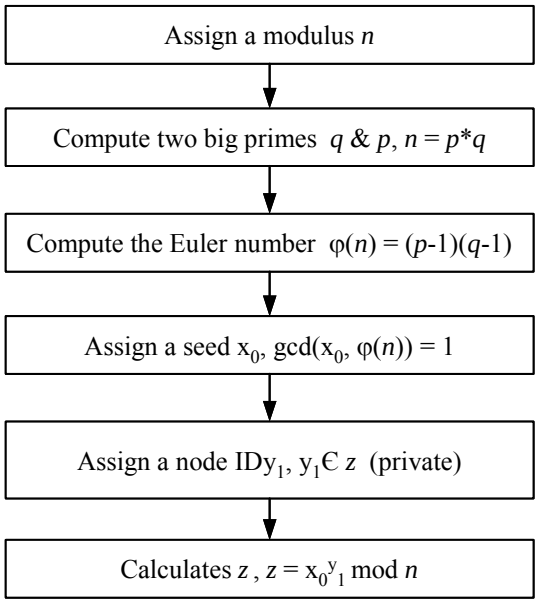

Fig. 4: The process of the initialization stage

Details of the Node Authentication Protocol

The node authentication protocol based on the proposed one-way accumulator in the preceding section can be divided into four stages, initialization stage, node adding stage, node deleting stage and node authentication stage.

Initialization stage

The initiation process of the protocol is shown in Figure 4. At this stage, some parameters such as $\varphi(n)$, p, q and y_1 are introduced, in order to accomplish the parameter initialization of the authentication protocol.

Node adding stage

Figure 5 shows the process of the node adding stage. Provided that there are not many nodes in the P2 SIP computer network, for example, the total node number is less than 100, all nodes in the network are regards as one group. The bootstrap node in the network is responsible for calculating the total accumulative value z. Other nodes in the P2P SIP network then calculate their own partial accumulative values (z_i) after receiving the accumulative value broadcasted by the bootstrap node.

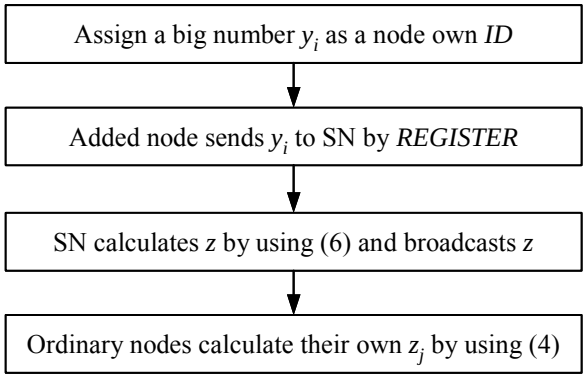

Fig. 5: The process of the node adding stage

Whereas, if there are more than 100 nodes in the P2P SIP network, the nodes in the network are divided into groups in order to improve the efficiency of node authentication. As a result, a super node (SN) is chosen for each group. The firstly added node of a group is acted as a temporary SN; with more nodes added to the group, the super node of the group is then selected according to the SN selection algorithm (Liu & Huang & Li, 2008). The computation of the accumulative value is accomplished by the super node, and ordinary nodes in the group calculate their own partial accumulative values after receiving the accumulative value broadcasted by the SN.

Node deleting stage

Having been added into the P2P SIP network, a new node should send periodically a REGISTER message to the bootstrap node or the super node. Note that the interval between two REGISTER messages can be adjusted in terms of the node number in a P2P network. Meanwhile, if the node number in the P2P network is too large, then the nodes in the network should be divided into multi-groups in order to decrease the load on the super node. This issue is discussed in detail in the following section. Otherwise, the bootstrap node or the SN will delete the ID of the new node from the node list, and update the z and z_j values by using equations (3) and (4). The bootstrap node or the SN is responsible for computing the new accumulative value and broadcasting it to ordinary nodes, which compute their own partial accumulative values once a node has been removed.

Node authentication stage

The process of node authentication is shown in Figure 6. If a node intends to establish a connection with its peer according to the best peer selection algorithm, it must pass the authentication by its peer first. Only if the authentication is successful, the node can then establish a connection with its peer by using the node REGISTER messaging as shown in Figure 2. Otherwise, the link cannot be established.

If the nodes in the P2P SIP network are divided into groups, the super nodes of the groups are required to perform node authentication using the authentication protocol. As long as a node passed node authentication, it may be regarded as a trustworthy super node by other ordinary nodes within the group.

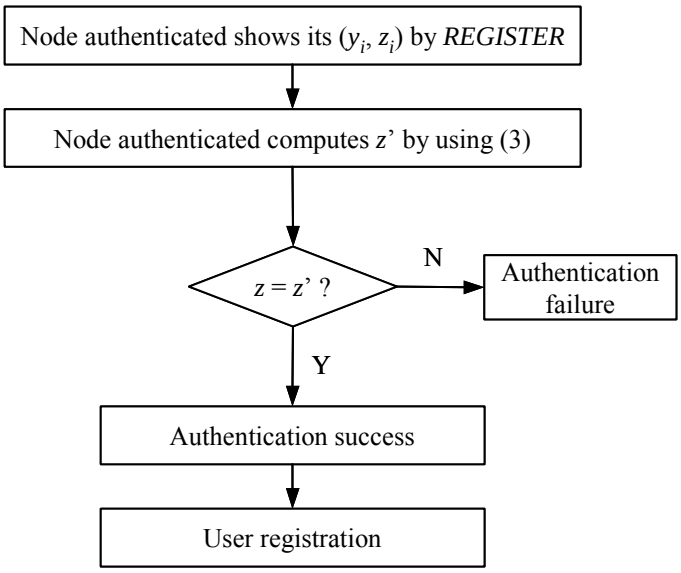

Fig. 6: The process of the node authentication stage

Evaluation of the Proposed Node Authentication Protocol

As the bootstrap node or the super node computes the accumulative value for all the nodes in P2P SIP networks, the performance of the node authentication protocol is dependent upon two factors. One is the hardware configuration of the bootstrap or the super node. The other is the complexity of the authentication protocol. It also depends largely on the complexity of the one-way accumulator on which the authentication protocol is based.

Table 1 lists the performance results for the complexity of the node authentication protocol described in the preceding section. In Table 1, the complexity of communication denotes the time of exchanging message. For example, O(2) means it needs to exchange two messages for a node to be validated. The complexity of computation indicates the time of an exponent operation, e.g. O(1) denoting two executions of the exponent operation.

Table 1: Complexity of the node authentication protocol

Operation	Complexity		
	Communication	SN Computing	ON Computing
Node added	O(m)	O(1)	O(1|)
Node deleted	O(m)	O(1)	O(1)
Node validated	O(2)	O(0)	O(1|)

The proposed node authentication protocol is simulated in our experiment platform with a piece of streaming media playing software being implemented on a P2P SIP network (Figure 7) (Liu & Huang & Li, 2008). The software, deployed on the CERNET2 network, is used to play on-demand TV and streaming media. The nodes in the P2P SIP network are divided into groups. Each group consists of the nodes that play the same streaming media program. A node must pass authentication before it can join the appointed group.

Fig. 7: A streaming media playing software on a P2P SIP network

To assess the performance of the node authentication protocol, some groups are organized in a way that they had different numbers of nodes ranging from 10 to 100 nodes. These nodes are configured with Intel duo core CPU, 1GB memory and windows XP. All applications support IPv6.

The delay times of adding a node, deleting a node and validating a node are measured respectively on our experiment platform, and the experimental results for the delay times are shown in Figure 8. The delay time of adding a node is the time spent by the bootstrap node to compute the accumulative value when a node joins the P2P SIP network. Similarity, the delay time of deleting a node is the time required by the bootstrap node for computing the accumulative value in the case of node deletion. The delay time of validating a node is the time taken by a node to validate the identity of its peer. All the three types of delay times include the communication delay, which is the time necessary for receiving and sending messages.

The results in Table 1 and Figure 8 show that the authentication algorithm is a validating symmetry, which means the computing and communication overhead of each node in the SIP P2P network are almost equal. Symmetry requires that node authentication is totally distributed and no node should bear more responsibility than others. The symmetry characteristic meets the distribution requirement of P2P networks. The delay times of validating a node demonstrate the authentication algorithm has an excellent symmetry. The delay times of adding a node and deleting a node have some slight varieties when the node number increases, which is due to the increasing overhead of communication while the overhead of computation is steady.

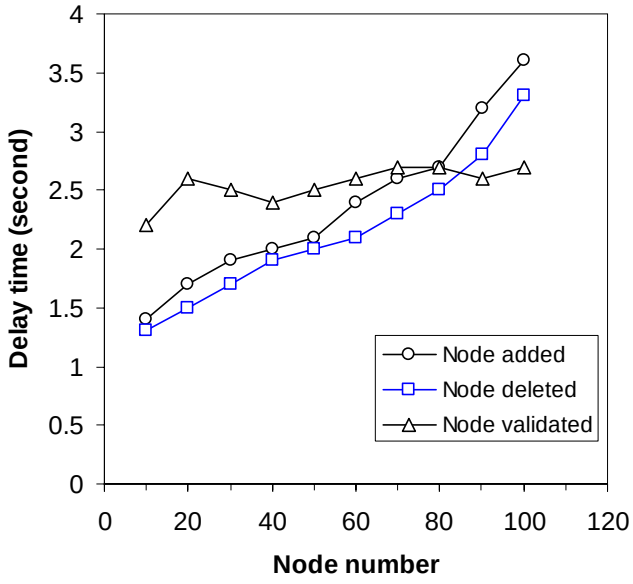

Fig. 8: The delay time of the authentication algorithm

The findings also reveal that the authentication algorithm has a high stability. As a dynamical and self-organized network, the P2P SIP network allows nodes to join or leave the network freely. So the node authentication algorithm needs to ensure the stability of the authentication overhead when the node number of the network varies frequently. The authentication overhead includes both the communication delay and the computing delay. As shown in Figure 8, the delay times of validating a node are almost constant despite the node number changes. In addition, the delay times of adding a node and deleting a node increase slightly when the node number increases from 10 to 100.

Conclusions

By analysing the differences between P2P (Peer-to-Peer) computing mode and traditional C/S (Client/Server) mode for SIP computer networks, the significance of node authentication in P2P over SIP computer networks has been emphasized by this study.

A mechanism for node authentication using a cryptographic primitive called one-way accumulator is proposed and presented in this paper to solve the node authentication for P2P SIP computer networks.

The performance study carried out on our P2P SIP experimental platform has proved that the proposed node authentication algorithm based on a one-way accumulator has been implemented on a P2P SIP network successfully. The test results indicate the proposed protocol has a high reliability and safety.

The further work of research is to design a better one-way accumulator, simplifying the procedures of node authentication for P2P SIP computer networks.

Acknowledgment

This work was supported in part by a grant from the National High Technology Research and Development Program of China (863 Program, No.2006AA01Z444), National Foundation Theory Research of China (973 Program, No.2007CB310806), and National Natural Science Foundation of China (No.60703053, No.60773140).

References

Bnaloh, J., & Dde Mare, M. (1994). One-way Accumulators: A decentralized alternative to digital signatures. In *Advances in Cryptology Eutocrypt'93, Proceedings of the Workshop on the Theory and Applications of Cryptographic Techniques*, LNCS 765. Springer-Verlag, Berlin.

Camenish, J., & Lysyanskaya, A. (2002). Dynamic accumulators and application to efficient revocation of anonymous credentials. In *Crypto'02*.

Castro, M., Jones, M.B., Kermarrec, A.M., Rowstron, A., Theimer, M., Wang, H., & Wolman, A. (2003). An evaluation of scalable application-level multicast built using peer-to-peer overlays. In *Proceedings of the Conference on Computer Communications* (IEEE Infocom).

IETF SIPPING (March 17, 2005,). Architecture for Peer-to-Peer Session Initiation Protocol. Internet P2P SIP Draft [Online]. Available: http//www.P2PSIP.org.

IETF SIPPING (June 15, 2005). A P2P Approach to SIP Registration and Resource Location. Internet P2P SIP Draft [Online]. Available: http//www.P2PSIP.org.

Lennox, J., & Schulzrinne, H. (2003). A protocol for reliable decentralized conferencing. In *ACMNOSSDAV 2003*.

Liu, H., Huang, Y.F., & Li, X. (2008). Research on Grouping strategy of SIP-based Streaming media P2P Live Broadcast Network. *Journal of Electronics and Information*. Accepted for publication.

Maricn, N., & Piftzmann, B. (1997). Collision-Free Accumulators and Fail-Stop Signature Schemes Without Trees. In *Eurocrypt'97*.

Michael, T., Goodrich, R., Tamaassia, & Hasic, J. (2002). An efficient dynamic and distributed cryptographic accumulator. Lecture Notes In Computer Science. In *Proc. 5th International Conference on Information Security*. Springer-Verlag, Berlin.

Milojicic, D., Kalogeraki, V., Lukose, R.M., Nagaraja, K., Pruyne, J., Richard, B., Rollins, S., & Xu, Z. (2002). Peer-to-peer Computing. Technical Publications Department, HP Labs Research Library, Tech. Rep. HPL-2002-57 20020315. Avail-able: http://www.hpl.hp.com /techreports/ 2002/HPL-2002-57.html.

Mukherjee, D. (2006, November 27). Format-independent authentication of arbitrary scalable bit-streams using one-way accumulators. Hewlett Packard Laboratories, Palo Alto, CA, USA [Online]. Available: http://www.hpl.hp.com/techreports/2006/HPL-2006-173.pdf.

Nowell, D.L., Balakrishnan, H., & Karger, D. (2002). Analysis of the evolution of peer-to-peer systems. In *ACM Conf. on Principles of Distributed Computing* (PODC), Monterey, CA, USA.

Rosenberg, J., Schulzrinne, H., Camarillo G., Johnston, A. R., Peterson, J., Sparks, R., Handley, M., & Schooler, E. (2002). SIP: Session Initiation Protocol, RFC 3261. Internet Engineering Task Force, June.

Singh, K., & Schulzrinne, H. (2004). Failover and Load Sharing in SIP Telephony. Computer Science Department, Columbia University, New York, USA, Tech. Rep. CUCS-011-04.

Xiong, L., & Liu, L. (2004). Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering*, vol. 16, no. 7, pp. 843-857.