The Design of Secure and Efficient P2PSIP Communication Systems

Xianghan Zheng, Vladimir Oleshchuk

The Design of Secure and Efficient P2PSIP Communication Systems

Xianghan Zheng and Vladimir Oleshchuk

Faculty of Engineering and Science, University of Agder, Norway.
{xianghan.zheng,vladimir.oleshchuk}@uia.no

Abstract. Recently, both academia and industry have initiated research projects directed on integration of P2PSIP paradigm into communication systems. In this paradigm, P2P network stores most of the network information among participating peers without help of the central servers. The concept of self-configuration, self-establishment greatly improves the robustness of the network system compared with the traditional Client/Server based systems. In this paper, we propose a system architecture for constructing efficient and secure P2PSIP communication systems. The proposed approach includes three-layer hierarchical overlay division, peer identifier assignment, cache based efficiency enhancement, proxy based security, and subjective logic based trust enhancement. A prototype with 512 P2PSIP peers is implemented.

Keywords: Peer-to-Peer (P2P), Session Initiation Protocol (SIP), P2PSIP, Chord, Chord Secure Proxy (CSP), Chord Secure Proxy Gateway (CSPG), Subjective logic.

1 Introduction

P2P computing has begun to infiltrate into SIP communication systems. In this paradigm, P2P network stores most of the network information on each participating peer without help of the central servers. The concept of self-configuration, self-establishment greatly improves the robustness of the network system compared with the traditional Client/Server based systems. IETF P2PSIP working group defines the concept and motivation behind P2PSIP [1] in the following way: "The concept behind P2PSIP is to leverage the distributed nature of P2P to allow for distributed resource discovery in a SIP network, eliminating (at least reducing) the need for centralized servers.

Both recent research projects (e.g. SIPPeer [2], P2PP [3], SIPDHT [4], and dSIP [6], etc.) and recent publications [6–10] have suggested many useful and interesting approaches for designing P2PSIP communication systems. However, two most critical problems existing currently are overlay efficiency and security.

Firstly, Chord based approach has been suggested as a mandatory overlay technology to support P2PSIP communication [1, 6–9]. However, as a protocol originally designed for background downloading applications, it is not efficient for real-time services. For example, Chord lookup efficiency might degrade with the increasing number of unstable peers (join/left the overlay frequently). Besides,

Chord lacks of cache mechanism to preserve the useful information (e.g. public IP, port, peer ID, etc) for future session establishment.

Secondly, the decentralized nature of P2P might cause a lot of security problems. For instance, a malicious intermediate peers are capable to misroute, discard, temper and replay received P2PSIP messages. Besides, it might be able to spy and record profile of the neighbouring peers (e.g. peer ID, public ID, port, etc) through parsing the incoming messages.

In this paper, we propose a system architecture that provides efficient and secure session initiation services. The proposed approaches include: three layer hierarchical overlay division, peer identifier assignment, cache based efficiency enhancement, proxy based security, and subjective logic based trust enhancement. After that, we build a prototype with 512 P2PSIP peers, including 496 normal peers, 13 CSPs (Chord Secure Proxy), and 3 CSPGs (Chord Secure Proxy Gateways). We also describe a typical use scenario to show the protection against malicious or compromised intermediate peers.

2 System Architecture

In this section, we present the proposed system architecture. After that, we specify the corresponding approaches in details, including three-layer hierarchical division, peer identifier assignment, cache mechanism, CSP based security, and subjective logic based trust enhancement.

2.1 Architecture overview

The proposed system architecture includes six main parts: P2PSIP peer, Chord Secure Proxy (CSP), Chord Secure Proxy Gateway (CSPG), Enrollment and Authentication (E&A) Server, Secure Opinion Server (SOS), and STUN[1], TURN[2] and ICE[3] server (shown in Figure 1).

P2PSIP peer, which can be a mobile phone, laptop, PC, etc., is connected to the Internet. CSP is the secure proxy that helps source peer to locate the destination peer. E&A server is the secure server that handle the enrollment and authentication task when P2PSIP peer joins overlay. Secure Opinion Server (SOS) is the trust server that stores and dynamic computes opinion for each P2PSIP peer. STUN/TURN/ICE server is responsible to provide NAT traversal for peers behind NAT protection.

In the system, the overlay is divided into three sub-layers. If the destination peer is in the same layer as the source peer, requests would be sent to CSP that is clockwisely nearest to the destination peer. Otherwise, the messages are directed to CSPG in source layer, then CSPG in destination layer, and finally, to the corresponding CSP that is clockwisely nearest to the destination peer. CSP is responsible for search and location of destination peer via "pingRequest

[1] STUN: Simple Traversal of UDP through NATs.
[2] TURN: Traversal Using Relay NAT
[3] ICE: Interactive Connectivity Establishment

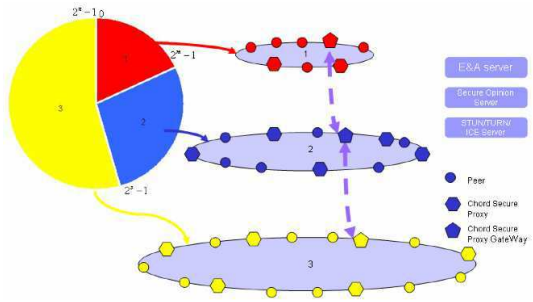

Fig. 1. System model.

multicast mechanism (described in Section 3.4). After that, the session between source and destination peers may be established.

2.2 Three layer hierarchical division

We divide the overlay into 3 sub-overlays according to peer capabilities (e.g. connection type, stability in the overlay, CPU processing power, bandwidth, etc). The first sub-overlay is the stable peers that hold public IP addresses, have more powerful CPU, and own stable connection. Such typical devices can be a web server. The second sub-overlay is the peers with enough stability and processing power, e.g. normal PC with Internet connection. Peers in this layer do not own public IP address, and might relay on STUN/TURN/ICE for traversing NAT. The lowest sub-overlay is those with unstable connection (e.g. mobile phones, PDA, laptops with wireless connection). Note that each sub-overlay contains a few CSPs and at least one CSPG that are stable P2PSIP peers.

It is reasonable to expect that many legacy P2PSIP peers in the future will be unstable peers (e.g. a large amount of mobile phones, PDA, laptops, etc) with wireless connections. Therefore, the division of three sub-overlay guarantees peer/resource lookup efficiency in the top two layers.

2.3 Peer identifier assignment

IETF P2PSIP WG is still discussing the assignment of peer identity in the overlay. Some researchers suggest use of conventional SHA-1 hash mechanism to produce 128/160 bits peer identifier. However, this solution might cause efficiency problems. For example, geographically close peers might be assigned with identifiers that are far away from each other in the overlay, and this causes long delay during connection establishment.

We advocate the idea that geographically close peers should be assigned close peer identifiers in the overlay because the most frequently communicated peers are those who are spatially related to each other [11, 12]. We propose to

incorporate this idea into our hierarchical system. In the beginning of enrollment, P2PSIP peer should contact an Enrollment and Authentication (E&A) server (which is a central server), submit information about peer capabilities (e.g. connection type, CPU processing power, bandwidth, storage, etc) and spatial information (e.g. public IP, etc), etc. Based on peer capabilities, E&A server allocates specific sub-overlay, based on spatial information, E&A server assigns specific peer identifier attached in specific sub-overlay.

2.4 Cache mechanism

Cache mechanism improves lookup efficiency indirectly through retaining communication history (e.g. previous communicated peer ID, public IP, port, etc., as shown in Table 1) for the future usage. For searching the destination peer, source peer first check its cache entry record. If the destination peer (peer identifier, public IP address, port, etc) is already inside, the session might be established directly. Otherwise, the source peer will execute normal lookup algorithm described above.

In stable overlay (e.g. first and second sub-layers) where peers do not join and left frequently, the cost might be only one hop. However, in unstable overlay (for instance, the third sub-layer) where peers are dynamically changed, this might cost even worse delay. Therefore, we do not suggest this approach to be implemented in the lowest layer sub-overlay.

2.5 Proxy-based Security

In our previous publication, we proposed a proxy-based system architecture to protect security of P2PSIP system [13]. The proposed architecture contains three main parts: P2PSIP Peer, Resource, Chord Secure Proxy (CSP), as shown in Figure 2. For locating a peer/resource in the overlay, the source peer first sends the P2PSIP request to a specific CSP (Step 1). The CSP acts as a proxy server to probe the destination peer through multicasting a PingRequest message to its successors by Chord algorithm. When the destination peer receives a "PingRequest message, it contacts the CSP to catch the original P2PSIP request (Step 2). After that, the connection between source and destination peers can be established (Step 3). The connections in the system architecture are SSL/TLS secured.

The use of "PingRequest message (in Step 2) makes sure that intermediate peers are incapable to receive original P2PSIP request. The proposed multicast mechanism (Step 2) guarantees on some level that "HelloRequest message could arrive to the destination peer. Therefore, this architecture provides secure P2PSIP session initiation.

2.6 Subjective Logic based Trust

The subjective logic [15] defines the term "opinion, which is a triple $\omega = \{t, d, u\}$, where t, d and u correspond to trust, distrust, and uncertainty respectively.

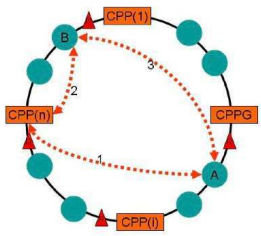

Fig. 2. System model.

Expressing trust by using three parameters instead of one simple trust level gives more adequate trust model of real world. Subjective logic also defines logical operators for combining opinions. For example, the recommendation operator $\otimes$ can be introduced to evaluate the trustworthiness of p which might be a statement like "the message traverse B to A is unchanged result of measurement, as following:

$$\omega_p^{AB} = \omega_B^A \otimes \omega_p^B = \{t_p^{AB}, d_p^{AB}, u_p^{AB}\}\, where$$

$$t_p^{AB} = t_B^A t_p^B, \quad d_p^{AB} = t_B^A d_p^B, \quad u_p^{AB} = d_B^A + u_B^A + t_B^A u_p^B \ .$$

ω_B^A is the opinion of A about trustworthiness of recommendation of B, and ω_p^B is the opinion of B about trustworthiness of p.

This approach is implemented in [16] in order to enhance security of P2PSIP. Suppose that a request goes from the source peer A, intermediate peers $B_1, B_2, \ldots, B_{n?1}$, and ends in the destination peer B_n . By applying the rules of subjective logic, the trustworthiness of this data flow is:

$$\omega_p^{AB_1B_2\ldots,B_n} = \omega_{B_1}^A \otimes \omega_{B_2}^{B_1} \otimes \omega_{B_2}^{B_1} \otimes \ldots \otimes \omega_{B_n}^{B_{n-1}} \otimes \omega_p^{B_n}$$

In this way, it is possible to evaluate the trust level for each message flow.

3 Evaluation

In this section, we evaluate the proposed system architecture. Firstly, we describe the prototype implementation. After that, we use a typical scenario to show the protection of system against malicious or compromised intermediate peers.

3.1 Prototype Implementation

We simulate the proposed system architecture with corresponding solutions by implementing the prototype in Java. The prototype of the system contains 512 peers (including 496 normal P2PSIP peers, 13 CSP peers, and 3 CSPG peers). Apache Derby is selected as the embedded database implementation for P2PSIP peers, CSPs, and CSPGs. Besides, we also build a Secure Opinion Server, which is

a web server for storing and handling dynamic opinion calculation. The SOS uses Apache Derby as the opinion database, and Apache tomcat as the background HTTP container.

The system is deployed on a platform with Windows XP professional system, 2×2.4G Intel Core CPU, 3G memory, and 100Mbps Ethernet connection. We define INVITE as the P2PSIP request and 180 ringing as the response (See Figure 3 and Figure 4). Note that all the messages sending and receiving are based on TCP.

We use the Wireshirk [17] to monitor the message transmission. The testing shows that the system works well.

```
INVITE 20 P2PSIP/2.0
Max-Forwards:10
From:3
To:20
Call-ID:472721
CSeq: 1 INVITE
Contact:3
Via:3 127.0.0.1:9003;
```

Fig. 3. P2PSIP INVITE.

```
P2PSIP/2.0 180 Ringing
To:20
From:3
Contact:20
CSeq: 1 Response
Content-Length: 0
Via:3 127.0.0.1:9003;
20 192.168.0.101:9020;
```

Fig. 4. P2PSIP 180 Ringing.

3.2 Security

We use a typical malicious use scenario implementation (Figure 5) to show both of trust upgrading and the protection of the networks from compromised or malicious intermediate peers.

We initiate a P2PSIP request from peer 80, searching for destination peer 1618. Then, we assume the intermediate peer 1617 is a malicious/compromised intermediate peer that might discard, misroute, modify or temper the data message. This makes impossible for the message flow to reach destination peer (based on the conventional Chord routing: Peer 80 → peer 1331→ peer 1593 → peer 1609 → peer 1617 → peer 1618).

However, the situation is different in our system. The request would be directed to CSPG 1, CSPG 1030, and then CSP 1536. After that, "PingRequest is multicasted and therefore causes several routes. Although one of the routes will be interfered by malicious peer 1617, two others can still reach the destination peer. Finally, the destination peer asks Secure Opinion Server (SOS) via sending HTTP "asking, asking for the best route.

We assume that in a certain period, the opinion of each related peer is: peer 1593 (0.8, 0.1, 0.1), peer 1600 (0.82, 0.08, 0.08), peer 1609 (0.92, 0.04, 0.04), peer 1618 (0.9, 0.05, 0.05). We simulate this by manually modifying the opinion database. According to the description of Section 3.6, the opinion of two routes

is:

$$\omega_p^1 = \{0.738, 0.042, 0.22\} \text{ with } v = 0.764$$
$$\omega_p^2 = \{0.662, 0.037, 0.301\} \text{ with } v = 0.738$$

After the opinion calculation, SOS returns the most trustful route to the destination peer 1618. Thus, the session can be established in the most trustful way.

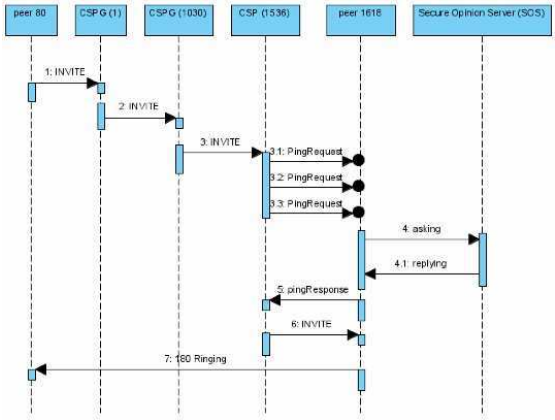

Fig. 5. A typical uses scenario.

4 Conclusion

In this paper we propose a new efficient and secure model for P2PSIP communication systems. The system model resolves several issues including three sub-overlay division, identifier assignment, cache mechanism, proxy based security, subjective logic based trust enhancement, NAT traversal, and message routing. These approaches improve the peer/resource lookup efficiency in P2PSIP session establishment and protect the system from security breaches, such as malicious or faulty intermediate peers.

In the future, we plan to study the extension function of CSP for legacy devices (e.g. mobile phone, etc) that lacks the capability to access P2PSIP overlay due to limited protocol support or other limitation in device capabilities (e.g. available computing, bandwidth, etc). A possible system architecture proposed in [19] can be further studied in this context.

References

1. P2PSIP. p. `http://www.p2p-sip.org`.

2. Kundan, S. and S. Henning, Peer-to-peer internet telephony using SIP, In Proceedings of the international workshop on Network and operating systems support for digital audio and video. 2005, ACM: Stevenson, Washington, USA.
3. Peer-to-Peer . p. http://www1.cs.columbia.edu/~salman/peer/.
4. SIPDHT2. p. http://sipdht.sourceforge.net/sipdht2/index.html.
5. MjSip. p. http://www.mjsip.org.
6. Bryan, D.A., Lowekamp, B. B., Zangrilli, M., The Design of a versatile, secure P2PSIP communications architecture for the public internet, In IEEE international Parallel and Distributed Processing Symposium. April, 2008: Lyon, France
7. C. Jennings, B.L., E. Rescorla, S. Baset, H. Schulzrinne, REsource LOcation And Discovery (RELOAD). draft-bryan-p2psip-reload-04, June, 2008.
8. D. Bryan, P.M., E. Shim, D. Willis, S. Dawkins, Concepts and Terminology for Peer to Peer SIP. draft-ietf-p2psip-concepts-02, July, 2008.
9. Matuszewski, M., Kokkonen, E., Mobile P2PSIP - Peer-to-Peer SIP Communication in Mobile Communities, In 5th IEEE Consumer Communications and Networking Conference, 2008. CCNC 2008. Jan, 2008: Las Vegas.
10. Xianghan Zheng, Vladimir Oleshchuk, Improving Chord lookup protocol for P2PSIP-based Communication Systems. In International Conference on New Trends in Information and Service Science (3rd NISS), June, 2008.
11. Guangyu Shi, Y.L., Jian Chen, Hao Gong, Hongli Zhang, T2MC: A Peer-to-Peer Mismatch Reduction Technique by Traceroute and 2-Means Classification Algorithm, In 7th International IFIP-TC6 Networking Conference. May 5-9, 2008: Singapore.
12. Huang, L., Location and Discovery of Subsets of Resources. Internet - Draft (working in process), July, 2008: p. http://tools.ietf.org/html/draft-licanhuang-p2psip-subsetresourcelocation-00.
13. Xianghan Zheng, Vladimir Oleshchuk, A Secure Architecture for P2PSIP-based Communication Systems, In 2nd International Conference on Security of Information and Networks (SIN 2009). Oct, 2009: North Cyprus.
14. Jsang, A., et al., Trust network analysis with subjective logic, In ACISP 2006, LNCS, Volume 48. 2006,
15. Xianghan Zheng, Vladimir Oleshchuk, Trust-based Framework for Security Enhancement of P2PSIP Communication Systems, In The 4th International Conference for Internet Technology and Secured Transactions (ICITST-2009). Nov, 2009: London.
16. David A. Bryan, B.B.L., Cullen Jennings, SOSIMPLE: A Serverless, Standards-based, P2P SIP Communication System First International Workshop on Advanced Architectures and Algorithms for Internet Delivery and Applications (AAA-IDEA'05) 2005: p. pp. 42-49.
17. Wireshark: Go deep.: p. http://www.wireshark.org/.
18. Stoica, I., Morris, R., Liben-Nowell, D., Karger, D. R., Kaashoek, M. F., Dabek, F., Balakrishnan, H., Chord: a scalable peer-to-peer lookup protocol for internet applications. IEEE/ACM Transactions on Networking, 2003. 11(1): p. 17-32.
19. Xianghan Zheng, Vladimir Oleshchuk, Hongzhi Jiao, A System Architecture for SIP/IMS-based Multimedia Services in International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE). Dec, 2007.