Secure Interworking with P2PSIP and IMS

Xianghan Zheng, Vladimir Oleshchuk
University of Agder, Norway
{xianghan.zheng, vladimir.oleshchuk}@uia.no

ABSTRACT

In this paper, we propose a secure system model for interconnection between P2PSIP and IMS domains. The interworking solution is based on P2P-IMS GateWay (PIGW), which acts as a normal peer in P2PSIP network and a 3rd party IMS Application Server (AS) in IMS network. The security is achieved by implementing Chord Secure Proxy (CSP) and enhanced with subjective logic based trust model. We also implement this system model and analyze it in several aspects: number of hops and delay, trust improvement and protection against malicious or compromised intermediate peers. We conclude that the proposed architecture is feasible and improves security. As far as we know our research is the first study that proposes secure internetworking P2PSIPS and IMS.

KEYWORDS: Peer Peer-to-Peer (P2P), Session Initiation Protocol (SIP), P2PSIP, Chord, Chord Secure Proxy (CSP).

1. INTRODUCTION

Currently, P2P computing has begun to infiltrate into SIP communication systems. The decentralized nature of P2P might provide distributed communication system without help of the traditional SIP server. In 2003, the SIPpeer [1] at University of Columbia and the SOSIMPLE [2] at William & Mary College were the first attempts to investigate the role of P2PSIP paradigm for communication systems. In the following years, the research has attracted great attention in both academia and industry [3-8]. IETF P2PSIP working group defines the motivation of P2PSIP [9]: 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.

IP Multimedia Subsystem (IMS) is a set of standards under development by 3rd Generation Partnership Project (3GPP) in partnership with a number of other standards [6]. It uses SIP protocol to setup, maintain and terminate multimedia sessions. IMS is expected to be an important solution to the future All-IP network and infrastructure.

Currently, researchers are beginning to study the possibility of interconnecting between P2PSIP and IMS networks. One typical proposal is described in [10], which implements a Gateway Application Server (AS) that is a peer in P2PSIP side and an Application Server in IMS side (shown in Figure 1). Through the bridge of Gateway AS, the users in different networks are capable to communicate with each other. The system model looks feasible from networking point of view.

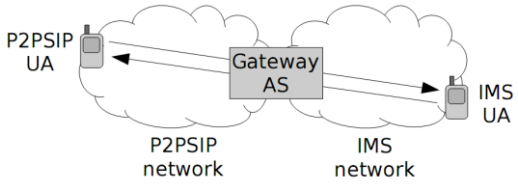


Figure 1. Interconnecting Model

However, the proposed interconnection model faces serious security challenges. Firstly, the confidentiality of signals traversing inside P2PSIP overlay is not guaranteed due to the distrust among participating P2PSIP peers. Let us consider a typical malicious model (shown in Figure 2), which also specifies how Gateway AS interacts with destination P2PSIP UA (peer D) with cooperation of intermediate peers B and C. Peer B (the panda) that acts as a malicious intermediate peer in P2PSIP overlay is capable to misroute, discard, temper, and replay the received P2PSIP signals.

978-1-4244-6622-1/10/$26.00 ©2010 IEEE

Secondly, Gateway AS is not secure enough since it is public to all P2PSIP peers, including malicious peers. For example, the panda is able to spy and record a profile of Gateway AS (e.g. peer ID, public IP, Port, etc.) through parsing incoming P2PSIP messages. Even if encryption is implemented, the incoming unencrypted parts of message header might still contain sensitive information (e.g. source IP, port, etc). This sensitive information privacy could be used to initiate DoS attack to consume resource of Gateway AS. Also, it might be used for SPAM attack to misdirect the system.

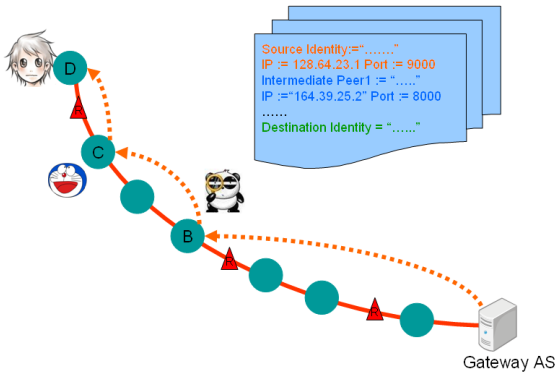


Figure 2. A Malicious Model

Therefore, in order to provide fully interconnected solutions, security issues should be taken into consideration, especially security inside P2PSIP network. In our design, we assure that following requirements are satisfied:

- Networking availability. At least one trusted gateway for relaying signal between P2PSIP and IMS domains is available.
- Security Guarantee. The message routing in P2PSIP domain should be security garanteed. Besides, the gateway should be resilient on a series of attack, e.g. DoS attack, SPAM, etc.

In this paper, we investigate on P2PSIP and IMS technical issues and propose P2PSIP-IMS GateWay (PIGW) as a secure interworking gateway between P2PSIP and IMS domains. Security are achieved by implementing Chord Secure Proxy (CSP) and PKI-based certificate, and enhanced by subjective logic based trust model.

The paper is organized as follows. In Section 2, we introduce the interconnecting system architecture and corresponding solutions. After that, three typical use scenarios are provided in Section 3. Section 4 analyses the proposed system architecture on number-of-hops and delay, and security enhancement. We draw the conclusions and open issues in Section 5.

2. SYSTEM ARCHITECTURE

In this section, we first introduce a possible solution that offers secure interconnecting services between P2PSIP and IMS. Then, we specify the technical issue about the system model, including networking and security issues.

2.1. Architecture Overview

Figure 3 shows the proposed system architecture, which contains following five elements:

- P2PSIP-IMS Interworking Gateway (PIGW) is the key interworking unit for translation of signals between P2PSIP and IMS networks.
- P2PSIP peer, which can be a PC, laptop, PDA, mobile phones etc., is connected to the internet. Each P2PSIP peer has a corresponding CSP as its master node.
- Chord Secure Proxy (CSP) is the secure proxy that relays the signals among PIGW and P2PSIP peers. The main task of CSP is to protect privacy sensitive PIGW.
- Enrollment & Authentication (E&A) Server handles enrollment and authentication task when P2PSIP peers join P2PSIP overlay.
- Secure Opinion Server (SOS) is the security enhancement server that handles dynamic opinion computing and storage task for each P2PSIP peer.

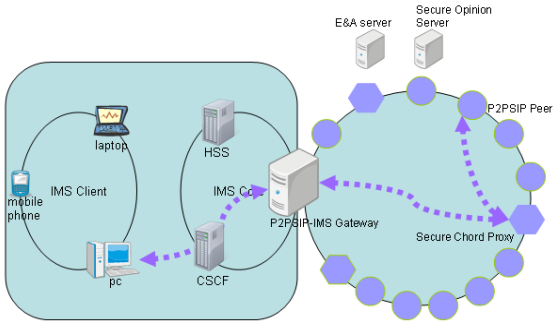


Figure 3. Secure System Architecture

Note that HSS (Home Subscriber Server) and CSCF (Call Session Control Function) are the basic elements in IMS core for SIP session establishment. Besides, CSPs and PIGW are pre-deployed backbone nodes in P2PSIP network. They are assumed to be trusted. In the following sections, we will specify technical approaches including networking and security.

2.2. P2PSIP-IMS Gateway

P2PSIP-IMS Gateway is the key inter-working unit, acting as bridge between P2PSIP and IMS networks. PIGW acts as a normal P2PSIP peer on P2PSIP side and an IMS application server on IMS side. There are five components inside PIGW (see Figure 4):

- P2PSIP Peer. This sub-component acts as a normal peer that receives/sends P2PSIP messages from/to P2PSIP network.
- Translation Logic. This part handles translation between P2PSIP and IMS signals.
- Forwarding Logic. This part decides which CSP P2PSIP message should be forwarded. It defines message routing strategy. For example, we can define the rule:"P2PSIP message is forwarded to a specific CSP that is anti-clockwisely nearest to the destination peer". Inside this subcomponent, there is a database recording all the connections to CSPs (e.g. CSP ID, public IP, port, etc) in P2PSIP overlay.
- IMS UA. IMS UA handles IMS client functionality that sends/receives IMS messages to/from IMS core. It contains UICC smart card for IMS authentication.
- IMS Application Server. This part receives IMS request from IMS client and sends the corresponding response to IMS core.

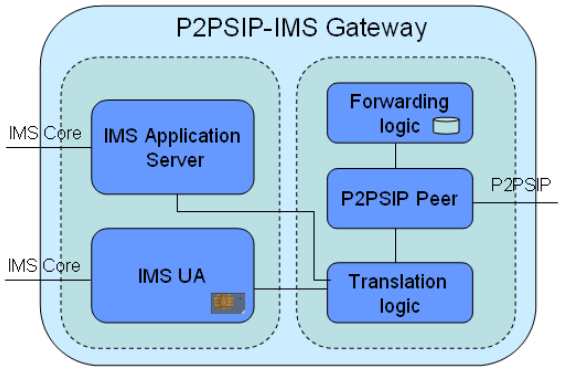


Figure 4. P2PSIP-IMS Gateway Internal

When IMS Application Server subcomponent receives IMS request, the translation logic subcomponent will parse the signals, retrieve destination peer identity and generate corresponding P2PSIP message. After that, P2PSIP UA sends out P2PSIP request to a specific CSP on direction of Forwarding logic subcomponent.

When receiving P2PSIP request, translation logic subcomponent will parse P2PSIP signals, retrieve IMS related information (e.g. destination IMS ID, etc), generate IMS signals, and forward to IMS UA subcomponent, which sends out IMS request.

In consideration of security problem, we suggest that PIGW is only capable to communicate with CSPs. Since CSP is assumed to be trusted, sensitive privacy data (e.g. PIGW peer ID, public IP, port, etc) is revealed to most of P2PSIP peers. Therefore, it makes malicious peer difficult to initiate Denial-of-Service (DoS) and SPAM attack to PIGW.

2.3. Chord Secure Proxy

Chord Secure Proxy (CSP) acts as a secure proxy between PIGW and destination peer. Each CSP is responsible to a certain part of P2PSIP overlay. When receiving P2PSIP request from PIGW, it reveals sensitive privacy (e.g. peer ID, public IP, port, etc) of PIGW by encapsulating and sending out a privacy unrelated message towards P2PSIP overlay. For example, we define a session layer "PingRequest" message (See Figure 5) that contains no private information related to PIGW. The use of "PingRequest" makes sure that intermediate peers are incapable to receive sensitive privacy of PIGW.

We propose CSP multicasts "PingRequest" to a few successors that are anti-clockwisely near to destination (as shown in Figure 6). "PingRequest" is forwarded based on Chord routing algorithm [11] hop-by-hop until the destination peer. Multicast mechanism guarantees to some degree that "PingRequest" message is resilient to message loss in case of compromised or faulty intermediate peers.

P2PSIP PingRequest
Call-ID : 9849303
CSP-ID: 512
CSP-IP: 158.36.228.48
CSP-Port: 9512
Dest-ID:586

Figure 5. "PingRequest" Message

When CSP receives P2PSIP request from P2PSIP peer, it checks validity of request. For example, if the request initiated from a peer that is out of responsible range of CSP, it might be discarded. Only passing the validity test, the request would be forwarded to PIGW, which sends out to IMS core.

2.4. Subjective Logic Based Trust Enhancement

When Destination peer receives several "PingRequest" from different routes (See Figure 6), it needs to choose one of them for handling. We propose to use subjective logic based trust model [12] for selecting the most trustful route.

The subjective logic defines the term opinion $\omega = \{t, d, u\}$, in which t, d and u correspond to trust,

distrust, and uncertainty respectively. Subjective logic defines logical operators to beal with specific entities called 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 from A to B is unchanged results of measurement", as following:

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

where ω_B^A and ω_p^A are two opinions about trustworthiness of A and B (for more details related to subjective logic the reader should consult [12]).

Suppose that a request goes through the source peer A, intermediate peers B_1 , B_2 , B_{n-1} , and ended in the destination peer B_n . By applying the rules of subjective logic recommendation, the trustworthiness of this data flow is:

$$\omega_p^{AB_1B_2\ldots B_{n-1}B_n} = \omega_{B_1}^A \otimes \omega_{B_2}^{B_1} \otimes \omega_{B_3}^{B_2} \otimes \ldots\ldots \otimes \omega_{B_n}^{B_{n-1}} \otimes \omega_p^{B_n}$$

In our previous publication [13] we describe implemention of this concept and prove that this approach can efficiently enhance the security during P2PSIP session establishment.

After computing the most trustful route, destination peer returns a session level "PingResponse" directly to source peer. Compare with "PingRequest", "PingResponse" contains two additionally fields: destination IP and destination port.

2.5. Certificate based Security

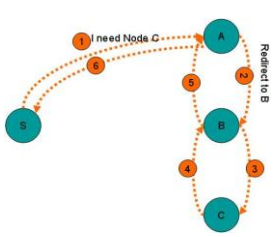
IETF P2PSIP Working Group has suggested use Public Key infrastructure (PKI) based certificate in P2PSIP peers [4, 8]. Certificate proves the legitimacy of the specific peer and helps establish secure session. In additional to a few basic elements (e.g. version number, signature algorithm, digital signature of the issuer, etc), P2PSIP peer certificate might include P2PSIP related information: peer specific ID and one or more user names (e.g. alice@operator.com, etc). Centralized E&A server is supposed to issue certificate for each P2PSIP peer.

The use of PKI certificate provides the data confidentiality, integrity and authentication among PIGW, CSPs, and P2PSIP peers. It could efficiently prevent the identity attacks (e.g Sybil attack, etc).

2.6. Message routing

We propose use Recursive routing (See Figure 6) for "P2PSIP MESSAGE" message transmission. In this routing, the request is initiated from source (IMS client or P2PSIP peer), forwarded by intermediate peers (including Gateway), hop by hop until the destination (IMS client or P2PSIP peer). The response (e.g. "200 OK", etc) follows the same route back to the source. The implement of this approach could efficiently protect the privacy sensitive data from understanding by other P2PSIP peers.

We also suggest Semi-recursive routing (See Figure 7) for "Ping" message transmission. The different with Recursive routing is that corresponding response is returned directly from the destination to the source. This approach reduces the total number of the message transmitted and therefore reduces the delay.



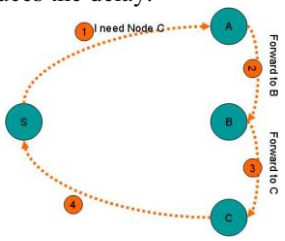


Figure 6. Recursive Routing **Figure 7. Semi-Recursive Routing**

2.7. Unreachable Target Notification

The request initiated might not be able to reach the target due to a few reasons. For example, IMS client or P2PSIP peer might loss the connection with network due to the limitation of device capability (e.g. no power, system deadlock, etc) or network problem (e.g. no signal, etc). Therefore, it is necessary to notify the source when the target is unreachable. We propose that PIGW handles the notification task by sending "P2PSIP MESSAGE" and "SIP MESSAGE". One typical example will be shown in Section 3.3.

3. USE SCENARIOS

In the following subsections we demonstrate the using of the proposed architecture for text based instant messing services, with three use cases. We define "P2PSIP MESSAGE" and "SIP MESSAGE" as the request, "P2PSIP 200 OK" and "SIP 200 OK" as corresponding response. Note that the proposed system architecture is able to be extendable for the other advanced services (e.g. presence services, VoIP, etc).

3.1. Use scenario 1

Use scenario 1 (see Figure 8) describes how IMS client sends message to a P2PSIP peer. Possible message flows are:

1. IMS client sends "SIP MESSAGE" message to PIGW (for example, 260 as P2PSIP ID and pigw@ericsson.com as IMS ID).
2. PIGW returns "SIP 200 OK" to IMS client.
3. PIGW sends "P2PSIP MESSAGE" message to the specific CSP that is responsible for destination peer.

4-6 CSP multicasts "PingRequest", which is then forwarded by intermediate peers until the destination.

7. Destination peer receives several "PingRequest" from different routes. It asks SOS server to select one of them.
8. SOS server returns the most trustful route.
9. Destination peer returns a "PingResponse" to corresponding CSP.
10. CSP forwards original "P2PSIP MESSAGE" to destination peer.
11. Destination peer returns a "P2PSIP 200 OK" the corresponding CSP.
12. CSP forwards original "P2PSIP 200 OK" back to PIGW.

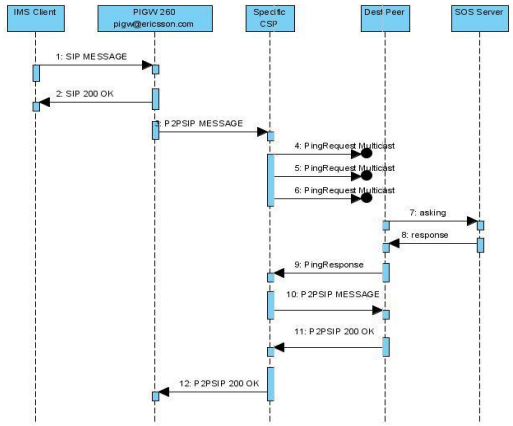


Figure 8. IMS Client MESSAGE P2PSIP Peer

3.2. Use Scenario 2

Figure 9 describes how P2PSIP peer sends message to IMS client. Possible message flows are:

1. P2PSIP peer sends "P2PSIP MESSAGE" to a responsible CSP.
2. CSP forwards "P2PSIP MESSAGE" to PIGW (for example, 260 as P2PSIP ID and pigw@ericsson.com as IMS ID).
3. PIGW returns "SIP 200 OK" to the corresponding CSP.
4. Corresponding CSP returns "P2PSIP 200 OK" back to P2PSIP peer.
5. PIGW sends "SIP MESSAGE" to IMS client.
6. IMS client returns "SIP 200 OK" to PIGW.

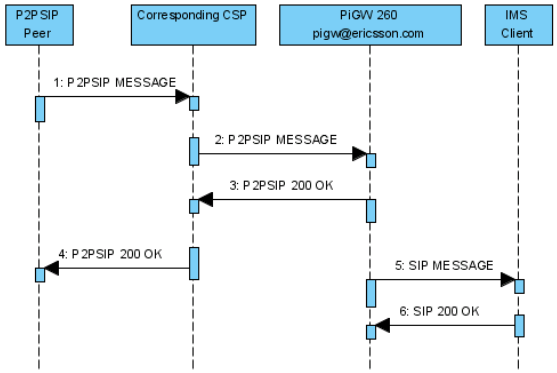


Figure 9. P2PSIP Peer MESSAGE IMS Client

3.3. Error Handling Scenario

Figure 10 shows the error handling use scenario when P2PSIP peer is unavailable to reach. Possible messages among source peer, CSP, intermediate peers and destination peer are:

1. P2PSIP peer sends "P2PSIP MESSAGE" to its corresponding CSP.
2. Corresponding CSP forwards "P2PSIP MESSAGE" to PIGW (for example, 260 as P2PSIP ID and pigw@ericsson.com as IMS ID).
3. PIGW sends "P2PSIP MESSAGE" to P2PSIP network.
4. Message retransmission after TTL.
5. PIGW replys with IMS client with "unreachable peer".
6. IMS client returns "SIP 200 OK" to PIGW.

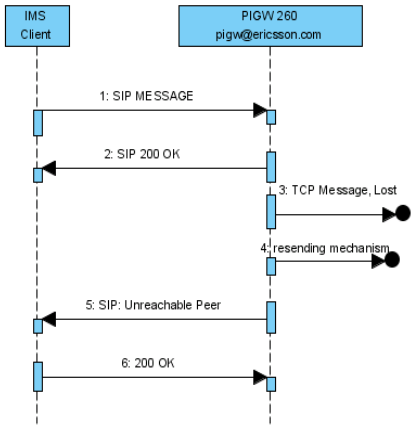


Figure 10. Unreachable P2PSIP Peer

4. PROTOTYPE SIMULATION

We construct a P2PSIP overlay of 512 P2PSIP peers, with 496 P2PSIP normal peers, 15 CSPs and a PIGW peer. After that, we import IMS application server function to PIGW, which then acts as an IMS application server (with ims id: greetings@ericsson.com) and a P2PSIP peer (with id: 260). Apache Derby is selected as the embedded database implementation for P2PSIP peers, CSPs, and PIGW.

We simulate IMS core network and IMS client by using Ericsson SDS 4.1 (Service Development Studio) and Ericsson IMS Testing Agent (See Figure 14) respectively [14]. We implement text based instant messaging service to show availability of proposed system with two use scenarios: IMS client MESSAGE P2PSIP peer, and P2PSIP peer MESSAGE IMS client. We manually define "P2PSIP MESSAGE" (Figure 11) as request and "P2PSIP 200 OK" (Figure 12) as response.

The system is deployed separately on a platform with Windows XP professional system, 2*2.4G Intel Core CPU and 3G memory. Wireshark [15] is used to monitor the message transmission. The testing shows that the system works well.

```
MESSAGE alice@ericsson.com P2PSIP/2.0
Max-Forwards:70
CSeq:MESSAGE
Content-length:20
Contact:586
From:586
To:alice@ericsson.com
Call-ID:517846
Via:586 158.36.228.48:9586;512 158.36.228.48:9512
```

Figure 11. P2PSIP Request

```
P2PSIP/2.0 200 OK
To:alice@ericsson.com
From:586
Contact:586
CSeq: 200 OK
Content-Length: 0
Via:586 158.36.228.48:9586;512 158.36.228.48:9512
```

Figure 12.P2PSIP 200 OK Response

Figure 13. P2PSIP MESSAGE Peer

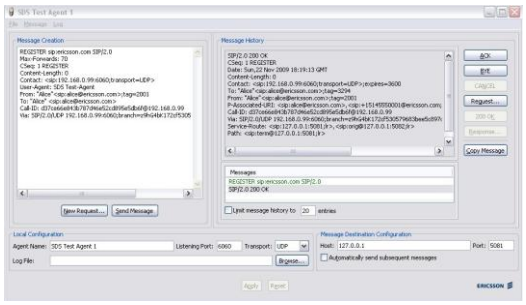


Figure 14. Ericsson IMS Test Agent

5. EVALUATION

In this section, we evaluate the proposed system model in three aspects. We analyze number of hop, and measure latency to show that proposed system is feasible and efficient. Then, we analyze the security upgrading according to the comparison with previous related proposal in [10].

5.1. Number of Hops and Measure of Delay

We assume that the number of P2PSIP peers in the overlay is N, including S CSPs. We first consider the number of hops in use scenario 1 (Section 3.1). According to Chord routing algorithm, the average number of hops of "PingRequest" is $\log_2(N/S)$. In additional to 3 hops among IMS client, PIGW, CSP, and SOS server (as shown in Figure 9), the average number of hops in use scenario 1 is $3+\log_2(N/S)$. As to use scenario 2 in Section 3.2, the number of hops is fixed as 3 (as shown in Figure 15).

Then we measure delays in two use scenarios (Section 5.1 and 5.2). We firstly select an IMS client (with ims id: alice@ericsson.com) as the initiator and randomly select 20 P2PSIP peers as destination. We send the request and measure the latency between "SIP MESSAGE" sent out from IMS client and "P2PSIP 200 OK" received in PIGW260. We get the average delay of 326ms. Using similar method, we get the delay of use scenario 2 of 408ms.

According to the result of num-of-hop and delay, it is convinced that the proposed interconnecting system architecture is feasible.

5.2. Security upgrading

In Section 1, we have introduced related proposal in [10], which faces serious security problem. In our proposed system, the security is greatly improved.

When P2PSIP peer initiates the request, it first contacts with its corresponding CSP, which relays the traffic to PIGW. Since CSP and PIGW are assumed to be trustful, the session is trusted. Therefore, the session initiated from P2PSIP peer is regarded to be secure.

Then, we consider the situation when IMS client initiates the session. We initiate a P2PSIP request from IMS client (coco@ericsson.com), for destination peer 1618. The request would be directed to PIGW, and then CSP 1536. After that, "PingRequest" is multicasted on three routes. Although one route is unavailable due to malicious or faulty intermediate peers, the other two can still reach the destination (Figure 15).

Based on the subjective logic (described in Section 3.4), SOS server calculates and chooses the most trusted route. Suppose that there are two route options. After calculation, SOS gets opinion result:

$\omega_p^1 = \{0.264, 0.012, 0.724\}$ with $v=0.605$

$\omega_p^2 = \{0.167, 0.005, 0.826\}$ with $v=0.570$

After that, SOS returns the first route which has higher v.

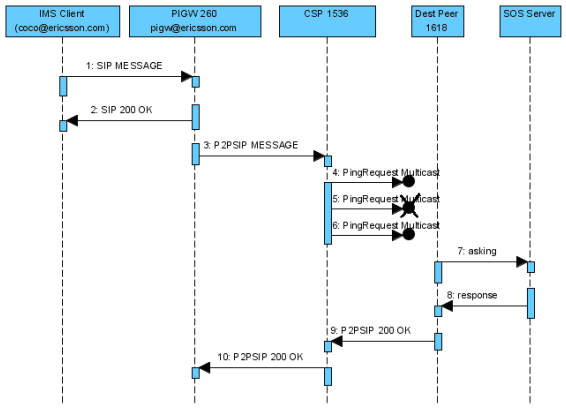


Figure 15. A Typical Use Scenario

6. CONCLUSION AND FUTURE WORK

In this paper we propose a possible secure architecture for interconnecting P2PSIP and IMS domains. The key interworking unit is P2PSIP-IMS GateWay, which acts as an IMS application server in IMS side and a peer in P2PSIP side. Security is mainly achieved by implementing Chord Secure Proxy, PKI based certificate, and subjective logic based trust. After that, we implement the prototype and analyze the system model based on the implementation.

In the future, we plan to study the extension function of CSP to 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 system architecture proposed in [16] might be further extended.

REFERENCES

[1] Kundan, S. and S. Henning, "Peer-to-peer internet telephony using SIP," Proceedings of the international workshop on Network and operating systems support for digital audio and video. 2005, ACM: Stevenson, Washington, USA.

[2] David A. Bryan, Bruce B. Lowekamp, 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.

[3] Bryan, D.A., Lowekamp, B. B., Zangrilli, M., "The Design of a versatile, secure P2PSIP communications architecture for the public internet," IEEE international Parallel and Distributed Processing Symposium. April, 2008: Lyon, France.

[4] C. Jennings, B.Lowekamp, E. Rescorla, S. Baset, H. Schulzrinne, "REsource LOcation And Discovery (RELOAD)," draft-bryan-p2psip-reload-04, June, 2008.

[5] Feng Cao, David A.Bryan, Bruce B.Lowekamp, "Providing Secure Services in Peer-to-Peer Communications Networks with Central Security Servers," International Conference on Internet and Web Applications and Services (ICIW), Feb, 2006.

[6] Matuszewski, M., Kokkonen, E., "Mobile P2PSIP - Peer-to-Peer SIP Communication in Mobile Communities," 5th IEEE Consumer Communications and Networking Conference, 2008. CCNC 2008. Jan, 2008: Las Vegas.

[7] Xianghan Zheng, Vladimir Oleshchuk, "Improving Chord lookup protocol for P2PSIP-based Communication Systems," 2009 International Conference on New Trends in Information and Service Science (3rd NISS), June, 2009.

[8] D. Bryan, P.Mathews, E. Shim, D. Willis, S. Dawkins, "Concepts and Terminology for Peer to Peer SIP," draft-ietf-p2psip-concepts-02, July, 2008.

[9] P2PSIP. p. http://www.p2p-sip.org.

[10] Jani Hautakorpi, Arturo Salinas, Erkki Harjula, Mika Ylianttila, "Interconnecting P2PSIP and IMS," Next Generation Mobile Applications, Services and Technologies. Sept, 2008: Wales, UK.

[11] 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.

[12] Audun, Josang, Ross Hayward, Simon Pope, "Trust network analysis with subjective logic," Proceedings of the 29th Australasian Computer Science Conference - Volume 48. 2006, Australian Computer Society, Inc.: Hobart, Australia.

[13] Xianghan Zheng, Vladimir Oleshchuk, "Trust-based Framework for Security Enhancement of P2PSIP Communication Systems," The 4th International Conference for Internet Technology and Secured Transactions (ICITST-2009). Nov, 2009: London.

[14] BitComet. p. www.bitcomet.com.

[15] Wireshark: Go deep.: p. http://www.wireshark.org/.

[16] Xianghan Zheng, Vladimir Oleshchuk, Hongzhi Jiao, "A System Architecture for SIP/IMS-based Multimedia Services," International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE). Dec, 2007.