Inter-working of P2P-SIP and Traditional SIP Network

Balamurugan KARPAGAVINAYAGAM

MADYNES TEAM, LORIA-INRIA Lorraine

Presented at
EMANICS P2P Workshop
March 3-4, 2008 - Zurich, Swiss
Outline

• Introduction
  • What is P2P-SIP?
  • Why P2P-SIP?
  • Different Approaches of P2P-SIP

• Inter-working of P2PSIP & Traditional SIP

• Integration in EMANICS VoIP testbed

• Conclusion
Introduction

• What is P2P-SIP?
  • Use the P2P techniques (like DHT) to resolve the SIP related functions
  • Leveraging the advantages of distributed network (P2P) for SIP network
    – Reliability, scalability etc.,

• Why P2P-SIP?
  • NO centralized server
    – Lower Maintenance cost, configuration
    – Better reliability with higher Latency, scalability, robustness

INVITE: bob@inria.fr
Contact: 192.168.1.4

INVITE: bob@inria.fr
Contact: 192.168.1.4

P2P Overlay
Introduction (cont..)

Different Approaches of P2P-SIP

• SIP using P2P
  • Replace the SIP location service with a P2P protocol

• P2P using SIP
  • Implement P2P using SIP messaging
    • i.e., Use SIP messages to transport P2P traffic
How is P2P-SIP works?

- Replace the SIP location service with a P2P protocol
- SIP URI are used for Hash key generation in DHT.
  - Eg., Sip:bob@test.bamboo => Hash(Key, identifier)
- Communication between the P2PSIP client and DHT uses P2P protocol
Inter-working of P2PSIP and Traditional SIP networks

• Problems
  • Finding the exact location of the clients (both P2P-SIP and conventional)
    – Because P2P-SIP domain uses overlay identifier rather than DNS entries.
    – Whereas conventional SIP uses DNS to locate domains
  • Solution
    – Need a gateway (proxy) kind of approach

• Different Approaches
  • P2P-SIP Peer can act as Standard SIP Proxy and Registrar for conventional SIP UA
    – The peer can insert the UA in the distributed database
    – Can retrieve contact information from the distributed database when proxying
Inter-working of P2PSIP and Traditional SIP networks (cont.,)

• **Different Approaches.**
  - Act as a SIP Proxy for the overlay
    - P2P-SIP peer has a fully qualified domain name (FQDN) that matches the overlay name.
  
  • **Use Hierarchical overlay architecture**
    - Has two level of overlays (Higher and Lower)
    - Higher level overlay will serve as the gateway for the lower level
      - i.e., the higher level overlay will be connected to the internet and lower level is just a P2P-SIP overlay
P2P-SIP Architecture

Components

- **P2P nodes**: deployed in EMANICSLAB
- **A SIP Proxy Server**: Serves as a Proxy for the traditional SIP clients and also connects to the P2P-SIP clients via an upper level overlay
P2P-SIP in EMANICS Testbed (cont.,)

• How is it deployed?
  • We use an existing open source implementation called Olyo P2P-SIP based VoIP system (http://code.google.com/p/olyo/)
  • Uses Bamboo DHT
  • A P2P-SIP adaptor (Modified PartySIP)
    – connects the SIP clients and P2P overlay

---

Internal Structure of P2P-SIP user node

Working of REGISTER and INVITE of two nodes in the P2P-SIP overlay
Conclusion

• About P2P-SIP
  • P2P-SIP is still in the beginning stage of its development and needs a standard architecture specification for interworking with traditional SIP networks.

• Some open Issues (Research to be done)
  • How do we connect many domains in the overlay?
  • Should we register one domain in many overlays?
  • Define User management or buddy list?
  • How are the authentication, authorization, accounting to be handled?
  • Provide traditional services like Voicemail, conferencing, emergency services, etc.,
  • P2P-SIP security (DoS attacks, etc.,)
Thank you

Any Questions?
Peer-to-Peer SIP
Implementation and monitoring

UPI Research Team
Existing infrastructure

- VoIP testbed based on Asterisk servers
- servers are interconnected through IAX
- system is hierarchical and secured
- authentication is needed to join in
- latency is low, voicemail and conferencing are active; PSTN connectivity is enabled
Map of the VoIP testbed
Peer-to-peer architectures

- P2P is not new, file sharing services are using it for quite some time with success
- Every user installs a copy of the network’s client and it announces the others of its presence, location and shared content when connecting
- Data flows directly form one peer to another
- System is reliable and scalable, without any server being a single point of failure
Client/server vs P2P
Commercial solution

- P2P + Voice = Skype
- free for now, but closed source and proprietary protocols, highly encrypted; no compatibility
- hybrid system, uses Global Index Server for authentication, friends list and user lookup
- nodes with enough resources and bandwidth become super-nodes, routing traffic (act as proxy) for users behind NAT and firewalls
P2P SIP architecture (1)

- SIP used as communication protocol between peers, and an existing P2P (preferably OSS) protocol for user registration (REGISTER) and lookup;
- a ring-structured DHT like Chord or Bamboo reduces latency to $O(\log(n))$, because every peer keeps information about $\log(n)$ of its neighbors
- a SIP ID (sip:user@domain) is associated with a hash key, based on the client’s IP address
- security may be an issue: privacy is not insured (call logging), and DoS attacks are possible
- solution: a PKI combined with a web of trust gives results
P2P SIP architecture (2)

- reliability: when a peer or a super-node shuts down, its absence is detected by the REFRESH messages that remain unanswered and Chord structures of the neighbors are updated accordingly.
- voicemail can be stored either at the sender, either on a super-node and delivered later, when the client connects.
- a super-node can become a mixer for multi-party conferencing between its clients.
- ICE can be used for NAT traversal, as every peer has integrated STUN and TURN server.
- Tested implementations: Olyo and P2P SIP Monitor.
Monitoring P2P SIP

- **Nagios**: widely used open-source monitoring platform, running on Linux as a daemon
- Open, plug-in-based architecture, with a web-based GUI for graphs and reports
- Periodically launches plug-ins against selected hosts (defined IPs) to check service availability
- In case of failures, it can automatically alert administrators by e-mail, Jabber or even SMS
- Has the ability to automatically run error-correcting scripts without intervention, by SSH
P2P monitoring diagram
NSCA Communication
check_p2p plug-in for Nagios

- Perl script that sends an OPTIONS message to every P2P SIP client on the standard port (5060), or a standard check_http against 6301 port of the partiesip client (Olyo) => client’s IP needed; **solution**: modify client to send IP to a java server that updates hosts.cfg

- another option is that the client sends messages to the Nagios Service Check Acceptor, calling send_nsca from the client code:

```bash
$ /usr/sbin/send_nsca -H localhost -c /etc/send_nsca.cfg
```
Thank you for your attention!

Questions & Answers