An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol

Written by: Salman A. Baset and Henning G. Schulzrinne (Colombia University, NY)
CIS 6000 Distributed Systems
Benjamin Ferriman
bferrima@uoguelph.ca

School of Computer Science
University of Guelph
Guelph, Ontario, Canada
Agenda

- Introduction
- Key Components
- Communication
- Conferencing
- Comparison of Similar Clients
- Conclusion
Introduction

- Skype
  - Peer-to-peer (p2p) Voice-over-IP (VoIP) client
  - Created by makers of Kazaa
  - Overlay p2p Network

- Supports: voice, video, chat, and even text messaging
Introduction

- Overlay Network consists of two nodes
  - Ordinary Nodes
  - Super Nodes
- Their connections are arranged in according to “Neighbor Relationships”
- There is also a Skype login server and SkypeIn/SkypeOut servers for PC-to-PSTN and PSTN-to-PC communications
Introduction

Figure 1: Skype Network Configuration [1]
Introduction

- Ordinary Node (SC)
  - The Skype Client
  - Keeps a table of reachable nodes
  - Holds IP and port number of super nodes
  - Referred to as **host cache** (HC) in Skype
  - Stored in an XML file
Introduction

- Super Node (SN)
  - End-point for client
  - Has public IP
  - Requirements: Sufficient CPU, Memory, and Network bandwidth
  - Authentication is done separately with the login server
  - This helps Skype ensure a global credential database, ensuring SkypeID uniqueness
Key Components

- Ports
- Host Cache
- Codecs
- Buddy List
- Encryption
- NAT and Firewall
Key Components - Ports

- Skype opens two ports for listening to TCP and UDP protocols
- Port number is randomly selected when client is installed
- Ports 80 and 443 are also opened to accommodate HTTP and HTTP-over-TLS traffic
Key Components – Host Cache

- List of super node IP and port pairings
- shared.xml
- Holds maximum of 200 entries
- If no entries in file Skype uses one of 7 hardcoded IPs
Key Components - Codecs

- Uses iLBC, iSAC, and iPCM
- Allows frequencies 50 to 8000 Hz
Key Components – Buddy List

- Stored as “config.xml”
- Unencrypted
- Stores Skype central login server
- Note: file is also replicated on the login server for better mobile service access
- Buddys are identified by their IDs
Key Components – Buddy list

<CentralStorage>
  <LastBackoff>0</LastBackoff>
  <LastFailure>0</LastFailure>
  <LastSync>1135714076</LastSync>
  <NeedSync>0</NeedSync>
  <SyncSet>
    <u>
      <skypebuddy1>2f1b8360:2</skypebuddy1>
      <skypebuddy2>d0450f12:2</skypebuddy2>
    </u>
  </SyncSet>

Figure 2: config.xml [1]
Key Components - Encryption

- Skype uses AES 256-bit encryption
- $1.1 \times 10^{77}$ possible keys
- Key Exchange facilitated through 1024-bit RSA
- RSA Certificates 1536 or 2048-bit
Key Components – NAT and Firewall

- Only hypotheses about technology behind
- Thought to use the STUN and TURN protocols
- Information stored in shared.xml
- A Skype client cannot prevent itself from becoming a super node (contrary to Kazaa)
Communication

Figure 3: Skype Login process (with no entries in HC file) [1]
Communication

- HTTP is used because version information is shared through GET requests.
- Calling and Tear down
  - Average of 3 Messages a Second
  - Voice Packet 70 to 100 bytes
  - Teardown is simply accomplished through a message with signaling information.
Communication

Figure 4: Skype Call (caller to callee) [1]
Communication

Figure 5: Skype call through NAT and Firewall [1]
Conferencing

- Skype uses a “Mixer” approach to message passing
- A central client sends out its and the remaining messages to their respected recipients
- It is assumed that at some point in the size of a conference Skype would use full mesh conferencing
Conferencing

Figure 5: Example of conference between 3 clients (A, B, C) [1]
Comparison of Similar Clients

- Yahoo
- MSN
- Google Talk

- Benchmarks were conducted on three laptops over a period of three days
- Data on these tests is limited
Comparison of Similar Clients

- Over the other 3 applications, Skype had the lowest mouth-to-ear latency time of the services.
- It is believed that this is the case due to a decentralized network with minimal centralized needs.
- Skype makes arrangements with OS to give it highest priority on CPU and Network bandwidth.
Figure 6: World Map of Super Nodes [1]
Figure 7: Host Cache File (shared.xml) [1]
Conclusion

- Skype is a highly distributed VoIP client
- Communication is performed with quality security practice
- Skype reduces messages when conferencing
- Skype has the lowest call latency time of the four largest free VoIP services
Conclusion

- Interesting Symptom described in papers conclusion
- If every client's bandwidth was capped, Skype would starve for Super Nodes and the network would effectively be broken
- I felt that this was a well written technical paper that utilized images and diagrams well
references

Thank You!