12

Reliable Session Initiation Protocol

Harold Zheng, Ph.D., and Sherry Wang, Ph.D.
Johns Hopkins University /
Applied Physics Laboratory
U.S.A.

1. Introduction

The IP Multimedia Subsystem (IMS) is a maturing technology. It has the potential to be used in Mobile Ad Hoc Networks (MANETs) to provide multimedia Internet experience for much diversified users with a variety of applications in a highly mobile environment. The introduction of the IMS into MANETs and futuristic mobile networks face unique challenges and needs.

The underlying signalling protocol for the IMS is the Session Initiation Protocol (SIP). In this chapter, we first investigate the "unreliable signalling" problem of using SIP for mobility support. Based on the investigation and the analysis, this chapter introduces an enhanced SIP signalling mechanism called Chain-Based SIP signalling (CBS) to mitigate the problem. The analytical performance analysis results will be given in the chapter as well.

1.1 Session Initiation Protocol (SIP)

The Session Initiation Protocol (SIP) (Rosenberg, J. et al., 2002) is an application-layer signalling and control protocol that performs user location, session setup, and session management. It works independently of underlying transport protocols and the type of sessions that are being established. The SIP is a core protocol for initiating, managing, and terminating peer-to-peer communication sessions on the Internet. These sessions may be text, voice, video, or a combination of these. SIP sessions involve one or more participants and can use unicast or multicast communications.

The SIP proposal began in 1995 in IETF Multiparty Multimedia Session Control (MMUSIC) Working Group (WG), then from February 1996 (draft-ietf-mmusic-sip-00, 15 ASCII pages with one request type) to March 1999 (RFC 2543, 153 ASCII pages, 6 methods) the first RFC was proposed. In November 1999, SIP WG was formed. In December 2000, it was recognized that the amount of work at SIP WG was becoming unmanageable, and consequently, numerous individual subsections were formed. In April 2001, a proposal for splitting SIP WG into SIP and SIPPING was announced. In June 2002, the RFC 2543 was obsolete and replaced by RFC 3261 (Rosenberg, J. et al., 2002). Today, there are over 100 IETF RFCs related to SIP and SIP implementations widely available. The SIP Status can be found at:

http://tools.ietf.org/wg/sip/.

The Table 1 lists some commonly used SIP related IETF RFCs.

RFCs	Description
RFC 2326: Real-Time Streaming Protocol (RTSP)	An application-level protocol for control over the delivery of data with real-time properties
RFC 2327: Session Description Protocol (SDP)	Describes multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation.
RFC 2976: The SIP INFO Method	Adds INFO method to the SIP protocol
RFC 3050: Common Gateway Interface for SIP	Defines a SIP CGI for providing SIP services on a SIP server
RFC 3261: Session Initiation Protocol (SIP)	The core SIP specification. It baselines the SIP protocol for multimedia session handling.
RFC 3262: Reliability of Provisional Responses in the SIP	Specifies an extension to provide reliable provisional response messages.
RFC 3263: SIP: Locating SIP Servers	Uses the DNS procedures to allow a client to resolve a SIP Uniform Resource Identifier (URI) into an IP address, port, and transport protocol of the next hop to contact for locating a server.
RFC 3264: An Offer/Answer Model with the SDP	Defines Offer/Answer model for the SDP use with the SIP.
RFC 3265: Session Initiation Protocol (SIP)-Specific Event Notification	Describes an extension of the SIP, by which SIP nodes can request notification from remote nodes indicating that certain events have occurred.
RFC 3266: Support for IPv6 in SDP	Describes the use of Internet Protocol Version 6 (IPv6) addresses in conjunction with the SDP.
RFC 3311: The Session Initiation Protocol (SIP) UPDATE Method	Adds an UPDATE method to the SIP protocol.
RFC 3312: Integration of Resource Management and SIP	Defines a generic framework for preconditions and discusses how network quality of service can be made in a precondition for the establishment of sessions initiated by the SIP.
RFC 3313: Private Session Initiation Protocol (SIP) Extensions for Media Authorization	Defines a SIP extension that can be used to integrate QoS admission control with call signalling and help guard against denial of service attacks.
RFC 3320: Signalling compression (SigComp)	Defines a solution for compressing messages generated by application protocols such as the SIP and the RTSP.
RFC 3323: A Privacy Mechanism for the SIP	Defines new mechanisms for the SIP in support of privacy.
RFC3329: Security Mechanism	defines new functionality for negotiating the security

RFCs	Description
Agreement for the SIP	mechanisms used between a the SIP user agent and its next-hop SIP entity.
RFC3372: Session Initiation Protocol for Telephones (SIP-T): Context and Architectures	Taxonomies the use of PSTN-SIP gateways, provides uses cases, and identifies mechanisms necessary for interworking.
RFC3407: SDP simple Capability Declaration	Defines a set of SDP attributes that enables SDP to provide a minimal and backwards compatible capability declaration mechanism.
RFC3428: Session Initiation Protocol (SIP) Extension for Instant Messaging	Defines SIP extensions for Instant Messaging.
RFC3515: The Session Initiation Protocol (SIP) Refer Method	Adds REFER method to the SIP protocol.
RFC3550: RTP: A Transport protocol for Real-Time Applications	A replacement of RFC 1889 (RTP). It describes the RTP and enhances the scalable timer.
RFC3605: Real Time Control Protocol (RTCP) Attributes in Session Description Protocol (SDP)	Describes the parameters of media streams used in multimedia sessions.
RFC3702: AAA Requirement for SIP	Provides basic authentication, authorization, and Accounting requirements for the SIP.
RFC3711: The Secure Real-time Transport Protocol (SRTP)	Describes the SRTP that can provide confidentiality, message authentication, and replay protection to the RTP traffic and to the RTCP.
RFC3840: Indicating User Agent Capabilities in the SIP	Defines mechanisms by which a SIP user agent can convey its capabilities and characteristics to other user agents and to the registrar for its domain.
RFC 3853: S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)	Updates the normative guidance of RFC 3261 to require the Advanced Encryption Standard (AES) for S/MIME.
RFC3856: A Presence Event Package for the SIP	Describes the usage of the SIP for subscriptions and notifications of presence. Presence is defined as the willingness and ability of a user to communicate with other users on the network.
RFC4028: Session timers in the SIP	Defines an extension to the SIP for a periodic refresh of SIP sessions through a re-INVITE or UPDATE request.
RFC4032: Update to the Session Initiation Protocol (SIP) Preconditions Framework	Updates RFC 3312, which defines the framework for preconditions in SIP.

RFCs	Description
RFC4083: Input 3GPP Release 5 Requirements on the SIP	Describes the requirements identified by 3GPP to support the SIP for Release 5 of the 3GPP IMS in cellular networks.
RFC 4168: SCTP as a Transport for SIP	Specifies a mechanism for usage of SCTP (the Stream Control Transmission Protocol) as the transport mechanism between SIP entities.
RFC 4189: Requirements of End-to-Middle Security for the SIP	Defines a set of requirements for a mechanism to achieve end-to-middle security.
RFC 4320: Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction	Describes modifications to the SIP to address problems that have been identified with the SIP non-INVITE transaction.
RFC 4353: A Framework for Conferencing with the SIP	Defines a framework for how conferencing can occur. This framework describes the overall architecture, terminology, and protocol components needed for multi-party conferencing.
RFC 4354: A SIP Event Package and Data Format for various settings in support for the PoC Service	Defines a SIP event package to support publication, subscription, and notification of additional capabilities required by the Push-to-Talk over Cellular (PoC) service.
RFC 4412: Communications Resource Priority for the SIP	Provides support for precedence handling within the SIP protocol
RFC 4780: Management Information Base for the Session Initiation Protocol (SIP)	Defines a portion of the Management Information Base (MIB) for use with SIP. It describes a set of managed objects that are used to manage SIP entities, which include User Agents, Proxy, Redirect, and Registrar servers.
RFC 4916: Connected Identity in the Session Initiation Protocol (SIP)	Provides a means for a SIP User Agent that receives a dialog-forming request to supply its identity to the peer User Agent by means of a request in the reverse direction, and for that identity to be signed by an Authentication Service.
RFC 5027: Security Preconditions for Session Description Protocol (SDP) Media Streams	Defines a new security precondition for the Session Description Protocol (SDP) precondition framework described in RFCs 3312 and 4032.
RFC 5367: Subscriptions to Request-Contained Resource Lists in the Session Initiation Protocol (SIP)	Specifies a way to create subscription to a list of resources in SIP.
RFC 5393: Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies	Normatively updates RFC 3261, the Session Initiation Protocol (SIP), to address a security vulnerability identified in SIP proxy behaviour.

RFCs	Description
RFC 5621: Message Body Handling in the Session Initiation Protocol (SIP)	Specifies how message bodies are handled in SIP.
RFC 5626: Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)	Defines behaviours for User Agents, registrars, and proxy servers that allow requests to be delivered on existing connections established by the User Agent.
RFC 5630: The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)	Provides clarifications and guidelines concerning the use of the SIPS URI scheme in the Session Initiation Protocol (SIP).
RFC 5922: Domain Certificates in the Session Initiation Protocol (SIP)	Describes how to construct and interpret certain information in a PKIX-compliant certificate for use in a SIP over Transport Layer Security (TLS) connection.
RFC 5954: Essential Correction for IPv6 ABNF and URI Comparison in RFC 3261	Corrects the Augmented Backus-Naur Form (ABNF) production rule associated with generating IPv6 literals in RFC 3261.

Table 1. Commonly Used SIP RFCs

1.2 SIP design

SIP is a text-based and transaction oriented (i.e. using request-response sequences) signalling protocol using a client/server model and relying on HTTP like messages that communicate between end-users and SIP servers. It is independent of lower layer protocols or media. SIP is suitable for applications that have a notion of session. SIP uses Uniform Resource Identifier (URI) to identify users. The URI associates the user and the carrying platform that uses an IP address. With this mechanism, it is convenient to support mobility for hosts, sessions, and users.

1.2.1 SIP methods

SIP uses Methods / Requests / Responses to establish sessions. There are six basic methods:

- INVITE – To initiate a session
- ACK – To confirm that the client has received a final response to an INVITE request
- BYE – To terminate a session
- CANCEL – To terminate any pending session but not terminate a session that has already been connected
- OPTIONS – To query for the capabilities support by other side (either a server or a client)
- REGISTER – To register contact information

There are other SIP-methods extensions:

- INFO – To allow for the carrying of session related control information that is generated during a session (RFC 2976). For example, carrying wireless signal strength information in support of mobility
- NOTIFY – To request notification from remote nodes indicating that certain events have occurred (RFC 3265)
- PRACK – To provide reliable provisional acknowledgement (RFC 3262)

- REFER – To ask the recipient to issue a SIP request (e.g. call transfer) for contacting a third party (RFC 3515)
- SUBSCRIBE – To request asynchronous notification of an event or set of events (RFC 3265)
- UPDATE – To update parameters of a session (RFC 3311)

1.2.2 SIP responses

The SIP uses specific messages to exchange information. These messages are classified into six groups:

- **Provisional (1xx)** – This is a type of informational response to indicate that the request is received and is continuing to be processed. For example:
  - 100 Trying (i.e. The request has been received by the next-hop server and an action is being taken on behalf of this request.)
  - 180 Ringing (i.e. The UA receiving the INVITE is trying to alert the user.)
  - 181 Call forwarded (i.e. To indicate that the call is being forward to a different destination)
  - 182 Queued (i.e. The called party is temporarily unavailable, the server queue the request instead of reject it.)
  - 183 Session in progress
- **Successful (2xx)** – Successful in terms of action, message received, and message understood. For example, 200 OK (i.e. The request has succeeded.)
- **Redirection (3xx)** – Extra actions are necessary in order to finish the request. For example:
  - 300 Multiple Choices (i.e. The request is resolved to several choices.)
  - 301 Moved Permanently (i.e. The user can no longer be found.)
  - 302 Moved Temporarily (i.e. The requesting client should try a new address.)
  - 380 Alternative Service (i.e. The call was not successful, but alternative services are possible.)
- **Request failure** (4xx) – It indicates a definite failure of a request from a particular server. For example,
  - 400 Bad Request (i.e. The request cannot be understood.)
  - 401 Unauthorized (i.e. The request requires user authentication.)
  - 403 Forbidden (i.e. The server understood the request, but refused to fulfill it.)
  - 404 Not Found (i.e. The server has definitive information that the user does not exist at the domain specified in the request.)
  - 486 Busy Here (i.e. The callee is currently not willing or able to take the call.)
- **Server failure (5xx)** – The server itself has erred and cannot process valid request. For example,
  - 500 Server Error
  - 501 Not Implemented (i.e. The server does not support the functionality required to fulfill the request.)
  - 503 Unavailable (i.e. The server is temporarily unable to process the request due to a temporary overloading or maintenance of the server.)
  - 504 Timeout (i.e. the server did not receive a timely response from an external server to process the request.)

- **Global failure (6xx)** – It indicates that a server has definitive information about a particular user's unsuccessful call and none of the requests can be fulfilled. For example,
    - 600 Busy Everywhere
    - 603 Decline
    - 604 Doesn't Exist (i.e. The server has authoritative information that the user indicated in the request does not exist anywhere.)
    - 606 Not Acceptable (i.e. the UA is contacted successfully but some aspects of the session such as requested media, bandwidth, etc. are not acceptable.)

These messages are designed to fulfill all signalling requirements. These messages and the process of these messages build the core of the SIP protocol (Rosenberg, J. et al., 2002).

1.2.3 SIP-based network entities

SIP defines a number of logical entities as described as the follows:

- *User Agent (UA)*
  A UA is a SIP-enabled end system that consists of two components: a User Agent Client (UAC) and a User Agent Server (UAS). A UAC initiates SIP requests or originates calls and a UAS listens to incoming calls and responses to the UAC's requests. A UA communicates with other UAs directly or indirectly via an intermediate server (e.g. a proxy server). A typical UA is a SIP phone or a voice mail server. Generally, UAs are the only elements where media and signalling converge.
- *Network Servers*
    - **Proxy server** – It decides next hop, forwards request, and relays call signalling. It performs routing function, i.e., determine to which hop, (UA/proxy/redirect) signalling should be relayed. It serves as a rendezvous point at which callees are globally reachable. It has a Forking function, which means that several destinations may be tried for requests sequentially or in parallel.
      A proxy server can be either stateless or stateful. A stateless proxy only forwards incoming requests without ensuing the request's reliability. A stateful proxy remembers the requests and related processes (*transaction*) so that it can reliably deliver a SIP request either sucessfully or return a response code. Only the stateful proxy can fulfill Forking function, which sends copies of the requrest to different destinations.
      A proxy cannot (usually) control media path because a proxy does not know all routing hops along an end-to-end media path. Unless route recording is used, subsequent SIP requests (including ACK with SDP) may take different paths.
    - **Redirect serve**r – It receives requests and return a response that indicates where the SIP requestor should send to in next step. That is, the redirect server does not forward incoming requests; instead, it sends the address of the next hop back to the caller, and then redirects the caller to other servers.
    - **Registrar** – It stores SIP URIs and associated contacts of SIP users. It accepts REGISTER requests from SIP users and maintains user's whereabouts at a location server.
    - **Location server** – It provides users' location details.

- **Application server** – It provides advanced services for users.

- *Gateways*

  A SIP gateway is an application that implements protocol translation, which is used to connect a SIP network to a network that uses different signalling protocols. A SIP gateway may only terminate signalling path, such as in the case of connecting to a H.323 enabled network. The SIP gateway translates SIP signalling messages to the H.323 format, while the media (using the Real-time Transport Protocol) can still run over the media path. A SIP gateway may also terminate both signalling and media paths, such as in the case of connecting to a Public Switched Telephony Network (PSTN) network. In this case, a SIP gateway converts signalling messages and a PSTN media gateway converts media data flows.

1.3 SIP security

The SIP security is based on 3GPP standards (23.228 IP Multimedia (IM) Subsystem - Stage 2, 33.203 Access Security for IP-Based Services, and 33.210 Network Domain Security) and IETF RFCs such as Security Mechanism Agreement for the Session Initiation Protocol (RFC 3329). SIP security should be able to fulfill the following goals (Arkko, J. et al. 2003):

1. The entities involved in the security agreement process need to find out exactly which security mechanisms to apply, preferably without excessive additional message exchanges.
2. The selection of security mechanisms itself needs to be secure.
3. The entities involved in the security agreement process need to indicate success or failure of the security agreement process.
4. The security agreement process should not introduce any additional state to be maintained by the involved entities.

1.3.1 SIP signalling security

The SIP signalling security uses both end-to-end signalling security and hop-by-hop signalling security mechanisms to satisfy the requirements. The end-to-end signalling security uses SIP authentication and SIP message body encryption. However, it cannot cover entire signalling messages since some fields need to be visible for routing purpose. Consequently, intermediate proxies can compomise security. The Hop-by-hop signalling security relies on transport-layer or network-layer security mechanisms, such as Transport Layer Security (TLS) and Internet Protocol Security Architecture (IPSec), to protect signalling messages. It may allow covering entire signalling message within a hop. A more appealing solution is to combine both mechanisms. Table 2 lists both security mechanisms and their related RFCs.

1.3.2 SIP signalling security threats

Network security is usually categorized into: authentication, confidentiality, integrity, and availability (Knuutinen, 2003), (Rantapuska, 2003), (Sawda & Urien, 2006). The text-based SIP messages are vulnerable to security attacks such as spoofing, hijacking, and message tampering (Geneiatakis, D. et al. 2006). Table 3 summarizes some threats, their impacts, and possible solutions.

SIP Security Mechanisms		Description	Standards
End-to-end security	Digest Authentication	Authentication of signalling message using HTTP digest	RFC 2617
	S/MIME	Authentication and encryption messages	RFC 2633
Hop-to-hop security	The Transport Layer Security (TLS) Protocol Version 1.1	Prevent eavesdropping, tampering, or message forgery at the transport layer	RFC 4346
	Internet Protocol Security (IPSec)	Authentication and encryption at the network layer	RFC 2412 RFC 4301 RFC 4303 RFC 4308 RFC 4835

Table 2. SIP Signalling Security

Threats	Security Aspects	Examples of Impacts	Possible Solutions
Denial-of-service (DoS) attacks, e.g. using • CANCEL • BYE • 4xx, 5xx, 6xx	Availability	Interrupt sessions, force servers unusable	Traffic filtering, access control, DoS protection, etc.
Hijacking, e.g. • Registration • Using 3xx redirect responses • Mid-session re-INVITE	Availability	Register malicious device as the contact address of the victim and deregister all connected contacts	Authenticate the originators of requests
Message tampering	Integrity	Change SDP message body to direct RTP stream to an eavesdrop device	Encryption
Replay messages to cause DoS	Availability	Overload a server	Sequencing message
Snooping	Confidentiality	Gain information on users' identities, services, media, network topology, etc. With the information, other attack can be further triggered.	Encryption, Privacy protection
Spoofing REGISTER	Confidentiality	Call redirection	Authenticate the originators of requests
Spoofing INVITE	Confidentiality	Bypass call filtering	Authenticate the originators of requests
Spoofing ICMP "port unreachable"	Availability	Interrupt sessions	Traffic filtering, access control

Table 3. Some Identified Threats, Impacts, and Solutions

2. SIP mobility support and signalling reliabilities

The mobility involves user devices and network equipment movement, sometimes at a high speed, which causes rapid changes in network topology and attachment points. A mobile node should be accessible by other nodes even when a network attachment point is changed. In addition, the ongoing communication should be reliable and the performance of the communication should be kept at a constant level before, during, and after the node movement. All these requirements present significant challenges to the usability of a signalling protocol such as the SIP.

2.1 SIP mobility

There are four types of mobility supported by the SIP (Schulzrinne, H. & Wedlund, E. 2000).

- Terminal Mobility – It allows Mobile Hosts (MHs) move between subnets without interrupting communications.
- Session Mobility – It allows a user to maintian a media session even while changing terminals.
- Personal Mobility – It allows to address a single user located at different terminals by the same logical address. A user can use more multiple devices to send and receive calls.
- Service Mobility – It allows a user to maintain access to their services while the user is moving or changing devices and network service providers.

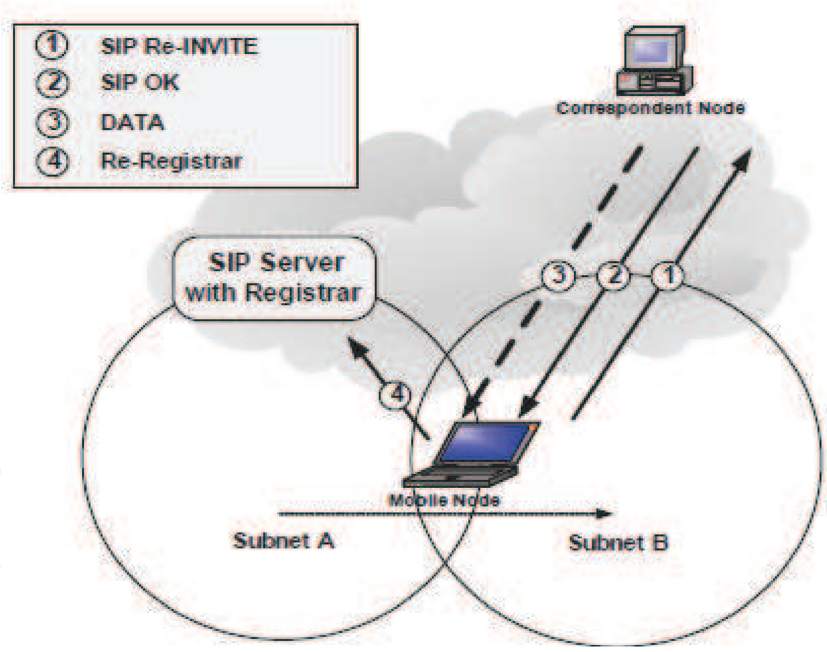


Fig. 1. An Notional Example of SIP Terminal Mobility Support

This chapter focuses on the terminal mobility and the associated unreliable signalling problem in its possible movement scenarios.

2.2 SIP mobility support scenario

The SIP mobility support usually has two challenging cases: 1) one of the two mobile hosts (MHs) moves during a session and 2) both hosts simultaneous move during a session (Wong and Woon, 2007). Details are discussed in next section.

2.2.1 Move during A Session

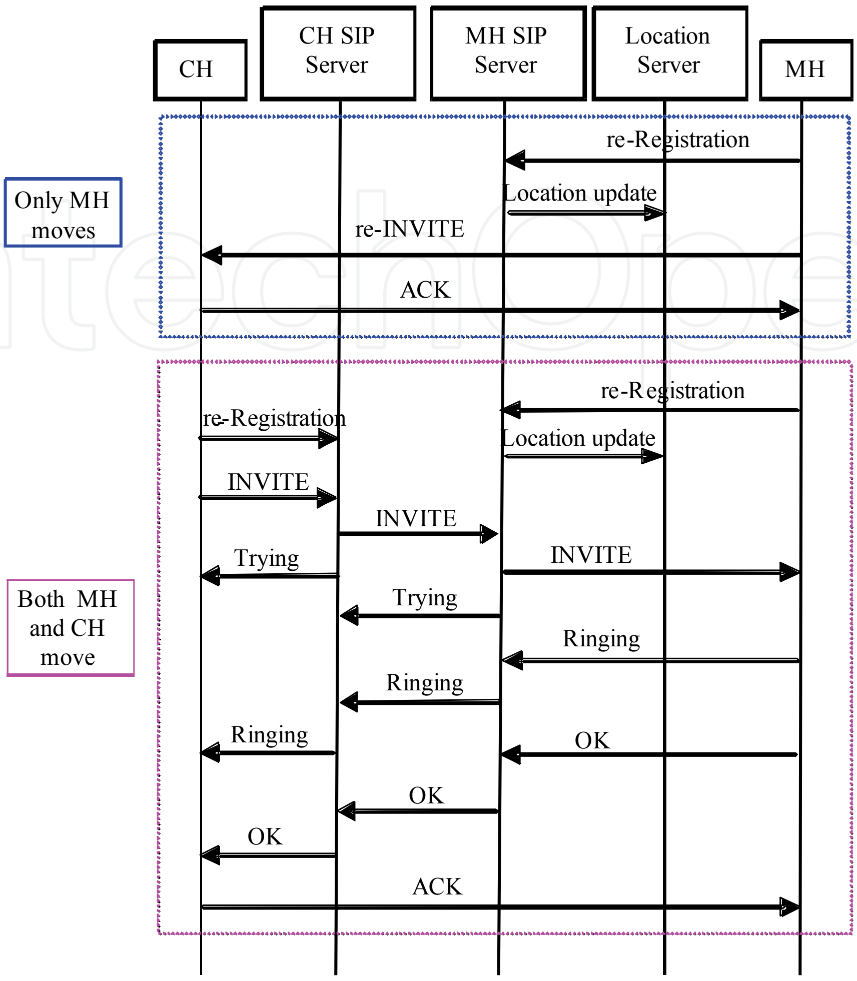
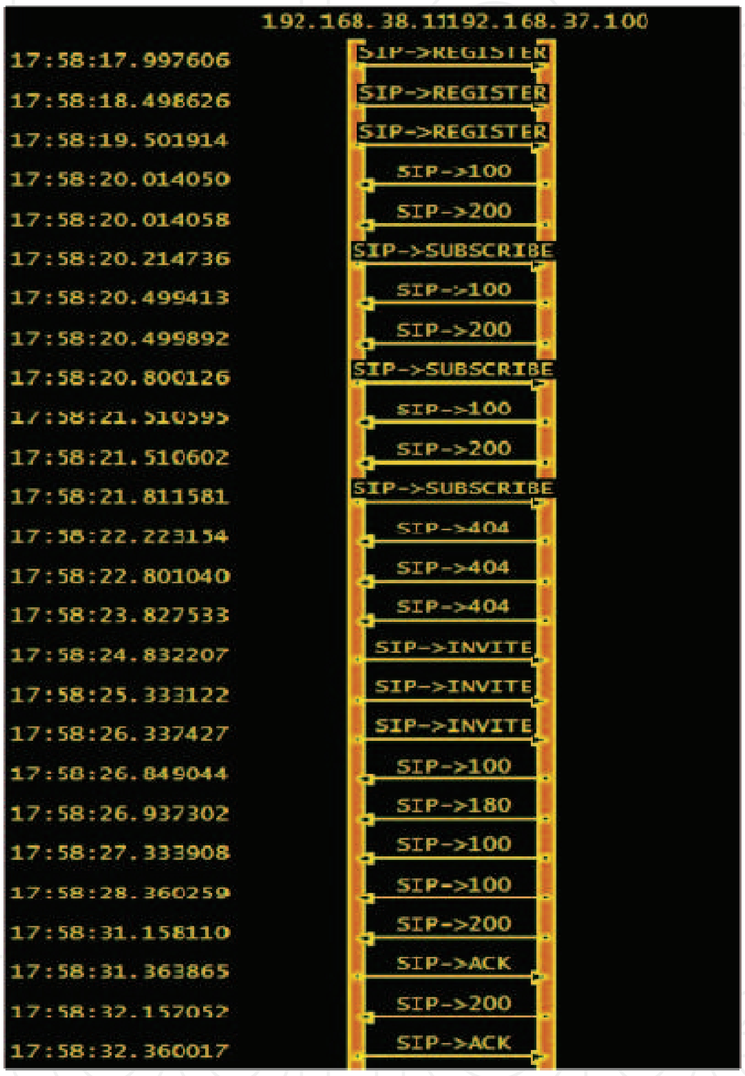


Fig. 2. SIP Message Flows for Move during A Call

This case happens when the MH (the caller) is moving during a session. It has been suggested (Wedlund and Schulzrinne, 1999) to use a "re-invited" message to inform the Correspondent Host (callee) when the caller is moving during a session. This is done via a registration process. The caller's home SIP register updates the MH's location server. This procedure keeps tracking the moving caller and provides possible lost-session reconnection when the SIP "re-INVITE" message does not arrive to the callee. The MH needs to update its current address to its home SIP server registrar and location server to let them know where it is, which provides the updated information for future communications. The Correspondent Host (CH) then acknowledges the message and the session re-starts (please refer to the case of "only MH moves (in blue)" in Figure 2).

2.2.2 Simultaneous move

The simultaneous move (Wong and Woon, 2007) is a special situation of the case "move during a session" (or "move during a call") where both MH and CH move at the same time. Neither of them can receive the "re-INVITE" message from the other party since both of them are changing their locations. In this case, after each host arrives to its new location, it registers its new location (IP address) to its home SIP servers (to both registrar and location server). After registration, either one of them or both of them will send a "re-INVITE" message to each of the host-home SIP servers. The home SIP server will contact the other party's home SIP server to get an updated location address. After that, another "INVITE" message will be sent out either from the MH or from the CH to the other party to start the communication. Figure 2 shows the message exchange flow for the case of "both MH and CH move". It is noticeable that there are many message exchanges for supporting mobile hosts maintaining an ongoing session.



```
                    192.168.38.11192.168.37.100
17:58:17.997606     SIP->REGISTER
17:58:18.498626     SIP->REGISTER
17:58:19.501914     SIP->REGISTER
17:58:20.014050       SIP->100
17:58:20.014058       SIP->200
17:58:20.214736     SIP->SUBSCRIBE
17:58:20.499413       SIP->100
17:58:20.499892       SIP->200
17:58:20.800126     SIP->SUBSCRIBE
17:58:21.510595       SIP->100
17:58:21.510602       SIP->200
17:58:21.811581     SIP->SUBSCRIBE
17:58:22.223154       SIP->404
17:58:22.801040       SIP->404
17:58:23.827533       SIP->404
17:58:24.832207      SIP->INVITE
17:58:25.333122      SIP->INVITE
17:58:26.337427      SIP->INVITE
17:58:26.849044       SIP->100
17:58:26.937302       SIP->180
17:58:27.333908       SIP->100
17:58:28.360259       SIP->100
17:58:31.158110       SIP->200
17:58:31.363865       SIP->ACK
17:58:32.157052       SIP->200
17:58:32.360017       SIP->ACK
```

Fig. 3. Delay Causes SIP Message Repetitions

2.2.3 Fragility of SIP signalling

The scenario depicted in Figure 2 shows that without correct and on-time registrations for a mobile host, a mobile network is at risk of losing communications. In a mobile environment, it may not be practical for a mobile host to update its location to a remote SIP server frequently. Home SIP servers (including a registrar and a location server) are usually located far away from an edge network. The connections between an edge network and its home network can be fragile due to many factors.

In addition, when both mobile hosts are constantly moving, the registration requests from each host may be triggered more frequently. The connectivity between an edge network and a SIP server may span a large geographic distance by using satellite links, which could cause a long delay for message exchanges (e.g. registration and call setup). Moreover, the network link capacity can be limited and a link could be unreliable because of unintentional interferences, hostile actions, terrain, foliage, weather, or other factors. Failure or delay of SIP registrations will significantly impact SIP mobility handling.

From our previous SIP performance study (Wang, S. & Zheng, H. 2009), we have observed that network delays, delay variations (jitter), and packet loss affect signalling quality and voice quality (measured by Mean Opinion Score) considerably. Figure 4 and Figure 5 show some examples. One disturbing observation was that when network delay increased, the number of SIP messages increased proportionally. This was caused by re-sending messages due to messages time out as shown in Figure 3. This repetition wastes radio resource and may result in a self-generated Denial of Service (DoS). It is evident that we need to modify the message forwarding mechanism in order to reduce redundant messages, to improve signalling reliability, and to enhance mobility support.

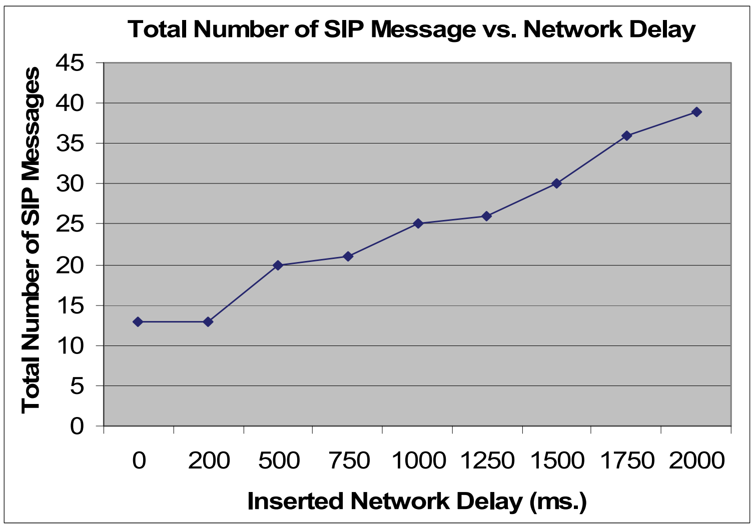


Fig. 4. Network Delay Impact on SIP

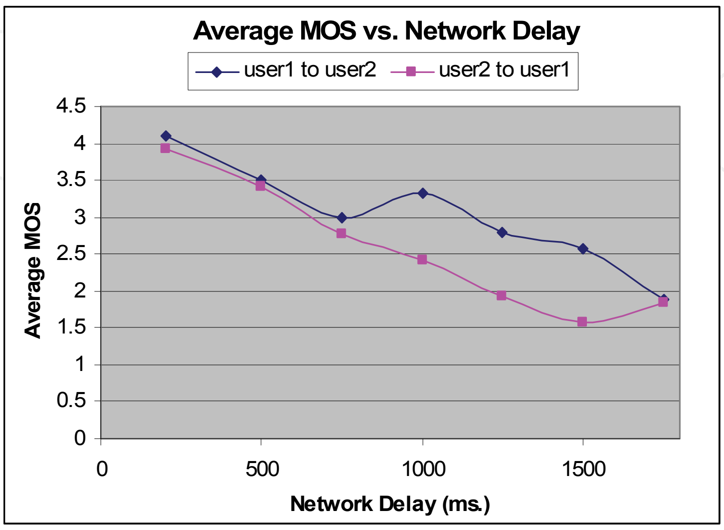


Fig. 5. Network Delay Impact on Voice Quality

Since the main function of the SIP is to provide signalling between two communication hosts, the challenges include how to let each host know where the other host is, how to connect to each other, and how to keep a session alive with or temporarily without the help from its home network. To solve this problem, a reliable SIP message forwarding mechanism [Zheng and Wang, 2007] has been proposed. The next section will present the details.

3. Reliable Chain-Based SIP (CBS)

In order to overcome the problem of unreliable registration in the SIP mobility support, a chain-based SIP signalling (CBS) mechanism has been proposed (Zheng, H. & Wang, S. 2007), which increased the signalling reliability by adopting Mobility Agent(s) to construct a signalling chain that facilitated a reliable signalling.

3.1 Chain-based signalling

Some existing studies have shown that it is feasible to have hierarchical mobility support by using SIP. Vali, D. et al. (2003) proposed the use of an intermediate SIP server called the SIP Mobility Agent (MA) to handle micro mobility. A MA is responsible for handling SIP message forwarding and supporting the intra-domain SIP mobility. The inter-domain SIP mobile handling is still based on the standard SIP mobility by sending "re-INVITE" messages to the home SIP server.

(Zheng, H. & Wang, S. 2007) proposed an idea of using a chain of mobility agents that traverse multiple domains. It proposed that SIP mobile agents could exist in each domain along a routing path that was from a mobile host to its Home SIP Server. The chain-based signalling is depicted in Figure 6, where the CBS employs a new network component called Mobile Agent (MA), which provides basic functions of a SIP proxy server.

In this proposal, a MA locally holds the information of mobile hosts resided in its reachable subnets and domains. The MA periodically updates the users' information to synchronize

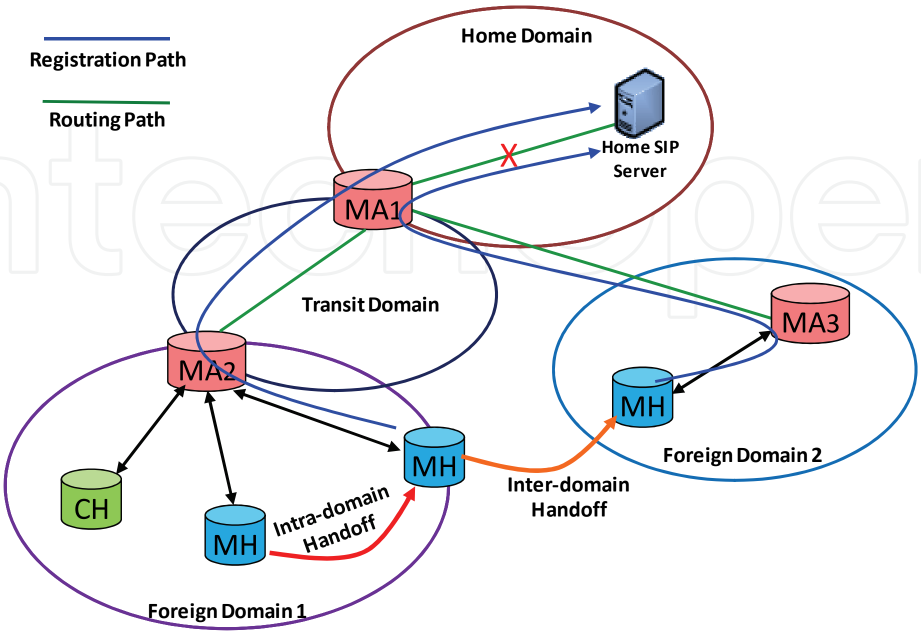


Fig. 6. Chain-based Mobile SIP Signalling

with the home network. The MAs can reside within routers along the routing path from the MH to the SIP home server. Usually, a MA is collocated with a domain border edge router. Since MAs are located within a standard routing path, it is not necessary for a Mobile Host (MH) to find where MAs are. The SIP messages naturally interact with MAs when these messages are traversed on the routing path to the Home SIP server.

Using the SIP registration as an example, the CBS signalling procedure can be explained as following. Each mobile host is required to register to its home SIP server before it can access to any application services. When a mobile host registers itself, it sends a registration message to its Mobility Agent (MA) in the current domain. After it registers the SIP mobile locally, the MA forwards the mobile registration request to the next domain that is in the path towards the home SIP server. This process continues until the request reaches the home SIP server. This type of registration is called "chained registration". The registration message forwarding within a registration chain is not the duty of the mobile host. Instead, it becomes a duty of the MAs. Therefore, as long as a mobile host registers itself to a local domain MA, the registration is considered as being finished. The rest of the registration processes will be completed at each MA along the routing path. It is not necessary to finish the whole registration process at once; instead, it can be done in a pair-wised fashion. As long as there is connectivity available between a pair of MAs, the registration process can continue forwarding the request. Therefore, this method significantly improves the survivability of a registration request.

In addition, each involved MA updates the hosts' registration requests referring to a time stamp. If a MA receives multiple registration requests, it saves the one with the latest time stamp. It also checks the SIP request ID. Multiple registration requests can be either from the mobile host or from lower chain rings of the MA registration chain. These two types of request are treated equally at each MA. In a registration chain, the home SIP server is the last ring of the chain. It always gets an updated host registration with the host location information when the connectivity between registration chain MAs is available. The link availability between a MA pair does not need to exist simultaneously. Instead, as long as a network link between two MAs exists, an updated registration is forwarded. In this fashion, the mobile host request can propagate to the home SIP server. Using this method, the intermittent link availability between a mobile host and its home SIP server is less of a hindrance. Figure 6 illustrates an example of forwarding SIP registration messages using the CBS. The details are given in the next section.

In addition to forwarding user SIP messages, MAs can potentially be functional as light-weighted SIP servers. SIP messages, such as SIP registrations, are kept within a MA in case the MA is selected as a SIP server. This mechanism eliminates extra user SIP registration request messages when the home SIP server is unavailable and a substitution of MA is elected.

3.2 Message-forwarding modes

The CBS SIP message forwarding has two modes. One is called ***forced forwarding***. In this mode, whenever a MA receives a registration request, it updates its own database, then immediately forwards the request to an upper ring if a communication link is available.

The other forwarding mode is called ***periodic forwarding***. An MA re-sends unsuccessfully forwarded requests to an upper ring based on a preset time interval. The forced forwarding normally happens the first time the MA receives a fresh registration request. If the forced forwarding fails, then the periodic forwarding will continue re-sending the request to the upper ring up to the maximum numbers of retrials. However, if there is a newer registration request arrives from the same mobile host, the MA resets the forwarding timer and abandons the older request. This happens when the current request is timed out and the host sends a new request.

If there is a broken link within the request-forwarding path, the MA at a lower part of the chain will serve as a SIP server to fulfil the SIP signalling functions locally relevant to the caller. The purpose is avoiding host request time out, thereby, to avoid redundant request messages. For example, in Figure 6, the link between the MA1 and the home SIP server is broken; then, the MA1 is served as an acting SIP server. Using this CBS request-forwarding mechanism, every server within the chain has the possibility to be an acting SIP server and may perform SIP signalling functions.

The choice of a server as an acting SIP server depends on the MA's logical location in the registration chain. In Figure 6, it is assumed that the link between the home SIP server (on the top of the figure) and MA1 is a satellite link. When the satellite link is broken, since MA1 is located at the top of registration chain, therefore, MA1 is designated as an acting SIP server. In this way, the SIP signalling process is not blocked by a broken link.

3.3 Intra-domain and Inter-domain soft handoff

Another advantage of using the chain structure is that it provides potential for fast handoffs. A handoff is a process of transferring an ongoing session from one network attachment to another. A seamless handoff (unnoticed by a user) will significantly improve communication quality during host movements. During a handoff, the transition period needs to be short. The quicker a handoff can be completed, the higher velocity a mobile user can achieve (Banerjee, N. et al. 2005).

The server that is responsible for performing the SIP procedures is at the lowest level (towards the CH) of the signalling chain. It knows both CH and MH addresses. In our case, it is MA2 in Figure 6.

In an intra-domain mobility situation as shown in Figure 6, the MH gets a new IP address before relinquishing its old IP address. It obtains the new IP address from an intra-domain visiting sub-network (see the red line in Figure 6). The MH registers itself at MA2 and sends a "re-INVITE" to MA2. The MA2 sends the "re-INVITE" message to the CH. The CH sends OK and it is ACKed by the MH. Then a new session is established and the communication continues.

If only the MH moves, it sends the "re-INVITE" message directly to the CH since the MH knows the CH location via the old connection. However, the MH still needs to register its new location to the MA2. For the sake of reducing handoff time, the MH can send two "re-INVITE" requests to both old CH address and MA2 (Wong, K. D. & Woon, W. L. 2007). If CH does not move, it can receive both messages. The CH can reject the message from the MA2 to avoid duplication. Since the handover process in this proposal does not need to send all the SIP messages to the home SIP server, the overall performance is improved.

Using signalling-server chain for inter-domain mobility handling is different from the standard SIP mobility support. The proposal uses a SIP proxy server (MA1 in our case) that is closer (physically) to the mobile host than the home SIP server is, which avoids using the original home SIP server that is far away and the satellite link may be broken. The inter-domain soft handoff procedure is similar to the intra-domain soft handoff for setting up a session. The improvement is to have a much shorter signal path than the one used by the standard SIP, which reduces the handoff time and increases the signalling reliability.

3.4 CBS performance assessment

Using a signalling chain can significantly improve the SIP request success probability and reduce message delay. These claims are proved in the following sections.

3.4.1 Message forwarding success probability analysis

We will analyze SIP message forwarding success probability in two cases. In case 1, a SIP client sends a SIP message only once; in case 2, a client can re-transmit the message *N* times. The results from both cases show that the CBS increases the success probability of SIP message transmission significantly, especially when the link reliability decreases. The definitions of parameters are as follows:

$P_{CBS:}$ The SIP registration success probability using chain-based mechanism
$P_{SIP:}$ The SIP registration success probability using standard SIP mechanism
M: Number of domains
N: Maximum number of times SIP registration request forwarding by each MA
$p_{i:}$ Packet transmission success probability in domain *i*.

3.4.1.1 Message forwarding success probability analysis – single try

In this simple situation, by using the standard SIP without re-transmission, the probability that a message successfully traverses M domains and reaches its destination can be expressed as:

$$P_{sip} = \prod_{i=1}^{M} p_i \tag{1}$$

While using the CBS, because of its "forced forwarding" and "periodical forwarding" mechanisms, the success probability is:

$$P_{CBS} = \prod_{i=1}^{M} (1-(1-p_i)^N) \tag{2}$$

Where a message success transmission probability is *1- (1-*p_i*)*^{N} in Chain *i* for a maximum of N retransmissions.

$$Let\ \ q_i = 1 - p_i;$$

$$Since\ \ 0 < q_i \le 1 \text{, then } \frac{1-(1-p_i)^N}{p_i} = 1 + q_i + q_i^2 + \cdots + q_i^{N-1} \ \ \ge\ \ 1 \text{, therefore,}$$

$$\frac{P_{CBS}}{P_S} = \prod_{i=1}^{M} \frac{1-(1-p_i)^N}{p_i} \ge 1,$$

Thus, $P_{CBS} \ge P_S$.

3.4.1.2 Message forwarding success probability analysis – multiple try

In this case, the probability of successfully using SIP is changed to:

$$P_{SIP} = 1 - \left(1 - \prod_{i=1}^{M} p_i\right)^N \tag{3}$$

Now, comparing Eq.2 and Eq.3, we can prove that P_{CBS} is still larger than P_{SIP}. The proof is as the followings.

Let a be a ratio between P_{CBS} and P_{SIP}, that is:

$$\alpha = \frac{\prod_{i=1}^{M}(1-(1-p_i)^N)}{1-\left(1-\prod_{i=1}^{M}p_i\right)^N} \tag{4}$$

Let's consider a special situation, in which each "chain" has the same message transmission success probability. Therefore, each $p_i = p$;

$$\begin{aligned}
\hat{\alpha}(p) &= \frac{\prod_{i=1}^{M}(1-(1-p)^N)}{1-\left(1-\prod_{i=1}^{M}p\right)^N} = \frac{\prod_{i=1}^{M}(1-(1-p)^N)}{1-(1-p^M)^N} \\
&= \frac{(1-(1-p)^N)^M}{1-(1-p^M)^N} = \frac{\left(1-\left(1-\binom{N}{1}p+\binom{N}{2}p^2-\ldots+(-1)^N\binom{N}{N}p^N\right)\right)^M}{\binom{N}{1}p^M-\binom{N}{2}p^{2M}+\ldots(-1)^{N-1}\binom{N}{N}P^{NM}} \\
&= \frac{\left(\binom{N}{1}p-\binom{N}{2}p^2+\ldots+(-1)^{N+1}\binom{N}{N}p^N\right)^M}{\binom{N}{1}p^M-\binom{N}{2}p^{2M}+\ldots+(-1)^{N+1}\binom{N}{N}P^{NM}} \\
&= \frac{\left[\binom{N}{1}p\right]^M\left(1-\frac{\binom{N}{2}}{\binom{N}{1}}p^1+\ldots+(-1)^{N+1}\frac{\binom{N}{N}}{\binom{N}{1}}p^{N-1}\right)^M}{\left[\binom{N}{1}p^M\right]\left(1-\frac{\binom{N}{2}}{\binom{N}{1}}p^M+\ldots+(-1)^{N+1}\frac{\binom{N}{N}}{\binom{N}{1}}P^{(N-1)M}\right)} \\
&= \frac{\left[\binom{N}{1}\right]^{M-1}\left(1-\frac{\binom{N}{2}}{\binom{N}{1}}p^1+\ldots+(-1)^{N+1}\frac{\binom{N}{N}}{\binom{N}{1}}p^{N-1}\right)^M}{\left(1-\frac{\binom{N}{2}}{\binom{N}{1}}p^M+\ldots+(-1)^{N+1}\frac{\binom{N}{N}}{\binom{N}{1}}P^{(N-1)M}\right)}
\end{aligned} \tag{5}$$

When p is small, we can have

$$\alpha(0) = \lim_{p \to 0^+} \frac{\left[\binom{N}{1}\right]^{M-1} \left(1 - \frac{\binom{N}{2}}{\binom{N}{1}} p^1 + \ldots + (-1)^{N+1} \frac{\binom{N}{N}}{\binom{N}{1}} p^{N-1}\right)^M}{\left(1 - \frac{\binom{N}{2}}{\binom{N}{1}} p^M + \ldots + (-1)^{N+1} \frac{\binom{N}{N}}{\binom{N}{1}} P^{(N-1)M}\right)} \tag{6}$$

$$= \left[\binom{N}{1}\right]^{M-1} = N^{M-1} \quad > \ 1$$

Similarly, when p is large or even close to 1, we have

$$\alpha(1) = \lim_{p \to 1^-} \frac{\left[\binom{N}{1}\right]^{M-1} \left(1 - \frac{\binom{N}{2}}{\binom{N}{1}} p^1 + \ldots + (-1)^{N+1} \frac{\binom{N}{N}}{\binom{N}{1}} p^{N-1}\right)^M}{\left(1 - \frac{\binom{N}{2}}{\binom{N}{1}} p^M + \ldots + (-1)^{N+1} \frac{\binom{N}{N}}{\binom{N}{1}} P^{(N-1)M}\right)}$$

$$= \frac{\left[\binom{N}{1}\right]^{M-1} \left(1 - \frac{\binom{N}{2}}{\binom{N}{1}} + \ldots + (-1)^{N+1} \frac{\binom{N}{N}}{\binom{N}{1}}\right)^M}{\left(1 - \frac{\binom{N}{2}}{\binom{N}{1}} + \ldots + (-1)^{N+1} \frac{\binom{N}{N}}{\binom{N}{1}}\right)} \tag{7}$$

$$= \frac{\left(\binom{N}{1} - \binom{N}{2} + \ldots + (-1)^{N+1} \binom{N}{N}\right)^M}{\left(\binom{N}{1} - \binom{N}{2} + \ldots + (-1)^{N+1} \binom{N}{N}\right)}$$

$$= \left(\binom{N}{1} - \binom{N}{2} + \ldots + (-1)^{N+1} \binom{N}{N}\right)^{M-1} = (1 - (1-1)^N)^{M-1} = 1.$$

In summary, when the message transmission success probability is low, which is represented by a small value of p, $p \approx 0$, the chain-based message delivery mechanism has a much higher probability (NM-1 times) to be successful as indicated by Eq. 6. When a link is reliable, this means that the p ≈ 1, both chain-based and the original SIP mechanisms have a similar performance.

For a 3-chain network infrastructure, we can have the reliability depicted in Figure 7. By using UDP as the transport protocol, SIP only sends the "invite" message 7 times[1], so we set N=7. We can see that the chain-based message transmission mechanism is much more reliable than the original SIP messaging does.

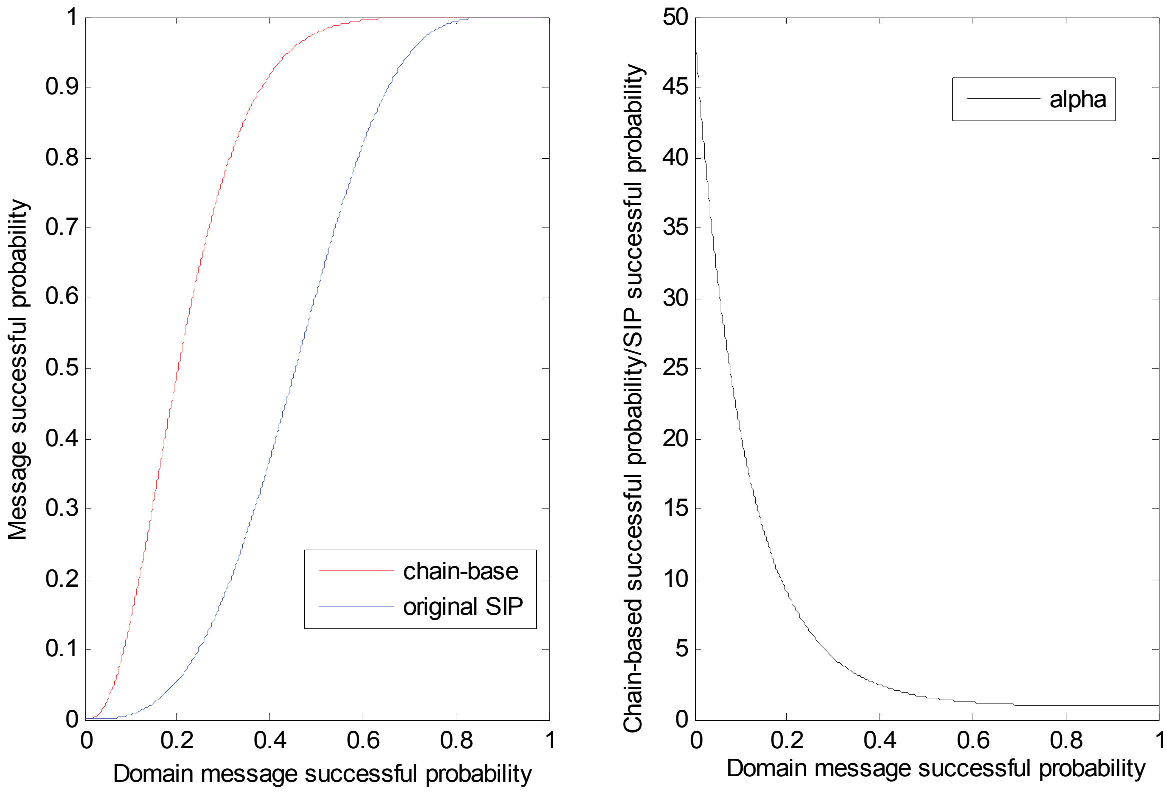


Fig. 7. Reliability Comparison of CBS and standard SIP

3.4.2 Delay analysis

Let p_i be the successful transmission probability at the chain domain i. Also, let d_i be the transmission delay for a message to be transmitted across different domains, which includes propagation delay and processing delay. It is assumed that the transmission delay is the same for both directions of a path. If a message is only retransmitted N times, the expected delay for a message to be transmitted over one "chain" can be considered as the following.

[1] A SIP UAC stops retransmitting a request after 7 tries without receiving a response. The first retransmitting is sent after 500 ms, the rest of are sent at a 1-second interval.

$$
\begin{aligned}
T_i &= d_i p_i + 2d_i p_i(1-p_i) + 3d_i p_i(1-p_i)^2 + \cdots \\
&\qquad + (N-1)d_i p_i(1-p_i)^{N-1} + D_{l\arg e}(1-p_i)^N \\
&= d_i(p_i + 2p_i(1-p_i) + 3p_i(1-p_i)^2 + \cdots \\
&\qquad + (N-1)p_i(1-p_i)^{N-1}) + D_{l\arg e}(1-p_i)^N \\
&= d_i p_i \sum_{k=1}^{N} k(1-p_i)^{k-1} + D_{l\arg e}(1-p_i)^N
\end{aligned}
$$

$$
\begin{aligned}
&Let\ \ q = 1 - p_i; \\
&T_i = d_i(1-q)\sum_{k=1}^{N} k\cdot q^{k-1} + D_{l\arg e}q^N \\
&= d_i(1-q)\frac{\partial}{\partial q}\sum_{k=1}^{N} q^k + D_{l\arg e}q^N = d_i(1-q)\frac{\partial}{\partial q}\left(\frac{1-q^N}{1-q}\right) + D_{l\arg e}q^N \\
&= d_i(1-q)\frac{(1-q)(-Nq^{N-1})-(1-q^N)(-1)}{(1-q)^2} + D_{l\arg e}q^N \\
&= d_i\frac{(1-q^N)-N(1-q)(q^{N-1})}{1-q} + D_{l\arg e}q^N \\
&= d_i\left(\frac{1-(1-p_i)^N}{p_i} - N(1-p_i)^{N-1}\right) + D_{l\arg e}(1-p_i)^N
\end{aligned}
\tag{8}
$$

Eq. 8 assumes that the message can be delivered within N times of re-transmissions. The delay is the expected value of the re-transmissions. However, if the message cannot be successfully sent within N re-transmissions, the delay will be infinity since the chain-based mechanism stops sending it to save network resources. There is a small probability for such a case. Each message has a probability equal to $(1-p_i)^N$ that it will not be sent. The delay for the message is infinity. We use a large number D_{large} to represent the large delay.

The total expected delay for using the chain-based message transmission mechanism can be expressed as a summarization of delays from each chain, assuming there are a total of M chains.

$$
T_{CBS} = \sum_{i=1}^{M} T_i = \sum_{i=1}^{M}\left(d_i\left(\frac{1-(1-p_i)^N}{p_i} - N(1-p_i)^{N-1}\right)\right) + D_{l\arg e}(1-p_i)^N \tag{9}
$$

As a comparison, the expected delay based on the traditional SIP message transmission can be expressed as:

$$
T_{SIP} = \left(\sum_{i=1}^{M} d_i\right)\cdot\left(\frac{1-\left(1-\prod_{i=1}^{M} p_i\right)^N}{\prod_{i=1}^{M} p_i} - N\left(1-\prod_{i=1}^{M} p_i\right)^{N-1}\right) + D_{l\arg e}\left(1-\prod_{i=1}^{M} p_i\right)^N \tag{10}
$$

We need to compare Eq. 9 and Eq. 10 to determine which one has a longer delay. To reduce the calculation complexity, it is assumed that the transmission success probability p_i is the same in all chains. Therefore, Eq. 9 and Eq. 10 become

$$T_{CBS} = \sum_{i=1}^{M} T_i = \left(\sum_{i=1}^{M} d_i\right) \cdot \left(\frac{1-(1-p)^N}{p} - N(1-p)^{N-1}\right) + D_{l\arg e}(1-p)^N \tag{11}$$

$$T_{SIP} = \left(\sum_{i=1}^{M} d_i\right) \cdot \left(\frac{1-(1-p^M)^N}{p^M} - N(1-p^M)^{N-1}\right) + D_{l\arg e}(1-p^M)^N \tag{12}$$

The last items in Eq. 11 and Eq. 12 represent the probabilities of messages that are not successfully transmitted. The probability $(1-p^M)^N$ in Eq. 12 is larger than $(1-p)^N$ from Eq. 11. This means that using the chain-based mechanism yields a smaller probability of non-successful transmission than what the traditional SIP mechanism does. This echoes the conclusion from the reliability analysis.

For delay analysis, we focus on the time used for the messages that have been successfully transmitted. In that term, we only compare the first items in Eq. 9 and Eq. 10. Again, it is assumed that each "chain" domain has the same success transmission probability. Hence, it has

$$T_{CBS} = \left(\sum_{i=1}^{M} d_i\right) \cdot \left(\frac{1}{p}\right), \qquad \text{and} \tag{13}$$

$$T_{SIP} = \left(\sum_{i=1}^{M} d_i\right) \cdot \left(\frac{1}{p^M}\right) \tag{14}$$

Eq. 11 converges to Eq. 13 when p is relative large. Similarly, Eq. 12 converges to Eq. 14. Comparing Eq. 13 and Eq. 14, we conclude that Eq. 13 yields a smaller value than Eq. 14; hence, T_{CBS} is smaller than T_{SIP}. The simulation result is shown in Figure 8. The simulation is based on M=3, N=20 and D_{large} = 4N.

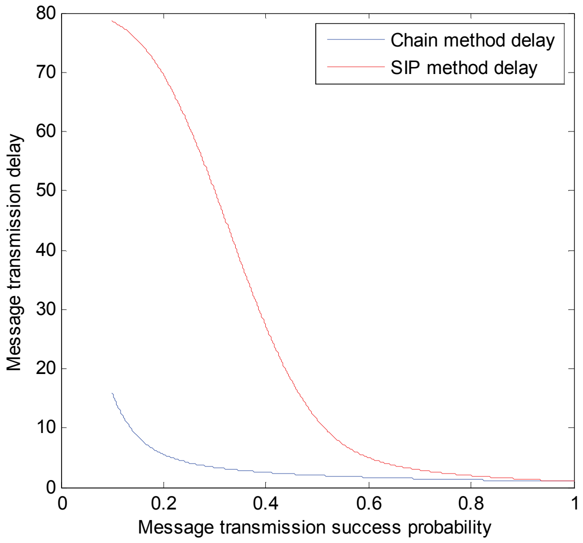


Fig. 8. SIP Message Forwarding Delay Comparisons

5. Conclusion

In this chapter, the problem of unreliable signalling caused by the deficiency of the standard SIP in an ad hoc mobile network environment was investigated. To mitigate the problem, several innovative ideas from protocol and network architecture perspectives have been introduced, which are important for furthering the SIP development and performance improvement.

6. References

Handley, M. & Jacobson, V. (1998). IETF RFC 2327, "SDP: Session Description Protocol"

Kent, S. & Atkinson, R. (1998). IETF RFC 2401, "Security Architecture for the Internet Protocol"

Orman, H. (1998). IETF RFC 2412, "The OAKLEY Key Determination Protocol"

Franks, J. et al., (1999). IETF RFC 2617, "HTTP Authentication: Basic and Digest Access Authentication"

Ramsdell, B. (1999). IETF RFC 2633, "S/MIME Version 3 Message Specification"

Schulzrinne, H. & Wedlund, E. (2000) Application-Layer Mobility Using SIP, *ACM SIGMOBILE Mobile Computing and Comminications Review, Vol. 4, Issue 3, pp47-57, July 2000, ISSN: 1559-1662*

Rosenberg, J. et al., (2002). IETF RFC 3261, "SIP: Session Initiation Protocol"

Cisco. (2002) Security in SIP-Based Networks *http://www.cisco.com/warp/public/cc/techno/tyvdve/sip/prodlit/sipsc_wp.pdf*

Arkko, J. et al. (2003) IETF RFC 3329, "Security Mechanism Agreement for the Session Initiation Protocol (SIP)"

Knuutinen, S. (2003). Session Initiation Protocol Security Consideration, *T-110.551 Seminar on Internetworking*

Rantapuska, O. (2003). SIP Call Security in an Open IP Network, *T-110.551 Seminar on Internetworking*

Vali, D. et al. (2003). An Efficient Micro-Mobility Solution for SIP Networks *Proceedings of IEEE 2003 Global Communications Conference (GLOBECOM 2003)*

Wong, K. D. et al. (2003). Managing Simultaneous Mobility of IP Hosts *Proceedings of IEEE Military communications Conference 2003 (MILCOM 2003)*

Banerjee, N. et al. (2005) SIP-based Mobility Architecture for Next Generation Wireless Networks *Proceedings of IEEE 3rd International Conference on Pervasive computing and communications, 2005 (PerCom 2005)*

Kent, S. (2005). IETF RFC 4303, "IP Encapsulating Security Payload (ESP)"

Geneiatakis, D. et al. (2006). SIP Security Mechanisms: A state-of-the-art Review *Proceedings of 2nd IEEE International conference on Information and Communication Technologies: from Theory to Applications (ICTTA'06)*

Avaya, (2006). Enterprising with SIP — A Technology Overview *https://www.avaya.com/usa/resource/assets/whitepapers/lb2343.pdf*

Dierks, T. & Rescorla E. (2006). IETF RFC 4346, "The Transport Layer Security (TLS) Protocol Version 1.1"

Sawda, S. & Urien P. (2006). SIP Security Attacks and solutions: a state-of-the-art review *Proceedings of 2nd IEEE International Conference Information & Communication Technologies from Theory: to Applications,* ICCTA'06.

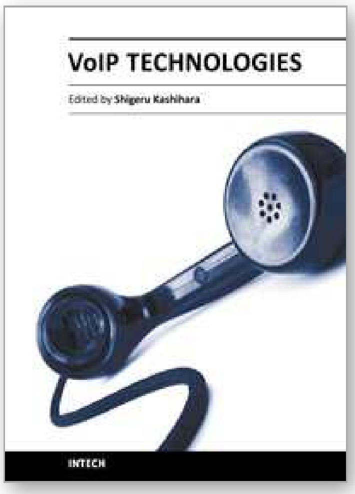
Manral, V. (2007). IETF RFC 4835, "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)"

Wong, K. D. & Woon, W. L. (2007). Analysis of Simultaneous Mobility under Asymmetric Mobility Conditions, *Proceedings of IEEE MILCOM 2007*.

Zheng, H. & Wang, S. (2007). Mobility Management in Disadvantaged Tactical Environments, *Proceedings of IEEE MILCOM 2007*.

Wang, S. & Zheng, H. (2008) Enhanced IP Multimedia Subsystems (IMS) for Futuristic Tactical Networks, *Proceedings of IEEE MILCOM 2008*.

Wang, S. & Zheng, H. (2009). SIP-based VoIP Experiment for Disadvantaged Tactical Edge Networks, Proceedings of ICST / ACM The 5th International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (TRIDENTCOM) 2009.



VoIP Technologies

Edited by Dr Shigeru Kashihara

ISBN 978-953-307-549-5

Hard cover, 336 pages

Publisher InTech

Published online 14, February, 2011

Published in print edition February, 2011

This book provides a collection of 15 excellent studies of Voice over IP (VoIP) technologies. While VoIP is undoubtedly a powerful and innovative communication tool for everyone, voice communication over the Internet is inherently less reliable than the public switched telephone network, because the Internet functions as a best-effort network without Quality of Service guarantee and voice data cannot be retransmitted. This book introduces research strategies that address various issues with the aim of enhancing VoIP quality. We hope that you will enjoy reading these diverse studies, and that the book will provide you with a lot of useful information about current VoIP technology research.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821