Algorithm for Elimination of Clipping effects and Ghost Ringing in SIP Initiated IPSec based VoIP

Jaspreet Singh
Computer Science & Engineering Department
Thapar University
Patiala, India

V.P. Singh
Computer Science & Engineering Department
Thapar University
Patiala, India

Ashish Aggarwal
Computer Science & Engineering Department
Thapar University
Patiala, India

ABSTRACT

The security in Voice over IP using SIP initiated IPSec tunnel with the help of Multimedia Internet Keying (MIKEY) protocol has been studied in this paper. Call establishment in SIP initiated IPSec deals with cryptographic processing at the caller and the recipient end. Cryptographic parameter negotiation for IPSec is done through the SIP INVITE message in the calling phase and 200OK response in the answering phase when the responder picks up his phone. This IPSec cryptographic processing at caller end makes it unable to send and receive the RTP media packets at the beginning of the RTP session. This situation is called as call clipping. The caller faces media transmit clipping and media reception clipping at the start of the call due to which the caller can neither send nor receive the RTP media packets for first few milliseconds and hence becomes QoS issue. Ghost ringing is the byproduct of the solution of clipping effect which is rectified with the use of another provisional response at the cost of delayed phone ringing in the ringing phase. An Algorithm for the elimination of clipping effects (Caller's transmission clipping, Caller's Reception Clipping) has been proposed in this paper. The Algorithm describes the process for shifting the IPSec cryptographic processing from the answering phase to the calling phase and a solution to ghost ringing.

General Terms

Ringing delay, answering delay, provisional response, final response, clipping effects, ghost ringing.

Keywords

VoIP, SIP, IPSec, MIKEY, MIME, PRACK, algorithm.

1. INTRODUCTION

Internet Protocol (IP) Telephony is the transmission of voice, fax and related services over packet-switched IP-based networks. Voice over IP (VoIP) has raised much interest as the number of providers offering VoIP services has increased in recent times. VoIP provides more flexible infrastructure than traditional Public Switched Telephone Network (PSTN) by being packet switched technology using all the facilities of Internet protocols. Protocol infrastructure of VoIP provides all the power at the application layer, hence independent from the below layers of TCP/IP suite as shown in Figure 1. The VoIP call consists of three parts namely signaling, encoding & transport, Gateway control. Signaling is provided by H.323 suite or SIP. SIP, as described in [1]**,** is the more popular signaling protocol from Internet Engineering task force (IETF). Encoding of analog voice to digital like G.711 (uses Pulse code modulation) standard is done to transport voice signals in the form of packets.

User Datagram Protocol (UDP) is used as a transport layer protocol because of its real time delivery requirement of VoIP technology which can't be achieved with TCP due to its high processing needs to provide reliable services. And those reliable services are provided to UDP by using Real Time transport Protocol (RTP) which works above the UDP i.e. at application layer and provides the sequencing and timestamp services to UDP. Gateway control comes into action at the time of VoIP communication in dissimilar networks and is maintained by Media Gateway Control Protocol (MGCP).

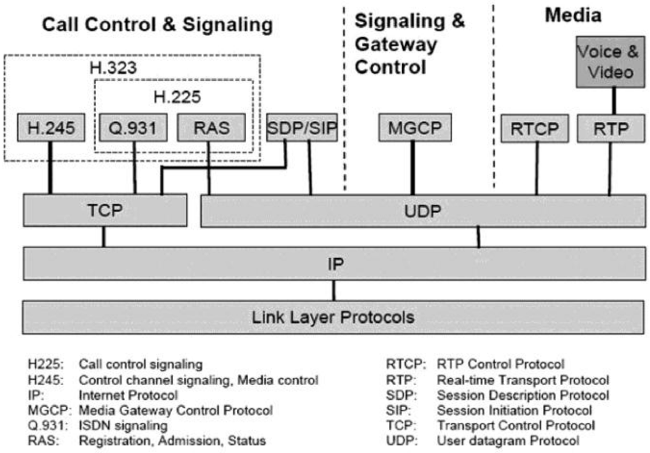

Call Control & Signaling
Signaling & Gateway Control
Media
Voice & Video
H.323
H.225
H.245
Q.931
RAS
SDP/SIP
MGCP
RTCP
RTP
TCP
UDP
IP
Link Layer Protocols
H225: Call control signaling
H245: Control channel signaling, Media control
IP: Internet Protocol
MGCP: Media Gateway Control Protocol
Q.931: ISDN signaling
RAS: Registration, Admission, Status
RTCP: RTP Control Protocol
RTP: Real-time Transport Protocol
SDP: Session Description Protocol
SIP: Session Initiation Protocol
TCP: Transport Control Protocol
UDP: User datagram Protocol

Figure 1: VoIP protocol Infrastructure

Security for Voice over IP (VoIP) is a critical issue of IP Security. VoIP is very sensitive to delays. Hence when security is employed, the risk of delays due to cryptographic processing increases. Security for VoIP can be achieved in different ways and can be divided into two main aspects. First, securing the call signaling i.e. the IP traffic used for establishing the call and second, securing the call itself, here referred to as the media session. VoIP signaling is done for initiating and disconnecting a call. It contains all the parameters of VoIP media session that it is going to establish. A simple two domain SIP trapezoid is shown in Figure 2 describing a VoIP call establishment.

Hence it is important to secure VoIP signaling. We can secure the VoIP signaling [2] by S/MIME (Secure Multipurpose Internet Mail Extension) and TLS (Transport Layer Security) for hop-by-hop protection of SIP messages. VoIP media sessions can be secured at different layers i.e. at application layer with Secure Real Time Protocol (SRTP) and at network layer with well established standard, Internet Protocol Security (IPSec). Although IPSec can secure the whole VoIP i.e. signaling as well as the media session, but this paper considers the SIP initiated IPSec that secures the media session as well as all other traffic of that host once a session is established. Multimedia Internet Keying (MIKEY), a keying protocol, is used to negotiate the IPSec security parameters instead of the standard Internet Keying Exchange (IKE). MIKEY/ IPSec cryptographic processing takes much more time than established standard of MIKEY/SRTP for VoIP. System calls setting the security association and IPSec policy are responsible for the main part of this delay.

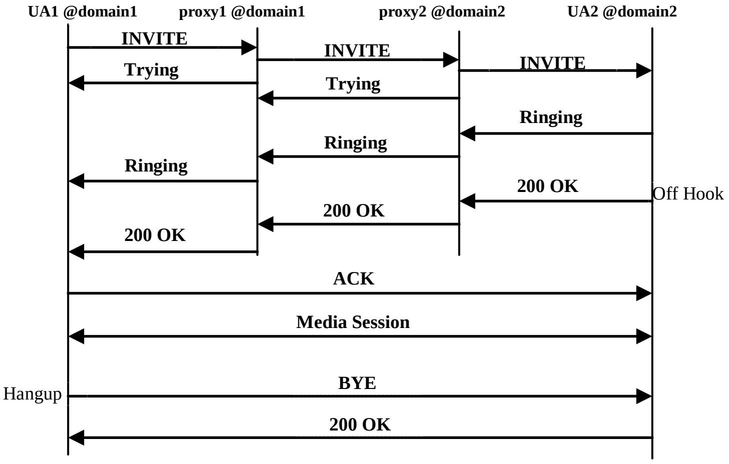


Figure 2: SIP trapezoid for setting up call between UA1 and UA2 in two different domains

2. LITERATURE REVIEW

Security in VoIP is an interesting research area that has been growing in recent years. Various security techniques available have its own limitations. IPSec, when initiated by SIP, uses less number of roundtrips with the help of MIKEY keying protocol. In the last decade, work in RTP media security focuses on key exchange methods and ways to address drawbacks of already established MIKEY/SRTP standard. Traditional Key exchange mechanism available for IPSec is IKE and for VoIP's SRTP is MIKEY whose impact is described in [3, 4]. It confirms that the MIKEY can exchange keys and other cryptographic parameters in one round trip which is a huge advantage in multimedia applications. The usage of MIKEY keying protocol for parameters negotiation of SRTP and IPSec significantly reduces the number of round trips. The idea described in it is to transport all IPSec parameters in MIKEY message instead of IKE method. It provides a good utilization of MIKEY protocol with the aggressive mode of IKE. In the case of SRTP, the MIKEY message that contains SRTP's cryptographic parameters is carried within the SDP. This is the most suitable option for SRTP as it is an application layer protocol and provides the confidentiality and authentication services at application layer.

In the case of SIP initiated IPSec, the MIKEY message that contains IPSec's cryptographic parameters is not carried in SDP. SDP is not a good option in the case of SIP initiated IPSec because IPSec protects the traffic at the network layer as opposed to SRTP which protects the traffic at application layer. If one wants to protect just the traffic described in the SDP, that information can be inserted in the SDP. The MIKEY message is carried in MIME payload in SIP. Using MIKEY for carrying IPSec parameters in SIP INVITE & 200OK response message provides a good utilization of Offer Answer model [6] of SIP. Cryptographic parameters of SRTP are transferred in SDP attribute [7]. For utilizing SIP initiated IPSec not only for VoIP session but also for all IP traffic of the host, IPSec cryptographic parameters are transferred in separate Multimedia Internet Mail Extension (MIME) body [8] for the whole session of that host. The MIME also facilitates the use of S/MIME for securing call signaling.

A physical media communication infrastructure is one possibility for screening of spam and Denial of Service (DOS) attacks during the call establishment as presented in [9]. The call establishment delays, as per [10], for a secure VoIP call (MIKEY/SRTP) is insignificant for a human user. But in case with MIKEY/IPSec, delays are longer due to system calls that sets the IPSEC security associations and policy. The MIKEY response containing negotiated IPSec parameter comes in 200OK from the responder to caller when responder picks up his phone i.e. in answering phase. The caller after processing SIP part of the 200OK response sends back the acknowledgement (ACK) immediately and starts its cryptographic processing which includes session key generation and setting the security associations and policy. All of this cryptographic processing is done in the answering phase. This leads to problem of clipping effects and then further to ghost ringing as described in [11]. The caller faces the call reception clipping for the first few hundreds of microseconds in which the caller discards all the RTP media packets coming from the responder. This happens because of the ongoing cryptographic processing at caller's operating system as shown in Figure 3.

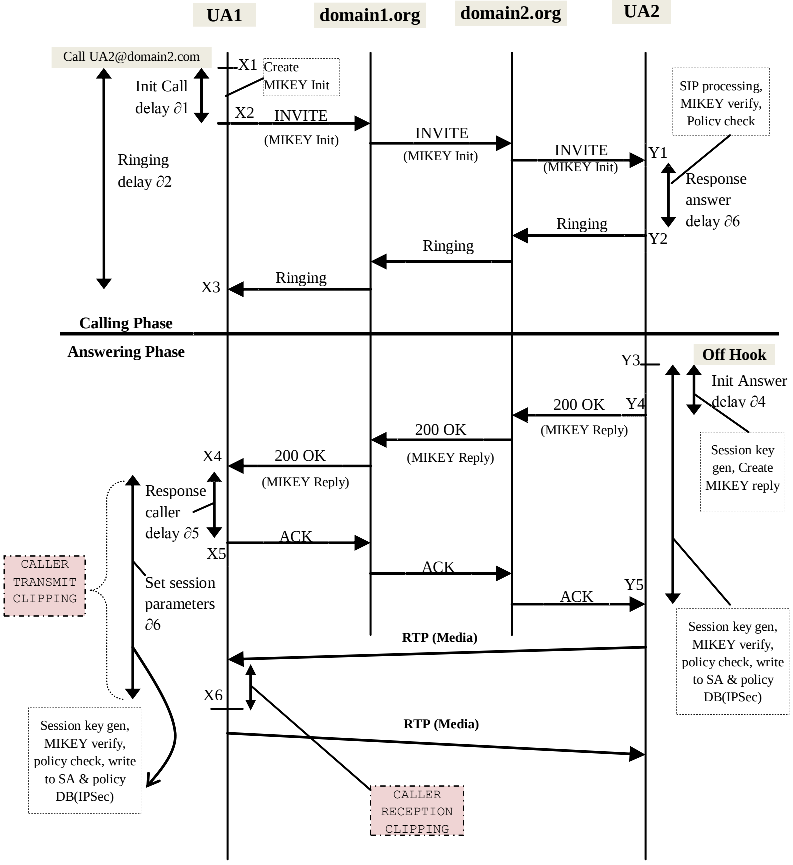


Figure 3: MIKEY reply in 200OK in answering phase

Our study differs from the latter in that 1) we provide a solution design that will eliminate the clipping effects; and 2) solution design to the problem of ghost ringing. Our solution design is based on providing reliability to unreliable 1xx responses using PRACK as described in [12]. To accomplish this, it requires both the User Agents (UA) to support PRACK and the solution also describes the successful and unsuccessful scenarios of PRACK support.

3. SOLUTION DESIGN

Due to high cryptographic processing delays in the answering phase, because of MIKEY Reply containing negotiated IPSec parameters in 200OK response message, the clipping of media packets (RTP packets) occurs at the beginning of the media session as shown in Figure 3. So to deal with this problem, the idea is to send the MIKEY reply earlier than the 200 OK response (before Receiver/Callee picks up the phone) i.e. to send the MIKEY reply in the calling phase rather than in answering phase.

To achieve this objective, the primary condition required to fulfill is:

$$(\partial 7 - \partial 4) > \partial 6 \qquad - (1)$$

Where:
∂6 is the processing delay by the caller after receiving the 200OK. It is the time it takes to process the 200OK reply (may contain MIKEY reply), send back the *ACK* message and setting up the security associations and policy.

∂7 is the *answering delay* of callee i.e. processing time a callee takes when he picks up the phone, sends 200OK and setup security associations and policy to the time he receive the *ACK* message from the caller.

∂4 is the *Initial answer delay* by the caller i.e. processing time a callee takes when he picks up the phone to the time he send 200OK response.

Equation (1) holds good when *'no security'* processing is involved in answering phase as described in the Literature Review. Equation (1) is satisfied by removing the cryptographic processing in the answering phase. This enables the SIP phone to perform only the general SIP processing in the *answering phase*.

So, for sending MIKEY reply, we are left with 3 options:

1. MIKEY Reply in *100 trying* (which is not a valid option, because of absence of standard support).

2. MIKEY Reply in *180 Ringing* response.

3. MIKEY Reply in *183 Session in Progress* response.

The User Agent Client (UAC) and User Agent Server (UAS) support to PRACK decides the behavior of the response from UAS. Table 1 shows the configuration combinations of UAS and UAC following which the behavior is decided as shown in the call processing column. To achieve the required solution, both the UAC and UAS should implement the support for PRACK (Provisional Acknowledgement). This is required because we need a reliable mechanism to get the confirmation of the delivery of MIKEY response when sent with unreliable 1xx responses. This solution also answers what will happen when the responder i.e. UAS, doesn't support the PRACK facility.

3.1 Mikey Reply in 180 Ringing

If Caller (UA1/UAC) announces PRACK (Provisional Acknowledgement) support in his SIP INVITE message, than Callee (UA2/UAS) can send the *MIKEY Reply* in the 180 Ringing message as mentioned in Table 1 and presented in Figure 4. Caller can send the PRACK immediately after authenticating the MIKEY message. The various processing delays are labeled as ∂ and are explained below:

∂1: The time from the point when the caller makes the call, the creation of SIP and MIKEY Initiation message, to the point where the INVITE message leaves the UA1.

⇨ $\partial 1 = X2 - X1$

Where X1: Timestamp when UA1 dials the phone
X2: Timestamp when UA1 completes the creation of SIP INVITE.

Table 1: The call behavior of UAC & UAS with various configuration combinations

UAC	UAS	*Call Processing*
PRACK Disabled	PRACK Disabled	*Normal Call*
PRACK Disabled	PRACK Supported	*Normal Call*
PRACK Disabled	PRACK Require	*Call Rejected*
PRACK Supported	PRACK Disabled	*Normal Call*
PRACK Supported	PRACK Supported	*PRACK Call*
PRACK Supported	PRACK Require	*PRACK Call*
PRACK Require	PRACK Disabled	*Normal Call*
PRACK Require	PRACK Supported	*PRACK Call*
PRACK Require	PRACK Require	*PRACK Call*

∂2: The time UA1 takes in processing the SIP 180 Ringing reliable provisional response. It includes the SIP and MIKEY verification, policy check processing and the creation time of PRACK message as per Algorithm UAC given later in this section.

⇨ $\partial 2 = X4 – X3$

Where X3: Timestamp when UA1 receives the *180 Ringing* reliable provisional response.
X4: Timestamp when UA1 completes SIP & MIKEY verification, policy check and the creation of PRACK message.

∂3: *Ringing delay* is the time from when Caller (UA1) dials callee's (UA2) number until it is notified that UA2 is ringing i.e. when Caller receives & process the 180 Ringing reliable provisional response from the Callee.

⇨ $\partial 3 = \partial 1 + \partial 2 + \partial 4 +$ Network dependent propagation delay

∂4: The time UA2 (Recipient) takes in processing the SIP INVITE. It includes the SIP & MIKEY verification, policy check, creation of MIKEY reply and 180 Ringing message as per Algorithm for UAS.

⇨ $\partial 4 = Y2 – Y1$

Where Y1: Timestamp when UA2 receives the SIP INVITE message.
Y2: Timestamp when UA2 completes the SIP & MIKEY verification, policy check, creation of MIKEY reply and 180 Ringing message.

∂5: The time UA2 takes in processing the PRACK till the creation of 200OK response for the PRACK.

⇨ $\partial 5 = Y4 – Y3$

Where Y3: Timestamp when UA2 receives the PRACK message.

Y4: Timestamp when UA2 completes processing of PRACK message and the creation of 200OK message for PRACK.

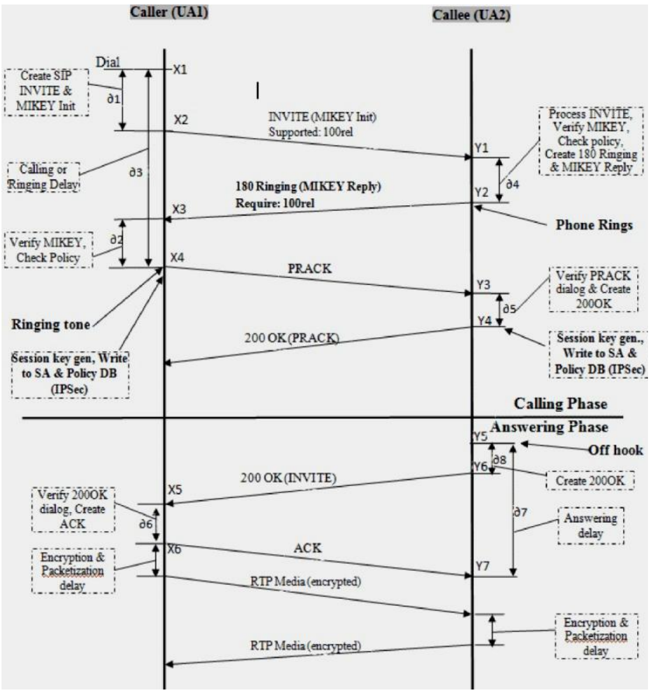

Caller (UA1)
Callee (UA2)
Dial
Create SIP INVITE & MIKEY Init
∂1
X1
X2
INVITE (MIKEY Init)
Supported: 100rel
Process INVITE, Verify MIKEY, Check policy, Create 180 Ringing & MIKEY Reply
Y1
Calling or Ringing Delay
∂3
180 Ringing (MIKEY Reply)
Require: 100rel
Y2
∂4
X3
Phone Rings
Verify MIKEY, Check Policy
∂2
X4
PRACK
Verify PRACK dialog & Create 200OK
Y3
∂5
Y4
Ringing tone
200 OK (PRACK)
Session key gen., Write to SA & Policy DB (IPSec)
Session key gen, Write to SA & Policy DB (IPSec)
Calling Phase
Answering Phase
Y5
Off hook
∂8
Y6
Create 200OK
200 OK (INVITE)
X5
Verify 200OK dialog, Create ACK
∂6
∂7
Answering delay
X6
ACK
Y7
Encryption & Packetization delay
RTP Media (encrypted)
Encryption & Packetization delay
RTP Media (encrypted)

Figure 4: MIKEY request in SIP INVITE & reply in provisional 180 Ringing

∂6: This is the response delay of caller. It includes the processing of 200OK INVITE & creation of ACK message for the UA2.

⇨ ∂6 = X6 – X5

Where X5: Timestamp when UA1 starts processing the 200OK message of SIP INVITE.

X6: Timestamp when UA1 sends the ACK message to UA2.

∂7: It is the Time when UA2 has picked up the phone till UA2 receive the ACK. This is the *answering delay*. It includes the time the callee's user agent (UA2) take in creation of 200OK response for INVITE till the reception of Acknowledgement.

⇨ ∂7 = Y7 – Y5

Where Y5: Timestamp when UA2 creates 200OK message for SIP INVITE.

Y7: Timestamp when UA2 completes processing of ACK message.

∂8: This is the initial answer delay. It is the time when the callee accepts the call to the point where 200OK final response leaves the message.

⇨ ∂8 = Y6 – Y5

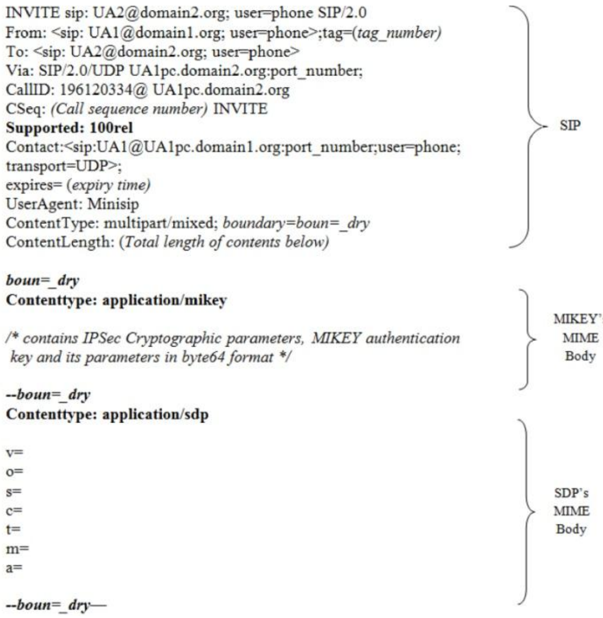
Where Y5: Timestamp when UA2 creates 200OK message for SIP INVITE.

Y6: Timestamp when UA2 sends the ACK message for UA1.

Inferences:

In this solution design, *answering delay* is reduced to the case of *no security*, in which the condition of equation (1) holds perfectly well i.e. *(∂7-∂8) > ∂6* in this case as shown in Figure 4. This solution design has removed the cryptographic processing from the answering phase. This logically proves the elimination of cryptographic delays from the *answering phase* and increase in ringing delay in *ringing phase* which has no effect on the quality of call. Format of SIP INVITE carrying MIKEY message and SIP reply carrying MIKEY response in *180 Ringing* is shown in Figure 5 & Figure 6 respectively.

As compared to the prior case (MIKEY reply in 200OK response message), Caller (UA1) experience a somewhat longer *Ringing delay*, since Callee (UA2) has to construct his *MIKEY Reply* before sending the 180 Ringing message. This does not constitute any problem since Callers are less sensitive to delays before he gets a local ringing tone as opposed to clipping effects at the beginning of the call. If Caller wants/needs to rejects the *MIKEY Reply*, he has to send a CANCEL message to Callee (this should happen instead of sending the PRACK). As in this solution, Callee's phone start ringing immediately after he sends the *MIKEY Reply*, this solution still suffers from *ghost ringing* whose solution design is presented in next section.



```
INVITE sip: UA2@domain2.org; user=phone SIP/2.0
From: <sip: UA1@domain1.org; user=phone>;tag=(tag_number)
To: <sip: UA2@domain2.org; user=phone>
Via: SIP/2.0/UDP UA1pc.domain2.org:port_number;
CallID: 196120334@ UA1pc.domain2.org
CSeq: (Call sequence number) INVITE
Supported: 100rel
Contact:<sip:UA1@UA1pc.domain1.org:port_number;user=phone;
transport=UDP>;
expires= (expiry time)
UserAgent: Minisip
ContentType: multipart/mixed; boundary=boun=_dry
ContentLength: (Total length of contents below)

boun=_dry
Contenttype: application/mikey

/* contains IPSec Cryptographic parameters, MIKEY authentication
 key and its parameters in byte64 format */

--boun=_dry
Contenttype: application/sdp

v=
o=
s=
c=
t=
m=
a=

--boun=_dry—
```

Figure 5: SIP INVITE message format carrying MIKEY message as MIME body

Algorithm for UAC:

Step 1- Create SIP INVITE message and insert Supported: 100rel in SIP header using the MIME structure with a separate body for MIKEY containing IPSec parameters in MIKEY Init Message.

Step 2- Prepare to send the SIP INVITE using DNS query or resolved host address and send it.

Step 3- Check whether the received provisional response message is from valid user and in the same dialog of SIP INVITE.

Step 4- If the response message is from valid user and same dialog and contains MIKEY message, than

Step 4.1 Process the MIKEY Payloads for authentication & policy check and copy the RSeq number.

Step 4.2 Else discard the response and wait for valid response till the timer expires

Step 5- If the 180 Ringing response doesn't contain Support/Require Header in SIP, than

Step 5.1- Exit this algorithm and call algorithm (Mikey reply in 200 OK)
Step 5.2- Else, create and send the PRACK message with RAck = RSeq, set with acknowledgement number equals to RSeq received in the 180 Ringing provisional response.

Step 6- Start the Local Ringing tone.

Step 7- Generate Session key from the master key using MIKEY.

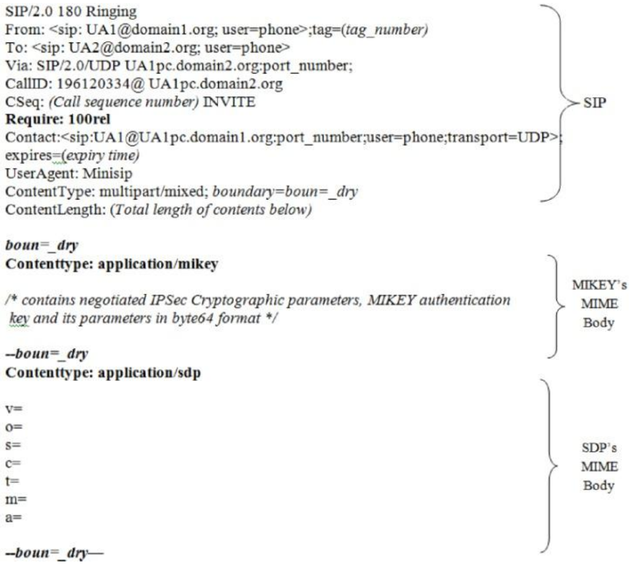
Step 8- Write the Security Association and policy received in the SA & Policy databases of IPSec by the system calls to kernel space.

Step 9- Resend the PRACK until 200 OK (PRACK) is received till timeout.

Step 10- If timeout expires, than

Step 10.1- Disconnect the call and generate PRACK unacknowledged error.

Step 10.2- Else Process the SIP final response to INVITE, 200 OK (INVITE) and stop the Local Ringing tone.



```
SIP/2.0 180 Ringing
From: <sip: UA1@domain1.org; user=phone>;tag=(tag_number)
To: <sip: UA2@domain2.org; user=phone>
Via: SIP/2.0/UDP UA1pc.domain2.org:port_number;
CallID: 196120334@ UA1pc.domain2.org
CSeq: (Call sequence number) INVITE
Require: 100rel
Contact:<sip:UA1@UA1pc.domain1.org:port_number;user=phone;transport=UDP>;
expires=(expiry time)
UserAgent: Minisip
ContentType: multipart/mixed; boundary=boun=_dry
ContentLength: (Total length of contents below)

boun=_dry
Contenttype: application/mikey

/* contains negotiated IPSec Cryptographic parameters, MIKEY authentication
 key and its parameters in byte64 format */

--boun=_dry
Contenttype: application/sdp

v=
o=
s=
c=
t=
m=
a=

--boun=_dry—
```

Figure 6: 180 Ringing message format carrying MIKEY message as MIME body

Step 11- Create and send the ACK, acknowledging the Callee about the reception of the 200 OK final response.

Step 12- Create and send the RTP media packets as per security association and policy established.

Algorithm for UAS:

Step 1- Process the SIP INVITE message received for the identity verification/spam.

Step 2- Process the MIKEY payload for authentication and policy check.

Step 3- If MIKEY authentication fails, than

Step 3.1- Drop the SIP INVITE message and create & send the 6xx error message to caller.

Step 3.2- Else Process the MIKEY & inspect the IPSec ciphers supported at UAS Application and create the MIKEY reply with respect to supported features and policy adopted (Parameter negotiation).

Step 4- If Require header field is present with tag Require= 100req, than

Step 4.1- Create and send 180 Ringing response with Require= 100rel and a new field RSeq for sequencing to an initial value indicating Reliable provisional requirement and insert MIKEY Reply in MIME body part.

Step 4.2- Else Create and send 180 Ringing provisional response without MIKEY reply and call algorithm (Mikey reply in 200OK) and exit from this algorithm.

Step 5- Start the Phone Ringing.

Step 6- Process the PRACK and check for the RAck value for being in the same dialog else drop the call.

Step 7- Create and send 200 OK for PRACK.

Step 8- Generate Session Key from the master key received using MIKEY.

Step 9- Write the Security Association and policy received in the SA & Policy databases of IPSec by the system calls to kernel space.

Step 10- If the User Agent accept/picks the call (OFF the hook), than

Step 10.1- Create and send the SIP response 200OK (INVITE).

Step 10.2- Else create and send BYE after timeout.

Step 11- Process the ACK message, create and send the RTP & RTCP media packets.

3.2 Mikey Reply in 183 Session in Progress

The *Ghost Ringing* is a situation in which nobody is on the caller side when callee picks up the ringing phone. This happens because callee's phone starts ringing immediately when he sends the *180 Ringing* provisional message to caller. If, for any reason, caller rejects the *MIKEY reply* in *180 Ringing*, the callee won't be able to ignore the ringing that started immediately after sending the *180 Ringing* message.

So there should be a mechanism that enables the caller and callee to get their local ringing tone after all the policy checks at both the ends. To eliminate the problem of *ghost ringing*, this solution design sends *MIKEY reply* in *183 Session in Progress* provisional reliable response message. The callee's phone rings first when the corresponding PRACK arrives and processed as depicted in the Figure 7. Although this will increase the *ringing delay* even more, but this is the most appropriate way to send the *MIKEY reply* that will eliminate the two ill-effects of delays i.e. *Call Clippings and Ghost Ringing*. In order for this approach to work, the caller has to wait until he has accepted callee's reply before he sends the PRACK. (If he rejects the message he should as usual send a CANCEL message). The process is all same except the introduction of new 183 Session in Progress provisional reliable response message and delay of the function call to local ringing tone at both the ends. To solve this problem of *Ghost Ringing* as well as the *Clipping Effect*, there are two conditions to satisfy:

1. Equation (1) (same as that of Solution design, mikey reply in 180 ringing)
2. Call to ringing function after the creation and reception of 180 ringing provisional message at UAS and UAC respectively.

The various processing delays, labeled as ∂ are explained as:

∂1: The time from the point when the caller makes the call, create SIP & MIKEY Initiation message, to the point where the INVITE message leaves the UA1.

⇨ $\partial 1 = X2 - X1$

Where X1: Timestamp when UA1 dials the phone

X2: Timestamp when UA1 sends SIP INVITE.

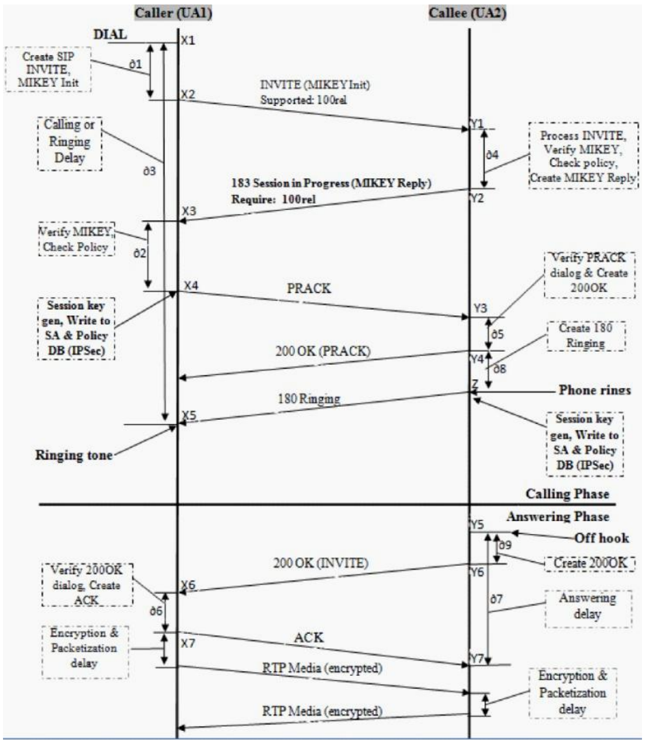

Caller (UA1)
Callee (UA2)
DIAL
X1
Create SIP INVITE, MIKEY Init
∂1
X2
INVITE (MIKEY Init)
Supported: 100rel
Y1
Calling or Ringing Delay
∂3
Process INVITE, Verify MIKEY, Check policy, Create MIKEY Reply
∂4
183 Session in Progress (MIKEY Reply)
Require: 100rel
Y2
X3
Verify MIKEY, Check Policy
∂2
X4
PRACK
Verify PRACK dialog & Create 200OK
Session key gen, Write to SA & Policy DB (IPSec)
Y3
∂5
Create 180 Ringing
200 OK (PRACK)
Y4
∂8
Z
Phone rings
180 Ringing
X5
Session key gen, Write to SA & Policy DB (IPSec)
Ringing tone
Calling Phase
Answering Phase
Y5
Off hook
∂9
Create 200OK
200 OK (INVITE)
Y6
Verify 200OK dialog, Create ACK
X6
∂6
∂7
Answering delay
Encryption & Packetization delay
X7
ACK
Y7
RTP Media (encrypted)
Encryption & Packetization delay
RTP Media (encrypted)

Figure 7: MIKEY Request in SIP INVITE & Reply in Provisional 183 Session in Progress

∂2: The time UA1 takes in processing the SIP 183 Session in Progress reliable provisional response. It includes the SIP & MIKEY verification, policy check and the creation of PRACK message as per Algorithm for UAC.

⇨ $\partial 2 = X4 – X3$

Where X3: Timestamp when UA1 receives the 183 Session in Progress reliable provisional response.

X4: Timestamp when UA1 completes the creation of SIP & MIKEY verification, policy check and the creation of PRACK message.

∂3: This is the Ringing Delay which includes the PRACK processing time & Creation of 200OK for PRACK. This is the time from when Caller (UA1) dials Callee's (UA2) number until she is notified that UA2 is ringing i.e. when Caller receives & process the 183 Session in Progress Reliable Provisional Response from the Callee.

⇨ $\partial 3 = \partial 1 + \partial 2 + \partial 4 + \partial 5 + \partial 8 _{+}$ N/W dependent propagation delay

∂4: The time UA2 (Recipient) takes in processing the SIP INVITE. It includes the SIP & MIKEY verification, policy check, creation of MIKEY reply and 183 Session in Progress message as per Algorithm of UAS.

⇨ $\partial 4 = Y2 – Y1$

Where Y1: Timestamp when UA2 receives the SIP INVITE message.

Y2: Timestamp when UA2 completes the SIP verification & MIKEY verification, policy check, Create MIKEY reply and 183 Session in Progress message.

∂5: The time UA2 takes in processing the PRACK till the creation of final 200OK response for the PRACK.

⇨ $\partial 5 = Y4 – Y3$

Where Y3: Timestamp when UA2 receives the PRACK message.

Y4: Timestamp when UA2 completes processing of PRACK and then creates 200OK for PRACK.

∂6: This is the response delay of caller. It includes the processing of 200OK INVITE & creation of ACK message for the UA2.

⇨ $\partial 7 = X6 – X5$

Where X5: Timestamp when UA1 process the 200OK message of SIP INVITE.

X6: Timestamp when UA1 create the ACK message for UA2.

∂7: It is the Time when UA2 has picked up the phone till UA2 receive the ACK. This is the *answering delay*.

⇨ $\partial 6 = Y7 – Y5$

Where Y5: Timestamp when UA2 creates 200OK message for SIP INVITE.

Y7: Timestamp when UA2 starts processing of ACK message.

∂8: This is the time used to create provisional unreliable *180 Ringing* message. It also includes the processing time of function of local phone ringing.

⇨ $\partial 8 = Z – Y4$

Where Z: Timestamp when UA2 create the *180 Ringing* message & process the local phone ringing function.

Y4: Timestamp when UA2 completes processing of PRACK message and the creation of 200OK message for PRACK.

∂9: This is the initial answer delay. It is the time when the callee accepts the call to the point where 200OK final response leaves the message.

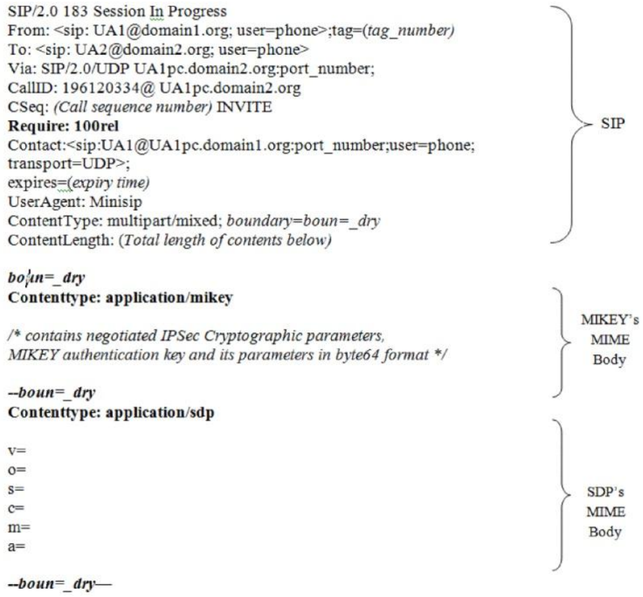
⇨ $\partial 9 = Y6 – Y5$

Where Y5: Timestamp when UA2 creates 200OK message for SIP INVITE.

Y6: Timestamp when UA2 sends the ACK message for UA1.

Inferences:
The two necessary conditions for elimination of *Ghost Ringing and Clipping effects* are satisfied. This logically proves the elimination of cryptographic delays from the *answering phase* and increase in ringing delay in *ringing phase* which has no effect on the quality of call. This solution design is an add on version of solution presented in 3.1, which not only removes the Clipping effects due to IPSec Cryptographic processing but also remove the Ghost Ringing.

In this solution, Caller (UA1) experiences a somewhat longer r*inging delay*. This is because this solution has delayed the 180 Ringing message after all the policy verification. This does not constitute any problem too since Caller is less sensitive to delays before he gets a local ringing tone as opposed to clipping effects at the beginning of the call. In this solution design, Answering Delaying remains same as solution design presented in MIKEY Reply in *180 Ringing*. The Equation (1) still holds perfectly.



```
SIP/2.0 183 Session In Progress
From: <sip: UA1@domain1.org; user=phone>;tag=(tag_number)
To: <sip: UA2@domain2.org; user=phone>
Via: SIP/2.0/UDP UA1pc.domain2.org:port_number;
CallID: 196120334@ UA1pc.domain2.org
CSeq: (Call sequence number) INVITE
Require: 100rel
Contact:<sip:UA1@UA1pc.domain1.org:port_number;user=phone;
transport=UDP>;
expires=(expiry time)
UserAgent: Minisip
ContentType: multipart/mixed; boundary=boun=_dry
ContentLength: (Total length of contents below)

boun=_dry
Contenttype: application/mikey

/* contains negotiated IPSec Cryptographic parameters,
MIKEY authentication key and its parameters in byte64 format */

--boun=_dry
Contenttype: application/sdp

v=
o=
s=
c=
m=
a=

--boun=_dry—
```

Figure 8: 183 Session in Progress message format carrying MIKEY message as MIME body

Algorithm for UAC:

Step 1- Create SIP INVITE message and insert Supported: 100rel in SIP header in the MIME structure with a separate body for MIKEY containing IPSec parameters in MIKEY Init Message.

Step 2- Prepare to send the SIP INVITE using DNS query or resolved host address and send it.

Step 3- Check whether the received provisional response message is from valid User and in the same dialog of SIP INVITE.

Step 4- If the response message is from valid user and same dialog, than

> Step 4.1 Process the MIKEY Payloads for authentication, policy check and check the timestamp and copy the RSeq number. In case of mismatch in timestamp, create & send a Cancel SIP message and drop the call.
>
> Step 4.2 Else discard the response and wait for valid response till the timer expires

Step 5- If the 183 Session in Progress response doesn't contain Support/Require Header in SIP, than

> Step 5.1- Exit this algorithm and call algorithm (Mikey reply in 200 OK)
>
> Step 5.2- Else, create and send the PRACK message with RAck = RSeq, set with acknowledgement number equals to RSeq received in the 183 Session in Progress provisional response.

Step 6- Generate Session key from the master key using MIKEY.

Step 7- Write the Security Association and policy received in the SA & Policy databases of IPSec by the system calls to kernel space.

Step 8- Resend the PRACK until 200 OK (PRACK) is received till timeout.

Step 9- Process the 200 OK received for PRACK.

Step 10- Process the 180 Ringing Provisional unreliable response message and call the Local ringing tone function.

Step 11- Start the Local Ringing tone.

Step 12- Process the SIP final response to INVITE, 200 OK (INVITE) and stop the Local Ringing tone

Step 13- Create and send the ACK, acknowledging the Callee about the reception of the 200 OK final response.

Step 14- Create and send the RTP media packets as per security association and policy established.

Algorithm for UAS:

Step 1- Process the SIP INVITE message received for the identity verification/spam.

Step 2- Process the MIKEY payload for authentication and policy check.

Step 3- If MIKEY authentication fails, than

> Step 3.1- Drop the SIP INVITE message and create & send the 6xx error message.
>
> Step 3.2- Else Process the MIKEY & inspect the IPSec ciphers support at UAS Application and create the MIKEY reply with respect to supported features and policy adopted.

Step 4- If Require header field is present with tag Require= 100req, than

> Step 4.1- Create and send 183 Session in Progress response with Require= 100rel and a new field RSeq for sequencing to an initial value indicating Reliable provisional requirement and insert MIKEY Reply in MIME body part with it.
>
> Step 4.2- Else Create and send 183 Session in Progress response without MIKEY reply and call algorithm (mikey response in 200OK) and exit this algorithm.

Step 5- Process the PRACK and check for the RAck value for being in the same dialog.

Step 6- Generate Session Key from the master key received using MIKEY.

Step 7- Write the Security Association and policy received in the SA & Policy databases of IPSec by the system calls to kernel space.

Step 8- Create and send 200 OK for PRACK.

Step 9- Create & send the 180 Ringing provisional message.

Step 10- Make a function call to start the Local Phone Ringing that starts the Phone Ringing.

Step 11- If the User Agent accept/picks the call (OFF the hook), than

Step 11.1- Create and send the SIP response 200OK (INVITE).

Step 11.2- Else create and send BYE after timeout.

Step 12- Process the ACK message, create and send the RTP & RTCP packets.

4. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards the research with suggestions and support throughout the period of this research paper.

5. CONCLUSION

SIP-MIME-MIKEY structure for establishing IPSec security association and policy negotiation is an effective technique for initiating IPSec using SIP. Call establishment in SIP initiated IPSec method suffers from high cryptographic processing at the caller and the recipient end. IPSec is a utility of operating system which requires system calls from user space to kernel space that makes the process time consuming with respect to SRTP method. The high delay of IPSec cryptographic processing at caller end disables the caller to send and receive the RTP media packets at the beginning of the call leading to media transmit clipping and media reception clipping at the start of the call. An Algorithm is provided in which Clipping Effects are eliminated by sending the MIKEY reply in 180 provisional reliable response message with PRACK as its acknowledgement, rather than sending MIKEY response in final response 200 OK. This algorithm suffers from ghost ringing which is than eliminated in second algorithm by sending reply in 183 provisional reliable response message. Hence the problem of Clipping Effects and Ghost Ringing, which arises in SIP initiated IPSec case, has been shifted from answering phase to calling phase i.e. from answering delay to ringing delay. The Algorithm presented would although increase the *ringing delay* (which is of an average 3-5 seconds in PSTN calls), but decrease the more time critical answering delay which is strongly related to QoS.

6. REFERENCES

[1] Rosenberg, J. Schulzrinne, H. Camarillo, G. Johnston, A. Peterson, J. Sparks, R. Handley, M. and Schooler, E. June 2006. SIP: Session Initiation Protocol. IETF RFC 3261.

[2] Park, P. 2009. Voice over IP Security. pp 67-73. Cisco Press.

[3] Arkko, J. Carrara, E. Lindholm, F. Naslund, M. and Norrman, K. August 2010. MIKEY: Multimedia Internet KEYing. IETF RFC 3830.

[4] Krishna, M. Ranganathan and Kilmartin, L. 2001. Investigations into the Impact of Key Exchange Mechanisms for Security Protocols in VoIP Networks. 1st IEI/IEE Telecommunication Systems Postgraduate Research Symposium, Dublin, Ireland.

[5] Andreasen, F. Baugher, M. Wing, D. Cisco Systems. July 2006. Session Description Protocol (SDP) Security Descriptions for Media Streams. IETF RFC 4568.

[6] Rosenberg, J. Schulzrinne, H. July 2004. An Offer/Answer Model with the Session Description Protocol (SDP). RFC 3264.

[7] Arkko, J. Lindholm, F. Naslund, M. Norrman, K. Ericsson. Carrara, E. Royal Institute of Technology, July 2006. Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP). IETF RFC 4567.

[8] Camarillo, G. Ericsson. September 2009. Message Body handling in the session initiation protocol. IETF RFC 5621.

[9] Si, D.F. Long, Q. Han, X.H. and Zou, W. June 2004. Security mechanisms for SIP-based multimedia communication infrastructure. IEEE Conf. on Comm, Circuits and Systems (ICCCAS), ed. Proc. of 2nd ed, pp 575-578, IEEE CS Press.

[10] Bilien, J. Eliasson, E. Orrblad, J. and Vatn, J.O. june 2005. Secure VoIP: Call establishment and media protection. 2ndWorkshop Secure VoIP, Washington DC.

[11] Bilien, J. Eliasson, E. and Vatn, J.O. March 2004. Call establishment delay for secure VoIP. WiOpt'04, Cambridge UK.

[12] Rosenberg, J. Schulzrinne, H. Columbia U. June 2002. Reliability of Provisional Responses in the Session Initiation Protocol. IETF RFC 3262.