Performance of Secure SIP and LoST Signaling in an NG-9-1-1 Testbed

Unnati Desai
Sindhu Alagesan
Ana Goulart
Walt Magnussen

What is NG-9-1-1?

….a new architecture to support IP-based citizen-to-authority emergency communication system

IP Phones

(fixed/mobile)

2005

FCC mandates that VoIP providers MUST offer 9-1-1 services

FCC

Vonage

Text Messages

Verizon Selects TCS to Provide National 9-1-1 Texting Gateway (5/4/12)

Sending Pictures, Video

Telemetry

OnStar

Is it secure?

Typical security threats, according to the VoIP Security Alliance (VoIPSA):

- Social threats, such as viruses and misconfigurations,
- Eavesdropping,
- Denial of service attacks,
- Service abuse threats such as toll fraud,
- Physical access threats,
- Interruption of services threats.

IETF - ECRIT Working Group requirements

Best Current Practices for Communications Services in Support of Emergency Calling (draft-ietf-ecrit-phonebcp-17) recommends:

“Either TLS or IPsec MUST be used when attempting to signal an emergency call. If TLS session establishment is not available, or fails, the call MUST be retried without TLS.”

“Either TLS or IPSEC MUST be used to protect the location”.

NENA Requirements

National Emergency Number Association (NENA):

" …emergency calls require a high degree of expediency in answering" (< 3sec)

Our Goal: To identify the main contributors to the call setup delay and evaluate the impact of security protocols, for IP-based emergency calls.

NG-9-1-1 Signaling – SIP and LoST

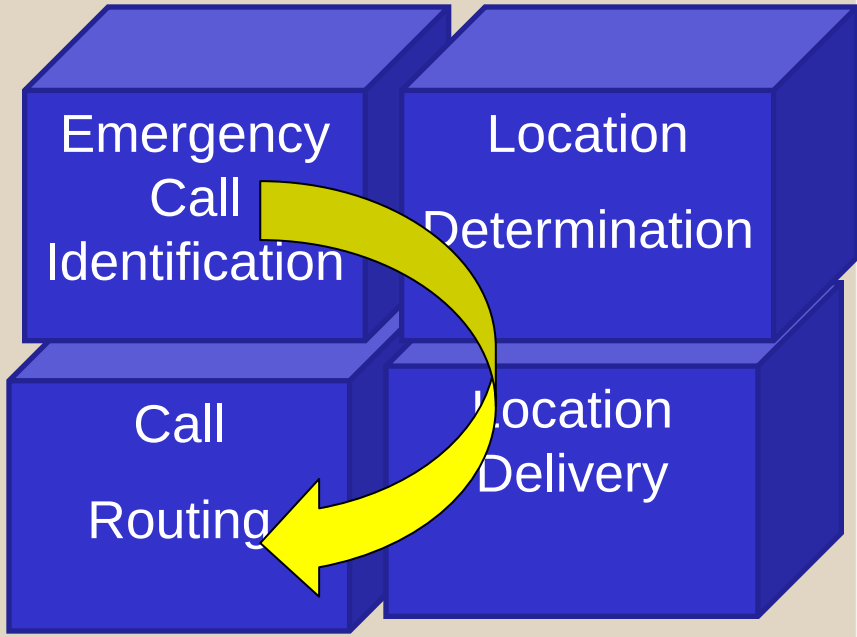
"Security mechanisms have a greater impact on call setup signaling than on voice quality."

SIP = Session Initiation Protocol

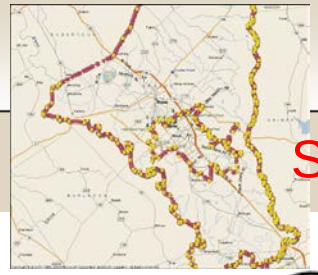
LoST = Location to Service Translation Protocol

NG-9-1-1 architecture's building blocks:

- emergency call identification (SIP)
- location determination
- location delivery (SIP)
- call routing (SIP and LoST)



NG-9-1-1 Testbed



Service Boundaries

VSP

GEO DATABASE

ESINet

SIP PROXY

tx-csec-1@tamu.edu

LOST Server

DEDICATED LINK

LOST Server

tx-csec-2.tamu.edu

ESRP

LIS

VOICE SERVICE PROVIDER

ESINet

ACCESS NETWORK

USER

SIP CLIENT

default@tamu.edu

User dials 9-1-1

Public Safety Answering Point (PSAP)

PSAPD

tx-csec-3@tamu.edu

voiplab55.tamu.edu

CALLTAKERS

PSAP

Test scenarios – Client queries LoST x VSP queries LoST

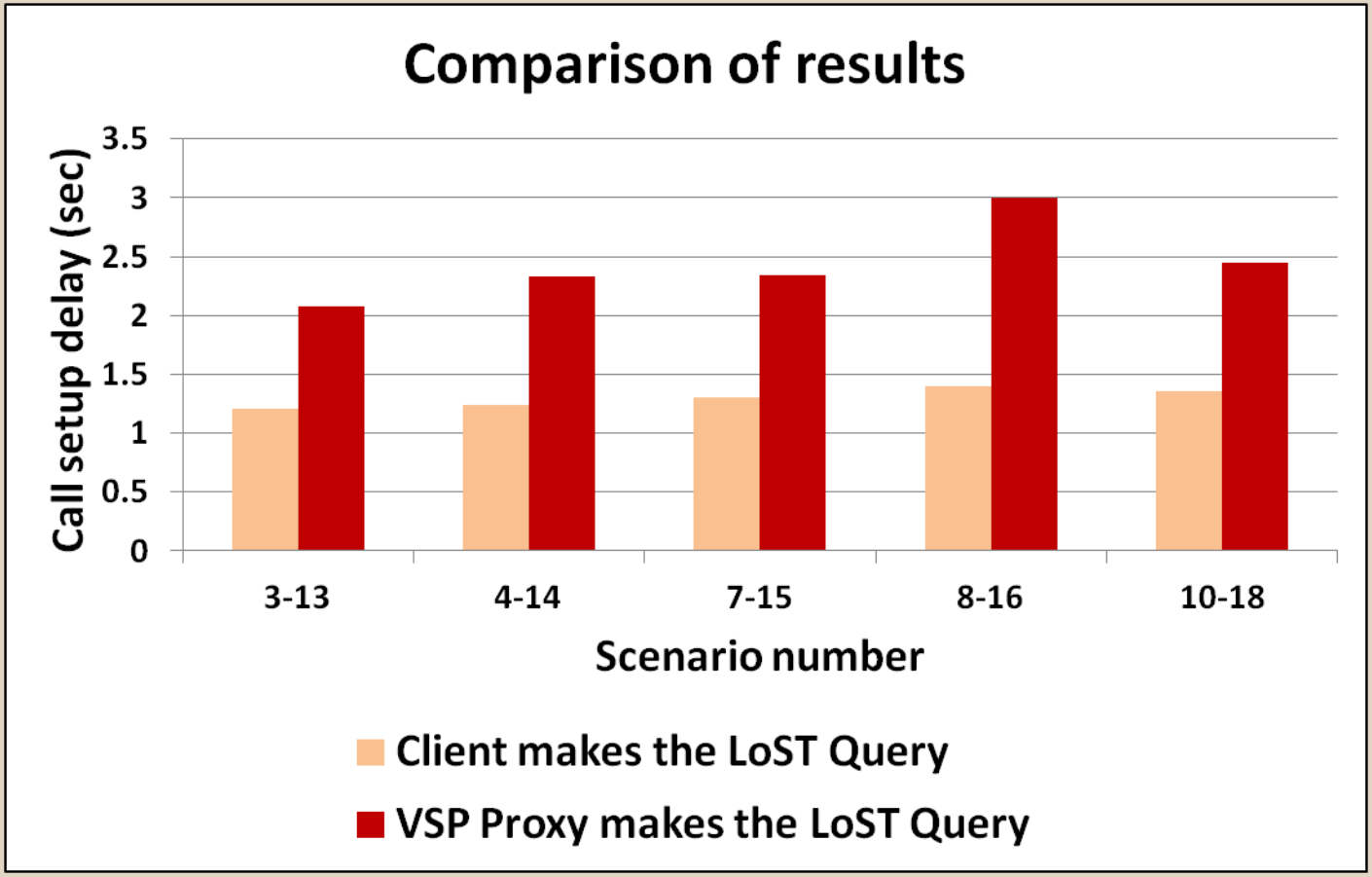
TABLE I
TEST SCENARIOS WITH CLIENT MAKING THE LOST QUERY.

			1	2	3	4	5	6	7	8	9	10
Client	sip	tcp	x	x	x	x						
		tls					x	x				
	lost	http	x	x	x	x	x	x				
VSP Proxy	sip	tcp	x	x	x	x	x	x				
		tls										
		ipsec			x	x	x	x				
ESRP	sip	tcp	x	x	x	x	x	x				
		tls										
		ipsec			x	x	x	x				
	lost	http	x		x		x					
		https		x		x		x				

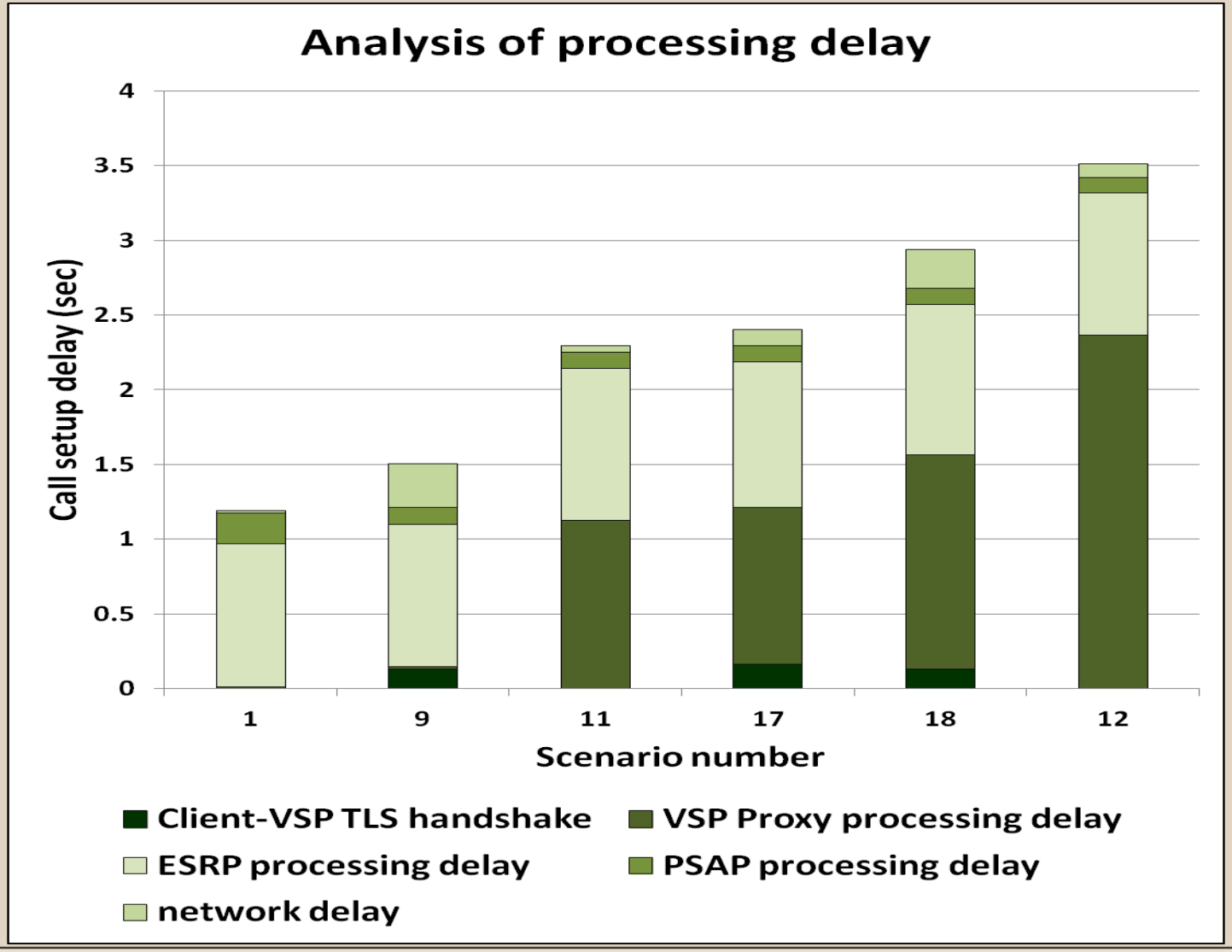
TABLE II
TEST SCENARIOS WITH VSP MAKING THE LOST QUERY.

			11	12	13	14	15	16	17	18
Client	sip	tcp	x	x	x	x				
		tls					x	x	x	x
VSP Proxy	sip	tcp	x	x	x	x				
		tls					x	x	x	x
		ipsec			x	x	x	x		
	lost	http	x		x		x		x	
		https		x		x		x		x
ESRP	sip	tcp	x	x	x	x				
		tls					x	x	x	x
		ipsec			x	x	x	x		
	lost	http	x	x	x		x		x	
		https				x		x		x

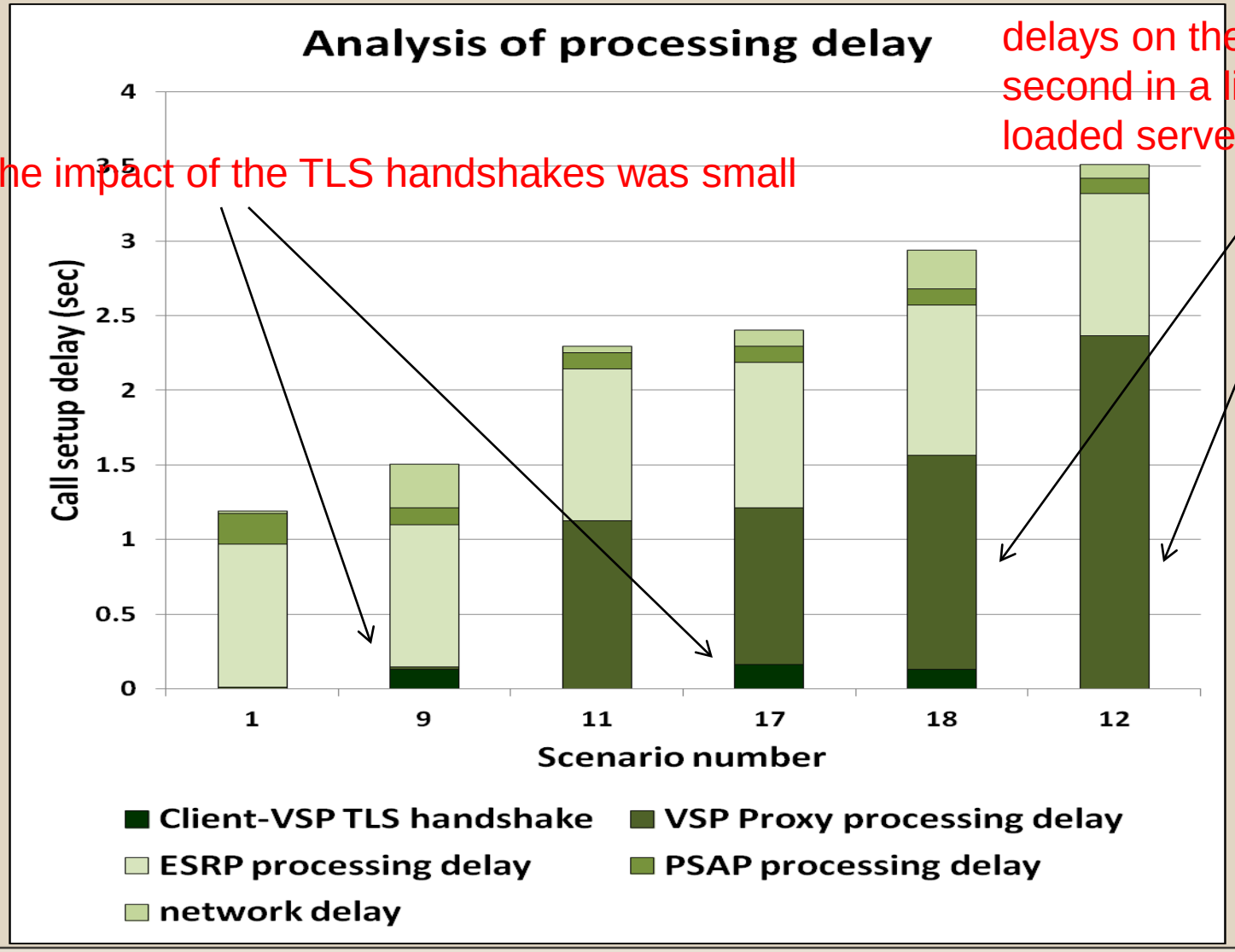
Comparing different scenarios



Call setup delay components



Call setup delay components

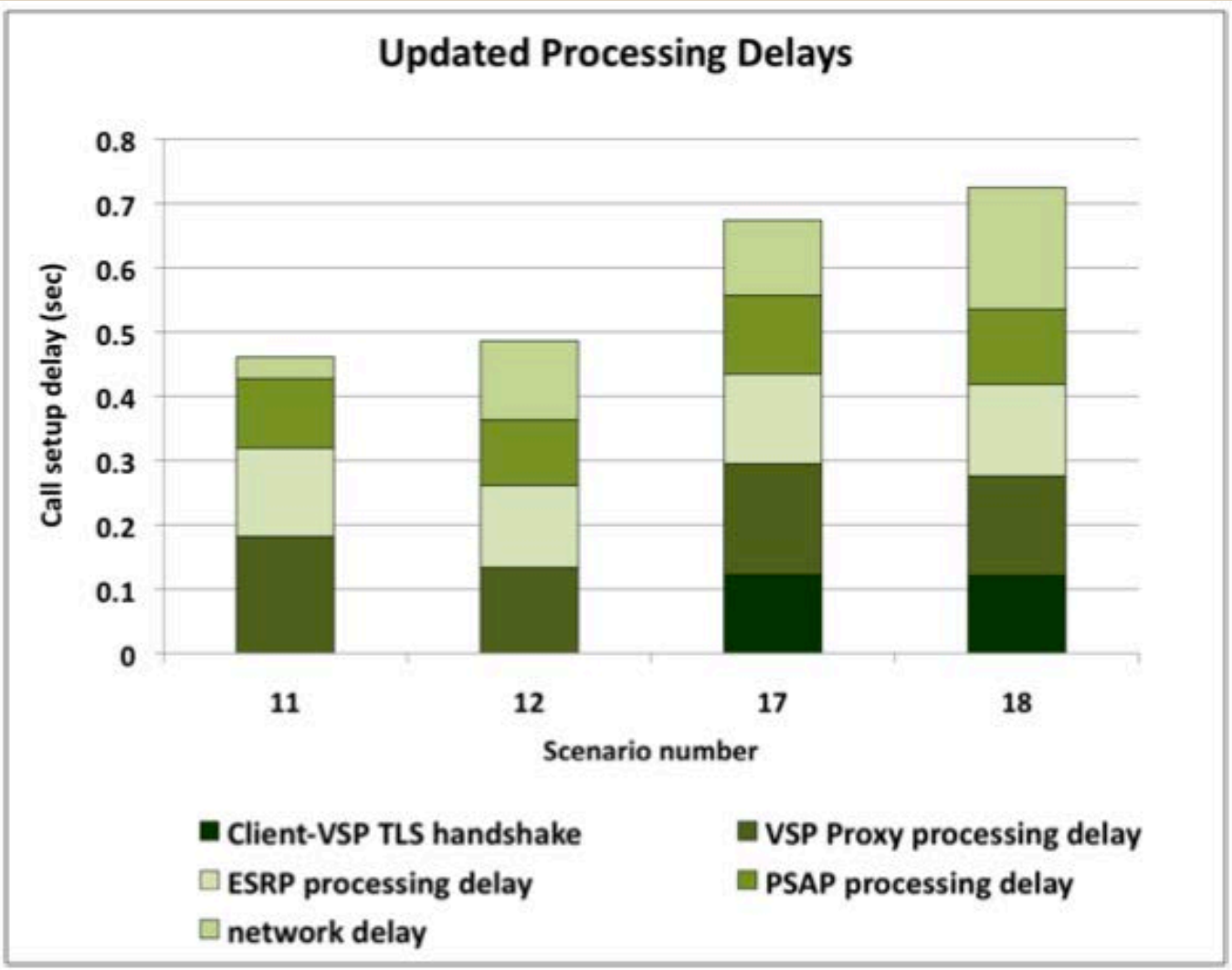


The impact of the TLS handshakes was small

delays on the order of 1 second in a lightly loaded server too high

New Results with Reduced Processing Delays

- We've identified a large delay component when the SIP server spawns a process that has the functionality of the LoST client.



Lessons Learned

- Performance is better when:
  - when the client provides the routing information (client makes the LoST query)
  - SIP server and LoST client work well together
- Impact of security on our testbed:
  - the TLS handshakes consist of approximately 20 percent of the call setup delay.
  - call setup delay increase can be as high as 56 percent when comparing with a scenario with no security at all.
- On-going work:
  - Testing persistent TLS Sessions
  - Integrating our testbed with IIT's NG-9-1-1 testbed to benchmark our performance results

Call Flow Overview