International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

SIP Over NON-TLS vs TLS Environment

Prapti Priya Nayak[1]**, G. Sujatha**[2]

[1]M. Tech (IT Dept.) SRM University Chennai, India

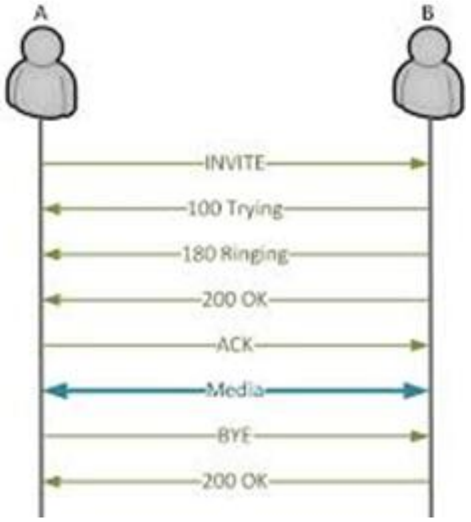
[2]Assistant Professor SRM University Chennai, India

Abstract: ***SIP is a dominant signalling protocol that is used over various transport protocols for a successful session establishment along with data/audio/video transfer. This paper gives a survey on SIP over both NON-TLS and TLS Environment. It also gives a performance study of SIP by using three transport layer protocols.***

Keywords: SIP, TLS, TCP, UDP, PBX, Performance Analysis.

1. Introduction

Session Initiation Protocol (SIP), an application-layer control (signalling) protocol for creating modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences. Media can be added to (and removed from) an existing session. SIP transparently supports name mapping and redirection services, which supports personal mobility- users can maintain a single externally visible identifier regardless of their network location.



SIP is based on an HTTP-like request/response transaction model. Each transaction consists of a request that invokes a particular method, or function, on the server and at least one response. In this example, the transaction begins with Alice's (A) softphone sending an INVITE request addressed to Bob's(B) SIP URI. INVITE is an example of a SIP method that specifies the action that the requestor (Alice) wants the server (Bob) to take. The INVITE request contains a number of header fields. Header fields are named attributes that provide additional information about a message. The ones present in an INVITE include a unique identifier for the call, the destination address, Alice's address, and information about the type of session that Alice wishes to establish with Bob. When Alice's soft phone receives the 180 (Ringing) response, it passes this information to Alice, perhaps using an audio ring back tone or by displaying a message on Alice's screen. In this example, Bob decides to answer the call. When he picks up the handset, his SIP phone sends a 200 (OK) response to indicate that the call has been answered. The 200 (OK) contains a message body with the SDP media description of the type of session that Bob is willing to establish with Alice. As a result, there is a two-phase exchange of SDP messages: Alice sent one to Bob, and Bob sent one back to Alice. This two-phase exchange provides basic negotiation capabilities and is based on a simple offer/answer model of SDP exchange. Session Initiation Protocol (SIP) protocol is used for signalling and the Real-Time Transport Protocol (RTP) for media transport. Consequently, appropriate security mechanisms must be provided for securing them. Secure media transport on VoIP communications is realized using either IPSec or Secure RTP (SRTP). SRTP is more efficient in terms of bandwidth. SIP RFC3261specifies several security mechanisms: Transport Layer Security (TLS) at transport level, IPSec at network level, SIPS URI Scheme for secure access to resources, HTTP Authentication for authentication and S/MIME for SIP messages body end-to-end confidentiality and integrity.

2. Sip Over NON-TLS

A lot of people would generally associate UDP with voip and probably leave it at that, but in simple terms there are two parts to voip - connection and voice data transfer.SIP is a very light weight protocol, once the connections is established it's effectively left idle until the infrequent event of someone making a phone call. TCP (unlike UDP) will actually reduce traffic to the server by eliminating need to;

1.Re-register every few minutes2.Refresh/ping server
You can run SIP over TCP and then use (as is recommended) UDP for RTP.As the number of devices grows, the equation tilts in UDPs favor. But then you also have to consider SIP User Agents expanding to cover multiple codecs, multimedia, video and screen-sharing. The INVITE packets can start to grow large and potentially run over the UDP single datagram size thereby tilting the equation again in favor of TCP.

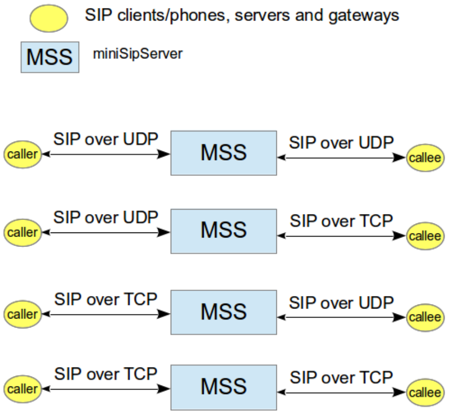
3. SIP Over TCP and UDP

SIP, which is the signalling path of a telephone call is usually handled via UDP (User Datagram Protocol). This protocol is similar to a "telegram" or normal "mail cover". Data is divided into packets that a theoretical maximum size of 1500 bytes may have. This size is limited, however, by additional information and further logical information to a usable size of 1300 bytes. Is now such a packet sent, the sender and the receiver is included in the package. However, there is no feedback to the sender if the package has really reached its recipient. This has also achieved the result that the UDP protocol is used, it needs to ensure and check that a package's recipient.This happens by means of the SIP protocol acknowledgment responses. An "INVITE" (call from A to B) follows in the case of a "TRYING", then a "PROGRESS", etc Should one fail to acknowledge the last packet is defined by timers at intervals until an acknowledgment is sent again. When a timeout expires, the session is terminated.

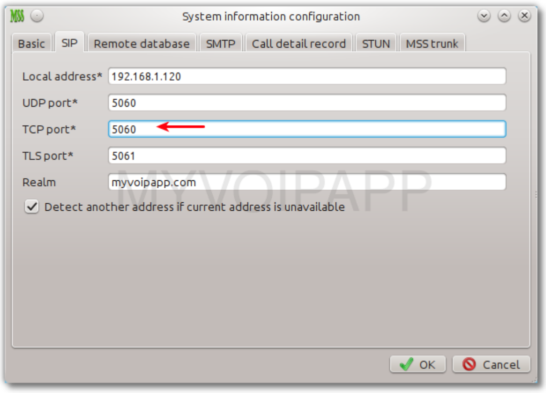
For SIP over TCP, the transport behaves fundamentally differently. Similar to a "registered letter". (Transmission Control Protocol), TCP is due to the concept in many ways "robust" as UDP. However, in contrast to UDP, but also some more traffic (overhead) of bandwidth for the same user data as UDP. However, this is negligible in the case of SIP far as possible. The advantages of TCP is the protocol architecture of the ansich. It contains built Mechanism to recover lost packets independently resend. Similarly, a TCP connection is set up in a dedicated form. This means before data is transmitted to the receiver already knows what the coming. There are more benefits of TCP are as compared to TCP for NAT (Network Address Translation) and correspondingly for firewalls easier to handle. What is now the "better" protocol does not really matter. It must meet the requirements for you as a customer. The dus.net GmbH offers you the opportunity to use both protocols for SIP. You make the settings for your particular device, the transport protocol to be used for SIP. For audio data, so the language is generally used UDP. The reason is inter alia the few "overhead" of the large payload fraction and less time-consuming trials and eventual replacement issues of packets that are undesirable so.

4. SIP over TCP

SIP over TCP, specially used for some enterprise unified communication servers.

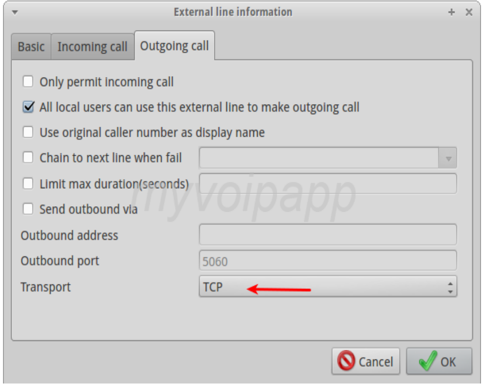


- In MSS main window click menu 'Data / System / SIP', then we can configure 'TCP port' as wish as we want. Please refer to following figure. If this port is changed, we must restart MSS to enable new port.



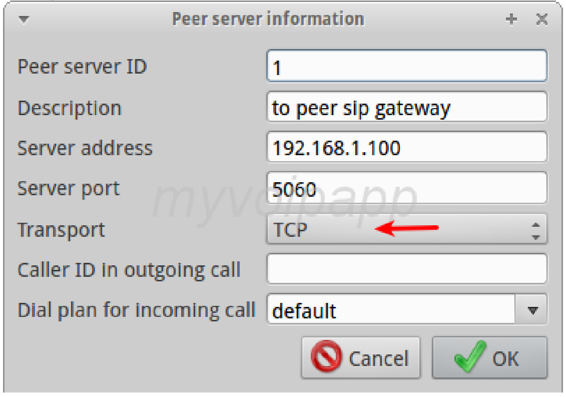
Local address* 192.168.1.120
UDP port* 5060
TCP port* 5060
TLS port* 5061
Realm myvoipapp.com
☑ Detect another address if current address is unavailable

- When MSS works with other gateways by using external line, we need configure it to useTCP or UDP to transport SIP messages. By default, MSS always uses UDP. For incoming calls, MSS will detect its transport automatically.



☐ Only permit incoming call
☑ All local users can use this external line to make outgoing call
☐ Use original caller number as display name
☐ Chain to next line when fail
☐ Limit max duration(seconds)
☐ Send outbound via
Outbound address
Outbound port 5060
Transport TCP

- It is same as external line, we need indicate MSS to use TCP or UDP for SIP trunk tomake outgoing call. Please click menu 'data / peer servers' to update your configuration.



Peer server ID 1
Description to peer sip gateway
Server address 192.168.1.100
Server port 5060
Transport TCP
Caller ID in outgoing call
Dial plan for incoming call default

5. SIP over TLS

TLS 1.0 is basically the same as SSL 3.1. It's just the latest version and now has a new name. TLS stands for "Transport Layer Security". Here any Tranportweg (HTTP, email, FTP, or just SIP) over the TCP protocol is secured as well as with SSL. The key aspect of secure VoIP communication is the security of the signalling path, which is provided by SIP protocol. The main components for securing SIP communication are: confidentiality and integrity of signalling messages and authentication of parties. Several SIP security mechanisms are specified in as mentioned before. TLS is a widespread and well-known transport protocol for secure communication. It provides confidentiality and integrity of the transmission channel for data exchanged between applications at higher level. TLS makes use of X.509 certificates to associate a public key with the certificate subject. This relationship is confirmed by the digital signature of the certificate authority (CA), which involves public key cryptography. TLS allows both entities in a communication link to authenticate each other. However, TLS with mutual authentication is impractical and a challenging implementation due to problems with keydistribution.TLS with mutual authentication can reduce performance by up to a factor of 17 compared to SIP-over-UDP. Further, TLS support is not yet fully implemented in all currently available SIP UAC softphone solutions. Some of them with TLS support are: Blink, Bria, Linphone, MicroSIP and Yate. Not all support mutual authentication using client certificates. For this reasons, in our proposed VoIP security approach we used HTTP digest authentication scheme for verifying the identity of users and performing message authentication. On the other side, with TLS clients authenticate the server using the server's public key associated with the server's certificate. This assured SIPmutual authentication. SIP message privacy protection is enabled using encryption with keys that are exchanged during TLS handshake procedure. TLS message integrity is ensuredby sending additionally a keyed digest of the original message using a secret key shared between the sender and receiver.

6. Performance Evaluation of SIP on TLS VS NON-TLS

The goal of the experiment was to analyze the ability of VoIP PBX Elastix server to handle multiple simultaneous registrations and call setups. We performed performance evaluation through testing hardware utilization of Elastix server during the SIP scenario .It is important to emphasize that our test scenario did notinvolve the exchange of media (RTP) traffic, because our goal was to test the impact of SIP signalling protocol overdifferent transport protocols on the performance of VoIP PBX server and VoIP service. Because of this after a call was established in the SIP scenario script we set a pause so that the call remained active for some time. Processor load and consumed RAM measuring was achieved using Zabbix network monitoring system as described in the previous section. SIP performance was evaluated using the proposed methodology for testing and benchmarking SIP infrastructure in RFC6076.The metrics we chose for testing are: RRD (Registration Request Delay) and SRD (Session Request Delay).RRD is a measurement of delay in responding to a UA REGISTER request. SRD is the time interval from when the first bit of the initial INVITE message is sent by the originating user agentto the intended destination agent, until the last bit of the first provisional response is received (180 Ringing). We measured RRD and SRD as specified in at the originating SIP UA just for successful session setup. This was achieved using the ability of SIP to dynamically display Statistics about running tests, includingresponse times. For this purpose we specified the start (with start_rtd_attribute) and the endpoint for two counters (with rtd attribute), each one for RRD and SRD computation. To dump the response times in an external.csv file the-trace_rtt option was additionally used at the SIP command line. This allowed us to effectively analyze and process the obtained results. Results for every single parallel SIP session that are collected from all machines from which we generated traffic were arithmetically averaged and as such are presented in the following section.

7. Results

Depending on the transport protocols over which SIP signalling is established, each figure has three corresponding characteristic curves. For each of the protocols we used the same scenario, but with different load level, or more precisely with different rates for generating concurrent calls. Each tested configuration regardless of the transport protocol has SIP authentication enabled. During testing we used TLS with TLS-AES chipper suite. The call generation rates were increased until we noticed that SIP enters in saturation. Saturation occurs when SIP starts to generate calls with rate less than rate that we specified when starting the generator. This problem was easily avoided by distributing the generation of calls on multiple machines. Due to the limitations of available equipment, the maximum achieved number of concurrent calls was 1300, after the distribution of SIP generator on4 machines. For each protocol peek throughput of concurrent calls. Also for each scenario we measured RRD,SRD, processor load, and consumed RAM memory. Below Figure shows the peek throughput of concurrent calls de-pending on transport protocol. As we expected SIP over UDP gives the best SIP server performance, followed by SIP over TCP and SIP over TLS respectively. Figures show RRD and SRD respectively, for different transport protocol configurations and call rates. Note that TCP and TLS from the standpoint of RRD and SRD have worse performance than UDP because of the time needed for establishing connections. These results should be viewed relatively, because SIP needs extra time to create call statistics. A better way to collect statistics would be to analyze packets captured by a network protocol analyzer. Figures show peek processor load and consumed RAM memory, for different transport protocol configurations and call rates. Higher call rates cause a greater processor load. Again UDP has best performance. The graphics of consumed RAM memory give interesting results. It should be noted that the consumption of RAM memory for each protocol individually is relatively constant regardless of the call rate. Similar results are shown in paper. However, TLS requires more RAM memory in regard to TCP and UDP, which have approximately the same demands on.

Figure shows Peak Throughput of concurrent calls:

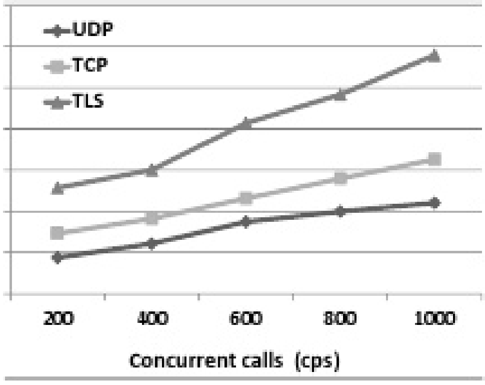


Figure shows Average Registration Request Delay vs. concurrent calls:

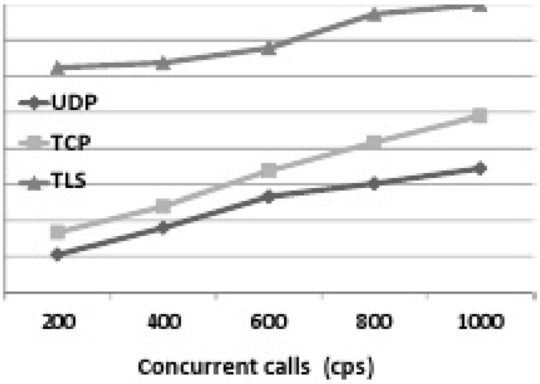
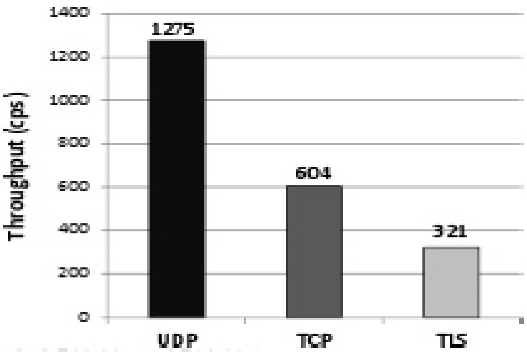
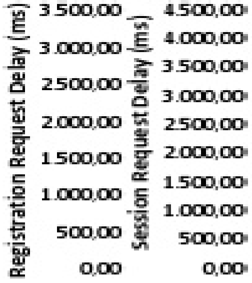


Figure shows Average Session Request Delay vs. concurrent calls :





8. Conclusion

This Survey paper focused on SIP over various Non-TLS(UDP and TCP) and TLS Environment. Securing the SIP signalization is one of the primary goals when implementing secure VoIP networks. Hence by using SIP over TLS based signalling, SIP signalization is better secured.

References

1.http://www.rfc-base.org/txt/rfc-3261.txt