SIP Based Intrusion Detection System for VoIP based Applications

Bela Shah
Vadodara Institute of Engineering,Kotambi, Vadodara
patel.bela07@gmail.com

Kinjal Dave
Ahmedabad, Gujarat
kjdave.27@gmail.com

ABSTRACT

VoIP applications are extensively used in current scenario. VoIP Security is very important aspect with increasing use of VoIP Applications such as Skype.SIP (Session Initiation Protocol) faces some security issues such as malicious SIP Packets, Malformed SIP Packets etc. Security measures to eliminate this risk include provision of cryptographic measures like TLS, DTLS etc. which are not up to mark as they provide only confidentiality. Hence through this paper effort has been made to provide SIP security through rule matching engine.

Keywords

DoS; SIP; TLS; VoIP

1. INTRODUCTION

VoIP is becoming an attractive communications option for consumers. Given the trend towards lower fees for basic broadband service and the brisk adoption of even faster internet offerings, VoIP usage should only gain popularity with time[5].

ICTCS '16, March 04-05, 2016,Udaipur,India © 2016 ACM. ISBN 978-1-4503-39629/16/03‥$15.00

DOI:http://dx.doi.org/10.1145/2905055.2905086

While VoIP vulnerabilities are typically similar to the ones users face on the internet, new threats, scams, and attacks unique to IP telephony are now emerging[6]. SIP(Session Initiation Protocol) has its own share of threats in VoIP Network.).Most current SIP applications in the real world employ a client/server transaction model similar to HTTP.

2. SIP ANOMALIES

SIP Registeration Hijacking-Registration hijacking occurs when an attacker impersonates

a valid UA to a registrar and replaces the legitimate registration with its own address. This attack causes inbound calls intended for the UA to be sent to the rogue UA.

SIP Message modification-Attacker by executing man-in the-middle attack like IP Spoofing, MAC Spoofing etc. does modification in attributes of message. Modification can be in a way where the attacker could impersonate a caller or reroute a call to an unintended party.

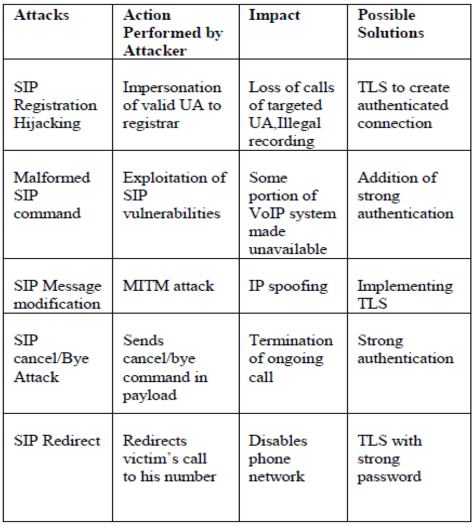
SIP Cancel/Bye Attack-Attacker creates SIP message with cancel or bye command in its payload. This leads to termination of ongoing call.

Malformed SIP command-The SIP protocol relies upon an hypertext markup language (HTML) like body to carry command information [1]. The downside is that it becomes very difficult to test the SIP parser with every possible input. Attackers can exploit these vulnerabilities as they find them by forming packets with malformed commands and sending them to susceptible nodes [1].

SIP Redirect [2]**:** SIP employs a server application that receives requests from a phone or proxy and returns a redirection response indicating where the request should be retried. This allows a person to have a call made to them ring at a different phone depending on where they are located, but the caller only dials a single number to reach the person. By attacking the redirect server and commanding it to redirect the victim's calls to a number specified by the attacker, the attacker can receive calls intended for the victim. If the attacker wishes to disable the phone network, they could redirect all users' phone numbers to a nonexistent or null type of device.

In RFC 3261 [3] several security mechanisms are recommended to secure SIP services such as TLS, S/MIME & IPsec.

Table 1. Attacks & Its Countermeasures[7]



Attacks	Action Performed by Attacker	Impact	Possible Solutions
SIP Registration Hijacking	Impersonation of valid UA to registrar	Loss of calls of targeted UA,Illegal recording	TLS to create authenticated connection
Malformed SIP command	Exploitation of SIP vulnerabilities	Some portion of VoIP system made unavailable	Addition of strong authentication
SIP Message modification	MITM attack	IP spoofing	Implementing TLS
SIP cancel/Bye Attack	Sends cancel/bye command in payload	Termination of ongoing call	Strong authentication
SIP Redirect	Redirects victim's call to his number	Disables phone network	TLS with strong password

2. PROPOSED SYSTEM

Chen [1] proposes a method to detect DoS attacks that involve SIP entities with illegitimate SIP messages like legitimate message flooding, Invalid message flooding and distribution reflection DoS (DRDoS).Chen also gives threshold parameters to confirm an attack. He modified the original finite-state machines for SIP transactions in such a way that transaction anomalies can be detected in a stateful manner. One drawback of this approach is that malformed SIP messages are not considered properly. Although this mechanism is very effective to detect DoS or flooding attacks, malformed SIP messages are definitely hazardous because they cause the malfunction of a VoIP service[4]. In contrast to this approach, we propose a mechanism that is able to detect both malformed SIP messages and spoofed messages at the same time.

Hence we decided to test our approach by first creating a VoIP environment and then did attacks on our system, hence finding out the differences between malformed and original SIP messages and using Snort we tested our rules effectively.

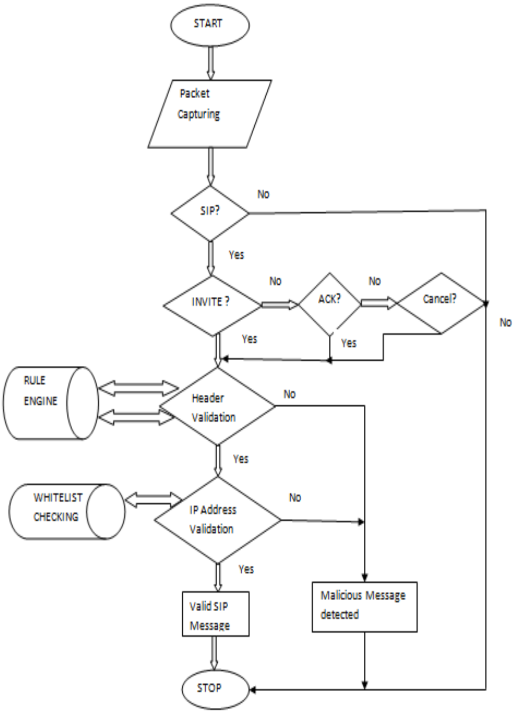


Figure 1.Proposed Sip Intrusion Detection System

As per our proposed system we first captured the packets during a VoIP call in progress. In a network simultaneously many packets flow, hence first aim was to determine which the SIP packets are. For the purpose of identification we check the source and destination port of the SIP Packet which has to be 5060.If the ports match then the packet is identified as a SIP Packet, else it is considered to be malformed and warning message is generated.

Next aim of the proposed system is to determine the type of SIP Request, thatis, whether it is SIP INVITE,SIP ACK or SIP CANCEL Request. This purpose is fulfilled by signature checking of various SIP messages against the original SIP Signatures. If the signatures match then only then message is taken to be valid else alert is generated.

Next stage is header validation, wherein the mandatory fields of the SIP Packet header are checked by collection of rules which make up the rule matching engine. If all the rules are satisfied only then the packet is considered to be valid else a alert is generated. For each kind of message we have devised a SIP Request specific rule file and also a general rule file. So basically at this stage checking for malformed messages is done.

If the message passes header validation stage, it proceeds to IP Validation wherein IP Addresses of the SIP Request messages are checked. For this purpose, at the testing stage, we devised white list wherein we have a collection of all IPs which are allowed to our network. So right now we have tested the system in static environment. If the packet passes the IP Validation stage it is taken to be a valid SIP Request, else spoofed message is detected.

Rule matching Engine checks the fields which are generally missing in different SIP message packets. It is clearly illustrated in Table 2.

Table 2. Signature database for checking type of message

Type of SIP Message	Signature Database
SIP Invite	49 4e 56 49 54 45
SIP Ack	41 43 4b
SIP Cancel	42 59 45

Table 3. Rule Matching Engine Field Check

Type of packet	Fields checked by Rule matching
SIP INVITE	-User agent, Date, Allow, Supported, Content length, Content type, Changes in positions of rest of the fields, Change in source port
SIP ACK	Content length, Changes in positions of rest of the fields, Change in source port
SIP CANCEL	Content type, Content length, Changes in positions of rest of the fields, Change in source port, MAX_FORWARD Field

4. Primary Requirements for Test bed

We require the following three things for a successful setup of our test bed

1.ASTERISKNOW 1.7.1 FreePBX

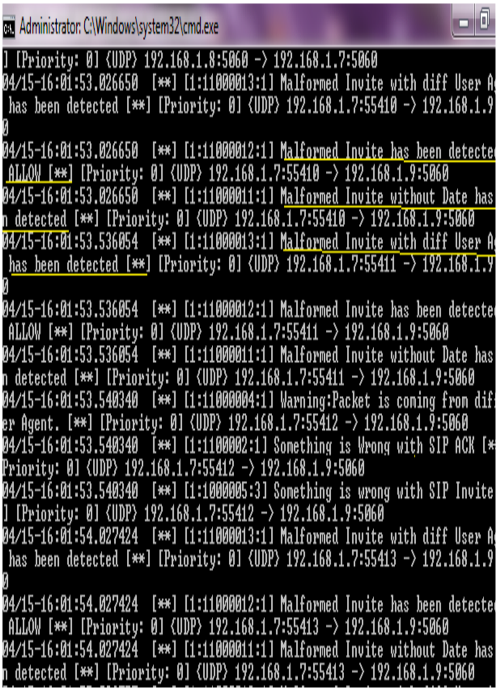
2.Two Zoiper softphones

3.Attacker tools

5. Results

5.1. Malicious SIP Invite detection

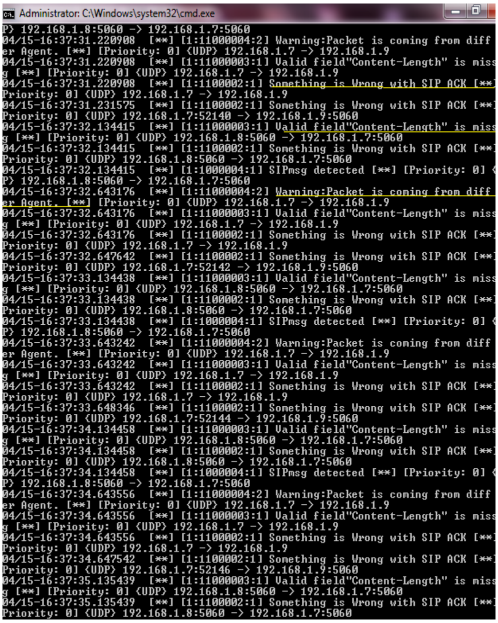
When using VoIPER, malicious packets were generated and at the same time snort arerun, activation of rules that we had included happens, owing to which malicious SIP Packets are detected.



```
] [Priority: 0] {UDP} 192.168.1.8:5060 -> 192.168.1.7:5060
04/15-16:01:53.026650  [**] [1:11000013:1] Malformed Invite with diff User A
 has been detected [**] [Priority: 0] {UDP} 192.168.1.7:55410 -> 192.168.1.9
0

04/15-16:01:53.026650  [**] [1:11000012:1] Malformed Invite has been detecte
 ALLOW [**] [Priority: 0] {UDP} 192.168.1.7:55410 -> 192.168.1.9:5060
04/15-16:01:53.026650  [**] [1:11000011:1] Malformed Invite without Date has
n detected [**] [Priority: 0] {UDP} 192.168.1.7:55410 -> 192.168.1.9:5060
04/15-16:01:53.536054  [**] [1:11000013:1] Malformed Invite with diff User A
 has been detected [**] [Priority: 0] {UDP} 192.168.1.7:55411 -> 192.168.1.9
0

04/15-16:01:53.536054  [**] [1:11000012:1] Malformed Invite has been detecte
 ALLOW [**] [Priority: 0] {UDP} 192.168.1.7:55411 -> 192.168.1.9:5060
04/15-16:01:53.536054  [**] [1:11000011:1] Malformed Invite without Date has
n detected [**] [Priority: 0] {UDP} 192.168.1.7:55411 -> 192.168.1.9:5060
04/15-16:01:53.540340  [**] [1:11000004:1] Warning:Packet is coming from dif
er Agent. [**] [Priority: 0] {UDP} 192.168.1.7:55412 -> 192.168.1.9:5060
04/15-16:01:53.540340  [**] [1:1100002:1] Something is Wrong with SIP ACK [*
Priority: 0] {UDP} 192.168.1.7:55412 -> 192.168.1.9:5060
04/15-16:01:53.540340  [**] [1:1000005:3] Something is wrong with SIP Invite
] [Priority: 0] {UDP} 192.168.1.7:55412 -> 192.168.1.9:5060
04/15-16:01:54.027424  [**] [1:11000013:1] Malformed Invite with diff User A
 has been detected [**] [Priority: 0] {UDP} 192.168.1.7:55413 -> 192.168.1.9
0

04/15-16:01:54.027424  [**] [1:11000012:1] Malformed Invite has been detecte
 ALLOW [**] [Priority: 0] {UDP} 192.168.1.7:55413 -> 192.168.1.9:5060
04/15-16:01:54.027424  [**] [1:11000011:1] Malformed Invite without Date has
n detected [**] [Priority: 0] {UDP} 192.168.1.7:55413 -> 192.168.1.9:5060
```

Figure 2.Detection Malformed SIP Message

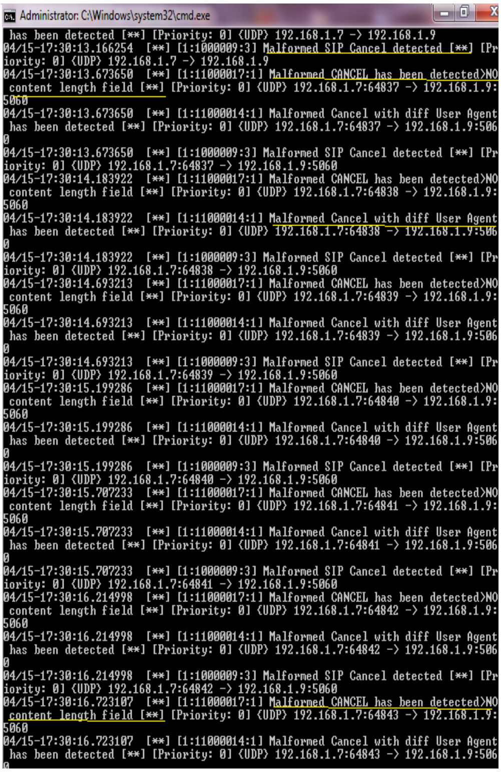
5.2. Malicious SIP Ack Detection



```
P} 192.168.1.8:5060 -> 192.168.1.7:5060
04/15-16:37:31.220908  [**] [1:11000004:2] Warning:Packet is coming from diff
er Agent. [**] [Priority: 0] {UDP} 192.168.1.7 -> 192.168.1.9
04/15-16:37:31.220908  [**] [1:11000003:1] Valid field"Content-Length" is miss
g [**] [Priority: 0] {UDP} 192.168.1.7 -> 192.168.1.9
04/15-16:37:31.220908  [**] [1:1100002:1] Something is Wrong with SIP ACK [**]
Priority: 0] {UDP} 192.168.1.7 -> 192.168.1.9
04/15-16:37:31.231575  [**] [1:1100002:1] Something is Wrong with SIP ACK [**]
Priority: 0] {UDP} 192.168.1.7:52140 -> 192.168.1.9:5060
04/15-16:37:32.134415  [**] [1:11000003:1] Valid field"Content-Length" is miss
g [**] [Priority: 0] {UDP} 192.168.1.8:5060 -> 192.168.1.7:5060
04/15-16:37:32.134415  [**] [1:1100002:1] Something is Wrong with SIP ACK [**]
Priority: 0] {UDP} 192.168.1.8:5060 -> 192.168.1.7:5060
04/15-16:37:32.134415  [**] [1:1000004:1] SIPmsg detected [**] [Priority: 0] {
P} 192.168.1.8:5060 -> 192.168.1.7:5060
04/15-16:37:32.643176  [**] [1:11000004:2] Warning:Packet is coming from diff
er Agent. [**] [Priority: 0] {UDP} 192.168.1.7 -> 192.168.1.9
04/15-16:37:32.643176  [**] [1:11000003:1] Valid field"Content-Length" is miss
g [**] [Priority: 0] {UDP} 192.168.1.7 -> 192.168.1.9
04/15-16:37:32.643176  [**] [1:1100002:1] Something is Wrong with SIP ACK [**]
Priority: 0] {UDP} 192.168.1.7 -> 192.168.1.9
04/15-16:37:32.647642  [**] [1:1100002:1] Something is Wrong with SIP ACK [**]
Priority: 0] {UDP} 192.168.1.7:52142 -> 192.168.1.9:5060
04/15-16:37:33.134438  [**] [1:11000003:1] Valid field"Content-Length" is miss
g [**] [Priority: 0] {UDP} 192.168.1.8:5060 -> 192.168.1.7:5060
04/15-16:37:33.134438  [**] [1:1100002:1] Something is Wrong with SIP ACK [**]
Priority: 0] {UDP} 192.168.1.8:5060 -> 192.168.1.7:5060
04/15-16:37:33.134438  [**] [1:1000004:1] SIPmsg detected [**] [Priority: 0] {
P} 192.168.1.8:5060 -> 192.168.1.7:5060
04/15-16:37:33.643242  [**] [1:11000004:2] Warning:Packet is coming from diff
er Agent. [**] [Priority: 0] {UDP} 192.168.1.7 -> 192.168.1.9
04/15-16:37:33.643242  [**] [1:11000003:1] Valid field"Content-Length" is miss
g [**] [Priority: 0] {UDP} 192.168.1.7 -> 192.168.1.9
04/15-16:37:33.643242  [**] [1:1100002:1] Something is Wrong with SIP ACK [**]
Priority: 0] {UDP} 192.168.1.7 -> 192.168.1.9
04/15-16:37:33.648346  [**] [1:1100002:1] Something is Wrong with SIP ACK [**]
Priority: 0] {UDP} 192.168.1.7:52144 -> 192.168.1.9:5060
04/15-16:37:34.134458  [**] [1:11000003:1] Valid field"Content-Length" is miss
g [**] [Priority: 0] {UDP} 192.168.1.8:5060 -> 192.168.1.7:5060
04/15-16:37:34.134458  [**] [1:1100002:1] Something is Wrong with SIP ACK [**]
Priority: 0] {UDP} 192.168.1.8:5060 -> 192.168.1.7:5060
04/15-16:37:34.134458  [**] [1:1000004:1] SIPmsg detected [**] [Priority: 0] {
P} 192.168.1.8:5060 -> 192.168.1.7:5060
04/15-16:37:34.643556  [**] [1:11000004:2] Warning:Packet is coming from diff
er Agent. [**] [Priority: 0] {UDP} 192.168.1.7 -> 192.168.1.9
04/15-16:37:34.643556  [**] [1:11000003:1] Valid field"Content-Length" is miss
g [**] [Priority: 0] {UDP} 192.168.1.7 -> 192.168.1.9
04/15-16:37:34.643556  [**] [1:1100002:1] Something is Wrong with SIP ACK [**]
Priority: 0] {UDP} 192.168.1.7 -> 192.168.1.9
04/15-16:37:34.647542  [**] [1:1100002:1] Something is Wrong with SIP ACK [**]
Priority: 0] {UDP} 192.168.1.7:52146 -> 192.168.1.9:5060
04/15-16:37:35.135439  [**] [1:11000003:1] Valid field"Content-Length" is miss
g [**] [Priority: 0] {UDP} 192.168.1.8:5060 -> 192.168.1.7:5060
04/15-16:37:35.135439  [**] [1:1100002:1] Something is Wrong with SIP ACK [**]
Priority: 0] {UDP} 192.168.1.8:5060 -> 192.168.1.7:5060
```

Figure 3.Detection Malformed ACK Message

5.3. Malicious SIP Cancel Detection



```
 has been detected [**] [Priority: 0] {UDP} 192.168.1.7 -> 192.168.1.9
04/15-17:30:13.166254  [**] [1:1000009:3] Malformed SIP Cancel detected [**] [Pr
iority: 0] {UDP} 192.168.1.7 -> 192.168.1.9
04/15-17:30:13.673650  [**] [1:11000017:1] Malformed CANCEL has been detected>NO
 content length field [**] [Priority: 0] {UDP} 192.168.1.7:64837 -> 192.168.1.9:
5060
04/15-17:30:13.673650  [**] [1:11000014:1] Malformed Cancel with diff User Agent
 has been detected [**] [Priority: 0] {UDP} 192.168.1.7:64837 -> 192.168.1.9:506
0
04/15-17:30:13.673650  [**] [1:1000009:3] Malformed SIP Cancel detected [**] [Pr
iority: 0] {UDP} 192.168.1.7:64837 -> 192.168.1.9:5060
04/15-17:30:14.183922  [**] [1:11000017:1] Malformed CANCEL has been detected>NO
 content length field [**] [Priority: 0] {UDP} 192.168.1.7:64838 -> 192.168.1.9:
5060
04/15-17:30:14.183922  [**] [1:11000014:1] Malformed Cancel with diff User Agent
 has been detected [**] [Priority: 0] {UDP} 192.168.1.7:64838 -> 192.168.1.9:506
0
04/15-17:30:14.183922  [**] [1:1000009:3] Malformed SIP Cancel detected [**] [Pr
iority: 0] {UDP} 192.168.1.7:64838 -> 192.168.1.9:5060
04/15-17:30:14.693213  [**] [1:11000017:1] Malformed CANCEL has been detected>NO
 content length field [**] [Priority: 0] {UDP} 192.168.1.7:64839 -> 192.168.1.9:
5060
04/15-17:30:14.693213  [**] [1:11000014:1] Malformed Cancel with diff User Agent
 has been detected [**] [Priority: 0] {UDP} 192.168.1.7:64839 -> 192.168.1.9:506
0
04/15-17:30:14.693213  [**] [1:1000009:3] Malformed SIP Cancel detected [**] [Pr
iority: 0] {UDP} 192.168.1.7:64839 -> 192.168.1.9:5060
04/15-17:30:15.199286  [**] [1:11000017:1] Malformed CANCEL has been detected>NO
 content length field [**] [Priority: 0] {UDP} 192.168.1.7:64840 -> 192.168.1.9:
5060
04/15-17:30:15.199286  [**] [1:11000014:1] Malformed Cancel with diff User Agent
 has been detected [**] [Priority: 0] {UDP} 192.168.1.7:64840 -> 192.168.1.9:506
0
04/15-17:30:15.199286  [**] [1:1000009:3] Malformed SIP Cancel detected [**] [Pr
iority: 0] {UDP} 192.168.1.7:64840 -> 192.168.1.9:5060
04/15-17:30:15.707233  [**] [1:11000017:1] Malformed CANCEL has been detected>NO
 content length field [**] [Priority: 0] {UDP} 192.168.1.7:64841 -> 192.168.1.9:
5060
04/15-17:30:15.707233  [**] [1:11000014:1] Malformed Cancel with diff User Agent
 has been detected [**] [Priority: 0] {UDP} 192.168.1.7:64841 -> 192.168.1.9:506
0
04/15-17:30:15.707233  [**] [1:1000009:3] Malformed SIP Cancel detected [**] [Pr
iority: 0] {UDP} 192.168.1.7:64841 -> 192.168.1.9:5060
04/15-17:30:16.214998  [**] [1:11000017:1] Malformed CANCEL has been detected>NO
 content length field [**] [Priority: 0] {UDP} 192.168.1.7:64842 -> 192.168.1.9:
5060
04/15-17:30:16.214998  [**] [1:11000014:1] Malformed Cancel with diff User Agent
 has been detected [**] [Priority: 0] {UDP} 192.168.1.7:64842 -> 192.168.1.9:506
0
04/15-17:30:16.214998  [**] [1:1000009:3] Malformed SIP Cancel detected [**] [Pr
iority: 0] {UDP} 192.168.1.7:64842 -> 192.168.1.9:5060
04/15-17:30:16.723107  [**] [1:11000017:1] Malformed CANCEL has been detected>NO
 content length field [**] [Priority: 0] {UDP} 192.168.1.7:64843 -> 192.168.1.9:
5060
04/15-17:30:16.723107  [**] [1:11000014:1] Malformed Cancel with diff User Agent
 has been detected [**] [Priority: 0] {UDP} 192.168.1.7:64843 -> 192.168.1.9:506
0
```

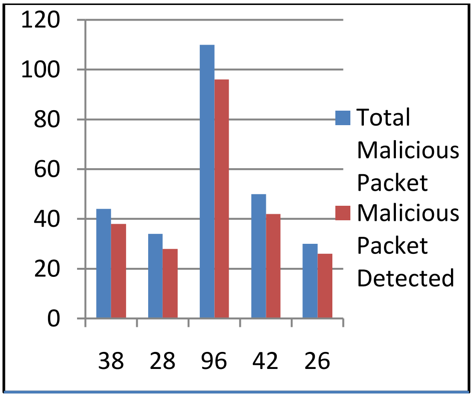
Figure 4.Detection Malformed ACK Message

5.4. Test Statistics

Table 4. Session log

Sessions	Total number of packets	SIP Original Packets	SIP Malicious Packets generated in the network by VoIPER(X)	Malicious Packet Alerts Generated By IDS(Y)	Accuracy (X/Y)*100 %
Session 1	100	56	44	38	86.36
Session 2	80	46	34	28	82.32
Session 3	165	55	110	96	87.27
Session 4	100	50	50	42	84
Session 5	75	45	30	26	86.6

Following plots show the consistency in the accuracy of the proposed system.



6. CONCLUSION

VoIP SIP Security is a very critical area of research.SIP being a widely used call initialization protocol; it requires great deal of protection. We have extensively researched the available security solutions in VoIP Security and have implemented cryptographic countermeasure such as TLS. Implementing TLS led us to a very important problem of compatibility between soft phones. Some soft phones like zoipersupport SRTP,while blink soft client supports TLS, ZRTP. Hence a need of platform independent and accurate approach arouse, leading us to design an Intrusion Detection System for SIP Security. The potential problem in existing IDS is less accuracy in detecting malformed and spoofed messages, which is to some extent solved by our proposed approach.

7. REFERENCES

[1]CHEN, E. Y. 2006. Detecting dos attacks on SIP systems. In *Proceedings of the 1st IEEE Workshop on VoIP Management and Security. 53–58.*

[2] D. Butcher, X. Li, and J. Guo. *Security challenge and defense in VoIP infrastructures*. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 37(6):1152–1162, November 2007.

[3] RFC 3261, *SIP: Session Initiation Protocol*

[4] Karapantazis, S. and Pavlidou, F. (2009). VoIP: a comprehensive survey on a promising technology. *Computer Networks*, 53(12):2050–2090.

[5] Ge Zhang. Towards Secure SIP Signaling Service for VoIP applications.Karlstad University Studies, 2009.

[6]"Voice over Internet Protocol. Definition and Overview". International Engineering Consortium. 2007 [http://www.iec.org/online/tutorials/int_tele/index.asp]

[7] Prof. Bela Shah. Reshma Patel"An approach towards SIP Based Instrusion Detection System", VIER Journal of Engineering, Volume 1, 2014.