An Intelligent SIP Message Parser for Detecting and Mitigating DDoS Attacks

Abdullah Akbar
Research Scholar, Department of Computer Science and Engineering
Jawaharlal Nehru Technological University Hyderabad, Hyderabad, Telangana, India

Dr. S. Mahaboob Basha
Professor, Department of Computer Science and Engineering
Al Habeeb College of Engineering & Technology, Ranga Reddy District, Telangana, India

Dr. Syed Abdul Sattar
Professor, Department of Electronics and Communication Engineering
Royal Institute of Technology and Science, Ranga Reddy District, Telangana, India

Dr. Syed Raziuddin
Professor, Department of Computer Science and Engineering
Deccan College of Engineering & Technology, Hyderabad, Telangana, India

Abstract- Voice over Internet Protocol (VOIP) is widely used for multimedia and voice calls transmission through internet telephony. Session Initiation Protocol (SIP) is predominantly used in establishing multimedia session among the nodes deployed in VoIP services implementations. The increasing usage of SIP servers for multimedia transmissions has resulted in a high and frequent experience of Distributed Denial of Service (DDoS) attacks. In this paper, we propose a solution through SIP message parser intelligence to detect DDoS attacks in the VoIP networks. To identify the malformed messages, we have used Support Vector Machine (SVM) based classifier mechanism. Our parser reduces time complexity better as compared to other methods since our method uses kernel tree analysis which does not require the representation of the entire SIP message as a feature space. Our parser have achieved 99.89% detection accuracy while tested with several different types of malformed SIP messages.

Keywords – SIP (Session Initiation Protocol), DDoS (Distributed Denial of Service), VOIP (Voice over Internet Protocol), SVM (Support Vector Machine)

I. INTRODUCTION

SIP is known as application layer signaling protocol which is used widely in Next Generation Networks and 3G IP (Internet Protocol) multimedia subsystems. It is basically used for initiation, management and termination of the voice calls and video call sessions in a VoIP network. It is a simple, open and scalable signaling protocol working on the principle of IP-Packet network. SIP server has predominant functionalities to consume average CPU time - Rachid El Khavari [2008]. The first and foremost functionality is parsing. Parsing translates the SIP messages into an internal structure utilized for further processing methods. The second step is transaction maintenance. This is used to maintain transaction state as specified by the protocol. The third functionality is message sending where we set the SIP header fields and is used to construct the outgoing SIP messages. It is also used to resolves the next hop address and calculate the checksum. Then it adds packet headers and delivers the packet to the IP Layer. SIP message is used for a request or an acknowledgement to a corresponding request. The request and acknowledgement is written in the header and message body. SIP messages are known as text based like HTTP format. The following message is well formulated SIP Message - Raihana Ferdous et.al [2012].

```
T INVITE sip:me@myorg.gr SIP/2.0
To: Researcher abdullah <dgen@theirorg.gr>
From: Abdullah Akbar
```

```
<sip:akbar@myorg.gr>;tag=76341
CSeq: 2 INVITE                                              [SIP Headers]
Authorization: Digest username="akbar",
realm="192.251.164.23", algorithm="md5",
uri="SIP:197.250.160.71",
nonce="41358a56632c7b3d382b39e0979ca5f98b9fa03b",
response="a6455dce70e7b098d127220584cd57"
Contact: <SIP:199.250.160.71:9380>;>
Content-Type: application/sdp

v=0
o=Ayesha Jahan 2890844526 IN IP4 wife.high-drama.org
c=IN IP4 102.105.108.102                                    [Session Description]
t=0 0
m=audio 49570 RTP/AVP 0                                     [Body]
a=rtpmap:0 PCMU/8050
```

According to RFC 3261, the SIP stacks are capable of processing the messages used for REGISTER, INVITE, ACKNOWLEDGE, CANCEL, BYE and OPTIONS - Lukas Kramer et.al. [2015].

SIP based multimedia transmission can be established between two users or callers. User A can send a SIP INVITE message to the corresponding proxy and the proxy can forward the message to the user B. At this junction, the SIP proxy server will parse the incoming message and identify the incoming request. It transforms into essential understandable format through parsing and stores it in the server for next action to be taken. Then it will read the address where the message has to be sent and then it will send the message to the appropriate user B in the VoIP network.

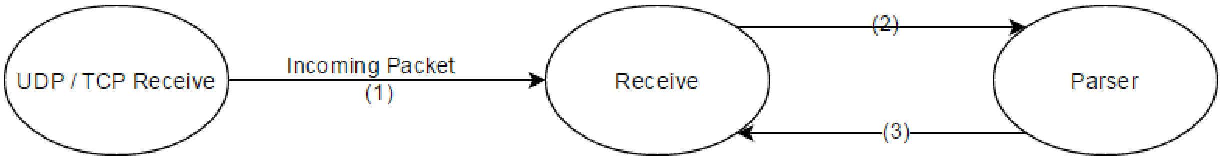

Figure 1. Processing / Parsing of a SIP message in SIP Proxy server

SIP servers are capable of performing the parsing process for well-formed SIP messages as depicted in Figure 1. A well formulated message will carry all the essential information in the header and body of the SIP message. Session Initiation Protocol is capable of initiating, terminating, managing the messages in the VoIP networks. During the session establishment time any attacker can send a malformed or a bogus message with various combinations. This kind of syntax is different from the well formulated SIP images. The SIP parser can’t understand the syntax of the malformed messages and subsequently drops them. This type of messages may be invalid and can’t be sent to the designated user or client system -Tasos Dagiuklas [2005].

II. RELATED WORK

SIP servers can perform different functionalities like parsing, transaction management, message transmission and dropping, withdrawing etc. SIP parsing predominantly perform the transformation of SIP message into a different format suitable for internal analysis used for further actions and functionalities. Transaction management keeps the message in a state suitable for transaction by the protocol - Jia Zou et.al [2015].

SIP parsers are predominantly utilized in SIP hierarchy IMS (IP Multimedia Subsystem) networks to perform input streaming to build specific and appropriate SIP messages. The headers of the SIP messages will be checked and compared with the standard syntax available in the SIP parser and approved messages will be sent it to the designated user or node of the network - Dimitris Geneiatakis et.al [2015].

SIP messages would be processed by the SIP parser and then sent to SIP server for further processing. The parser can read the header of SIP messages directly from the input stream. SIP parser can process the messages of both TCP and UDP transport protocols. The structured messages would be parsed and send to server for processing. The unstructured messages can be read and dropped by the SIP parser - Zifu Fan, Xiaoyu Wan [2009].

DDoS attacks are seemingly the more commonly observed attacks in the IMS networks. An example of such a DDoS attack is portrayed in Figure 2. The vulnerabilities in application and protocol stack are markedly observed and can influence the operating system performance. The attacker can instigate the DDoS attack from his system to the target machine in IMS networks. The result of DDoS attack can expose the vulnerabilities in application servers, network stacks and gives rise to more general operating system vulnerabilities. The impact of such vulnerabilities can't be predicted. They can influence the projects and system resources with more massive attacks and make them destroyed or eavesdropped. DDoS attacks from internal or external source prediction with normal mechanism are not impossible and unstoppable. The mounting of attack is generally performed with unpredictable and uncommon methods. There is no proper methodology used to launch a DDoS attack to destroy a target network. The attacker will have several different choices to enforce the Distributed Denial of Service Attacks - Md. Ruhul Islam et.al [2011].

SIP message is defined to be text based protocol session establishment and negotiation of session constraints. It is incorporated via transport layer transmission. SIP messages can exchange the signaling information according to the elementary client server principle. SIP messages predominantly classified as SIP requests and SIP responses. SIP messages are rich with header field and message body. This predominant quality has been used by the SIP parsing mechanism to identify the malformed messages and appropriate messages –Rachid El Khayari [2008].

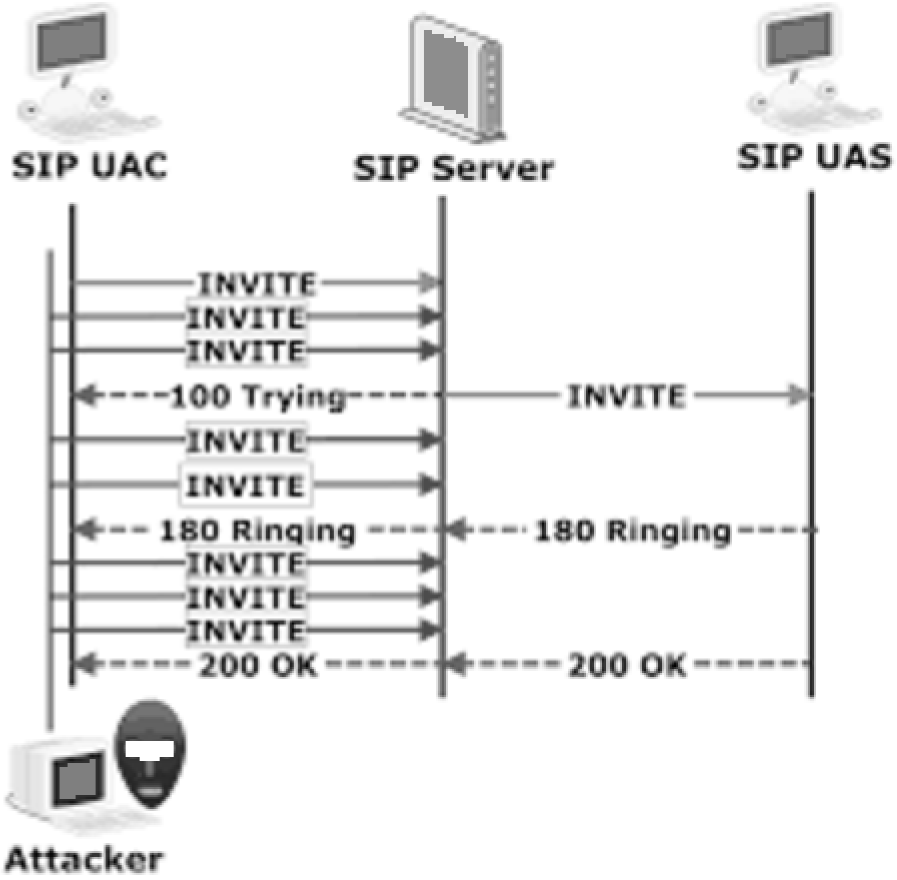

Figure 2. DDoS attack in IMS networks

SIP parsing model is very much possible in various IMS network entities to handle the potential vulnerabilities and malformed SIP messages generated through Distributed Denial of Service attacks. In this method the malformed SIP messages are generated through DDoS attacks - Lukas Kramer et.al. [2015]. The SIP server would be kept in SIP parsing mode with self-defined rules. SIP parsing mode is activated to protect the network from malformed messages with malformed values and structure. Once the malformed messages are generated and sent to the SIP server which is activated with SIP parsing, then the SIP parsing would read the messages and identify the malformed or DDoS attacks. The malformed SIP messages would be dropped by the SIP parsing server component - Yulong Wang [2013].

IMS network is rich with layered architecture consists of application plane, control plane and user plane. SIP is regarded as the most suitable application layer control protocol for IMS networks. If the Distributed Denial of Service attack generates any vulnerability during SIP processing, the malformed SIP message could enter into the IMS network and create abnormal state and affect the quality of services of the IMS network. As a result the attached assets and services of IMS would be damaged – Hongbin Li et.al. [2010]. Therefore to administer the situation SIP parsing mode is introduced. The SIP parsing mode parses the SIP messages received by the SIP server and manipulate the SIP fields after they are extracted by SIP entity. The SIP parsing can transform the messages into a separate format to perform storage, string segmentation, matching and dropping and sending to the designated node etc. - Dimitris Geneiatakis et.al [2008]. SIP parsing mode is specific to IMS network alone. When the DDoS attack generates the malformed SIP messages it can be parsed easily during the SIP parsing mode. The specific values of SIP fields available in SIP messages comply with fixed format. This format is different from the format generated by the DDoS attacks and malformed SIP messages - Ajay Kumar Shrestha et.al [2014]. The parsing mode can test match the syntax of the SIP messages generated by DDoS attacks with the standard format of SIP messages header and body syntax as specified in the introduction of this paper. Then the functionality of SIP parser can drop the message from transmission of network. This is the core functionality of the SIP parser to identify the DDoS attacks and its malformed SIP messages.

III. Proposed Architecture

The proposed malformed SIP message detector consists of a lexical analyzer and an intelligent SIP parser as shown in Figure 3. The lexical analyzer scans the incoming SIP message and breaks the message into lexemes and stores into a table according to their class. The lexical analyzer discards syntactically incorrect SIP messages. Syntactically correct SIP messages are passed to Support Vector Machine (SVM) based on intelligent SIP parsing. SIP messages are represented into a structured data structure like syntax parse tree in order to apply machine learning techniques. Basically the intelligent SIP parser is a classifier which classifies the incoming syntactically correct SIP messages as valid SIP message or invalid (malformed) using tree kernel method.

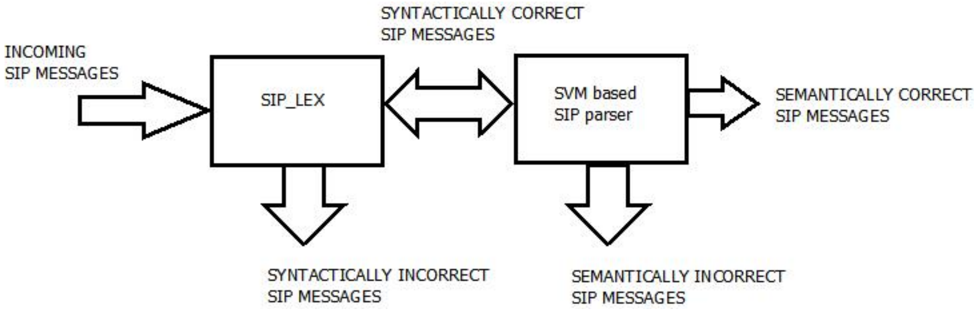

Figure 3. SIP Message Parsing Architecture

IV. Implementation Methology

The main aim over here is to illustrate the SIP parsing technique which is used to detect malformed SIP messages emanating from a network of bots. Existing SIP parsers use signature based technique to detect the malformed messages. The disadvantage of this technique is they cannot process large datasets. Some machine learning methods like multi class classifier approach suffer with the inability to represent the entire SIP message into a feature space. We have used SVM based technique to categorize incoming SIP messages as well-formed and malformed. We represent the incoming SIP message as a parse tree (T2). We will select one of the valid SIP parse tree (T1) from database and apply kernel tree method on both structures to calculate similarity between T1 and T2. Similarity score is a feature vector used for training the SVM. Training is carried out on subset of known valid messages and malformed messages until we get reasonable detection rate specified in SIP standard. Once SVM classifier is successfully trained it is able to detect any new SIP message either as malformed or well-formed. This entire flow is described aptly in Figure 4.

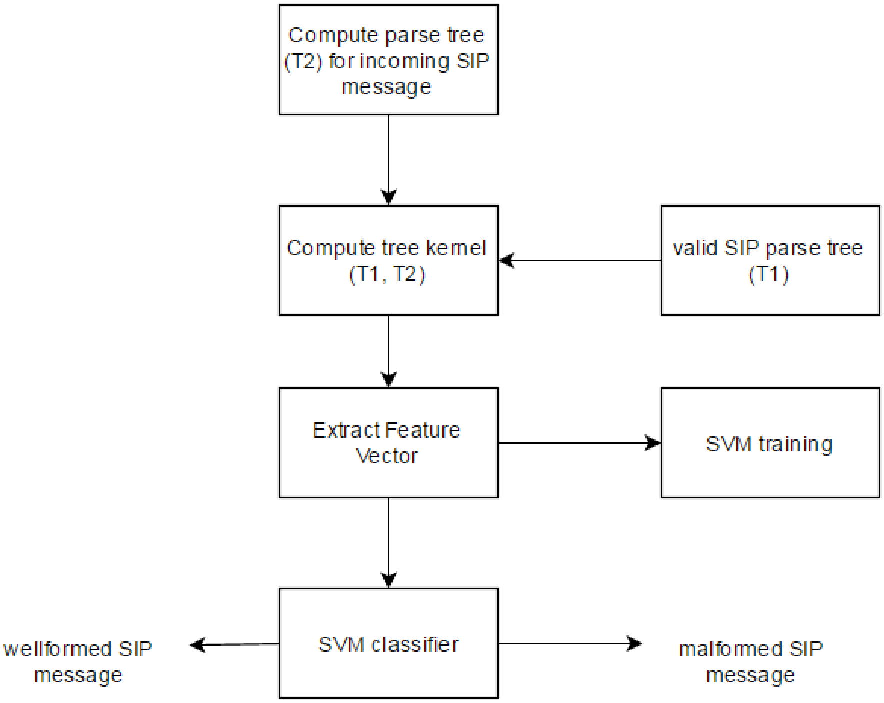
Compute parse tree (T2) for incoming SIP message
Compute tree kernel (T1, T2)
valid SIP parse tree (T1)
Extract Feature Vector
SVM training
SVM classifier
wellformed SIP message
malformed SIP message

Figure 4. SIP Message Classification using Support Vector Machine

III. PERFORMANCE EVALUATION AND RESULTS

To evaluate the performance of SIP parser in terms of detection accuracy and time to detect we have used a large number of SIP traces consisting of several types of malformed message as described in Table I. Malformed SIP messages are in accordance to RFC 4475 which describes several SIP traces to trouble the SIP applications. Valid SIP messages given for parser are according to RFC 3261. A total of 5000 SIP message are generated by a message generator consisting of both malformed and valid messages. A total of 500 well-formed messages and 4500 malformed messages are categorized into several types as shown below in Table I.

TABLE I - TEST SCENARIOS USED FOR PERFORMANCE EVALUATON

Test Scenario	Description	No of messages
TS-1	Error in Request line	512
TS-2	Syntactic error in mandatory field	455
TS-3	Missing mandatory header	1125
TS-4	Duplicate entry in unique header	328
TS-5	Presence of invalid string in message	456
TS-6	Message with multiple Request method	236
TS-7	Message with unknown content	543
TS-8	Message with invalid method name	845

We can conclude from test results shown in Table II, that our intelligent SIP parser can better detect DDoS attack compared to both rule based and multiple classifier system based techniques.

TABLE II - DETECTION RATES FOR PROPOSED INTELLIGENT SIP PARSER

TEST SCENARIO	Detection Rate (%)		
	Rule based	Multiple classifier system	Proposed Method
TS-1	93.3	97.2	99.2
TS-2	91.2	96.1	98.6
TS-3	94.8	95.2	98.5
TS-4	95.3	97.3	99.4
TS-5	98.4	98.8	99.8
TS-6	97.5	98.4	99.5
TS-7	95.3	97.4	99.3
TS-8	94.5	96.5	98.5

We have achieved 99.1% detection rate for SIP malformed messages as detailed in Table II.

IV.CONCLUSION

This paper has analyzed the possible attacks to SIP networks and the simple mechanism of SIP server functionality. Based on the SIP messages construction with header and body, the SIP parser is distinguishing the malformed messages and well-formed messages with SVM based classifier. The paper has suggested a novel technique for SIP parsing mechanism to detect the malformed messages. This mechanism can effectively encounter the malformed messages generated by the DDoS attackers with faster detection time accuracy compared to conventional approaches.

REFERENCES

[1] Dimitris Geneiatakis, Georgios Kambourakis, Tasos Dagiuklas, Costas Lambrinoudakis and Stefanos Gritzalis [2004] Framework for Detecting Malformed Messages in SIP Networks published in the framework of the IST 2004-005892 project SNOCER, Funded By European Union.

[2] Jia Zou, Wei Xue, Zhiyong Liang, Yixin Zhao, Bo Yang, Ling Shao [2015] SIP Parsing Offload: Design and Performance

[3] Zifu Fan, Xiaoyu Wan [2009] The Design And Realization Of Sip Dos Attack Detection Plugin Based On Balanced Message Number Principle published in IEEE Proceedings of ICCTA2009

[4] Hongbin Li, Hu Lin, Xuehua Yang, Feng Liu [2010] A Rules-Based Intrusion Detection and Prevenetion Framework Against SIP Malformed Messages Attacks published in Proceedings of IC-BNMT2010 of IEEE

[5] Sohil Aziz, Mehroz Gul [2010] A Self Learning Model for Detecting SIP Malformed message attacks published in IEEE proceeding of IC-BNM 2010

[6] I. Skuliber, V. Jankovic, R. Zec, Ericsson Nikola Tesla d.d., Zagreb, Croatia [2011] Multicore SIP Parsing with Imperative and Declarative Implementations published in IEEE 2011

[7] Raihana Ferdous, Renato Lo Cigno, Alessandro Zorat [2012] On the Use of SVMs to Detect Anomalies in a Stream of SIP Messages Published in 2012 11th International Conference on Machine Learning and Applications978-0-7695-4913-2/12 $26.00 © 2012 IEEE

[8] Ajay Kumar Shrestha [2014] Security of SIP-Based Infrastructure against Malicious Message Attacks published in 978-1-4799-6399-7/14 ©2014 IEEE

[9] Lukas Kramer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, Christian Rossow [2015] AmpPot: Monitoring and Defending Against Amplication DDoS Attacks published in springer 2015

[10] Yulong Wang, Dong Wang and Lei Wang [2013] A Parsing Mode based Method for Malformed SIP Messages Testing for IMS network published in Journal Of Networks, VOL. 8, NO. 4, APRIL 2013

[11] Md. Ruhul Islam, Smarajit Ghosh [2011] Secure SIP from DoS based Massage Flooding Attack International Journal of Computer Applications in Engineering Sciences [VOL I, ISSUE II, JUNE 2011]

[12] Tasos Dagiuklas, Dimitris Geneiatakis, George Kambourakis, Dorgham Sisalem, Sven Ehlert, Jens Fiedler, Jiří Markl, Michal Rokos, Olivier Botron, Jesus Rodriguez and Juntong Liu [2005] Low Cost Tools for Secure and Highly Available VoIP Communication Services

[13] Dimitris Geneiatakis, Tasos Dagiuklas, Costas Lambrinoudakis, Georgios Kambourakis and Stefanos Gritzalis [2008] Novel Protecting Mechanism for SIP-Based Infrastructure against Malformed Message Attacks:Performance Evaluation Study

[14] Rachid El Khavari [2008] SPAM over Internet Telephony and how to deal with it published in Technische Universitat Darmstadt

[15] Anil Mehta, Neda Hantehzadeh, Vijay K. Gurbani, Tin Kam Ho and Flavia Sancier [2012] On using multiple classifier systems for Session Initiation Protocol (SIP) anomaly detection published in IEEE ICC 2012 - Communication and Information Systems Security Symposium

[16] Nikos Vrakas, Costas Lambrinoudakis [2013] An intrusion detection and prevention system for IMS and VoIP services published in Int. J. Inf. Secur. (2013) 12:201–217 DOI 10.1007/s10207-012-0187-0 Regular Contribution

[17] Jin Tang, Yu Cheng and Yong Hao [2012] Detection and Prevention of SIP Flooding Attacks in Voice over IP Networks published in IEEE Infocom 2012 Proceedings

[18] A. Mehta, N. Hantehzadeh, V. K. Gurbani, T. K. Ho and F. Sander, "On using multiple classifier systems for Session Initiation Protocol (SIP) anomaly detection," Communications (ICC), 2012 IEEE International Conference on, Ottawa, ON, 2012, pp. 1101-1106.