Analysis of DDoS Attacks in Heterogeneous VoIP Networks: A Survey

Amita Chauhan, Nitish Mahajan, Harish Kumar, Sakshi Kaushal

Abstract:* *Significant changes have been taking place in interactive media transmission as traditional circuit-based PSTN is substituted by packet-based networks called next generation networks (NGN) that use internet protocol (IP). NGN is believed to completely restructure the communication systems. Voice over IP (VoIP) with its cost effective deployment has transpired as a paramount instrument for multimedia communication. Session Initiation Protocol (SIP) is currently the most popular application layer protocol used for signalling purposes to control VoIP connections between communicating parties. SIP, being a simple text-based protocol, is pregnable to various security breaches and Distributed Denial of Service (DDoS) attacks happen to be one of the most devastating cyber threats. In this paper, a detailed analysis on detection of DDoS attacks in SIP based VoIP networks is presented. Machine learning evolves as a building block in cyber security solutions with a large number of techniques available to automate the detection of network attacks and make robust and quick network defence systems. Numerous approaches exist in state of the art for identifying anomalous behaviour in VoIP traffic. This paper includes important aspects that need to be taken into account by the professionals when developing cyber security systems for such networks.

Index Terms:* *Distributed Denial of Service (DDoS), Next Generation Networks (NGN), Session Initiation Protocol (SIP), Voice over IP (VoIP).

I. INTRODUCTION

Voice over Internet Protocol (VoIP) technology has emerged as a strapping alternative to Public Switched Telephone Network (PSTN). VoIP constitutes a set of protocols that allow communication of multimedia (text, audio and video) over an IP network and provides mechanisms for migration from PSTN. Session Initiation Protocol (SIP) is the most popular VoIP protocol that is used for signalling multimedia calls over IP. Functions provided by SIP include controlling the signal during the establishment, execution and termination phases of multimedia sessions between two or more participants. It provides VoIP applications with the same kind of reliability and high quality as delivered by traditional telephone systems. SIP is a text-based protocol which has an HTTP-like request/response transactional model making it easy to program.

Although SIP has gained popularity in recent years, being a text-based protocol it has some security vulnerabilities. The techniques which are used for the security of VoIP/SIP based data are still in the development phase. With the wide deployment of VoIP networks, it has become extremely important to address the security issues of SIP servers. In recent past numerous security attacks have surfaced in VoIP/SIP networks. Some of the breaches that occur in SIP based networks most often are registration hijacking, impersonating a server, session hijacking, tampering with message bodies, denial of service (DoS) and amplification, tearing down sessions and bots and distributed denial of service (DDoS) attacks. Among all, DDoS attacks are one of the most scandalous cyber threats. A DDoS attack is a kind of denial of service in which multiple systems coordinate to attack one or more targets. The objective behind DDoS attacks is to cause partial or total unavailability of the services provided by the computer systems. It is achieved by exhausting the processing and connectivity resources of the targets so as to make legitimate users unable to access the services.

DDoS attacks are broadly categorized into flooding, misuse and unintentional attacks. In a flooding attack a large number of messages are sent to the SIP servers to overwhelm them. The flooding attacks to which SIP is vulnerable are INVITE flooding, REGISTER flooding, BYE flooding, multi-attribute flooding and TCP-SYN flooding. Misuse attacks are those in which a hacker misuses the services by modifying SIP messages to cancel or redirect calls. In unintentional attacks the attacker targets the supporting services like DNS, call billing in order to distract or restrict the service. Fig. 1 shows the major security attacks that happen in VoIP/SIP networks.

DDoS attacks have devastating consequences on SIP based networks because of the one-to-many relation between the attacker systems and the target system. It is forecasted by the scientific community that the disruptive power of DDoS attacks, their sophisticated implementation and ability to cause potential damage will tend to increase at a very high rate [9],[14],[16],[17],[24]. It has been reported that 93% of the DDoS attacks are application layer DDoS attacks [3]. A Digital Attack Map gives a real-time overview of current DDoS attacks and sceptical networks activities that are happening around the globe at any particular time. Fig. 2 shows one such analysis for Nov 16, 2018 [4].

Well known organizations were found to be among the victims of DDoS attacks. Github, for instance, suffered a massive DDoS attack that took it down for 6 days [19]. According to Kaspersky [5], in quarter one of 2016, the longest DDoS attacks lasted for 197 hours (8.2 days). The longest DDoS attack in quarter two of 2018 lasted 258 hours (approximately 11 days) [6] The frequency of DDoS attacks, as reported by Cox Business in 2017, has increased more than 2.5 times since 2014 [1] The size of DDoS attacks has become huge nowadays. Arbor networks reported a major DDoS attack on a US service provider that suffered an attack size of 1.7 Tbps [2],[3].

Revised Manuscript Received on April 12, 2019.

Amita Chauhan, UIET, Panjab University, Chandigarh, India.
Nitish Mahajan, UIET, Panjab University, Chandigarh, India.
Harish Kumar, UIET, Panjab University, Chandigarh, India.
Sakshi Kaushal, UIET, Panjab University, Chandigarh, India.

DDoS attacks may have a negative impact on an organization as the target system becomes unable to provide sevices to its legitimate users or customers.

The downtime of servers results in the loss of revenue and damages reputation of the service providers. Hence, it is essential to develop apposite solutions for detection of these ruinous attacks. The adoption of machine learning in identifying security attacks has become necessary as cyber threats continue to grow at a high rate. Sophisticated strategies are being developed by hackers to bypass the traditional cyber security systems. Hence, in order to stay ahead, intelligent algorithms that are complex and even-more powerful need to be deployed by the network defence systems. In this paper, different machine learning based anomaly detection models that detect DDoS attacks in VoIP networks are presented.

II. RESULTS & DISCUSSIONS

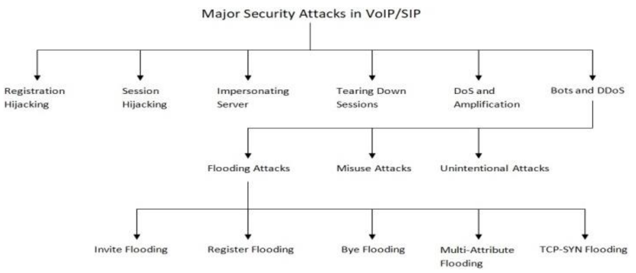

Fig. 1. Major Security Attacks in VoIP/SIP

The downtime of servers results in the loss of revenue and damages reputation of the service providers. Hence, it is essential to develop apposite solutions for detection of these ruinous attacks. The adoption of machine learning in identifying security attacks has become necessary as cyber threats continue to grow at a high rate. Sophisticated strategies are being developed by hackers to bypass the traditional cyber security systems. Hence, in order to stay ahead, intelligent algorithms that are complex and even-more powerful need to be deployed by the network defence systems. In this paper, different machine learning based anomaly detection models that detect DDoS attacks in VoIP networks are presented.

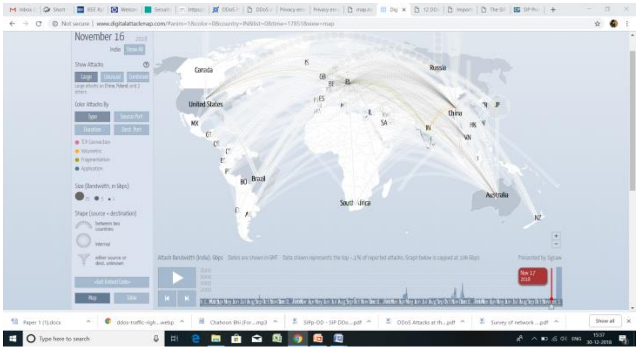

Fig. 2. Digital Attack Map [4]

III. LITERATURE REVIEW

This section provides details of the methodologies present in state-of-the-art to detect and prevent DDoS attacks.

Akbar M.A. and Farooq M. [8] presented a real-time traffic classification model that identifies SIP DoS and DDoS attacks. The system conducts packet-based analysis by considering the spatial and temporal feature sets which significantly reduces memory and processing overheads as compared to those related with flow-based anaylsis. Authors collected real-time SIP traffic provided by a VoIP vender and tested the proposed system on this data by introducing malicious packets in it and reported high accuracy as compared to F-SVM and Hellinger Distance schemes.

Akbar A., Basha S.M., Sattar S.A. and Raziuddin S. [7] A Support vector Machine based system with an intelligent parser for SIP messages is proposed for identifying DDoS attacks. The model does not need to represent SIP packets as a feature space but uses data structures like syntax parse trees to analyze and collect syntactically valid packets, thus, reduces time complexity.

Tsiatsikas Z., Geneiatakis D., Kambourakis G., and Gritzalis S. [23] examined the suitability of certain popular Machine Learning techniques in identifying SIP based DDoS attacks. Authors tested each ML classifier for detection accuracy and processing overhead in 15 different scenarios of DoS and DDoS attacks and concluded that ML models need to be experimented further to achieve better accuracy in real world.

Golait D. and Hubballi N. [12] Explores detection of attacks related to flooding and attacks that are executed in a coordinated manner. Authors modeled different SIP operations in the form of discrete event systems (DES). They designed a state transition machine named as “probabilistic counting deterministic timed automata (PCDTA)” for describing the SIP operations’ behaviour. An anomaly detection technique identifies the anomalies that occur in the DES model these anomalies are then mapped to existing DoS attacks. The paper illustrates various algorithms for DoS attack detection by deploying suggested state-transition based model. Authors experimented with a SIP traffic simulated using computers and reported that the proposed DES model has a high accuracy and detection rate for detecting the anomalies (attacks).

Kurt B., Yildiz C., Ceritli T.Y., Sankur B. and Cemgil A.T. [15] put forward a anomly detection model using bayesian change point technique. The framework follows a hierarchical probability based hidden Markov model. The model associates network traffic features and server load statistics to hidden variables. The hidden variables reflect state of the system in terms of change or no-change. The ultimate goal of the model is to get the posterior probability calculated at fixed time intervals that indicates change. In addition to the change point model, they deployed a model for SIP network simulation. This model follows a probabilistic approach to emulate real-time SIP traffic.

Tas I.M., Ugurdogan B. and Baktir S. [21] implemented a controlled environment for simulating DDoS attacks on VoIP/SIP communication systems. They developed two types of DDoS attacks namely “incomplete INVITE transaction DDoS with non-responding destination” and “incomplete INVITE dialog DDoS without ACK” against SIP servers using IP spoofing technique and exploiting SIP

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

transmission vulnerabilities. Authors also propose a two phased defense mechanism against these attacks. First phase deals with network flow statistics and decides flow thresholds to detect DDoS attacks. If the first phase flags the traffic as irregular, second phase is triggered that uses rule-based mechanisms to detect anomalies.

Semerci M., Cemgil A.T. and Sankur B. [20] proposed a system deploying two level mechanism for intelligent DDoS detection and attacker identification. The two levels of the system are: (i) Monitor for the detection of presence of a DDoS attack and (ii) Discriminator for identifying the attacker. The monitor is a change-point model that traces the changes in Mahalanobis distances between selected feature vectors. The discriminator separates malicious and innocent users by running a clustering model over the similarity scores based on behavioural patterns between the users. A SIP based simulated telephone network is used to deploy the proposed model.

Dassouki K., Safa H., Nassar M. and Hijazi A. [10] proposed an adaptive and dynamic INVITE flood detection and mitigation approach that aims to protect SIP based networks from flooding attacks. The presented framework comprises of two algorithms: one for the detection of attacks which uses SIP's temporal characteristics so as to get quick and correct detection and another one for mitigation which is based on the whitelist history composed of SIP session's fingerprints. There are three major entities in the approach presented by the authors, namely (i) flood attack detector, (ii) normal and abnormal IP finger-print databases and (iii) filter entity, which work together to provide solution for attack identification and mitigation. Virtual machines are geographically distributed at distant cloud data centers are used to perform experiments.

Dayanandam G., Reddy E.S. and Babu D.B. [11] employed machine learning models for detection and prediction of DDoS attacks on SIP server. They used Stochastic Gradient Boosting Model (GBM), Generalized Linear Model (GLM), Random Forest (RF) and Neural Networks (NN) regression algorithms and proved that they perform better than KNN and SVM algorithms.

Tsiatsikas Z. et al. [22] focuses on the efficacy of Machine Learning (ML) techniques in detecting DoS attacks in SIP-based VoIP networks. Authors conducted experimentations with five different anomaly detection classifier models. They compared their results for DDoS detection with those of two other anomaly-based methods of detection: Entropy and Hellinger Distance. Their outcomes conveyed that Machine Learning based detection, in the general case, provides a promising false alarm rate and stands out similar methods in detecting DDoS attacks.

Guti´errez S.A. and Branch J.W. [13] presented a systematic literature survey to provide an approach to state of the art in employment of Machine Learning to detect DDoS attacks. Following a structured mapping study, authors selected relevant papers that were reviewed to identify the type of attacks addressed by their authors, the techniques that provide excellent performance and the techniques that corroborate their use in distributed environments. Authors, through this review, concluded that detection of application layer protocols is an important topic that researchers should take into consideration. They also concluded that objective of detection techniques must be to increase accuracy, reduce detection times and avoid false detections.

Safoine R., Mounir S. and Farchi A. [18] presented a study of different flooding detecting mechanisms. Authors compared two particular proposed techniques for anomaly detection and notifying users about possible intrusions. One of those detection algorithms provides solution according to the port number used to transmit the message. It was developed in C language and composed of three processes: collection of traffic from network, analysis of packet headers and detection of SIP based VoIP packets which are unprotected. The other one is a probabilistic solution with two phases: training phase that collects and builds standard VoIP SIP behavior profile based on Poisson distribution and testing phase that detects flooding attacks by comparing current SIP operation profile with the normal profiles built during training phase. Authors proposed a method for the detection of flooding attacks in VoIP networks which provides specific security algorithm depending on the characteristics of the ports used in the transmission. System raises an alarm whenever a packet is considered to be unprotected or as an attack.

IV. RESEARCH ISSUES

With the convergence towards next generation networks for multimedia communication, it has become necessary to have the support for traditional PSTN internetworking, high availability and scalability. SIP, being able to provide such services in next generation networks like 4G/LTE and 5G, emerges as the core protocol deployed at the application level of their architecture. Hence, securing SIP based information becomes critical and strong and intelligent measures need to be developed for this purpose.

It can be stipulated that for securing VoIP networks against DDoS attacks, researchers need to develop a test setup that depicts a real-time scenario. Hence, setting up an emulation system has become necessary for it helps in detecting and correcting erroneous events in the virtual environment before deploying the actual system. As carrier grade has evolved as a mandate for VoIP communication networks, emulation systems must be designed to achieve these standards. Carrier grade standards in real-time test setups provide low failure rates and minimize maintenance costs for the actual system making it reliable. These features alleviate the influence of equipment failures on services including hard, soft and transient failures, and allow system optimization so that it is able to meet the real-time performance requirements. The overall system setup must be designed to provide failover addressing capabilities and customized load balancing. This benefits the user with better availability and Quality of Service.

To develop an intelligent intrusion detection model

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

against DDoS attacks, a dataset that pictures actual VoIP traffic needs to be created. According to the survey, it is found that the datasets used by the researchers either do not contain purely SIP based information or are small in size. The key ingredient for machine learning based models is big data. Therefore, there is a need to create a huge database containing information specific to SIP based RTP packets and having features that are highly relevant and contribute to discriminate anomalous packets from the normal traffic. Also, the model should aim to increase accuracy, reduce detection times and avoid false detections.

V. CONCLUSION

Voice over IP has emerged as a strong substitute to PSTN in next generation networks for multimedia communication. In spite of being the most favored protocol to manage VoIP communication sessions, SIP is vulnerable to various security attacks with DDoS attacks being one of the most distructive cyber breaches. This paper provides a study of state-of-the-art for detection and prevention of DDoS attacks in SIP based VoIP networks. We stipulate key issues that should be taken into consideration by the cyber security experts while designing attack detection systems against these threats. As big data is the crucial element for machine learning, it is important to create a dataset that represents real world SIP traffic with a large number of RTP packets. Another essential aspect is development of real-like emulation environment to achieve carrier grade standards so as to have low failure rates and high reliability. Other important aspects include creation of dataset with only highly relevant and useful features specific to SIP/VoIP, developing models with high accuracy and low detection times and setting up a test system that has potential to address failover and provides tailored load balancing.

REFERENCES

1. Cox Business. (2017). 12 DDoS Statistics That Should Concern Business Leaders [Online]. Available: https://www.coxblue.com/12-ddos-statistics-thatshould-concern-business-leaders/
2. Iain Thomsan. (2018, March 5). World's biggest DDoS attack record broken after just five days [Online]. Available: https://www.theregister.co.uk/2018/03/05/worlds_biggest_ddos_attack_record_broken_after_just_five_days/
3. Cody Arsenault. (2018, September 13). DDoS Protection – Why It Is Needed Now More Than Ever [Online]. Available: https://www.keycdn.com/blog/ddos-protection
4. Google Ideas, Arbor Networks. Digital Attack Map [Online]. Available: http://www.digitalattackmap.com
5. Kaspersky Lab. (2016, April 28). Kaspersky DDoS Intelligence Report for Q1 2016 [Online]. Available: https://securelist.com/kaspersky-ddos-intelligence-report-for-q1-2016/74550/
6. Timur Ibragimov, Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. (2018, July 24). DDoS attacks in Q2 2018 [Online]. Available: https://securelist.com/ddos-report-in-q2-2018/86537/
7. Akbar, A., Basha, S.M., Sattar, S.A., Raziuddin, S.: An intelligent sip message parser for detecting and mitigating ddos attacks. Int. J. Innov. Eng. Technol. 7(2), 1–7 (2016)
8. Akbar, M.A., Farooq, M.: Securing sip-based voip infrastructure against flooding attacks and spam over ip telephony. Knowledge and information systems 38(2), 491–510 (2014)
9. Chen, C.M., Ou, Y.H., Tsai, Y.C.: Web botnet detection based on flow information. In: Computer Symposium (ICS), 2010 International, pp. 381–384. IEEE (2010)
10. Dassouki, K., Safa, H., Nassar, M., Hijazi, A.: Protecting from cloud-based sip flooding attacks by leveraging temporal and structural fingerprints. Computers & Security 70, 618–633 (2017)
11. Dayanandam, G., Reddy, E.S., Babu, D.B.: Regression algorithms for efficient detection and prediction of ddos attacks. In: 2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), pp. 215–219. IEEE (2017)
12. Golait, D., Hubballi, N.: Detecting anomalous behavior in voip systems: a discrete event system modeling. IEEE Transactions on Information Forensics and Security 12(3), 730– 745 (2017)
13. Gutierrez, S.A., Branch, J.W.: Application of machine learning techniques to distributed denial of service (ddos) attack detection : A systematic literature review (2013)
14. Kim, D., Kim, B., Kim, I., Oh, J., Jang, J., Cho, H.: Automatic control method of ddos defense policy through the monitoring of system resource. In: Proceedings of the 2nd international conference on Applied informatics and computing theory, pp. 140–145. World Scientific and Engineering Academy and Society (WSEAS) (2011)
15. Kurt, B., Yıldız, C¸., Ceritli, T.Y., Sankur, B., Cemgil, A.T.: A bayesian change point model for detecting sip-based ddos attacks. Digital Signal Processing 77, 48–62 (2018)
16. Liu, H., Sun, Y., Kim, M.S.: Fine-grained ddos detection scheme based on bidirectional count sketch. In: Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on, pp. 1–6. IEEE (2011)
17. Patil, R.Y., Ragha, L.: A rate limiting mechanism for defending against flooding based distributed denial of service attack. In: Information and Communication Technologies (WICT), 2011 World Congress on, pp. 182–186. IEEE (2011)
18. Safoine, R., Mounir, S., Farchi, A.: Comparative study on dos attacks detection techniques in sip-based voip networks. In: 2018 6th International Conference on Multimedia Computing and Systems (ICMCS), pp. 1–5. IEEE (2018)
19. Sanders, J.: Chinese government linked to largest ddos attack in github history. TechRepublic, April (2015)
20. Semerci, M., Cemgil, A.T., Sankur, B.: An intelligent cyber security system against ddos attacks in sip networks. Computer Networks 136, 137–154 (2018)
21. Tas, I.M., Ugurdogan, B., Baktir, S.: Novel session initiation protocol-based distributed denial-of-service attacks and effective defense strategies. Computers & Security 63, 29–44 (2016)
22. Tsiatsikas, Z., Fakis, A., Papamartzivanos, D., Geneiatakis, D., Kambourakis, G., Kolias, C.: Battling against ddos in sip: Is machine learning-based detection an effective weapon? In: e-Business and Telecommunications (ICETE), 2015 12th International Joint Conference on, vol. 4, pp. 301–308. IEEE (2015)
23. Tsiatsikas, Z., Geneiatakis, D., Kambourakis, G., Gritzalis, S.: Realtime ddos detection in sip ecosystems: Machine learning tools of the trade. In: International Conference on Network and System Security, pp. 126–139. Springer (2016)
24. Yu, J., Lee, H., Kim, M.S., Park, D.: Traffic flooding attack detection with snmp mib using svm. Computer Communications 31(17), 4212–4219 (2008)

AUTHORS PROFILE

Amita Chauhan has done B.E. in Computer Science and Engineering from CCET, Panjab University, Chandigarh, India. She has worked with Infosys Pvt. Ltd., Bangalore, India and Clicklabs, Chandigarh, India. She is currently pursuing her masters in Computer Science and Engineering from UIET, Panjab University, Chandigarh, India. Her research areas include Machine Learning and VoIP.

Nitish Mahajan is pursuing his Ph.D. from UIET, Panjab University, Chandigarh, India. He had done B.E in Information Technology from Himachal Pradesh University, Himachal Pradesh, India and M.E from UIET, Panjab University, Chandigarh, India. His research areas include Machine Learning, Next Generation Networks, VoIP and IoT.

Harish Kumar is a professor at Department of Computer Science and Engineering in UIET, Panjab University, Chandigarh, India. He received his Ph.D. in Computer Science and Engineering from Panjab University, Chandigarh, India. His research areas include Traffic Profiling, Next Generation Telecommunication Networks, Software Test Estimation, Entrepreneurship and e-learning. He has published more than 55 research papers.

Sakshi Kaushal is a professor at Department of Computer Science and Engineering in UIET, Panjab University, Chandigarh, India. She received her Ph.D. in Computer Science and Engineering from Thapar University, Patiala, India. Her research interests include Computer Networks, Cloud Computing and Social Networks. She has published various papers in the field of mobility in wireless networks, analysis and implementation of mechanisms to optimize network performance in high speed networks and cloud environment.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication