2020 International Conference on Data Analytics for Business and Industry: Way Towards a Sustainable Economy (ICDABI)

Slow Hypertext Transfer Protocol Mitigation Model in Software Defined Networks

Opeyemi Aderiike Abisoye *Department of Computer Science Federal University of Technology, Minna*
Niger State, Nigeria o.abisoye@futminna.edu.ng

Oluwatobi Shadrach Akanji *Department of Computer Science Federal University of Technology, Minna*
Niger State, Nigeria akanjioluwatobishadrach@yahoo. com

Blessing Olatunde Abisoye *Department of Computer Engineering*
Federal University of Technology Minna
Niger State, Nigeria b.abisoye@futminna.edu.ng

Joseph Awotunde
Department of Computer Science University of Ilorin
Kwara State, Nigeria awotunde.jb@uniilorin.edu.ng

Abstract—**Distributed Denial of Service (DDoS) attacks have been one of the persistent forms of attacks on information technology infrastructure connected to a public network due to the ease of access to DDoS attack tools. Researchers have been able to develop several techniques to curb volumetric DDoS attacks which overwhelms the target with large number of request packets. However, compared to volumetric DDoS, low amount of research has been executed on mitigating slow DDoS. Data mining approaches and various Artificial Intelligence techniques have been proved by researchers to be effective for reduce DDoS attacks. This paper provides the scholarly community with slow DDoS attack detection techniques using Genetic Algorithm and Support Vector Machine aimed at mitigating slow DDoS attack in a Software-Defined Networking (SDN) environment simulated in GNS3. Genetic algorithm was employed to select the features which indicates the presence of an attack and also determine the appropriate regularization parameter, C, and gamma parameter for the Support Vector Machine classifier. Results obtained shows that the classifier had detection accuracy, Area Under Receiver Operating Curve (AUC), true positive rate, false positive rate and false negative rate of 99.89%, 99.89%, 99.95%, 0.18%, and 0.05% respectively. Also, the algorithm for subsequent implementation of the selective adaptive bubble burst mitigation mechanism was presented.**

Keywords—genetic algorithm, slow DDoS mitigation, slow distributed denial of service, software defined network, support vector machine.

I. Introduction

Distributed Denial of Service (DDoS) attacks are assaults against network, digital and information technology infrastructure which involves the use of Internet-enabled and connected devices to synchronously send either legitimate or illegitimate requests to the victim at a rate which overwhelms the processing and response rate of the victim [1], [2]. A large portion of DDoS attacks reported have been volumetric DDoS attacks that send large numbers of requests at a rate faster than the victim can process. Due to the ease with which volumetric DDoS attacks easily triggers control measures, attackers have resorted to using a form of DDoS that occupies resources in a manner that resembles the way a legitimate client would request for resources [3], [5]. This form of DDoS is known as slow DDoS.

Slow DDoS or low-rate attacks [6], [7] are hard to detect and usually exploit the operation of the application layer. It exploits application layer protocols such as HTTP, Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), and Internet Message Access Protocol (IMAP) by behaving either as a legitimate client sending traffic over a slow connection or one with low response processing capacity [2, 7, 8]. Slow DDoS causes service unavailability by occupying all or most connections to the victim and sustaining the connection for a long time by sending data to the victim over the connections [9]. Attackers use variations of the slow DDoS, known as slow HTTP DDoS, to target web servers due to large number of web services on the Internet.

Slow HTTP DDoS attack is a type of slow DDoS targeted at web servers which is launched after a Transmission Control Protocol (TCP) connection has been established with the victim web server [9], [10]. There are three variations of slow HTTP DDoS: slow HTTP header, slow HTTP POST, and slow read DDoS attacks. Slow HTTP header DDoS attacks, also known as slow GET attacks, sends HTTP GET messages to the web server without transmitting two carriage return (CR) line feed (LF) which signifies the end of the GET request. In essence, the request from the client is not concluded which makes the web server wait indefinitely for the completion of the request before processing of the header can begin [5, 7, 10]. Slow HTTP POST DDoS attacks uses the *Content-Length* field in the header to inform the web server of a large *data* transfer. However, instead of sending the data at once, the attack focuses on sending the data in small chunks thus prolonging the connection to the web server [10], [11]. Unlike slow HTTP header and POST DDoS attacks which are based on data transmission from the attacker to the web server, slow read attacks are based on data transmission from the web server to the attacker. The slow read DDoS attacker requests for a resource on the server that has large data to be transmitted but adjusts the TCP window of the attack machine so as to force the web server to send the data in small bytes thus prolonging the connection time.

Mitigation of the slow HTTP DDoS attack refers to the use of methods that prevent service degradation or resource exhaustion on the web server [12] when an attack is detected by halting or diminishing the rate of attack [4]. Previous volumetric and slow DDoS attack mitigation techniques include redirecting the traffic to a verifying device [13], [15], limiting the rate of attack [16], [17], dropping the attack traffic selectively [18], or spreading the traffic to replicas of the attack victim [19], [20]. A global view of the network status and traffic that traverses the

978-1-7281-9675-6/20/$31.00 ©2020 Crown