Active DDoS Attack Mitigation and Secure Threat Intelligence Sharing

Khuda Bux*, Akhtar Hussain Jalbani, Ghulam Hussain Jalbani**, Saima Siraj Soomro**, and Salma Jamali****

*Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan.

**Department of Information Technology, Quaid-e-Awam University of Engineering, Science &Technology, Nawabshah, Pakistan.

bux.khuda@gmail.com, jalbaniakhtar@quest.edu.pk, ghjalbani@gmail.com, saimasiraj@quest.edu.pk, salma.jamali@quest.edu.pk

ABSTRACT

The DDoS (Distributed Denial of Service) attacks are increasing by each passing day on networks. There is a need to mitigate or prevent the networks from these types of attacks. To mitigate the DDoS active attack there are too many entities involved for sending signals and messages securely.This incident information is shared with the help of DoSTS (Denial of Service Open Threat Signaling). The DOTS framework provides a separate path along with DOTS clients and DOTS server for the process of information-sharing regarding active DDoS attack on attack target. For detection and mitigation of DDoS attack or any other malicious traffic on the network there is a need for continuous monitoring and automate all this process. Security Automation and Continuous Monitoring is deployed, with this, the incident threat information will be shared securely. The detection of active DDoS attacks, tracing of source, and mitigation is processed with the help of Managed Incident Lightweight Exchange. These incident messages are shared with the modified XML (Extensible Markup Language) or JSON (JavaScript Object Notation) function for security and privacy of network information on the attack target. With the help of a service provider or a third party, the active DDoS attack will be mitigated. These three frameworks are proposed by the standard body IETF (Internet Engineering Task Force). In this paper, we have proposed to combine these three frameworks for good results. Due to these frameworks, the existing devices and protocol are used to share the threat information and mitigate the active DDoS attack also. Due to this, the action against the malicious traffic on the network will be taken timely for detection and mitigation. And also, the services of attack targets for their customers will remain offline for a short period of time.

Key Words: DDoS Attacks, Mitigation, Targeted Network, Network Security, Security Events, Information Sharing, Attack Targets.

1. INTRODUCTION

The DDoS attacks area big risk to real-time service providers or to a computer network. Such as online taxi services, ISPs (Internet Service Providers), smart houses, and online banking services, etc. A DDoS attack is described by attempting to block the services for legitimate users [1]. The objective of a DDoS attack is to cut off clients from a server or system asset by overloading it with requests for services. While a straightforward DoS includes one "attack" system and one unfortunate casualty, conveyed DoS depend on the number of infected or "bot" systems ready to do tasks at the same time. The impact of DDoS attacks in this way loses clients, money, time and reputation of the company. It all depends on the attack density, the services will not be available for several hours or too many numbers of days. Due to this attack, the services of any organization has been denied for the real user. It will consume a huge amount of bandwidth on the network. As these attacks are carried out on the targeted network consumes less bandwidth. Due to this functionality of attack, it is hard to differentiate the real traffic and malicious traffic on the network.

To send a signal for mitigating the active DDoS attack on the targeted network the standard body suggested DDoS (DOTS) [2]. DOTS characterizes a strategy for planning cautious measures between willing peers to mitigate the attack quickly and proficiently. Activating hybrid attack response locally or near to the target of a functioning attack, or anyplace in-way between attack sources and target. How these security event signals will be communicated and monitored automatically another method has been proposed by the standard body is SACM (Security Automation and Continuous Monitoring) [3]. The SACM main focus on by what means to gather and share this data subject to utilize cases that incorporate demonstration examination of clients/servers. Versatile also feasible accumulation, articulation, then assessment of clients/servers information are central to SACM's objective [4]. This should most likely decide, offer, and utilize this data in a protected, advantageous, unsurprising, and with an auto, approach to perform client/server present assessments. To communicate with each other in the ecosystem – each player of this communication is known as SACM components. These SACM components may play one or more roles in this ecosystem.

After the communication of security event signals regarding DDoS active attack on the targeted network. How to mitigate it, the standard body proposed a method known as MILE (Management Incident Lightweight Exchange) [5]. Incident handling the care includes the detection, revealing, distinguishing proof and mitigation of the incident. For example, it very well may be a configuration of issue, IT (Information Technology) issue, an infraction to a SLA (Service Level Agreement),

framework bargain, socially structured phishing assault, or a DoS assaults, and so on. At the point when an incident is identified, the reaction may incorporate just recording information, warning to the source of the incident. A mitigation solicitation to a SP (Service Provider) or a solicitation to discover the source of the assault. The RID (Real-Time Inter-Arrange Defense) utilized as a dynamic between organizing correspondence for sharing incidents taking care of data by coordinating with existing location, following, source recognizable proof, and mitigation framework for a total occurrence taking care of solution. These security groups are not limited to only DDoS attack events, but these can handle any type of security incidents. In early work for the mitigation or detection of DDoS attack SDN (Software-Defined Network) is used. This is divided into two methods mostly, one is the signal controller and the second is data. The SDN is deployed only for the DDoS attack mitigation or detection. All this is based on the threshold of routers on a network for all applications running on the attack target. To overcome all shortcomings of existing work, we have proposed to combine the three standard body security groups (DOTS, SACM, and MILE) frameworks to mitigate or detect the DDoS attack or another malicious traffic on the network.

The rest of this paper is sorted as follows: Section-2 gives an overview of standard body security groups. Section-3 describes related work for DDoS mitigation and threat information sharing. In section-4, we have proposed a combined methodology of standard body security groups. Section-5, the tools and incident information sharing method are discussed. Last, section-6, the conclusion of the paper is given.

2. OVERVIEW OF STANDARD BODY SECURITY GROUPS FOR DDOS MITIGATION

Standard body SA (Security Area) has defined a few mechanisms for the mitigation of DDoS active attack on the targeted network. First SG (Security Group) all the parties involved coordinating for a defensive response to a DDoS active attack. They must define a common understanding of mechanisms and roles for signaling. The DDoS Open Threat Signaling has been introduced by the standard body for the signaling layer and supplementary messaging. Second SACM and SG have developed a method that defines how to continuously monitor and automate security events information sharing. Third SG has defined methods on how to mitigate active DDoS attacks and send security events by using JSON, XML or UML (Unified Modeling Language). It is known as MILE. To share threat information between peers of detection or mitigate the malicious traffic on the network. The secure method of XML or JSON has been defined in the MILE framework for sharing security incidents.

2.1 DOTS Signaling and Data Sharing Architecture

To mitigate the active DDoS attacks there be situated to share information regarding that attack. To meet this need the DDoS open threat signaling has been introduced with its own DOTS client and DOTS server as shown in Fig. 1.

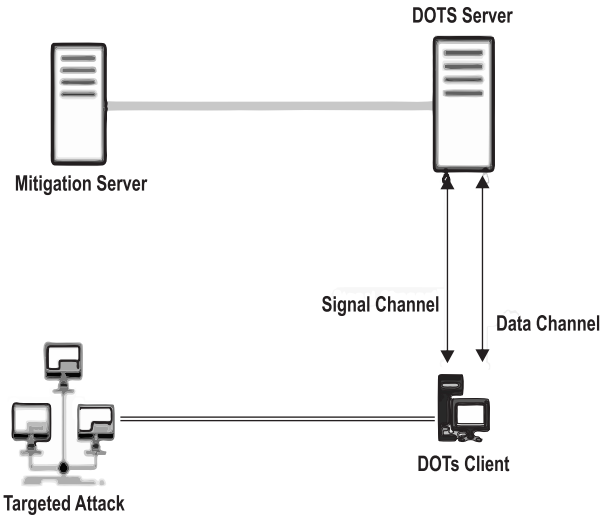

FIG. 1. DDOS OPEN THREAT SIGNALING ARCHITECTURE

In the above architecture, the signaling channel is used for communication between DOTS clients and servers. As the DOTS server receives signals from DOTS client it may change the path of destined traffic for the attack targets. The organization takes a DOTS user, which gets information regarding the DDoS attack and sends a signal to the DOTS server for assistance to mitigating the attack. The DOTS server thus activates at least one mitigator, which is entrusted with mitigating the real DDoS attack. By this to decrease the malicious traffic and allow the legitimate traffic to be accessible on attack target. The main function of DOTS is to provide the signaling channel and data channel for information sharing. The communication process of information is not secure among the DOTS user and DOTS server.

2.2 SACM Architecture

To mitigate or detect the DDoS attack on attack target a continuous monitoring and security event information sharing system need to deploy. The SACM will assess and compare data models from the collected information, check the interfaces and protocols are being used in communication. The SACM architecture comprises of a number of SACM Components, and named components are planned to encapsulate at least one explicit capabilities. Communicating with these abilities will require at least two degrees of interface determination. The first is a logical interface determination, and the

second is at least one binding to an explicit transfer system, as shown in Fig. 2. This will be further elaborated in section 5.

2.3 MILE Tracing and Mitigation

The managed incident lightweight exchange is used for the mitigation of active DDoS attacks and secure incident information sharing on the attack targets. The network used for the correspondence should comprise of out-of-band or secured passages or else encoded passages devoted to vehicle RID communications. The correspondence connections should be immediate associations (virtual or physical) among companions who have settled upon utilizing and misuse approaches via a consortium. The security, setup, and assurance scoring plans regarding RID informing peers and should be consulted with peers. This communication should meet some criteria general prerequisites for a completely associated system (Web, government, training, and so forth.) through the peering and additionally a consortium-based understanding. The incident information will be shared by RID and the active DDoS attack will be mitigated by a service provider or a third party as shown in Fig. 3.

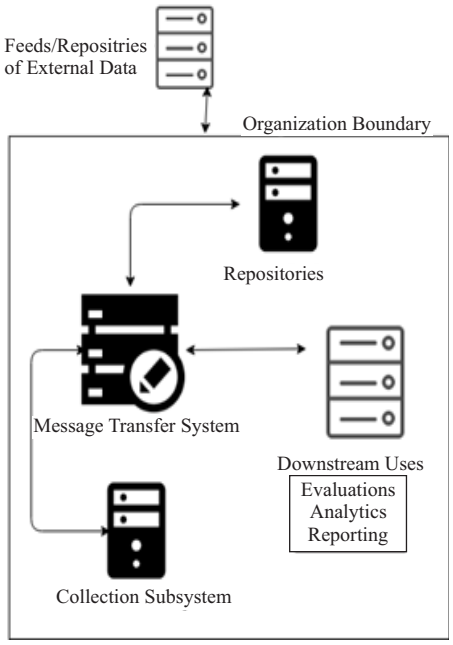

FIG. 2. AN OVERVIEW OF SCAM INFORMATION SHARING

FIG. 3. MILE MITIGATION PEERS

3. RELATED WORK AND THEIR LIMITATIONS

For the mitigation of active DDoS attacks on the attack target, there are few important components. These components are used for information sharing, tracing of attack source, detection, and mitigation of DDoS attack. The FLEX (Flow-Based Event Exchange Format) has been used for the communication process. It will support to achieve the awareness of the current threat, its expertise, and resources used by this attack on the attack target [6]. A multi-level DDoS mitigation system for the IoT (Internet of Things) that incorporates an edge computing level, a fog computing level, and a cloud computing level. The edge computing level uses an SDN-based IoT gateway to oversee and secure the IoT perception layer. An IMCU (Internet Management Control Unit) is comprised of fog computing. To identify and check DDoS attacks by utilizing the IMCU bunch with the SDN controllers and it is applications [7]. The SDN framework is also implemented to mitigate the DDoS attack. Verizon's apparent SDN framework has been utilized as a contextual investigation by researchers. The SDN architecture divides the network into two planes control and data. Due to this separation of the network traffic will be operated and managed dynamically as per customer need. For the defense of DDoS attacks, the central control and functionality of the SDN feature are also in use plus malicious traffic on attack targets [8].The machine learning method has been used by researchers for the detection of DDoS attacks. They have used public repositories of intrusion detection datasets for covering DDoS attack evaluation to create the machine learning models. The specific dataset has been taken for the test of legitimate traffic and malicious DDoS attack traffic [9].To control DDoS attack traffic the data model of PT-DCTL+TS (Progressive Transfer Deep Coordinated Team Learning with Team Structure) has been used. The router throttling is used to deal with DDoS attacks by three proposed methods. The first with, they have utilized profound system as opposed to the tile coding for this DDoS issue with deep learning strategies. Second, they add group structure information to the state so pros with the heterogeneous gathering structure can even now share on deep systems. Third, their dynamic trade learning can show signs of improvement approach with less time usage [10]. The SDN has been divided into three layers: application, control and data processing. The processing starts as a packet reaches the data layer which contains the packet handles and, if there is a need, it will be forwarded to the control layer. In last the control layer may need different types of applications with multiple functionalities. The SDN has useful capabilities for the DDoS attack defense, which makes it more useful for protecting too many types of network topologies [11]. The researchers have proposed the ProDefense, it can be configured for each application as per the need of network

traffic threshold. By implementing this custom configuration will be used for the detection of DDoS attacks. The distributed controller framework used by deploying load balancing and this will decrease the probability of controller failure. As per the researcher, ProDefense can be used in different types of networks which may include cyber-physical systems, smart grid, and e-governance [12]. Another method has been proposed to mitigate the DDoS attack with lightweight information sharing, efficient, and easy to deploy SDN. The researcher has been designed a secure protocol known as C-to-C communication for SDN-controllers in between multiple AS (Autonomous Systems). By effective communication between the SDN controller and with the neighboring domains controllers about the active DDoS attack. Due to this, SDN-controller will be able to do these two tasks. First, block the malicious traffic on the attack target. Second, send information signals regarding the active attack to neighboring domains or networks [13]. The sFlow [14] framework has been used for the SDN-controller to improve accuracy and timeliness. The entropy-based technique has been used for checking the network feature changes, and a machine learning method used to detect network anomalies automatically. The DDoS attack can be detected at an early stage by using this mentioned method. As the controller-based, sFlow-based data gathering technique, entropy-based feature extraction technique, and SVM (Support Vector Machine)-based classification should be deployed to improve the accuracy and timeliness of active DDoS attack detection [15]. For the detection of a DDoS attack, the deep belief network feature of extraction has been used along with LSTM (Long Short-Term Memory) method. The deep belief network is used for the extraction of IP (Internet Protocol) packet details. After that network, the traffic pattern has been taken by using LSTM. This proposed model by a researcher is suitable for DDoS attack detection only [16]. The TAXII (Trusted Automated Exchange of Indicator Information) is network-driven exertion, these defines ideas, protocols, and message trades to share cyber threat data for detection, counteractive action, what's more, relief between confided in accomplices. The improvement of TAXII is composed of Miter. The TAXII data traded is spoken for the XML STIX (Structured Threat Data Expression) program [17]. Firecol et. al. [18] is a cooperative framework that identifies flooding DDoS attacks at the ISP level and gives an administration to which clients can subscribe. This membership structure disseminated engineering of numerous IPSs that figures furthermore trade conviction scores on potential attacks. On the off chance, that Firecol identifies an attack, the attack is hindered as close as conceivable to its source(s). Further, the IPS that identifies the attack advises its upstream IPSs, which thus likewise performs moderation strategies.

3.1 Related Work: State-of-the-Art

For the protection against the DDoS attacks, researchers have made a suggestion. Like as particular blackholing updates ISPs with information for (DDoS) assaults. The technique effectively expels contorted parcels from the system, limiting the potential harm that could be caused [19]. To speak to and investigate the stream tablespace of a switch, the author has given a lining hypothesis-based scientific model to speak to the stream table-space of a switch. From that point forward, the researcher has displayed a novel stream table sharing a way to deal with increment the obstruction of the SDN-based cloud during stream table over-loading DDoS assaults. The focal point of their commitment is to viably share the unused stream table-space of different switches with a switch right now enduring an onslaught with negligible inclusion of the controller [20]. The researcher has seen that danger insight (TI) has numerous points of interest around there. Finding clandestine digital assaults and new malware, giving early admonitions, and specifically conveying TI information is only a portion of these favorable circumstances. They have given a clear meaning of danger insight and how writing subdivides it. By researcher concentrated on specialized danger insight (TTI) and the serious issues identified with it [21].

Most of the tools and techniques proposed by the researchers are depends on SDNs. The SDN provides two channels for control and messaging on the same path. And it depends on the same threshold of the router for all the applications which are used within a domain network. In these tools and techniques, the functionality of mitigation or detection or threat information sharing is provided. However, no tool provides all services for DDoS attacks by them currently. Another major drawback of security and privacy during threat information sharing is less consideration from these tools.

4. PROPOSED SOLUTION AND METHODOLOGY

Insecurity incidents, there may be network compromises, viruses, worms, phishing attacks, and denial of service attacks. By these few mentioned attacks on any attack, the target may lose critical data, services to its customers, and maybe loss human and system resources. To handle this security incident, the service provider and CSIRT (Computer Security Incident Response Team) need to be fully ready and prepared with tools to help in tracing security incidents and communicate before any event of an attack. To achieve this, we have proposed standard body security group DOTS, SACM, and MILE frameworks should be combined to get good results. The DOTS will provide an alternate path on the attack target. The DOTS client and DOTS server will communicate on two channels signaling and data, these channels are used for information sharing. The SACM is used for the automated processes of information sharing and continuous monitoring of the network. The main

functionality of SACM how the information will be collected and shared regarding security events on the attack target [22]. Third, the MILE is used for detection of security event or DDoS attacks, it will trace the source of attack also. The MILE will mitigate the DDoS attack with the help of a service provider or third party support. The security event messages are shared securely by using redefined XML or JSON function format for data transfers. The architecture for the detection, tracing of the source, and mitigation of active DDoS attack described in Fig. 4.

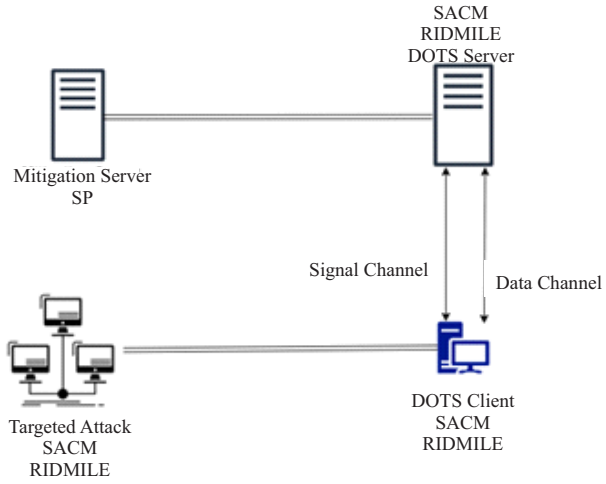

FIG. 4. PROPOSED ARCHITECTURE FOR DDOS ATTACK MITIGATION

The RID traces preemptive inter-network communication strategy to encourage sharing incident-handling information. This method will be incorporating with existing identification, tracing, source ID, and mitigation of total incident-handling solution. A secure method of incident information communication is provided by RID via enabling the interchange of IODEF (Incident Object Description and Exchange Format) [23] with XML documents. The exchange of critical information, policy, and privacy are highly considered as the security of an organization by RID.

4.1 DOTS Signaling and Data Description

For sharing incident information, the signaling has been used for defending an active DDoS attack. For this, DDoS and DOTS use the two channels for signaling and messaging. These two channels of signaling and messaging are used between DOTS clients and the DOTS server. The DOTS clients will send a signal of active DDoS attack to the DOTS servers. The DOTS server will change the destined traffic path for the attack targets; this all depends on the policy of the organization to mitigate it. Generally, the DOTS are considered more effective when there is a need for coordination regarding attack response between two or more network domains.

Table 1, the DOTS will not specify how an attack target is under DDoS attack and also does not specify how this DDoS attack will be mitigated. The request for mitigation of active DDoS attacks will be initiated by the DOTS clients. This active DDoS attack may not be mitigated at all it depends on DOTS server ability and will to mitigate it on the request of DOTS clients. But the basic function of DOTS is to share the information regarding active DDoS attacks via an alternate path on attack targets.

4.2 SACM Information Sharing and Monitoring

To mitigate or minimize the growing number of security threats there is a need for an automated process of sharing security information. And the protection of user information, the system which stores information, process, and transfers that information [24]. There are a different number of ways to detect security threats. The main objective of SACM is to collect authentic information, scalable, expression, and evaluation of that information endpoint as the main points shown in Table 2.

The SACM environment contains too many data models, protocols, and transfers that information. The SACM transfer protocol runs on the top of the TCP/IP (Transport Control Protocol/Internet Protocol). It carries different operations such as requests or responses and transfer of information. SACM is divided into a design and data concentrated off tending requirements for deciding, sharing, and utilizing stance data safely via stance data suppliers plus stance data of customers.

TABLE 1. DOTS FEATURES FOR DDOS ATTACK MITIGATION

Features	Yes	No
Message Signaling	Yes	-
Information Gathering		-
Message Security	-	No
DDoS Detection	-	
Mitigation	-	
Source Tracing	-	
Alternate Path	Yes	-

TABLE 2. SACM FEATURES

Features	Yes	No
Information Sharing	Yes	-
DDoS Detection	-	No
Information Security	Yes	-
Source Tracing	-	No
DDoS Mitigation	-	
Network Monitoring	Yes	-
Automated Processes		-

TABLE 3. MILE FEATURES

Features	Yes	No
Information Sharing	Yes	-
DDoS Detection		-
Incident Security		-
Source Tracing		-
DDoS Mitigation		-
Information Gathering		-
Network Monitoring	-	No

4.3 MILE Detection and Tracing of DDoS Attack

To facilitate communication and tracing security incident the service provider or incident response team should be prepared with tools along with processes before any attack on the attack target. For this MILE working group has given a Real-time Inter-network Defense RID framework, it will be a proactive solution used for security incidents [25]. The features of MILE are shown in Table 3.

For sharing threat intelligence, information theses should be combined with the current detection, finding, identification of the source and solution for the mitigation of DDoS attacks. This all is provided by the RID such as its nature of proactive communication within a network. The XML is used for the data in RID messages with the help of IODEF and RID documents. Security and privacy contemplations are of high worry since possibly delicate data might be gone through RID messages.

5. PROPOSED SOLUTION

The DDoS attack is a big threat to real-time service of any organization, such as Webhosting service providers, cloud computing, taxi app services, online banking, or internet service provider and so on. To avoid this, as per industry practice too many tools and techniques are used for mitigation, detection or threat information sharing. These all services of active DDoS attacks are not supported by any single tool. But they need extra tools or techniques to provide complete services, like as detection, tracing of the source, secure threat or incident information sharing, and mitigation of DDoS attack on attack targets. To get 100% results of mitigation, detection and tracing of the source as we have proposed to combine the three frameworks DDoS Open Threat Signaling DOTS, Security Automation, and Continuous Monitoring SACM, and Managed Incident Lightweight Exchange MILE of the standard body.

5.1 DDoS Mitigation and Detection Tools

To mitigate and detect active DDoS attack the SDN is used, as few of them shown in Table 4. The services provided by Cloudflare, F5 Networks, Akamai, Arbor Networks, Incapsula, Level 3, and Verisign are known as DDoSPS (Protection Service) [26]. They are providing DDoSPS for any application or for the complete network.

TABLE 4. TOOLS USED FOR DDOS DETECTION AND MITIGATION

Tools	DOTS	SACM	MLE
Cloudflare	No	No	Yes
F5 Networks			
Akamai			
Arbor Networks			
Incapsula			
Level 3			
Verisign			
Verizon			

The main functionality of DPS architecture is to divert the traffic of an application or network. This service can be enabled for always-on or on need-based.

Cloudflare provides DDoS attack mitigation as a service with a low price [27]. However, the services are provided for mitigation only and applications should be hosted at the Cloudflare platform, which is not applicable for every organization. Another tool, Verizon's, has implemented virtualized SDN-enabled architecture with the trust of the root [7]. The simulated anti-DDoS scouring programs are activated automatically close to the source of a DoS attack detected. The traffic will be routed from these functions. These functions are configured with prioritization rules to give priority to real traffic of the network dynamically and reduce the resources for the malicious traffic. Mostly these types of service for DDoS attack detection and mitigation are applied on applications with the help of router threshold.

5.2 Threat Information Sharing Tools

As the number of threats and security breach incidents are growing day by day. So that these incidents need to be detected and should be handled as soon as possible to decrease the damage of the organization. To do that there is a need for threat information sharing with a secure method. Some threat information tools are mentioned in Table 5.

The community framework known as the MISP (Malware Information Sharing Platform) is used for threat information sharing [28]. There are two main parts of the MISP data model and sharing model. In the data model, the simple and easy format has been designed. Due to the simple format, users can define which level of information will be shared with the community. The different levels of information sharing have been defined, such as organization only, the community only, connected communities, and with all as the default function of MISP communities. YARA Kim et. al. [29] is an unadulterated marker layer technology that depicts regular expression examples and conduct. YARA is an engine and language for checking documents and memory squares. At the point when a standard matches a design, YARA presumes to arrange the subject as

TABLE 5. TOOLS USED FOR THREAT INFORMATI ON SHARING AND DETECTION OF THREAT

Tools	DOTS	SACM	MLE
MISP	Yes	Yes	Yes
HELK			
SQHUNTER			
CHIRON ELK			
BANG			
YARA			
MAL TINDEX			
Onion Share			
XRay			

indicated by the standard's conduct. YARA can coordinate different string arrangements like ASCII, UTF (Unicode Transformation Format), and different encodings; YARA can likewise parse on PERL standard articulations and has Python and Ruby ties.

5.3 Prevention and Threat Information Sharing

There are a number of tools for threat information sharing and prevention, some of them are community-based and commercial. OWASP (Open Web Application Security Project) community framework to detect and prevent the websites from DoS attacks on the application layer. For a web server HTTP (Hyper-Text Transfer Protocol) headers contain noteworthy data, which is originating from the client, while the solicitations are handled, web server holds back to catch total solicitation of HTTP headers before handling for a message as an affirmation to the request sender. The HTTP slow header attack works by misusing the customer inactive break esteem on the unfortunate casualty web server [30]. This break is designed at the server side to drop a customer association if a customer was found inert during the timespan. The slow header assault finds the evaluated break worth set on the injured individual server-side and after that picks a worth which is lower than the designed worth. At that point, this assault produces HTTP demands with incomplete header or the deficient header to the injured individual web server. It keeps sending one header dependent on the chose worth with the end goal that customer inactive break won't be activated on the victim individual web server and solicitations won't be finished (Table 6).

Suricata is one of the genuine instances of open-source IDS/IPS accessible on all stages [29]. It recognizes an assault by assessing organize information against predefined standard mark rule-set accessible from developing dangers. Suricata gives name, seriousness, and kind of assault. To stay up with the latest, a logging specialist contacts the organization server to check the accessibility of new marks in the inward database. In the event that another mark is found, the logging operator naturally refreshes the Suricata ruleset.

6. CONCLUSION

To share threat information during an active DDoS attack is a big challenge for security persons. The second one is protection against the DDoS attacks on any service providers or on the network infrastructure of any organization. One existing method to detect and mitigate these types of attacks is software-defined networks SDNs. We have suggested combining three different frameworks of the standard body. By using these frameworks, the process of threat information sharing and DDoS attacks protection, and securely with the automated process. The DOTS will be used for information sharing between server and client. The security of incident messages and continuous monitoring of the attack target has been done via the SACM framework. To detect, trace the source of the attack and mitigate the active DDoS attack done with the help of MILE. The communication between two or more peers regarding incident information shared securely by RID protection techniques, such as the security and privacy policy of the organization. As we have combined all these three methods proposed solely by the standard body. The desired results can be achieved by implementing our proposed method during the active DDoS attack. The main focus was on the uptime of service provided by any organization during this attack.

TABLE 6. TOOLS USED FOR THREAT INFORMATION SHARING AND FIREWALL

Tools	DOTS	SACM	MLE
LOIC	No	No	Yes
XOIC			
HULK			
DDOSIM-Layer7			
R-U-Dead-Yet			
OWASP DOS HTTP POST			
DAVOSET			
GoldenEye HTTP Denial of Service Tool			
SURICATA	Yes	Yes	

7. FUTURE WORK

In the future we will implement it on a network to analyze it through software.

ACKNOWLEDGEMENTS

Authors are thankful to Riphah Institute of System Engineering, Islamabad, Pakistan, and Quaid-e-Awam University of Engineering, Science & Technology, Nawabshah, Pakistan, for providing facilities to conduct this research paper.

REFERENCES

[1] Mirkovic, J., and Reiher, P., "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", ACM SIGCOMM Computer Communication Review, Volume 34, No. 2, pp. 39-53, 2004.

[2] Reddy, T., Boucadair, M., Patil, P., Mortensen, A., and Teague, N., "Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Specification", Internet-Draft. Reddy, 2017.

[3] Montville, A., and Munyan, B.,"Security Automation and Continuous Monitoring (SACM) Architecture", IETF Internet-Draft, 2019.

[4] Birkholz, H., Lu, J., Strassner, J., Cam-Winget, N., and Montville, A.,"Security Automation and Continuous Monitoring (SACM) Terminology", IETF Internet-Draft, 2018.

[5] Inacio, C., and Miyamoto, D., "Management Incident Lightweight Exchange (MILE) Implementation Report. Management", Internet Engineering Task Force, 2017.

[6] Steinberger, J., Kuhnert, B., Sperotto, A., Baier, H., and Pras, A., "Collaborative DDoS Defense Using Flow-Based Security Event Information". IEEE/IFIP Network Operations and Management Symposium, pp. 516-522, April, 2016.

[7] Yan, Q., Huang, W., Luo, X., Gong, Q., and Yu, F.R.,"A Multi-Level DDoS Mitigation Framework for the Industrial Internet of

Things", IEEE Communications Magazine, Volume 56, No. 2, pp. 30-36, 2018.

[8] D'Cruze, H., Wang, P., Sbeit, R.O., and Ray, A., "A Software-Defined Networking (SDN) Approach to Mitigating DDoS Attacks", Information Technology-New Generations, pp. 141-145, Springer, Cham, 2018.

[9] Aamir, M., and Zaidi, S.M.A., "DDoS Attack Detection with Feature Engineering and Machine Learning: The Framework and Performance Evaluation", International Journal of Information Security, pp. 1-25, 2019.

[10] Xia, S.M., Zhang, L., Bai, W., Zhou, X.Y., and Pan, Z.S., "DDoS Traffic Control Using Transfer Learning DQN With Structure Information", IEEE Access, Volume 7, pp. 81481-81493, 2019.

[11] Swami, R., Dave, M., and Ranga, V.,"Software-Defined Networking-Based DDoS Defense Mechanisms", ACM Computing Surveys, Volume 52, No. 2, pp. 28, 2019.

[12] Bawany, N.Z., Shamsi, J.A., and Salah, K., "DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions", Arabian Journal for Science & Engineering, Volume 42, No. 2, pp. 425-441, 2017.

[13] Hameed, S., and Khan, A.H., "SDN Based Collaborative Scheme for Mitigation of DDoS Attacks", Future Internet, Volume 10, No. 3, pp. 23, 2018.

[14] Panchen, S., Phaal, P., and McKee, N.,"InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed networks", Published in RFC. 2001.

[15] Hu, D., Hong, P., and Chen, Y., "FADM: DDoS Flooding Attack Detection and Mitigation System in Software-Defined Networking", IEEE Global Communications Conference, pp. 1-7, December, 2017.

[16] Li, Y., Liu, B., Zhai, S., and Chen, M., "DDoS Attack Detection Method Based on Feature Extraction of Deep Belief Network", IOP Conference Series: Earth and Environmental Science, IOP Publishing, Volume 252, No. 3, pp. 032013, April, 2019.

[17] Kampanakis, P., "Security Automation and Threat Information-Sharing Options", IEEE Security & Privacy, Volume 12, No. 5, pp. 42-51, 2014.

[18] François, J., Aib, I., and Boutaba, R.,"FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks", IEEE/ACM Transactions on Networking, Volume 20, No. 6, pp. 1828-1841, 2012.

[19] Cotton, M., "DDoS Attacks: Defending Cloud Environments", Information Technology-New Generations, pp. 907-909, Springer, Cham, 2018.

[20] Bhushan, K., and Gupta, B.B., "Distributed Denial of Service (DDoS) Attack Mitigation in a Software-Defined Network (SDN)-Based Cloud Computing Environment", Journal of Ambient Intelligence and Humanized Computing, Volume 10, No. 5, pp. 1985-1997, 2019.

[21] Tounsi, W., and Rais, H., "A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber-Attacks", Computers & Security, Volume 72, pp. 212-233, 2018.

[22] Cam-Winget, N., and Lorenzin, L., "Security Automation and Continuous Monitoring (SACM) Requirements", An IETF Working Group, 2017.

[23] Danyliw, R., Meijer, J., and Demchenko, Y., "RFC 5070: Incident Object Description Exchange Format (IODEF), Network Working Group, 2012.

[24] Cam-Winget, N., and Lorenzin, L., "RFC 8248: Security Automation and Continuous Monitoring (SACM) Requirements", Engineering, Computer Science, Published in RFC 2017.

[25] Moriarty, K., "RFC 6545: Real-Time Inter-Network Defense RID" Internet Engineering Task Force, 2012.

[26] Jonker, M., Sperotto, A., van Rijswijk-Deij, R., Sadre, R., and Pras, A.,"Measuring the Adoption of DDoS Protection Services" ACM Proceedings of Internet Measurement Conference, pp. 279-285, November, 2016.

[27] "Advanced DDoS Attack Protection", https:// www.cloudflare.com/ddos/, (Accessed on 30, July 2019).

[28] Wagner, C., Dulaunoy, A., Wagener, G., and Iklody, A., "Misp: The design and Implementation of a Collaborative Threat Intelligence Sharing Platform", ACM Proceedings of Workshop on Information Sharing and Collaborative Security, pp. 49-56, October, 2016.

[29] Kim, E., Kim, K., Shin, D., Jin, B., and Kim, H., "CyTIME: Cyber Threat Intelligence Management Framework for Automatically Generating Security Rules", ACM Proceedings of 13th International Conference on Future Internet Technologies, pp. 7, June, 2018.

[30] Behal, S., and Kumar, K.,"Characterization and Comparison of DDoS Attack Tools and Traffic Generators: A Review", International Journal of Network Security, Volume 19, No. 3, pp. 383-393, 2017.