Denial of Service (DoS) attack identification and analyse using sniffing technique in the network environment

Kagiraneza Alexis Fidele[1*], *Suryono*[2], *Wahyul* Amien Syafei[3]

[1,2]Department of Information System, School of Postgraduate Studies Diponegoro University, Semarang – Indonesia
[3]Data Entry and Update Taxpayer's Registry in Rwanda Revenue Authority(RRA) Kigali-Rwanda

Abstract. Network-based intruders such as (DoS) attacks have become one of the most significant internet interruptions. Some operations that rely on the internet, such as banking transactions, education, trade marketing, and social networking, have become the primary targets. The attacker is trying to surround and making it difficult for the system to defend. The research's objective is to recognize the characteristics and level of DoS attacks. In understanding the behavior of intruders against a target web server, Wireshark was used in all traffic networks—capturing the traffic in a networked environment. In this research, the user identifies the attack levels (TCP SYN, UDP, and HTTP protocol), ranging from low (Q1), medium (Q2), and high (Q4) attacks. The approach is to simulate the TCP, HTTP, and UDP flood attacks and analyze the attacks' effects on the network environment. In this work, normal scenarios and pattern attacks were compared. In this case, the intruder floods unwanted packets to the victim with a massive number of request packets; the SYN from the corresponding SYN-ACK replies are not achieved. This paper will identify the DoS attacks level and analyze the behavior of traffics.

Keywords. DoS attacks level Identification and traffic analysis criteria of traffic.

1. INTRODUCTION

In modern technology, most of the users, depending on the internet to access their information resources instantly, the network performs a significant function for the users [1, 2]. Nowadays, network- based attacks have become more adverse and continue to increase in number day by day [3-5]. The necessitate of the internet is significantly crucial if the users wish to obtain information resources or to communicate among themselves. In this case, the internet network allows its customers to use distributed resources on the internet for computations. However, the implementation of security becomes a big challenge in the development of a network environment [6-8]. The various techniques must be immediately

* Corresponding author: alexkagiraneza@gmail.com

implemented in improving the reliability and mitigating information system risks in information system technology [9].

The main reason for security in the network environment is preserving the integrity of data, resource availability, and confidentiality. The network system gives the users access to their information resources and communication; therefore, accessibility is essential [10-12]. In the generation where technology is dominant, information technology involves almost every daily activity to make things more comfortable to use. Therefore, the utilities of the internet to society have become the main target by trespassers to reduce the performance of network and service to legitimate users [13]. In the network environment, the intruders sent an enormous number of unwanted packets to the targeted server and put down the entire website [14, 15]. These attackers and intruders achieved their objectives within the organization and website by making network resources unavailable for use[16, 17].

Attackers success their mission by sending a massive number of fake packets to the target server. The unwanted flood packets, which can cause the failure of network. The attackers consume network bandwidth and CPU usage, as a result, the server cannot serve the users of internet [18]. In this paper, we identify and analyze making and filtering in DoS attacks with packet sniffing.

2. LITERATURE REVIEW

To foresee unwanted problems in the network security environment, especially in Denial of Service (DOS), researchers proposed the various types of methods against those attacks [19]. Kamesh and Sakthi Priya (2012a) Kamesh and Sakthi Priya (2012b) proposed packet marking methods which employed to locate such attackers approaching their sources. The packet mark consists of some traceback information about a router being combined in the IP packet properties. In this system, a path identifier was introduced to identify an attacker. The path identifier used to collect the attack packets to present a smart solution to measure protection against future attacks. The effects of an on-going attack cannot harm the system. [22] The methods programmed in self-learning include simple rule-based and include simple statistics, which also consist of rule modeling, immune system, neural network-based, and statistical methods.

The proposed method consists of identifying unusual events in time-series data and analyzing packets payloads. Denial of Service (DoS) involves sending multiple requests to a web server, which considered such as a collective anomaly [23, 24]. Sun et al. (2018) proposed a probabilistic approach to defend those attacks and apply a prototype system ZePro for a zero-day path identification. A graph of a zero-day attack is essential to capture the malicious packet. A diagram is first built depending on the chart named object. The build system is based on Bayesian upon the instance graph. The Bayesian network is capable of analyzing the probability number of the affected objects.

DoS attack keep on growing in this era, and an intruder comes with new techniques to reduce the performance of the internet. There are many types of seizures in the internet system; therefore, the different methods to avoid, prevent, or to detect these attacks must deal with numerous techniques [26].

Gairola and Singh (2016a) Gairola and Singh (2016b) proposed two ways to identify the denial of service or DoS attacks by performing a Cumulative Sum algorithm (CUSUM). In this algorithm, the first techniques are to discover if the new IPs acts as the source of DDoS attacks by initializing the procedure with a designed monitoring IP address. The second method referred to as the technique takes place upon the occurrence of DDoS attacks, and the next process is to find out the actual attackers. Here, [29] proposed a method of pre-processing and covariance analysis (PCA) to divide historical data of the network. This method can also predict the behavior of future data in the system to respond best to predict

attack threats—other techniques utilized to predict attacks. Besides, created a set of rules to anticipate attacks and built these sets [29].

3. METHOD

The attacker uses different techniques to flood malicious packets to the targeted web server. In this case, the user used Low Orbit Ion Cannon (LOIC) DoS attacking tool to create pattern attacks. This section describes the methods used while conducting current research. The technique consists of two main phases, data collection, identification and analyzes features of an attacker. By identifying the behavior of attacks, two nodes are used, one acting as an attacker machine, and another computer acts as the victim with an installed a tool for capturing all network traffic coming into the network environment. The occurrence of strange malicious decreases network performance that prohibits users from accessing online services. This method to captures ongoing packets using packet sniffing, identifies, and analyses the behaviour of attacks, explained in the next section.

3.1 Packet Sniffing

3.1.1 Data collection

The tool offers a variety of features such as filters, color-coding, and so forth that lets user analyze network road and investigate any individual packets. Besides that, this tool gives a simple way in network identification, load, frequency, and latency between specific hops. The TCP, UDP, and ICMP are likely to be the most common packets on the network system. The data collection phase will be capturing all packets from an attacker such as UDP and TCP traffic flood, using a packet sniffer. After catching UDP, HTTP and TCP from captured packets, the user identifies the behaviour of pattern attacks. The Quartile used to identify the level of attacks. The total number of captured allows calculating the quartile, Q1, Q2, Q3, and Q4 to identify the level of attacks.

Q1 = Low attacks

Q2 = Medium attacks

Q3 = Upper half attacks

Q4 = High attacks

3.1.2 Attacking Scheme

The attacker uses different techniques to flood malicious packets to the targeted web server. The identification of signatures attack is significant; this permits user to find the way of DoS attack detection. The method proposed two separate machines, and an attacker simulator is physically located on one of the devices. It can perform several attack types on the target machine: one machine used as an attacker to flood the malicious packet to the server machine where there is the tool for monitoring and capturing efficiency all traffics in real-time. For more details, it displayed below in the standard architecture of the DoS attack in Figure 1.

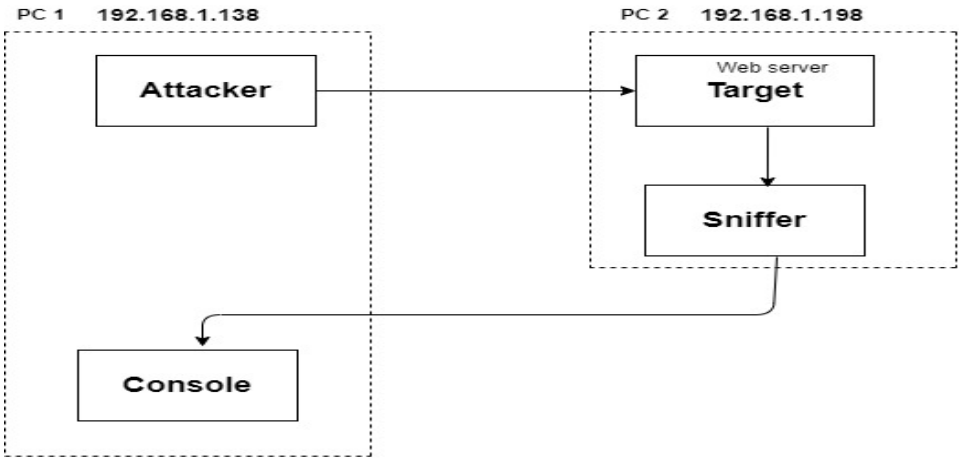

Figure 1. Standard Architecture of DoS Attack.

3.1.3 TCP SYN Flood Packet Attacks

One of the most adverse types of DoS attacks is the TCP SYN flood. When clients & servers need to communicate their first establish connectivity by performing three-way hand sharke, "SYN- SYN-ACK and ACK". In this case, attacks try to be trusted client and the servers keep waiting for acknowledging until TCP timeout. These attacks were made to cunsume server equipment such as firewalls and communication tools. Figure 2. shows the captured and analyzed TCP using Wireshark.

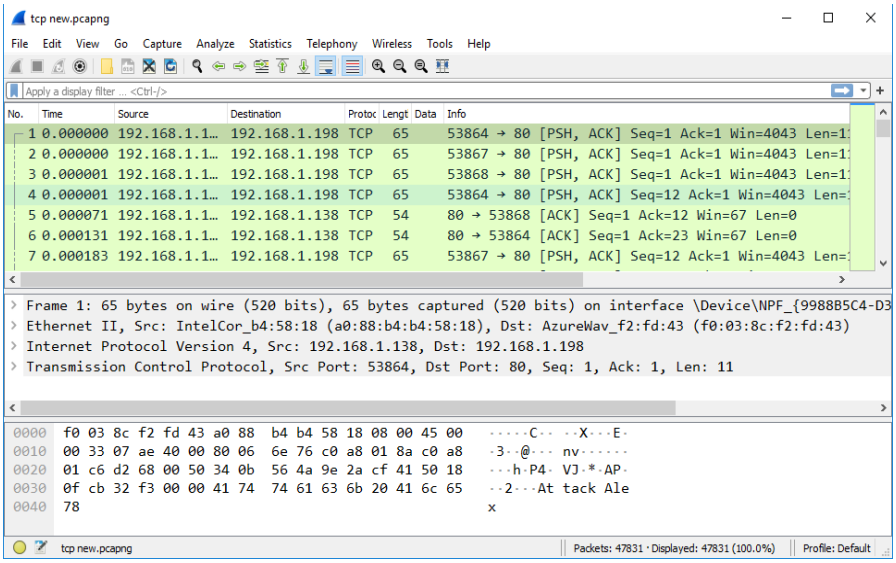

Figure 2. Analyzing TCP Flood Attack Using Wireshark

The packet's behavior of TCP flooding of (DDoS) attacks, the packets are sent to the victim server. By seeing the information details of malicious packets, you simply select them from the menu "Statistics,">> Flow Graph, you can see the packet sequence graphically. This tool permits you to trace the TCP connections and behavior, as described in Figure 3.

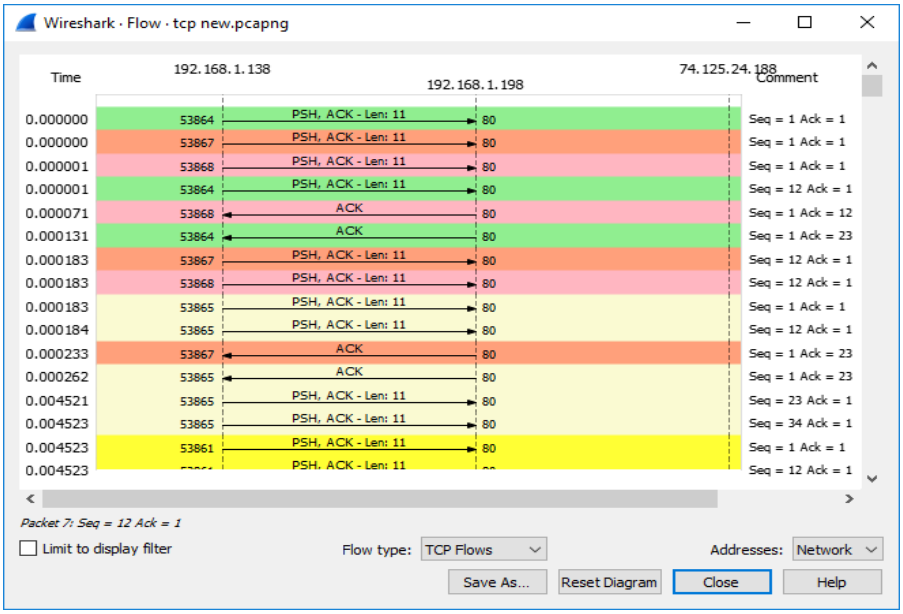

Figure 3. Screenshot of TCP Flow Graph

According to Figure 3., time is in second (s), the IP address of the source is 192.168.1.138, and the port number is random from 53861 to 53868 p (port). The IP address of the destination is 192.168.1.198, and the destination port number is 80 p (port). Here the source sends the attack packets, which have an unfixed port number. The client IP (192.168.1.138) establishes a TCP connection with the IP (192.168.1.198) called as a server. Network engineers, through Wireshark traces, could recognize some suspicious downloads (PSH ACK and TCP DUP ACK) as they belong to abnormal packets. For example, the hacker can apply PSH ACK to formulate a similar attack like TCP ACK attacks.

3.1.4 UDP Flood Attack

The second popular DDoS attack method goes to the UDP flood as it exploits UDP services by flooding malicious packets to ports on the server to determine which ports are exposed as victims. In this method, the user need to type “UDP” in a filter zone or other protocols the results will display on user interface. A flood consists of massive volumes of sent spoofed UDP packets to various ports from a single server, and the server together with ICMP responds to all requests as "destination unreachable’" notification, stating that the sources are overwhelmed. captured traffics and analyzed using Wireshark, as seen in Figure 4.

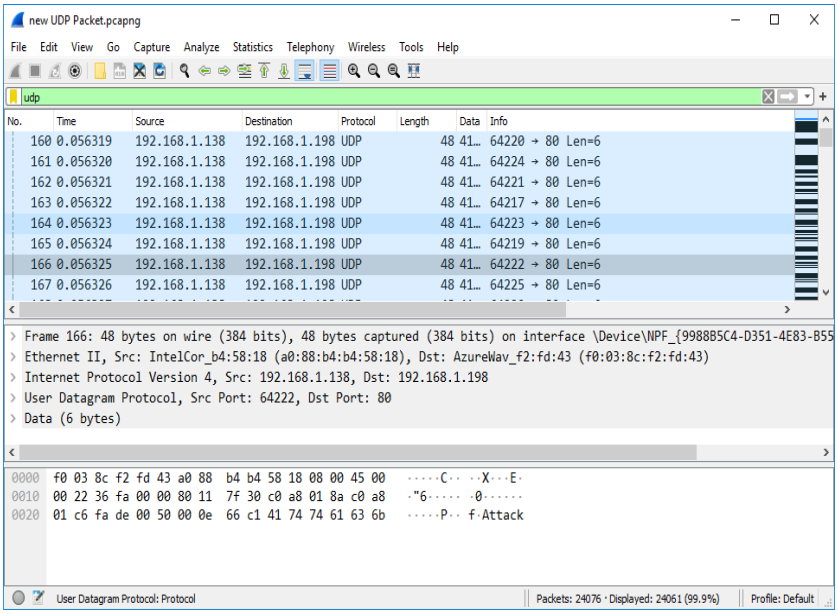

Figure 4. Analyzing UDP Flood Attack.

3.1.5 Packets analysis and identify the length of attacks

After capturing all packets needed from day one up to day three, users used Ms. Excel to identify the behavior of pattern attacks; this helps them to process and analyze all the packets captured at different times using Wireshark. Ms. Excel provides excellent information to identify the packets user captured in particular total time and the length of the packet. The impact of attacks is measured by differentiating the attack's sizes, either small or big.

All data collected from an attacker was processed using Ms. Excel by identifying the average of all data to categorize the level of attacks, such as low, medium, and high, as described in Figure 5.

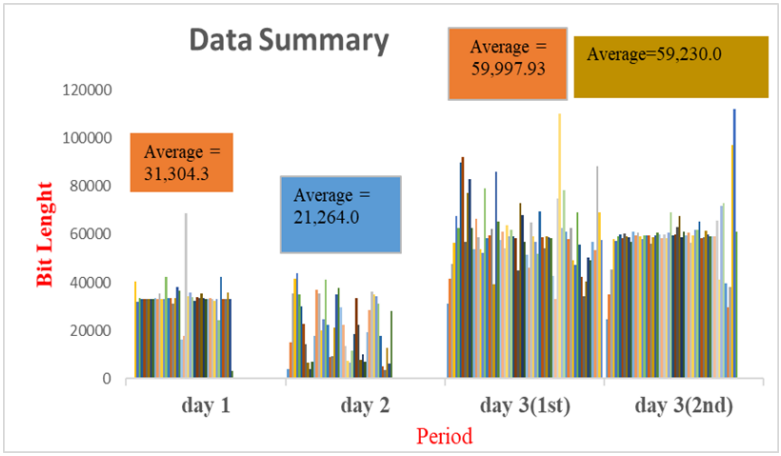

Figure 5. Average data collected in three days**.**

Figure 5. above shows the average length of captured flood packets that comes at different times depending on attackers' loads. By analyzing the average length and calculating the quartiles, users have the opportunity to identify and understand the level of attacks with a formula (Equation) as follow:

$$QN = (Dmax - Dmin) \quad (1)$$

Where:
N = 1,2,3, and 4;
Dmax = maximum average (59998,93);
Dmin = minimum average (212640).
Therefore,Range = 59998 – 21264 = 38734 bit length

$$Quartile = \frac{Range}{4} \quad (2)$$

Quartile= 9684 bit length
Q1 = 21264 to (21264 + (1 x 9684)) = 21264 to 30948
Q2 = 30949 to (21264 + (1 x 9684)) = 30949 to 40631
Q3 = 40632 to (21264 + (1 x 9684)) = 40632 to 50315
Q4 = 50316 to (21264 + (4 x 9684)) = 50316 to 59998

Table 1. describes the times the flood packets were collected: Periods (seconds), Length (s), Quartile (s), and Attack levels. Referring to the identification of quartiles and range ($Q1, Q2, Q3,$ and $Q4$), the user can easily identify the level of attacks such as low, medium, and high.

In all levels, they achieve goals by stopping a legitimate user from accessing the essential services.

Table 1. Summarizing level of attacks**.**

No	Time	Sec	Length	Quartile	Attack Level
1	06:59	48	31,304.3	Q2	Medium attack
2	14:01	48	21,264.0	Q1	Low attack
3	14:27	71	59,997.93	Q4	High attack
4	10:34	60	59,230.0	Q4	High attack

The table above illustrates the level of attacks. The intruders can attack a system using small packets with many loads; these attackers cause the targeted system to consume too much network bandwidth resources and make services unavailable to legitimate traffic. By analyzing the attack time and length of all data collected in three days, users can identify the level of attacks from Q1, Q2, and Q4 scaling systems. The average of attacks Q1 seems to be a low attack, whin means the impact is not quickly put down the server, Q2 is medium attacks where the volume of attack is upper to Q1; finally, Q4 the higher than others level attacker sent a huge of fake packets to the victim server to make source unavailable to legitimate users.

4. Results and Discussion

Nowadays, in the technology world, networking security is paramount for people. Mainly, the network allows users to communicate and access resources easily. All user’s necessity of

the internet to serve as a global information source, so the availability of the internet is crucial. Because of the services, it provides to the users, the main target of attacks is to make services unavailable. Initially, after an attacker compromising essential services such as emails, websites, and other online interactions, users are prevented from having access when a machine or the entire network connection is entirely under sabotage.

Hackers can increase the attack's level of DoS by carrying out these attacks in a distributed manner called a Distributed Denial of Service (DDoS). In a DDoS attack, a multitude of compromised machines projecting ordered strikes against a single victim [30]. An attacker sends a different type of attack, whereby multiple UDP and TCP packets with various packets of the amount at the time are sent to the victim's machine. As a result, the tool successfully monitors and captures the network packets sent by an attacker. The UDP and TCP flood attacks are considerably faster in exhausting server resources as it consumes all network bandwidth on the server's network link by denying access to legitimate users.

5. Conclusion

The availability of the internet is critical as it serves global information sources for all users; due to those advantages, the internet became the subject of attackers. One of the key challenges is to identify the DoS attack in the user network system. In this research, the researcher created DoS attacks using the LOIC tool, whereby attackers flooded unwanted packets to the victim server.

A sniffing technique is used to capture and analyze the pattern attacks (DoS) by sniffing all incoming network traffic sent by attackers to the targeted server such, as TCP, UDP, and HTTP packets. After collecting the patterns, the user identifies the packets and understands the behavior of attackers by comparing them with regular data communication. The user utilizes Ms. Excel to identify the length of data sent at different times and know the classification of attacks level by using Quartile to measure the low, medium, and high attacks.

The first example of aggressive behavior is when the attack's home base does not care whether the response from the victim is received or not yet still attacking its target with an abundance of ineffective packets.

Second, an attacker can be identified based on packet header and contents. In order to identify malicious traffic from their behaviors, the receiver first determines where the incoming packet belongs to by analyzing its tuple (source IP address, source port number, destination IP address, destination port number).

Generally, the client and web servers perform a three-way handshake to establish communication, but when the attacker transfers enormous TCP and UDP requests to the victim server, corresponding SYN-ACK replies do not exist as it consumes computer resources.

An attack is mostly intended to stop the legitimate user from accessing essential services. The level of attack varies based on their class, ranging from Q1, Q2, and Q4.

References

1. S. Sundaresan, W. De Donato, N. Feamster, R. Teixeira, S. Crawford, and A. Pescapè, "Measuring home broadband performance," *Commun. ACM*, vol. **55**, no. 11, pp. 100–109, (2012).
2. E. Y. M. Muharish, "Packet Filter Approach To Detect," *i*, (2016).
3. N. S.Mangrulkar, A. R. Bhagat Patil, and A. S. Pande, "Network Attacks and Their Detection Mechanisms: A Review," *Int. J. Comput. Appl.*, vol. **90**, no. 9, pp. 37–39, (2014).

4. D. Chasaki, Q. Wu, and T. Wolf, "Attacks on network infrastructure," *Proc. - Int. Conf. Comput. Commun. Networks, ICCCN*, no. September, (2011).
5. P. P. Laskowski, "Internet security – Technology and social awareness of the dangers," *Stud. Logic, Gramm. Rhetor.*, vol. **50**, no. 1, pp. 239–252, (2017).
6. Q. Yan and F. R. Yu, "Distributed denial of service attacks in software-defined networking with cloud computing," *IEEE Commun. Mag.*, vol. **53**, no. 4, pp. 52–59, (2015).
7. S. Pareek, A. Gautam, and R. Dey, "Different Type Network Security Threats and Solutions, A Review," *IPASJ Int. J. Comput. Sci.*, vol. volume **5**, no. issue 4, pp. 1–10, (2017).
8. P. D. Bojović, I. Bašičević, S. Ocovaj, and M. Popović, "A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method," *Comput. Electr. Eng.*, vol. **73**, no. August, pp. 84–96, (2019).
9. P. Dzurenda, Z. Martinasek, and L. Malina, "Network Protection Against DDoS Attacks," *Int. J. Adv. Telecommun. Electrotech. Signals Syst.*, vol. **4**, no. 1, (2015).
10. U. Farooq, "Network Security Challenges," *Researchgate*, no. August, pp. 2–7, (2018).
11. P. A. Devi, S. R. Laskhmi, and K. S. Vaishnavi, "A Study on Network Security Aspects and Attacking Methods," *Int. J. P2P Netw. Trends Technol.*, vol. **3**, no. 2, pp. 97–103, (2013).
12. K. Ahmad, S. Vivekananda, and U. Pradesh, "Classification of Internet Security Attacks Classification of Internet Security Attacks," *Researchgate*, no. October, pp. 1–4, (2015).
13. R. H. Puspita and D. Rohedi, "The Impact of Internet Use for Students," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. **306**, no. 1, (2018).
14. W. Dou, Q. Chen, and J. Chen, "A confidence-based filtering method for DDoS attack defense in cloud environment," *Futur. Gener. Comput. Syst.*, vol. **29**, no. 7, pp. 1838–1850, (2013).
15. S. Patil and S. Chaudhari, "DoS Attack Prevention Technique in Wireless Sensor Networks," *Procedia Comput. Sci.*, vol. **79**, pp. 715–721, (2016).
16. A. Madhuri, "Attack Patterns for Detecting and Preventing Ddos and Replay Attacks," *Int. J. Eng. Sci. Technol.*, vol. **2**, no. 9, pp. 4850–4859, (2010).
17. Z. Yi, L. Qiang, and Z. Guofeng, "A real-time DDoS attack detection and prevention system based on per-IP traffic behavioral analysis," *Proc. - 2010 3rd IEEE Int. Conf. Comput. Sci. Inf. Technol. ICCSIT 2010*, vol. **2**, no. August, pp. 163–167, (2010).
18. K. Zeb, O. Baig, and M. K. Asif, "DDoS attacks and countermeasures in cyberspace," *2015 2nd World Symp. Web Appl. Networking, WSWAN 2015*, no. June, (2015).
19. H. Rahmani, N. Sahli, and F. Kamoun, "Distributed denial-of-service attack detection," *Researchgate*, no. September 2011, pp. 2542–2554, (2011).
20. Kamesh and N. Sakthi Priya, "A survey of cyber crimes Yanping," *Secur. Commun. Networks*, vol. **5**, no. December 2009, pp. 422–437, (2012).
21. Kamesh and N. Sakthi Priya, "A survey of cyber crimes Yanping," *Secur. Commun. Networks*, vol. **5**, no. July 2014, pp. 422–437, (2012).
22. T. Ait Tchakoucht and M. Ezziyyani, "Building a fast intrusion detection system for high-speed-networks: Probe and dos attacks detection," *Procedia Comput. Sci.*, vol. **127**, pp. 521–530, (2018).
23. M. Ahmed, A. Anwar, A. N. Mahmood, Z. Shah, and M. J. Maher, "An Investigation of Performance Analysis of Anomaly Detection Techniques for Big Data in SCADA Systems," *EAI Endorsed Trans. Ind. Networks Intell. Syst.*, vol. **2**, no. 3, p. e5, (2015).
24. A. Dhaka, A. Nandal, and R. S. Dhaka, "Gray and Black Hole Attack Identification Using Control Packets in MANETs," *Procedia Comput. Sci.*, vol. **54**, pp. 83–91, (2015).
25. X. Sun, J. Dai, P. Liu, A. Singhal, and J. Yen, "Using Bayesian Networks for

Probabilistic Identification of Zero-Day Attack Paths," *IEEE Trans. Inf. Forensics Secur.*, vol. **13**, no. 10, pp. 2506–2521, (2018).
26. A. Singh and D. Juneja, "Agent Based Preventive Measure for UDP Flood Attack in DDoS Attacks," *Int. J. Eng. Sci. Technol.*, vol. **2**, no. 8, pp. 3405–3411, (2010).
27. T. Gairola and K. Singh, "A Review on DOS and DDOS Attacks in Cloud Environment & Security Solutions," *Int. J. Comput. Sci. Mob. Comput.*, vol. **57**, no. 7, pp. 136–141, (2016).
28. T. Gairola and K. Singh, "International Journal of Advanced Research in Cloud Security Issues : Counter DDOS Attack by Integrating IP Monitoring and Routing Protocol," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. **6**, no. 7, pp. 217–222, (2016).
29. A. N. Jaber, "Methods for Preventing DDoS Attacks in Cloud Computing," *Am. Sci. Publ.*, no. May 2017, 2016.
30. A. Bijalwan, M. Wazid, E. S. Pilli, and R. C. Joshi, "Forensics of Random-UDP Flooding Attacks," *J. Networks*, vol. **10**, no. 5, (2015).