A Deep and Efficient Analysis of DDOS Attack in Software Defined Network

Monika Dandotiya
Madhav Institute of Technology & Science
Rajni Ranjan Singh (rrsingh@mitsgwalior.in)
Madhav Institute of Technology & Science
Abhinandan Singh Dandotiya
Madhav Institute of Technology & Science
Nidhi Dandotiya
Madhav Institute of Technology & Science

Research Article

Keywords: DDOS attack, SDN, Review, Dense, Mitigation

Posted Date: April 15th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1501210/v1

Abstract

DDoS assaults are one of the most serious issues that the Internet has to deal with. Various defense strategies have been offered to remove this form of assault, the number of which has risen over the research period. However, no detection method capable of entirely thwarting the assaults has yet been discovered. As a result, computer security experts must be vigilant in detecting and defending against DDoS assaults. This study gives a comprehensive assessment of the scholarly literature on DDoS attack detection strategies. The key components of detection have been defined based on the literature. Methods, variables, tools-kits, positioning site, point in time, and detection precision were recognized as four factors for examination in this inquiry. It was discovered that each strategy for detecting assaults takes use of certain aspects of network load, user requirements, and specialized kits. Finally, it was able to pinpoint the mechanisms with the greatest impact. The datasets they utilize, for example, can affect detection accuracy. It's been determined that a thorough examination of the aforementioned components of DDoS attack detection underwrite the development of an adequate approach for Defending against the attacks. These approaches bank on better router functionality or fluctuations to present protocols. The pros and cons of current research approaches in this issue are also describe.

1 Introduction

During the previous few years, DDoS assaults have gotten a lot of attention on the internet. Introduced and extensively investigated in the last several years are the ideas and methods behind Software Defined Networking (SDN). Due to the modifications in architecture b/w the SDN network and the conventional network, DDoS attacks can endanger the SDN's availability. The SDN controller in particular is very susceptible to DDoS occurrences. In general, a DoS attack aims to stop legitimate users from retrieving a network's resources. A DoS attack on an SDN was carried out by Shin and Gu [1] using independent logic in SDN control and data planes, with an n/w scanning tool was devised to identify an SDN. When they implemented their method, they used a scanner that could scan the network and variation in network header fields to gather time values for existing and new flow response times because the controller was querying the data path. Flow requests were sent to target n/w, which were sent through the data track to controller once the network was determined to be an SDN network. Because more data flows mean more requests for flow setup on controllers, this will eventually result in a broken data path. According to Fonseca et al. [2], an SDN controller DDoS assault happens when an attacker sends IP packets with random headers to overload controller. To make [2] more stable, a second controller was employed. Though a DDoS detection system was needed meanwhile secondary regulators may also be targeted by DoS or DDoS assaults, hence it was vital to have one. In this case, the use of multiple controllers still wouldn't be enough to solve the problem of DDoS attacks, because multiple controllers could fail at the same time. [3] [4]. A DDoS attack can hurt SDN controllers if the Internet Service Provider doesn't protect them (ISP) [5]. DDoS attacks that are malicious and have 500 or 600 Mbps of speed aren't going to fill up the target's internet connection, but the controller and the whole network could be down. It could be attacked because the controller is the only thing that could go wrong with the whole network. It happens

when a client asks for something that doesn't match an existing flow in an SDN OpenFlow network. The switch is told to send a packet event to the controller. The controller can then make a judgement about how best to deal with the request, or not. Often, a DDoS assault is carried out by delivering a stream of packets to a victim. This stream takes up a vital resource, rendering it unavailable to the victim's genuine customers. An intruder may send you a few messages that aren't what they appear to be if your computer is under attack. The computer may freeze or reboot as a result of a programmed or protocol becoming confused. September 2002 saw a large number of assaults on the Internet infrastructure that did not specifically target any individuals. Taking over machines in a victim network and using up a crucial resource is another approach to prevent service. This prevents authorized clients from the same network from accessing any service either within or outside the network. This is by no means an exhaustive list.

1.1 DA: Degree (Automation)

Every operation of recruiting, infecting, exploiting, and utilizing may be done manually or automatically. We distinguish between manual, semiautomatic, and automated DDoS assaults grounded on degree of automation. Only initial types of attack attacks were categorized as manual. Almost all components of employment process were quickly automated. Semi-Automatic DA-2 The DDoS network in semi-automated assaults is made up of handler (master) and agent devices. Automated processes are used to recruit, exploit, and infect. When an attack begins, the attacker communicates this information to the agents, who then refer packets to the victim through a handler. Communication Mechanism (DA-2:CM) (DA-2:CM) [8].

1.2 Direct Communication

1.2.1 (DA-2:CM-1)

To communicate during straight communication assaults, the agent and handler machines must know one other's identities. This is commonly accomplished by hard-coding the handler machines' IP addresses into the attack code, which is then installed on agent system. Each agent then informs the handlers of his or her readiness, and the handlers save the agent's IP address for future contact. For the attacker, the obvious disadvantage of this strategy is that the detection of one hacked system can depiction the entire DDoS network. Furthermore, because agents and handlers attend to network influences, n/w scanners can identify them [9].

1.2.2 DA-2:CM-2:

Communication that isn't straight Indirect communication attacks synchronize agent operations by using a lawful communication service. IRC (Internet chat programmed) channels have been utilized in recent attacks. The usage of IRC services substitutes function of a handler since the IRC channel proposals adequate anonymity for an attacker. Scanners will not be able to separate the agents' control packets from typical IRC activity since they do not actively listen to n/w connections (thus avoiding detection). IRC server's ability to detect connected clients is utilized to identify the DDoS network. Attackers

commonly employ channel hopping to evade detection even further, by using any IRC channel for a limited period. Investigations are hindered by a wide distribution of the Internet's IRC service and the fact that a given IRC server might be located anywhere in the globe. IRC is the first recognized example of indirect communication, although other permitted systems may be corrupted by attackers to achieve the same purposes [10].

1.3 DA-3: Automatic

There is no prerequisite for contact between the DDoS attacker and any of the agent machines in an automatic DDoS assault because the whole process is automated. The attack code sets the time, attack type, period, and target of attack in advance. Attackers in this attack class are only exposed to one command, which is given at the beginning of recruitment. This limits the attacker's exposure to a minimum. Either the DDoS network is being used for a single purpose, or the system is rigid because of the attack's hardcoded specification. The transmission techniques, on the other hand [11]. The first part defines the overview of DDoS attacks, second part gives the state of art methods in the area of literature review. Section third defines the analysis part and the last section defines the conclusive point.

2 Literature Review

According to the guidelines, the search results were narrowed down using inclusion and exclusion criteria. To determine if these works are relevant to the current study, a preliminary examination of their content was required.

Some DDoS detection approaches were proposed by the authors in [12–14]. Researchers found that the SDN's behavior features were critical to detect DDoS attacks, even though these approaches were sensitive to other conditions. Our research thus included several elements and traffic behavior analysis in response to a DDoS assault to give suggestions for SDN DDoS detection. The Detection Algorithms Based on the Degree of Attack and DDoS Detection Algorithms Based on ML (DDML) have also been presented (named DAMDL) (called DAMDL).

The suggested methods are capable of detecting DDoS assaults in the SDN context. The most prevalent cyber-attacks are distributed denial of service assaults (DDoS). Consequently, academics are becoming more interested in DDoS detection methods. The development of these systems necessitates the creation of statistical and machine learning models. Modeling accuracy is the primary goal of mechanism design. Research into these approaches' scalability and performance is critical because of the massive volume of network traffic. DDoS assaults are detected using the Apache Spark framework in this investigation. For experimental study, this work employs the NSL-KDD Cup dataset. The results reveal that in terms of pre-processing and training time, random forests outperform decision trees, and that distributed dispensation progresses presentation using pre-processing and training period [15][16].

In [17–19] the author proposed two ways for detecting DDoS attacks in SDN. To identify a DDoS assault, one way uses the severity of the attack. The updated KNN approach based on Machine Learning (ML) is

utilized in the other strategy to identify the DDoS assault. The outcomes of the theoretical study, as well as the practical results on datasets, demonstrate that our suggested approaches are more successful than existing methods at identifying DDoS assaults. For decades, the Distributed Denial of Service (DDoS) assault has significantly affected network availability, and there is still no real protective mechanism in place. However, the growing Software Defined Networking (SDN) technology offers a new method to consider DDoS defenses.

In Internet, DDoS attacks are a rapidly increasing threat. The war between the shield and the sword continues in sphere of DDoS attacks, as it does in all other areas of cybersecurity. Attackers are becoming more sophisticated in their approaches. Solution vendors are following suit, launching new products to thwart nefarious intent. To avoid becoming a victim of cybercriminals, old tools must be replaced with fresh approaches and tools. Under the effect of shifting cybercriminal techniques, this document analyses the development route that technologies for preventing DDoS attacks take [20][21].

The graph of above Fig. 2 depicts the most significant statistics in field of DDoS attacks for publication. The trend in quantity of articles available demonstrates priority that the scientific community has placed on this field of study.

DDoS includes overwhelming a targeted system's bandwidth or resources in order to make an online service inaccessible. Insider attacks are easier to perpetrate when an insider with legitimate access to system circumvents any security restrictions. This study presents a moving target defensive technique that isolates insiders from innocent customers utilizing attack proxies to combat insider-assisted DDoS attacks. In cloud computing, DDoS assaults necessitate rapid data absorption. DDoS attack mitigation is usually accomplished by dynamically scaling cloud resources to immediately recognize and combat the onslaught features. The resource scaling comes at a cost, which in the case of lengthier, more sophisticated, and recurrent attacks, could prove to be a significant disruption. We study whether resource scaling during an assault always leads to quick DDoS mitigation in this research. We execute real-time DDoS assault studies to examine attack absorption and mitigation for several target services in the occurrence of dynamic cloud resource increasing for this aim. The high resource use created by the attack has been proved to imperil jobs for example attack absorption, which delivers quick attack data i/p to attack analytics. Further, an effective technique to identify and mitigate insider attacks is created using the load balancing idea, with a goal of exploiting attack isolation while lowering the overall quantity of proxies applied [22][23].

The DDOS Attempt in Different Countries is depicted in the graph above in Fig. 3. DDoS Attempts from the top 10 nations are shown in Fig. 3. Even the Microsoft blog claims that if a 30 Mbps attack goes undetected, it can cause service outages.

The graph above in Fig. 4 depicts the frequency of attacks in various countries. It is clear that this technique is the most widely utilized. Six assault detection studies use entropy. This technique is employed because it enables the identification of DDoS attacks by classifying sure properties of a data flow.

3 Analysis

The obtained data were examined with the research questions as a reference. The results are accessible in tables that include an explanation of the feature under investigation as well as the names of the authors who employed it

Q1. What are main detection methods used?

Table 1
Anti-DDOS attack detection methods.

Serial Number	Techniques	Description
1	Cluster analysis [24]	CA is a way of categorizing data so that items in one group are identical to those in other groups but different from those in other groups. If variables complicated in the attack are dissimilar, we can use cluster analysis to divide normal traffic and every stage of the DDoS assault into separated clusters.
2	The Correlation analysis [25]	Correlation is a term applied to indicate how comparable two flows are. It may, however, suggest zero connection in rare circumstances. Even though the two flows are connected, there is a phase variation between them.
3	Genetic algorithms [26]	This sort of heuristic search is inspired by natural evolution and is known as a genetic algorithm. It is one of the larger families of evolutionary algorithms (EA) that use the principles of natural evolution to solve optimization issues. Genetic algorithms
4	KNN [27]	KNN technique is a feature space prediction approach that uses the k-closest training samples to forecast flow classes. The majority vote of a flow's neighbors is used to classify it.
5	Filtering of Hop-Count [28]	When calculating overall hop count for this IP address, the source IP address is applied as an index. If the packet's determined hop-count ties its stored hop-count, it has been verified.
6.	Joint Deviation Rate (JDR) [29]	JDR (Joint Divergence Rate) is a novel statistic for describing the rate of deviation of network traffic states. The variations of all the numerous characteristics in Network Traffic State are combined in JDR (NTS).
7	Fuzzy logic [30]	On the mean packet between arrival times, a fuzzy estimator is used. It does a good job at understanding the rules, but it has the drawback of not being able to learn them automatically.
8	Hidden semiMarkov model (HsMM) [31]	An HsMM method that detects App-DDoS assaults during a flash crowd event and characterizes the stochastic process as it changes over time.
9	Firewall [32]	As with the previous firewall function, the defender has the ability to select a number that is beginning over which all packets in a flow are discarded.
10	Cuckoo search [33]	The parasitic behaviour of some Cuckoo birds sparked this technique. Cuckoo species are unable to finish their reproductive cycle without a suitable host.

The data in the Table 1 above summarizes the findings of 10 different research on how to identify DDoS attacks. The computational and logical capabilities of this approach make it the most preferred for spotting discrepancies in data flow.

Q.2 How precise are the approaches for detecting a DDoS attack?

Flows and DDoS datasets were used in this research, and only studies with a detection or accuracy rate of more than or equal to 99 percent were examined. The following equation may be used to calculate the detection rate: TN DDoS attacks may be detected with high accuracy using these methods.

Table 2
Detection methods of DDoS attack which presented best ratios.

Detection Rate (%)	Researches	Dataset
99.76	[34]	CAIDA, TUIDS and DARPA
98.45	[35]	Generation of CAIDA 2007, DARPA 2009, BONESI
98.34	[36]	KDD Cup (1999)
97.31	[37]	Knowledge Discovery and Data mining (KDD) Cup (1999)

As indicated in Table 2, achieved the highest level of precision with their detection technique. This mechanism was discovered 99.9% of the time. This strategy combines three methods to do this (Random Forest, nearest K-neighbors, and Bagging). Furthermore, because this strategy is network-based, detection occurs during the assault, limiting the impact once the system recognizes it.

Q 3 In a DDOS attack, where are detection measures used?

DDoS detection techniques can be applied at four separate points: source, destination, network, and hybrid. The source of the assault is referred to as source, while the target of the attack is referred to as a destination. The network is where information flows, and hybrid denotes that detection takes place in multiple areas, with collaboration between implementation sites being the norm. The four implementation sites, as well as the writers who use them, are listed in Table 3.

Table 3
Locations where detecting systems are put into place.

Studies	Deployment Position	Total
[38–41]	Source	3
[42–50]	Destination	7
[51–65]	Hybrid	13
[66–70]	Network	4

Network has included the bulk of the detection approaches, accounting for roughly 58 percent of the total quantity, as shown in the table below. As a result, the mechanisms use Networks more frequently while creating a detection method. The Source, on the other hand, is where the approaches are used on a smaller scale since they require a high level of data network collaboration, which limits the creation of a bigger number of data networks of devices capable of anticipating an attack.

Q 4 In a DDOS attack, where are defensive techniques used?

Table 4
Review overview[71].

Defense Method	Benefit	Loopholes
Defense Architecture (Victim-end) [72]	Because web servers that provide harmful services are always attempting to safeguard their resources from legitimate users, this is the most realistic protection approach.	During DDoS assaults, the victim's resources, such as broadband networks, are typically overburdened, and these techniques are unable to block traffic from going through the victim's routers.
Defense Architecture (Source-end) [73]	In the input stage, the mitigation mechanism takes less amount of resources to test the smallest quantity of traffic.	DDoS assaults are difficult to detect on the source side since sources are widely dispersed over the network and one source might appear to be normal traffic.
Defense Architecture (Core-end) [74]	Traffic is aggregated, which means that legitimate packets and malicious packets arrive at the same time at the router, which is the optimum spot to limit all traffic.	All Internet routers should employ this discovery approach for optimum accuracy, as being unobtainable on a router might interfere with discovery and espionage methods.

Findings suggest that present mitigation measures are only appropriate in certain situations or designs. There are several promising ideas, but they lack experimental evidence, demanding more study to prove their validity and utility in DDoS mitigation. Additionally, there are still questions about the approaches' scalability in real-world circumstances, which is being researched. Data utilized in learning systems may also be outdated, reducing the effectiveness of the solutions that are now in use. The ever-increasing complexity and volume of DDoS assaults necessitate the evaluation of current and future solutions in the context of real-world scenarios. Traffic and infrastructure must be able to mimic real-world conditions in simulation scenarios.

4 Conclusion

In this study's comprehensive assessment of the literature, the key components associated with the detection of DDoS attacks were revealed, with an emphasis on strategies, variables, tools, as well as areas where it was done with the point of detection throughout period. The study's findings provided replies to the six research queries that were submitted. We've discussed many ways for detecting and mitigating DDoS attacks, as well as their benefits and drawbacks, depending on when and where they're

detected in reaction to DDoS assaults. To ensure that data flows are evaluated before they spread a server, the most commonplace is to implement a method in the network. Because detection occurs in real-time during an attack, this is the most common moment to apply a tactic.

Declarations

Conflicts of Interest. There is no conflict of interest in this paper.

Acknowledgments. I would like to express my very great appreciation to Dr. Rajni Ranjan Singh Makwana for his valuable and constructive development of this research work. His willingness to give his time generously has been very much appreciated.

Funding declaration This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

1. Anstee, D., Chui, C.F., Bowen, P., Sockrider, G.: Worldwide Infrastructure Security Report. Arbor Networks Inc., Westford (2017)
2. Zargar, S.T., Joshi, J., Tipper, D.: A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks. IEEE Commun. Surv. Tutorials **15**(4), 2046–2069 (2013)
3. Cao, Y., Gao, Y., Tan, R., Han, Q., Liu, Z.: Understanding internet DDoS mitigation from academic and industrial perspectives. IEEE Access. **6**, 66641–66648 (2018)
4. Hoque, N., Bhattacharyya, D., Kalita, J.: Botnet in DDoS attacks: trends and challenges. IEEE Commun. Surv. Tutor. **99**, 1–1 (2015)
5. Criscuolo, P.J.: Distributed Denial of Service, Tribe Flood Network 2000, and Stacheldraht CIAC-2319. Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev, 1. Lawrence Livermore National Laboratory (2000)
6. Todd, B.: (2000) Distributed Denial of Service Attacks. [online] http://www.linuxsecurity. com/resource files/intrusion detection/ ddos–whitepaper.html
7. Mirkovic, J., Reiher, P.: A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communications Review **34**(2), 39–53 (2004)
8. Ranjan, S., Swaminathan, R., Uysal, M., Knightly, E.: DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection. IEEE INFOCOM'06 (2006)
9. Chang, R.K.C.: Defending against flooding-based distributed denial of service attacks: A tutorial Computer. J. IEEE Communication Magazine **40**(10), 42–51 (2002)
10. Puri, R.: (2003) Bots and Botnet –an overview. [online] http://www.giac.org/practical/GSEC/ RamneekPuriGSEC.eps
11. CERT, (2001) Denial of Service Attacks. [online] http://www.cert.org/tech tips/denial of service.html

12. Shin, S., Gu, G.: (2013) Attacking software-defined networks: A first feasibility study. in Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw. (HotSDN), pp 165–166
13. Liu, J., Xiao, Y., Ghaboosi, K., Deng, H., Zhang, J.: (2009) Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures. EURASIP Journal Wireless Communications and Networking 1–11
14. Rodríguez-Gómez, R.A., Maciá-Fernández, G., García-Teodoro, P.: Survey and taxonomy of Botnet research through life-cycle. ACM ComputSurv (CSUR) **45**(4), 45 (2013)
15. Kousar, H., Mulla, M.M., Shettar, P., NDG: (2021) DDoS Attack Detection System using Apache Spark. International Conference on Computer Communication and Informatics (ICCCI), pp 1–5. doi: 10.1109/ICCCI50826.2021.9457012
16. Jia, B., Liang, Y.: Anti-D chain: A lightweight DDoS attack detection scheme based on heterogeneous ensemble learning in blockchain. China Commun. **17**(9), 11–24 (2020). doi:10.23919/JCC.2020.09.002
17. Dong, S., Sarem, M.: DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks. IEEE Access. **8**, 5039–5048 (2020). doi:10.1109/ACCESS.2019.2963077
18. Bhuyan, M.H., Kashyap, H.J., Bhattacharyya, D.K., Kalita, J.K.: Detecting distributed denial of service attacks: methods, tools and future directions. Comput. J. **57**(4), 537–556 (2013)
19. Devi, S.R., Yogesh, P.: A hybrid approach to counter application layer DDoS attacks. Int. J. Crypt. Inform. Secur. (IJCIS) **2**(2), 45–52 (2012)
20. Cheskidov, P., Nikolskaia, K., Minbaleev, A.: (2019) Choosing the Reinforcement Learning Method for Modeling DDos Attacks. International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), pp 1–4. doi: 10.1109/FarEastCon.2019.8934416
21. Saleh, M.A., Abdul Manaf, A.: (2015) A novel protective framework for defeating HTTP-based denial of service and distributed denial of service attacks. The Scientific World Journal, 2015:19. https://doi.org/10.1155/2015/238230
22. Kansal, V., Dave, M.: (2017) DDoS attack isolation using moving target defense. International Conference on Computing, Communication and Automation (ICCCA), pp 511–514. doi: 10.1109/CCAA.2017.8229853
23. Somani, G., Gaur, M.S., Sanghi, D., Rajarajan, M. M: Scale Inside-Out: Rapid Mitigation of Cloud DDoS Attacks. IEEE Trans. Dependable Secur. Comput. **15**(6), 959–973 (2018). doi:10.1109/TDSC.2017.2763160
24. Jean Shilpa, V., Jawahar, V.K.: Advanced Optimization by Profiling of Acoustics Software Applications for Interoperability in HCF Systems. Journal of GreenEngineering. Alpha publishers **9**(3), 462–474 (2019)
25. Radha, P., Preethi, B.Meena B: Machine Learning Approaches For Disease Prediction From Radiology And Pathology Reports. J. Green Eng. Alpha publishers **9**(2), 149–166 (2019)

26. Higgins, K.J. (2010) Researchers to Demonstrate New Attack That Exploits HTTP. [online] http://www.darkreading.com/vulnerability-management/167901026/security/attacks-reaches/228000532/index.html
27. Kumar, A.S.: (2018) Obfuscating Software puzzle for Denial of Service attack mitigation. Int. J. Pure Appl. Math. 115–122. doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2016.45
28. Kowsigan, M., Priyadharshini, S.: Security in Data & Dissemination of Distributed Data in Wireless Sensor Network. Int. J. Pure Appl. Math. **118**, 1513–1520 (2018)
29. Higgins, K.J. (2010) Researchers to Demonstrate New Attack That Exploits HTTP. [online] http://www.darkreading.com/vulnerability-management/167901026/security/attacks-reaches/228000532/index.html
30. Bhuvaneswari, K., Rauf, H.A.: (2009) Edgelet based human detection and tracking by combined segmentation and soft decision. International Conference on Control Automation, Communication and Energy Conservation, Issue 5204487
31. Hoque, N., Bhattacharyya, D.K., Kalita, J.K.: Botnet in DDoS Attacks: Trends and Challenges. IEEE Commun. Surv. Tutorials **17**(4), 2242–2270 (2015)
32. Alomari, E., Manickam, S., Gupta, B.B., Karuppayah, S., Alfaris, R.: Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art. Int. J. Comput. Appl. **49**(7), 24–32 (2012)
33. Kanmani, R., Basha, A.J.: Performance analysis of wireless OCDMA system using OOC, PC and EPC codes. Asian J. Technol. **15**(12), 2083–2089 (2016)
34. Peng, T., Leckie, C., Rao, R.M.: (2004) Detecting distributed denial of service attacks using source IP address. monitoring. Proceedings of the 3rd International IFIP-TC6 Networking Conference, Athens, Greece, Springer-verlag, pp 771–782
35. Cheng, J., Yin, J., Wu, C., Li, Y.: (2009) DDoS attack detection method based on linear prediction model. Proceedings of the 5th international conference on Emerging intelligent computing technology and applications, Ulsan, South Korea, Springer-Verlag, pp 1004–1013
36. Udhayan, J., Hamsapriya, T.: Statistical segregation method to minimize the false detections during DDoS attacks. Int. J. Netw. Secur. **13**, 152–160 (2011)
37. Gilad, Y., Herzberg, A.: LOT: A defense against IP spoofing and flooding attacks. ACM Trans. Inform. Syst. **15**(2), 1–30 (2012). https://doi.org/10.1145/2240276.2240277
38. Shimeles, S.N., Katos, V., Karakas, A.S., Papadopoulos, B.K.: Real time DDoS detection using fuzzy estimators. Comput. Secur. **31**, 782–790 (2012)
39. Spyridopoulos, T., Karanikas, G., Tryfonas, T., Oikonomou, G.: A game theoretic defence framework against DoS/DDoS cyber-attacks. Comput. Secur. **38**, 39–50 (2013). doi:10.1016/j.cose.2013.03.014
40. Liu, Y., Cukic, B., Gururajan, S.: Validating neural network-based online adaptive systems: A case study. Softw. Qual. Jounal **15**, 309–326 (2007)

41. Liu, Y., Li, J., Gu, L.: (2010) DDoS Attack Detection Based on Neural Network. Proceedings of IEEE 2nd International Symposium on Aware Computing (ISAC), pp 196–199. doi: 10.1109/ISAC.2010.5670479
42. Agarwal, P.K., Gupta, B., Jain, S., Pattanshetti, M.K.: Estimating Strength of a DDoS Attack in Real Time Using ANN Based Scheme. Commun. Comput. Inform. Sci. (Springer) **157**, 301–310 (2011)
43. Chang-Lung, T., Chang, A.Y., Ming Szu, H.: (2010) Early Warning System for DDoS Attacking Based on Multilayer Deployment of Time Delay Neural Network. Proceedings of IEEE 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), pp 704–707
44. Jalili, R., Imani-Mehr, F., Amini, M., Shahriari, H.R.: (2005) Detection of distributed denial of service attacks using statistical pre-processor and unsupervised neural networks. Proceedings of the International conference on information security practice and experience, Singapore, Springer-verlag, pp 192–203
45. Karimazad, R., Faraahi, A.: (2011) An anomaly-based method for DDoS attacks detection using rbf neural networks. Proceedings of the International Conference on Network and Electronics Engineering, IACSIT Press, Singapore, pp 44–48
46. Gavrilis, D., Dermatas, E.: Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features. Comput. Networks ISDN Syst. **48**, 235–245 (2005)
47. Wu, Y.C., Tseng, H.R., Yang, W., Jan, R.H.: DoS detection and traceback with decision tree and grey relational analysis. Int. J. Ad Hoc Ubiquitous Comput. **7**, 121–136 (2011)
48. Kumar, P., Selvakumar, S.: Distributed denial of service attack detection using an ensemble of neural classifier. Comput. Communication **34**, 1328–1341 (2011)
49. Akela, A., Bharambe, M., Reiter, M., Seshan, S.: (2003) Detecting DDoS attacks on ISP networks. Proceedings of the Workshop on Management and Processing of Data Streams, ACM, San Diego, CA, pp 1–2
50. Nguyen, H., Choi, Y.: Proactive detection of DDoS attacks utilizing k-NN classifier in an Anti-DDoS framework. Int. J. Electr. Comput. Syst. Eng. **4**, 247–252 (2010)
51. Gil, T.M., Poletto, M.: (2001) MULTOPS: a data-structure for bandwidth attack detection. Proceedings of the 10th conference on USENIX Security Symposium, vol 10, Berkeley, CA, USA, pp 13–17
52. Thomas, R., Mark, B., Johnson, T., Croall, J.: (2003) Net Bouncer:Client-legitimacy-basedhigh-performance DDoS filtering. Proceedings of the 3rd DARPA Information Survivability Conference and Exposition, Washington, DC, IEEE CS, USA, pp 111–113
53. Wang, J., Phan, R.C.W., Whitley, J.N., Parish, D.J.: (2010) Augmented attack tree modelling of distributed denial of services and tree-based attack detection method. Proceedings of the 10th IEEE International Conference on Computer and Information Technology, Bradford, UK, 1009–1014
54. Limwiwatkul, L., Rungsawang, A.: (2004) Distributed denial of service detection using TCP/IP header and traffic measurement analysis. Proceedings of the IEEE International Symposium Communications and Information Technology, Sapporo, pp 605–610

55. Zhang, G., Parashar, M.: Cooperative defence against DDoS attacks. J. Res. Pract. Inform. Technol. **38**, 1–14 (2006)
56. Wu, D., Lu, K., Fan, J., Todorovic, S., Nucci, A.: Robust and efficient detection of DDoS attacks for large-scale internet. Comput. Netw. **51**, 5036–5056 (2007)
57. Hwang, K., Dave, P., Tanachaiwiwat, S.: (2003) Net Shield: Protocol anomaly detection with datamining against DDoS attacks. Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection, Pittsburgh, PA, Springer-verlag, pp 8–10
58. Chen, Z., Chen, Z., Delis, A.: An inline detection and prevention framework for distributed denial of service attacks. Comput. J. **50**, 7–40 (2007)
59. Lee, K., Kim, J., Kwon, K.H., Han, Y., Kim, S.: DDoS attack detection method using cluster analysis. Expert Syst. Appl. **34**, 1659–1665 (2008)
60. Sekar, V., Dueld, N., Spatscheck, O., van der Merwe, J., Zhang, H.: (2006) LADS: large-scale automated DDoS detection system. Proceedings of the annual conference on USENIX Annual Technical Conference, Boston, MA, USENIX Association, pp 16–29
61. Rahmani, H., Sahli, N., Kammoun, F.: (2009) Joint entropy analysis model for DDoS attack detection. Proceedings of the 5th International Conference on Information Assurance and Security, IEEE CS, Xian, China, pp 267–271
62. Xiang, Y., Li, K., Zhou, W.: Low-rate DDoS attacks detection and traceback by using new information metrics. IEEE Trans. Inf. Forensics Secur. **6**, 426–437 (2011)
63. Francois Aib, I.J., Boutaba, R.: Fire Col: A collaborative protection network for the detection of flooding DDoS attacks. IEEE/ACM Trans. Netw. **20**, 1828–1841 (2012)
64. Jeyanthi, N., Iyengar, N.C.S.N.: An entropy-based approach to detect and distinguish DDoS attacks from flash crowds in VoIP networks. Int. J. Netw. Secur. **14**, 257–269 (2012)
65. Li, M., Li, M.: (2009) A new approach for detecting DDoS attacks based on wavelet analysis. Proceedings of the 2nd International Congress on Image and Signal Processing, Tianjin, China, pp 1–5
66. Zhong, R., Yue, G.: (2010) DDoS detection system based on data mining. Proceedings of the 2nd International Symposium on Networking and Network Security, Academy Publisher, Jinggangshan, China, pp 062–065
67. Agrawal, R., Srikant, R.: (1994) Fast algorithms for mining association rules in large databases. Proceedings of the 20th International Conference on Very Large Data Bases, Morgan Kaufmann Santiago de Chile, Chile, pp 487–499
68. Dainotti, A., Pescape, A., Ventre, G.: A cascade architecture for DoS attacks detection based on the wavelet transform. J. Comput. Secur. **17**, 945–968 (2009)
69. Tripathi, S., Gupta, B., Almomani, A., Mishra, A., Veluru, S.: Hadoop based defense solution to handle distributed denial of service (ddos) attacks. J. Inform. Secur. **4**(03), 150 (2013)

70. Waguih, H.: A data mining approach for the detection of denial of service attack. IAES Int. J. Artif. Intell. **2**(2), 99 (2013)
71. Jain, A., Singh, A.K.: Distributed denial of service (ddos) attacks-classification and implications. J. Inform. Oper. Manage. **3**(1), 136 (2012)
72. Ni, T., Gu, X., Wang, H.: Detecting DDoS Attacks Against DNS Servers Using Time Series Analysis. Indonesian J. Electr. Eng. Comput. Sci. **12**(1), 753–761 (2014)
73. Criscuolo, P.J.: (2000) Distributed denial of service, tribe flood network 2000, and stacheldraht CIAC-2319, Department of Energy Computer Incident Advisory Capability (CIAC). UCRL-ID-136939, Rev. 1., vol 19, Lawrence Livermore National Laboratory
74. Choi, J., Choi, C., Ko, B., Kim, P.: A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment. Soft. Comput. **18**(9), 1697–1703 (2014)

Figures

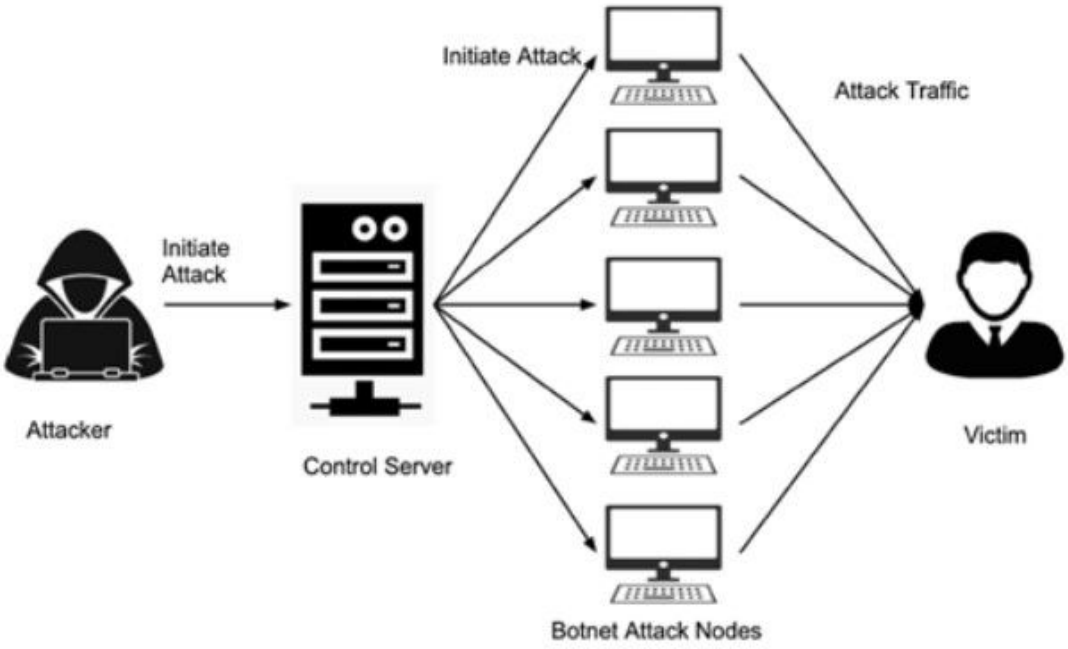

Figure 1

DDoS attack mechanisms taxonomy [7]

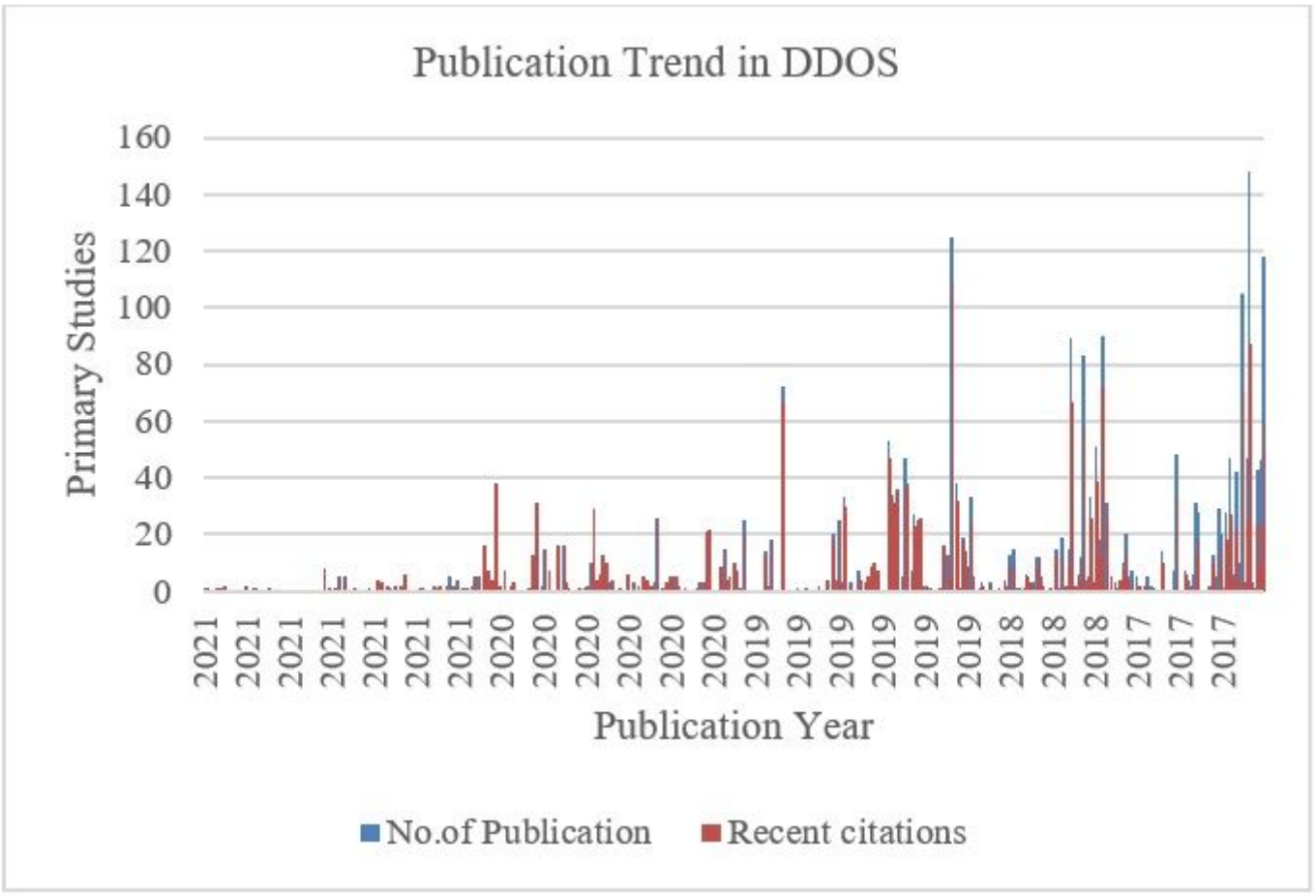

Figure 2

The publication trend in the area of DDoS

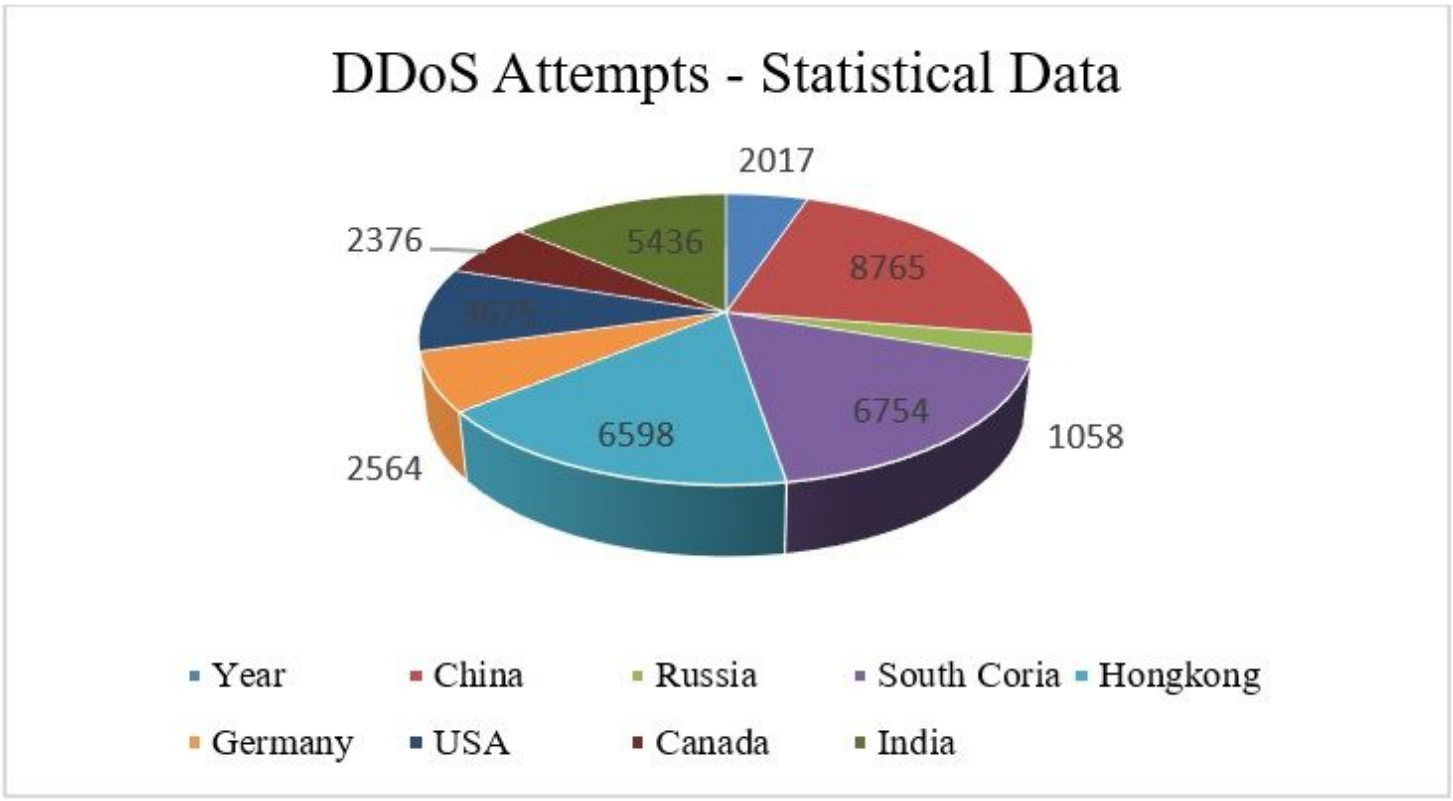

Figure 3

The DDoS attempt in different countries

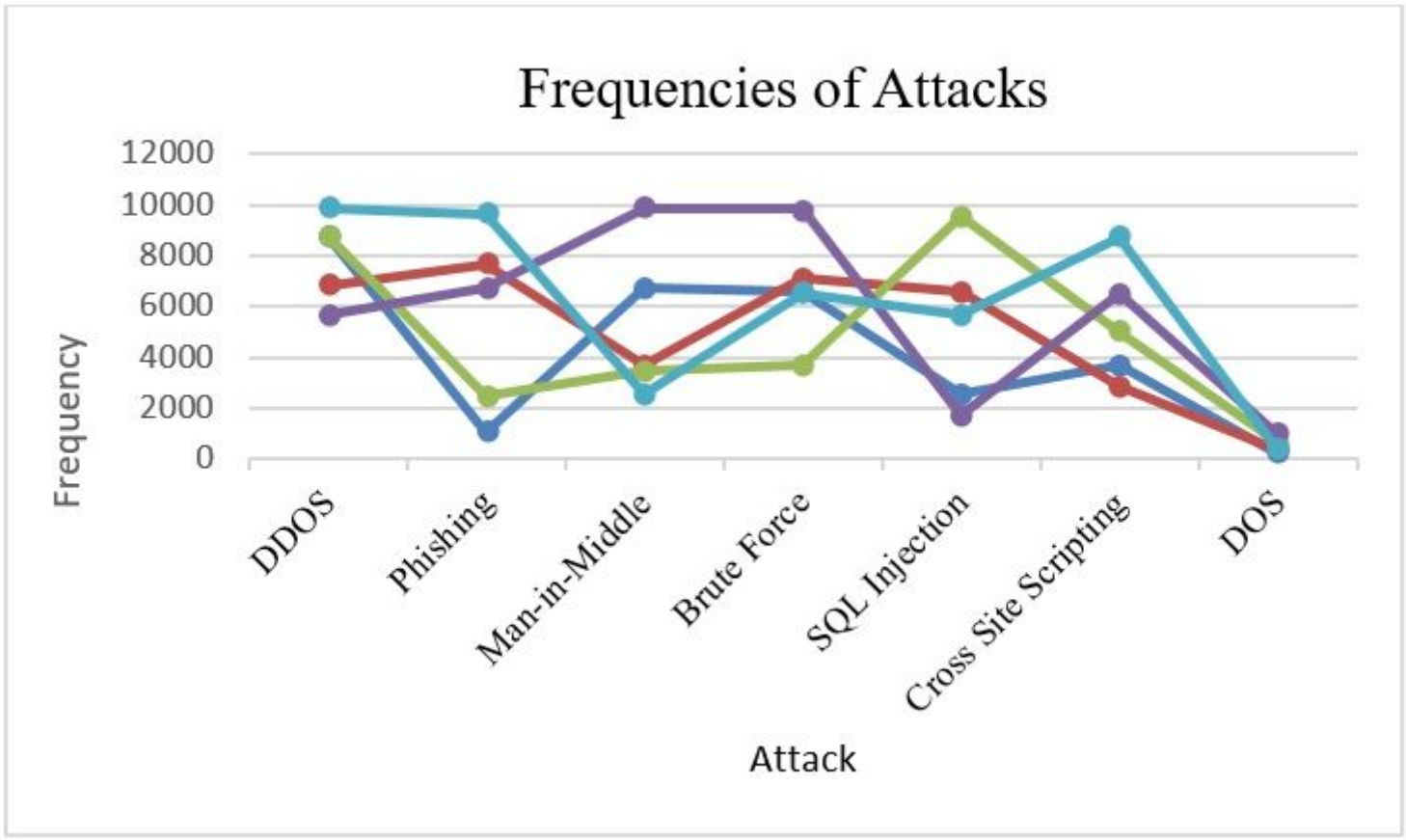

Figure 4

The frequencies of attacks in different countries