A New Model for Real-Time Intrusion Prevention Systems for DDoS Attacks

Mohammed Nadir Bin Ali, Mohamed Emran Hossain, Touhid Bhuiyan, Mohammed Shamsul Hoque, and J. Karthikeyan

Abstract Nowadays the internet has made a momentous impact on our daily life but we are not safe enough in the internet world. Last two decades, network security scholars have shown several innovative and practical solutions to save us from network and internet attacks. Among all the internet threats denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks are considered the most notorious and devastating ones. These attacks are one of the main threats that are a serious security problem for today's internet. To exhaust the resources of target networks, these attacks are launched by generating a huge amount of network traffic. This study proposes a new model for real-time intrusion prevention systems for DDoS attacks. It is true that creative attackers are continuously developing effective attacking tools and techniques to impose maximum damage due to the rapid technological advancement. The proposed Efficient Detection System of Network Intrusion (EDSONI) model makes use of both the detection and prevention of this malicious activity properly. CICIDS2017 dataset has been applied to this proposed system to experiment with the detection and prevention performance.

Keywords DDoS · EDSONI · Attack · Detection · And prevention

M. N. B. Ali (✉) · M. E. Hossain · T. Bhuiyan · M. S. Hoque
Daffodil International University, Dhaka, Bangladesh
e-mail: it@daffodilvarsity.edu.bd

M. E. Hossain
e-mail: emran@daffodilvarsity.edu.bd

T. Bhuiyan
e-mail: tauhidt.bhuiyan@daffodilvarsity.edu.bd

M. S. Hoque
e-mail: hoque.eng@daffodilvarsity.edu.bd

J. Karthikeyan
Vellore Institute of Technology, Vellore, India
e-mail: sigashanmu@svcet.in

V. Goyal et al. (eds.), *Proceedings of International Conference on Communication and Artificial Intelligence*, Lecture Notes in Networks and Systems 435,
https://doi.org/10.1007/978-981-19-0976-4_7

1 Introduction

Nowadays, networks and internet have had a noteworthy effect on our day-to-day life. We are fully dependent on internet for sharing confidential and valuable information. Then again, on account of high dependence on the internet, hackers always investigate the shortcomings of the internet to paralyze the targeted servers or devices. Using this weakness, attackers always want to gain illegal access to damage targeted resources. In the world of computing, different security domains exist, and each one addresses various aspects of security [1]. Quite a few firewalls and cyber security systems are in action these days but they are not safe enough from cyber-attacks. Different cyber security systems are continuously implementing their defense mechanisms but dangerous attacks like zero-day are on the attack more dangerously on a daily basis. DDoS (Distributed Denial-of-Service) attacks are known to be the strongest and most destructive ones.

1.1 DoS and DDoS Attacks Overview

There is plenty of evidence on the DoS and DDoS attacks on the internet nowadays. DoS attacks typically flood servers and networks and practically perturb their victim's resources. On the other hand, a DDoS security attack uses a lot of compromised computers to attack a targeted traffic, slowing the computer and its network connection to a halt. This is a very powerful many-to-one technique, which is difficult to prevent. When a DDoS attack strikes, all users of a website or other online resources are completely denied access, halting the operations of the victim organization websites in its tracks. A typical attack scenario involves a good number of login attempts or calls to a website or server. The huge volume of requests floods the targeted resource, which loses the ability to tend to its legitimate users. There are three basic categories of attack (Table 1).

Table 1 Different categories of attack [2]

S No.	Categories	Description
1	Volume-based attacks	This attack uses high traffic to flood the network bandwidth. Example-ICMP flood
2	Protocol attacks	Protocol attacks are directed to servers, Routers, and Firewall, e.g., SYN flood and Smurf attacks
3	Application attacks	These attacks target web applications and are regarded as the most modern and fatal attacks. This is GET floor for http, DNS, SMTP, and SSL

1.2 Some Common Types of DDoS Attacks

DDoS attack has two types [3]: one, the bandwidth exhaustion create abstraction leading to the breakdown of network; two, resource exhaustion that exhausts key resources, memories, etc. Leading to the breakdown of the server [4]. There are different vectors of DDoS attacks, which aim to overwhelm the servers, firewalls, and different devices that vary destructively (Tables 2 and 3).

Table 2 Well-known DDoS attacks

Attacks	Description
SYN flood	SYN flood is a type of denial-of-service attack in networks where attackers continuously send SYN requests to the target network server to make it unresponsive and over consumed. This type of attack sends spoofed messages and is able to shut down the server services
UDP flood	In UDP flood attack, the target server receives a huge number of fake UDP packets sent by the attacker with the aim of occupying the whole resources
HTTP flood	HTTP flood is an HTTP Distributed Denial-of-Service attack method where the attackers exploit target web server and application by sending seemingly-legitimate session-based sets of an HTTP POST or GET request
Ping of death	By sending malicious pings to a system ping of death influences IP protocols. It was a well-known DDoS attack and nowadays it is less effective in network
Smurf attack	Smurf is a malware program that exploits by spoofing IP and pings using ICMP in a network
Slowloris	Slowloris is a type of denial-of-service attack distinctly different from other types. It uses legitimate HTTP traffics perfectly by opening and maintaining several simultaneous HTTP connections between the target server and the attacker. Thus, it makes overwhelms the target server
Application-level attacks	Application-level attack refers to comprise seemingly legitimate and innocent requests to the target server application by exploiting application vulnerabilities where the goal of this attack is to overwhelm the target application with requests
Botnet	Botnet refers to a group of malware-infected computer devices controlled by attackers with the aim to perform DDoS attacks, command and control, steal data, and so on
Zero-day DoS	Zero-day refers to a type of attack that is totally unknown to the vendors. This attack uses previously unknown flaws to exploit target network or system. Zero-day DoS attacks amplify malicious network traffic and prevent legitimate users to use network resources

Table 3 Last four years some well-known DDoS attacks

Year	Target	Brief description
2018	GitHub engineering	Due to DDoS attacks, GitHub.com was unavailable on February 28 from 17:21 to 17:26 UTC [5]
2017	Melbourne IT	On April 13 domain name registrar Melbourne IT, two of its subsidiaries TPP Wholesale and Netregistry suffered a DDoS attack. [6]
	UK national lottery	UK National Lottery www.national-lottery.co.uk and its mobile app were unavailable due to DDoS attacks on local time 23:00 to 03:00, September 30 [7]
2016	HSBC internet banking	HSBC's internet banking service in United Kingdom's was unavailable for several hours in January 2016 due to DDoS attack [8]
	Bank of Greece website	Website server of Bank of Greece was remain offline for more than 6 h under a series of DDoS attacks [9]
2015	Canadian government websites	DDoS attack affects Government of Canada website which impacted internet access, email, and information technology assets on June 17, 2015 [10]
	BBC websites	All the BBC's websites were unavailable early on Thursday (31st December) morning because of a large web attack [11]

1.3 DDoS Prevention Techniques

It is difficult to stop DDoS attacks completely. We can mitigate in tolerant level by developing and using different techniques. There are many DDoS defense mechanisms that try to prevent systems from DDoS attacks:

- Should disable unused port and services.
- Should install latest security patches.
- Should disable IP broadcast.
- Should use Firewalls and Routers.
- Ingress/Egress filtering [12].
- Router-based packet filtering.
- Load balancing.

1.4 Challenges of DDoS Attacks

The dangerous history of DDoS attacks shows the prevention of DDoS is nearly impossible. DDoS Protection is a challenge; the reasons are:

Table 4 Comparison of different parameters

Authors	Year	Attacks	Defense	Challenges	Recommendation
Shruthi [13]	2017	Yes	Yes	No	No
Vinko et al. [14]	2017	Yes	Yes	Yes	No
This paper	2018	Yes	Yes	Yes	Yes

- Difficulty in Managing Legitimate and Attack Traffic.
- Lack of large-scale testing approaches.
- Lack of infrastructure and expertise.
- Lack of effective traffic analysis and defense system.
- There are no common characteristics of DDoS.

2 Related Works

A deep study of the existing literature on DDoS architecture, detection, and prevention issues was assumed earlier to the introduction of the EDSONI model on DDoS attacks. In order to find out where further improvement could be made, relevant literature was reviewed. The study revealed that the threat implications should be the initial consideration in producing improved better detection and prevention techniques on DDoS attacks. Table 4 shows the comparison of the few existing relevant papers with our work.

2.1 DDoS Attack Tools and Their Comparison

There are several tools that are able to produce legal traffic and attack traffic [15]. Researchers hardly paid attention to the fact that DDoS use botnets to launch any attacks (Table 5).

3 EDSONI Research Methodology

EDSONI research methodology including detailed explanations of lab architecture, Dataset, hardware, and software are used for finding expected results are presented below.

Table 5 Comparison of DDoS attack tools

Year	Tools	Target impact	Type of attack	OS supported	Number of Zombies	IP spoofing	Attack model
2011	Aldi Botnet [16]	Resources	http, TCP	Widows	Multiple	Yes	web base
	SSL DoS [17]	Resources	TCP	Widows, Linux	Single	–	–
2012	GoldenEye [18]	Resources	TCP	Windows, Linux	Single	No	–
	HOLC [19]	Resources	TCP	Windows	Multiple	No	–
	HULK [20]	Resources	TCP	Windows, Linux	Single	No	–
2015	Advanced UDP attack tool	Bandwidth	UDP	Windows	–	Yes	IRC based
2016	LOIC-IFC	Bandwidth	HTTP flooding	Linux	Multiple	Yes	Agent base

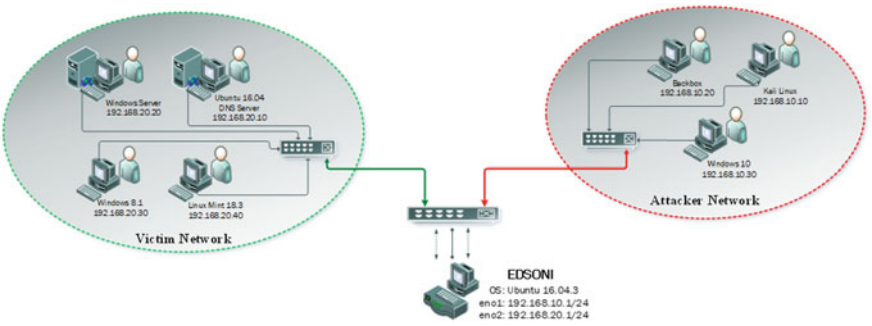

Fig. 1 Lab architecture

3.1 Lab Architecture

See (Fig. 1; Table 6).

3.2 Dataset

For dataset, we have used CICIDS2017 for network security and intrusion detection as it has diverse set of attacks. In this dataset, seven attack profiles based on the last updated list of common DDoS attack families have been created. The dataset is executed by using related tools and codes (Table 7).

Table 6 Hardware and software are used in lab architecture

	Devices	OS	IP
Victim network	Servers	Ubuntu16.04(DNS server)	192.168.20.10
		Web server (Windows)	192.168.20.20
	PCs	Linux Mint 18.3(64-bit)	192.168.20.30
		Windows 8.1(64-bit)	192.168.20.40
EDSONI	PC (Router)	Ubuntu16.04.3(64-bit)	192.168.10.1 192.168.20.1
		Scapy, Yara v3.7.0, Scapy-python3 v0.25, Yara-python v3.7.0	
Attacker network	PCs	Kali Linux(64-bit)	192.168.10.10
		Backbox 5.1(64-bit)	192.168.10.20
		Windows10(64-bit)	192.168.10.30

4 Findings

The details of the proposed enhanced Efficient Detection System of Network Intrusion (EDSONI) model are discussed below (Fig. 2).

i. Sniffer

The very first step of EDSONI is Sniffer. In this system, the "raw socket" has used for sniffing the packets from specific interface. Here all packets are saved in a file with PCAP extension that is the reason it is easy to analyze traffic for further analysis.

ii. Extractor

Generally, when a raw packet is sniffed, it contains information that is padded with both signed and unsigned bits and characters. In extractor step from every raw packet, EDSONI extractor unpack and collect all possible information from the packet. After extracting, it is easy to get version, Internet Header Length, Type of Service, length of the packet, identification tag, flag, fragment offset, TTL, protocol, Header Checksum, source IP address, destination IP address, source MAC address, destination MAC address, and Payload, etc. of the packet.

iii. Normalizer

In this step, normalizer normalizes all the data that were collected from extractor step for post-processing. So that the module selector engine and other post-processing steps can process them easily.

iv. *Module Selector*

In Module Selection Engine, it selects the correct module such as TCP, UDP, ICMP, and other modules based on the analysis of PDU (Protocol Data Unit) and Packet Header.

v. Pre-processor

Table 7 Similarities and differences between CICIDS2017 dataset and public datasets based on last IDS dataset evaluation framework [21]

	Network	Traffic	Label	Interact.	Captu.	Protocols					Attack diversity					
						http	https	SSH	FTP	Email	Browser	Bforce	DoS	Scan	Bdoor	DNS
DARPA	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No	No
KDD99	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No	No
DEFCON	No	No	No	Yes	Yes	Yes	No	Yes	No	No	No	No	No	Yes	Yes	No
CAIDAs	Yes	Yes	No	No	No	–	–	–	–	–	No	No	Yes	Yes	No	Yes
LBNL	Yes	Yes	No	No	No	Yes	No	Yes	No	No	–	–	–	Yes	–	–
CDX	No	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No	No	Yes	Yes	No	Yes
KYOTO	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TWENTE	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No	Yes	No	Yes	No	No
UNASS	Yes	No	Yes	No	Yes	Yes	No	No	No	No	No	No	No	No	No	No
ISCX 2012	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
ADFA 2013	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes	No
CICIDS 2017	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

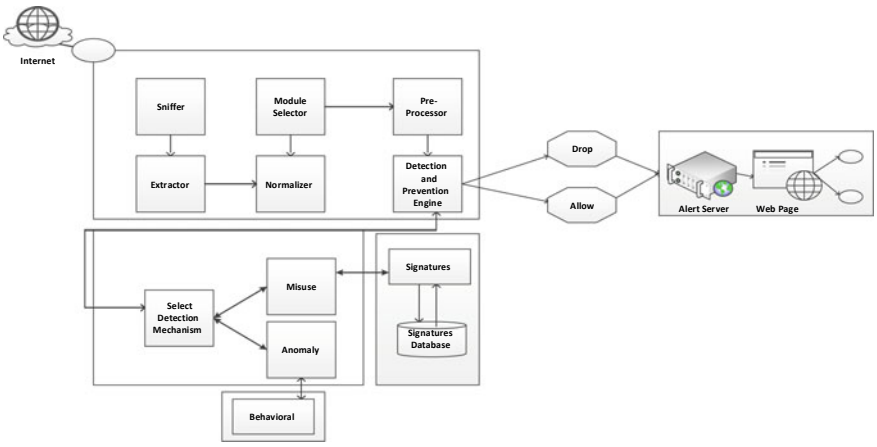

Fig. 2 Proposed EDSONI model

Pre-processor is used for examination of packets and detection of suspicious activity, modification of packets so that the detection engine can properly interpret them. It analyzes sessions, payload, fragments, segments under particular module which saves the processing time. After that traffic will go to detection engine.

vi. Detection and Prevention Engine

After pre-processor detection engine triggers a detection process in real-time with the help of selection of the detection mechanism. It is stated that EDSONI works in two modes. These are detection and prevention modes. In detection mode it only detects the intrusion, logs the information, and forwards the packet to the prevention mode.

vii. Logs and visualization

Finally, visualize the results and logs of the detection and prevention.

4.1 Implementation and Experimental Result

Table 8 shows the experimental results of evaluation metrics in terms of weighted average for the six selected machine-learning algorithms derived from generated dataset. Execution time for the testing process is also calculated and shown in the table. Among six applied machine-learning algorithms Adaboost, J48, K-Nearest Neighbors (KNN), Multilayer Perceptron (MLP), Naïve Bayes, and Random Forest (RF), we have observed that based on the execution, MLP the slowest one requires 2836 s with 97.689% classification accuracy rate and on the contrary, the fastest one KNN requires only 1.2 s with 97.397% classification accuracy rate. Additionally, based on the weighted average of three evaluation metrics (Pr, Rc, and F-Measure), the highest accuracy rate refers to Naïve Bayes, Adaboost, and J48 algorithms.

Table 8 Experimental performance result of 6 machine learning algorithms

Algorithm	Testing dulii size	Accuracy	TPR	FPR	Pr	Re	F-measure	Exec. time (sec)
Adaboost	3523 1	97.779	0.978	0.016	0.983	0.978	0.979	128.4
J48	3523 1	97.745	0.977	0.018	0.982	0.977	0.979	23.4
KNN	3523 1	97.397	0.974	0.027	0.977	0.974	0.975	1.2
MLP	35231	97.689	0.977	0.034	0.977	0.977	0.975	2836
Naïve Bayes	3523 1	97.782	0.978	0.001	0.987	0.978	0.981	15
RF	3523 1	97.407	0.974	0.023	0.979	0.974	0.976	333.6

Considering the evaluation metrics and the execution time, Naïve Bayes is the best algorithm with the highest accuracy rate and short execution time among six applied machine-learning algorithms (Fig. 3; Table 9).

As an evaluation metrics, we have used above table features which are given below:

$$\text{Accuracy} : (\text{TP} + \text{TN})/(\text{TP} + \text{TN} + \text{FP} + \text{FN}), \tag{1}$$

$$\text{TPR} : \text{True Positive Rate} = \text{TP}/\text{TP} + \text{FN}, \tag{2}$$

$$\text{FPR} : \text{False Positive Rate} = \text{FP}/\text{FP} + \text{TN}, \tag{3}$$

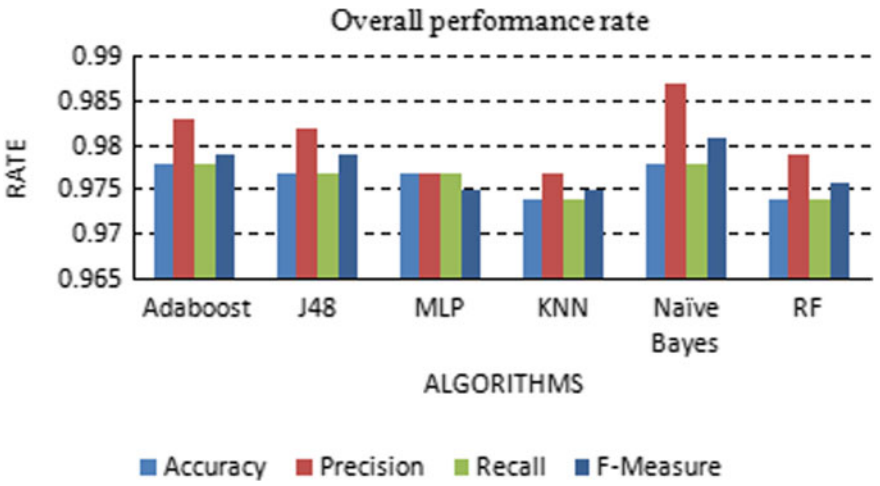

Fig. 3 Overall performance rate of different algorithms

Table 9 Results of Naïve Bayes

Attacks	Testing data size	Accuracy	TPR	FPR	Precision	Recall	F-measure	MCC
BENIGN	27165	97.76	0.97	0.01	1.00	0.97	0.98	0.94
DDoS	299	99.11	0.97	0.09	0.49	0.97	0.65	0.69
DoS GoldenEye	6202	99.97	1.00	0.00	0.99	1.00	0.99	0.99
DoS Hulk	181	99.98	0.99	0.00	0.99	0.99	0.99	0.99
DoS Slowlons	700	99.97	1.00	0.00	0.99	1.00	0.99	0.99
DoS Slowhttptest	628	98.69	0.99	0.13	0.58	0.99	0.73	0.76
Heartbleed	56	99.99	1.00	0.00	0.97	1.00	0.98	0.98

Precision (P_r): It is the ratio of correctly classified attack flows (TP), in front of all classified flows (TP + FP).

Recall (R_c): It is the ratio of correctly classified attack flows (TP), in front of all generated flows (TP + FN).

F-Measure: It is a harmonic combination of the precision and recalls into a single measure.

$$P_r = \frac{\text{TP}}{\text{TP} + \text{FP}}, R_c = \frac{\text{TP}}{\text{TP} + \text{FN}}, F_{\text{measure}} = \frac{2}{\frac{1}{\text{Pr}} + \frac{1}{\text{Rc}}} \tag{4}$$

Matthews's correlation coefficient (MCC): MCC is defined in terms of True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN).

5 Conclusion and Future Work

It appears to be really difficult to completely defend the network from denial-of-service (DDoS) attacks on the internet today. In this study, we propose a system that evaluated a model called EDSONI for DoS and DDoS attacks. This article concludes that it is possible to train a Naïve Bayes that would successfully classify unseen data in different scenarios with a high accuracy in computer-generated simulation. Challenges and different DDoS prevention approaches are discussed in this paper. The proposed system can be used for the commercial purpose and it can implement as a part of firewall system to combine the working of detection and prevention systems. The enhancement can be made to check the same approach for different other attacks over the network in future.

References

1. Aldibotnet, DDoS Attack Tools, 2012. https://asert.arbornetworks.com/ddos-tools
2. Behal S, Kumar K (2017) Characterization and comparison of DDoS attack tools and traffic generations: a review. IJ Netw Secur 19(3):383–393
3. DDoS Attack on Bank of Greece https://www.hackread.com/anonymous-ddos-attack-bank-greece-website-down/. Accessed 8 June 2018
4. eSecurity Planet, 4 May 2017, www.esecurityplanet.com/network-security/types-of-ddos-attacks.html. Accessed 11 June 2018
5. GitHub engineering, DDoS incident Report. https://githubengineering.com/ddos-incident-report/. Accessed 9 June 2018
6. Github (2013), DDoS Attack Tools. https://github.com/
7. Hacker group 'Anonymous' claims credit for federal cyber-attacks. http://ottawacitizen.com/news/politics/federal-computer-servers-cyber-attacked-clement. Accessed 9 June 2018
8. HSBC internet banking services down after DDoS attack. https://www.theguardian.com/money/2016/jan/29/hsbc-online-banking-cyber-attack. Accessed 9 June 2018
9. Kali Linux Tutorials (2011) THC-SSL-DoS—a denial of service tool against secure web-servers and for Testing SSL-Renegotiation. https://www.thc.org/thc-ssl-dos
10. Kritikos K, Kirkham T, Kryza B, Massonet P (2017) Towards a security-enhanced PaaS platform for multi-cloud applications. Futur Gener Comput Syst 67:206–226
11. Hu L, Bi X (2011) Research of DDoS attack mechanism and its defense frame. In: Computer research and development (ICCRD), 3rd international conference, pp 440–442
12. Melbourne IT, DDoS Attacks of 2017 https://www.tripwire.com/state-of-security/featured/5-notable-ddos-attacks-2017/. Accessed 9 June 2018
13. Mittal A, et al (2011) A review of DDOS attack and its countermeasures in TCP based networks. Int J Comput Sci Eng Surv (IJCSES) 2. https://doi.org/10.5121/ijcses.2011.2413
14. Ferguson P, Senie D (1998) Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing. In: RFC 2267, the internet engineering task force (IETF)
15. Packet Storm (2015) DDoS Attack Tools. http://packetstormsecurity.org
16. Sharafaldin I, et al (2018) Toward generating a new intrusion detection dataset and intrusion traffic characterization. In: Proceedings of the 4th international conference on information systems security and privacy (ICISSP)
17. Shruthi P (2017) Network security in digitalization: attacks and defence. Int J Res Comput Appl Robot
18. Sourceforge (2012) DDoS Attack Tools. http://sourceforge.net/projects
19. UK National Lottery (2017) DDoS Attacks of 2017 https://www.tripwire.com/state-of-security/featured/5-notable-ddos-attacks-2017/. Accessed 9 June 2018
20. Vinko Z, KF, VS (2017) Denial of service attacks, defenses and research challenges. Springer Science Business Media New York. https://doi.org/10.1007/s10586-017-0730-x
21. Web attack knocks BBC websites offline https://www.bbc.com/news/technology-35204915. Accessed 9 June 2018