Recent Trends in Development of DDoS Attacks and Protection Systems Against Them

Vladimir Galyaev, Evgenia Zykova, Dmitry Repin, and Denis Bokov
(Corresponding author: Vladimir Galyaev)

Laboratory of Mathematical Modelling and Information Technologies,
State Institute of Information Technologies and Telecommunications (SIIT&T "Informika")
Brusov per., 21 str.2, Moscow, Russian Federation, 125009
(Email: v.galiaev@informika.ru)
(Received Mar. 30, 2018; Revised and accepted July 7, 2018; First Online May 28, 2019)

Abstract

Distributed denial of service (DDoS) attacks are considered the most common and often the most destructive among all threats to network infrastructure. For the last decade the number of DDoS attacks constantly grows. They become more elaborate and sophisticated making standard security techniques went out of date quickly. In the review we collected, investigated and link together data from academic publications and information security reports provided by top companies in the field. We marked out tendencies in evolution of DDoS attacks, characterized protection systems, and summarized the last achievements and future developments in application of intellectual methods for network security.

Keywords: DDoS Attack; Intellectual Methods; Network Protection; Network Security

1 Introduction

Distributed Denial of Service (DDoS) attack is a type of cyberattacks that aims to exhaust network resources (server capacity, information channel bandwidth) causing resource deny from providing access to legitimate system users. It uses a number of compromised or vulnerable hosts distributed in the Internet to create malicious traffic and send it to a victim.

DDoS attacks are destructive for the network infrastructure and can very quickly disable a server or an entire network. There are following aspects that determine the effectiveness of DDoS attacks [5]:

- There is a large number of interdependencies in the network architecture.
- The resources of network devices are limited.
- Compromised devices may participate in two or more botnets belonging to different attackers and can be used against several target servers or networks.
- Information and resources that can be used to prevent impending attacks are under control of different people.
- Simple and direct routing principles are commonly used in the Internet infrastructure.
- There are inconsistencies in the architecture of different local networks. The speed difference between network devices of the core and the boundary usually occurs.
- Network management is often low-level.
- In general, the useful practice of sharing information and technical resources has its drawbacks.

Any organization may become a target for DDoS attacks, regardless of its size or business scope. Few years ago most common victims for DDoS attacks were top corporations with income highly dependent on network resources: financial institutions, hosting companies and providers of cloud services, major media outlets. Nowadays attacks may also affect small and medium-size enterprises in any sphere of business, from public health institutions and social insurance to e-sport organizations. From surveys involving all around the world organizations from various spheres and with different outcome, it follows that most of the victims suffered financial losses up to $255,000 per hour of an attack [41]. Records are breaking almost every quarter: the maximum duration of one continuous attack is up to 277 hours and the maximum number of attacks per day is 1497 attacks [24]. With increase of average duration, volume and the number of DDoS attacks targeted to a company cost of the damage from DDoS attacks is growing day by day making protection systems much in demand.

Various organizations choose different tactics to protect their resources from DDoS attacks. Some assess their risks as minimal and do not take any additional measures believing that a correctly built network infrastructure can

withstand most threats. However, the development of DDoS as a service increases the chance for a company to become a victim of DDoS attacks. There are no universal means for countering DDoS attacks. In general there are three basic approaches used to provide security measures:

1) Network infrastructure improvement with aim to increase its stability and survivability;

2) Application of specialized hardware and software solutions;

3) Resource protection as a service by top system integrators. Each of the approaches has its advantages and drawbacks and can be used both independently and together (see more details in Section 3).

Taking into account the complexity of DDoS attacks, their multiple vectoring, volume and constant modification, only implementations that are able to adapt to changing conditions will be able to successfully cope with them. Therefore, the mathematical and algorithmic basis for software and hardware solutions are intelligent methods of data analysis. Over the last 10 years a number of research works have been published in this field, suggesting to use as a mathematical basis statistical, signature, heuristic analysis, expert systems, queuing networks, multi-agent systems, genetic and behavioral algorithms. However, the major disadvantages of most solutions are the narrow specialization of the developed methods, as well as determinacy of incoming traffic classification.

This work aims to bring a systematic view of recent DDoS attacks developments, introduce main defence strategies and highlight possible protection mechanisms improvements. We have analysed data for the last year from DDoS attacks reports provided by a number of companies in the field and defined main trends and possible further evolvement.

The rest of the paper is organized as follows. In Section 2 we introduced social and economic aspects of DDoS attacks, attacks classification and statistics of threats, taking in consideration quarter and annual statistics that is available in information security reports of top companies in the field. In Section 3 we paid attention to most commonly used DDoS protection mechanisms for network security and highlighted their advantages and drawbacks. Section 4 is devoted to in-depth traffic analysis via application of intellectual systems and sophisticated statistical algorithms. Finally, we present the concluding remarks in Section 5.

2 Main Tendencies in Development of DDoS Attacks

2.1 Social and Economic Aspects of DDoS Attacks

DDoS attacks evolve from demonstrative actions into a prominent niche of the shadow market. It bears on unfair competition (temporal blockage of the competitor, reputational damage), fraud on electronic stock exchanges and e-sports events, blackmailing and extortion with the threat of an attack on company's resources. In particular, the DDoS for Ransom strategy keeps developing: demonstrating a DDoS attack with a promise of continuing it if the ransom is not paid. The business model explains some DDoS attacks that might look like an attempt to set a new record: attackers demonstrate their capabilities on popular websites to frighten potential victims [23]. Apart from the main goal of the intruder a DDoS attack can also serve as a mask for hacking information resources, penetrating a protected perimeter and stealing confidential data or money.

Often DDoS attacks are used to draw attention and even for revenge. A group of attackers conducted a powerful DDoS attack on the site of famous American journalist Brian Krebs, who writes popular analytical articles about information security and cybercriminals, — KrebsOnSecurity.com. The attack was carried out in September 2016 and by that time became the largest of the officially recorded: volume of malicious traffic reached 620 Gbit/s and the attack duration was almost 2 days. Most of the traffic consisted of generic routing encapsulation data packets, and the attack was carried out using a botnet of hundreds of thousands of IP cameras and video game consoles.

Originally, botnets based on infected computers were used to implement DDoS attacks. Recently new technologies for infection and use of network devices appeared, and botnets on the basis of "smart" things included in Internet of Things (IoT) are being used more frequently. Especially, two record-breaking DDoS attacks on the French hosting company OVH and the American DNS provider Dyn were conducted with help of botnets based on IP cameras, printers and other devices. There is information about revealed vulnerabilities of a number of household appliances, for instance "smart" dishwashers Miele and kitchen stoves AGA [8]. Usually such devices are equipped with inexpensive samples of operating systems with free software and no security support. Most devices have a password and a login "by default", so their hacking is easy. At the same time, the variety of "smart" devices is constantly expanding, and each of them can potentially be used for illegal purposes. The issue is called in press as the phenomenon of "microwave threat".

According to forecasts of top IT companies, the proportion of IoT devices will grow rapidly in the coming years and exceed the number of other devices at 2020 [11]. It is clear that the number of botnets created on the basis of weakly protected mobile devices and IoT elements will grow as well. Major companies have started to pay attention to security issues and are developing security tools for their IoT devices. However market is overflowed with cheap products (most of them are made in China) without any protection systems. Meanwhile the number of scumware samples for "smart" devices is constantly growing creating huge basis for IoT botnets (see Figure

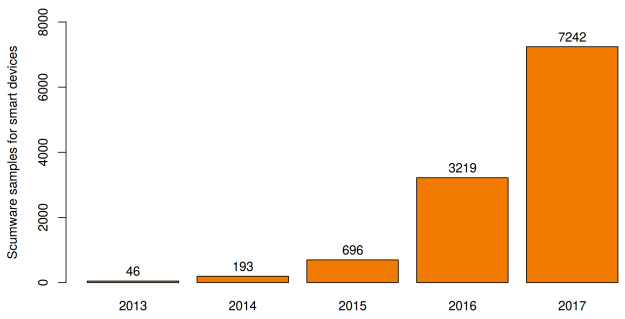

Figure 1: The number of scumware samples for "smart" devices is constantly growing

1, [35]).

Another trend is complication of DDoS attack mechanisms. Intruders are using a few types of DDoS attacks in a single act (multi-vector attack), combining vulnerabilities of different network protocols. In this case, two areas of implementation can be clearly identified. The first one includes ineffective, but massive and easily self-upgrading attacks based on finished products. The second one includes specialized developments that are created individually to attack a particular company, taking into account its specific vulnerabilities and the architecture of its information system. The developments are much more expensive, but as a result they are more effective: in most cases they bypass standard protection systems.

Meanwhile, the cost of conducting a DDoS attack is significantly lower than the cost of protective actions. The price for DDoS attacks is decreasing, and the number of services is constantly growing. In 2017 a DDoS attack with use of 1,000 workstations has a cost price about $7 per hour. A customer could order a one-hour DDoS attack of this level on a special web-service for only $25 [32].

Based on a survey conducted among US and Canadian companies in 2016, Incapsula came to a conclusion that 45% of American and Canadian organizations were a subject to attacks, 91% of them faced this threat at least once a year. It also revealed that 43% of respondents have lost credibility of clients, 51% recorded a decline in profits, some companies informed about losses of intellectual property (19%), personal data of customers (33%) or financial information (26%). Incapsula analysts have also estimated an approximate amount of financial losses of a company (direct and indirect) [17]. There is still a consistent trend for reputational costs to prevail over other forms of financial losses. The Kaspersky Security annual report in 2016 have shown results of the survey attended by more than 4,000 companies around the world [1]. It follows from the survey that most companies estimate their reputational costs as the most significant, while the reaction time to the incident plays a critical role: a direct dependence of the financial losses on reaction time of the company have been revealed.

2.2 Classification of DDoS Attacks

In the last publications, including reviews and analytical reports of top companies in the field of information security, various classifications of DDoS attacks are given. Attacks can be distinguished by differences in functionality, final action, use of protocols, and other characteristics. One of the most complete classifications was proposed by Mirkovich *et al.* [34], it takes into account the type of attack, the degree of automation, the frequency of attack, the type of impact, *etc.*

In general there are two types of DDoS attack mechanisms: direct and amplificated (reflected) attacks. Direct attacks try to overload the information resource or communication channel by directly sending a large number of packets to the target (packet flood). Amplification attacks are based on another principle: attackers send packets with small queries to vulnerable resources aimed to get large size responses from them redirected to the victim resource. Direct attacks are dependent on large computational resources and require botnet of a proper size to be used. In contrary amplification attacks are less demanding in resources, however, searching for network vulnerabilities and their correct usage is critical.

Companies specializing in information security use the following classification of DDoS attacks [11, 17, 29, 36]:

- **HTTP flood.** During HTTP flood attacks a great amount of HTTP requests GET are sent on the 80th port of a victim server. It leads to server overloading and inability to handle other requests. Attacks of this type can be aimed at failing the server, as well as overflowing the network bandwidth. In recent years significant complication of HTTP flood DDoS attacks took place: requests can be dynamically self-modified according to certain rules, queries might address not the root of the website, but scripts, consuming a large amount of resources, as well as they can simulate the simplest actions of the user. It significantly impedes HTTP flood attacks detection.

- **SYN flood.** The attacks employ features of the so-called three-way handshake — the procedure that is used to establish a connection between two nodes in the network. Infected computers send multiple SYN requests for connection, and at the same time ignore response requests sent by the victim, thereby creating a queue of "half-open" connections on the target server.

- **UDP flood.** UDP flood attacks overflow the communication channel by sending multiple UDP-packets to the ports of various UDP services.

- **TCP flood.** The attacks are aimed at overwhelming the session/connection tables. It makes legitimate server requests rejected as well.

- **ICMP flood.** An ICMP flood attack appear to be a simple and easy-to-implement method for bandwidth

overflow through multiple sending of ICMP ECHO requests (so-called "pings"). It is usually not very effective, but it works well with resources that are not prepared for DDoS attacks.

- **DNS flood.** DNS flood attacks exploit the vulnerability of DNS systems using UDP. The attacks are based on sending multiple requests to the DNS server overflowing the victim's server with requests and consuming its resources.
- **DNS amplification.** During an attack the intruder's DNS server sends requests in which the target computer is specified as the source address. Thus, the DNS server of the victim suffers from a critical situation.
- **SSDP amplification.** An SSDP amplification attack uses a vulnerability of the SSDP protocol — the feature that is intended to provide network clients the capability to recognize various network services. It initiates a dispatch for the UDP port 1900 by substituting the sender's address in the SSDP protocol request.
- **NTP amplification.** Attacks use the functionality of the monlist request to the NTP server: a list of the last 600 ntpd clients is returned on request. As a result a small request with a fake IP address sends a large UDP stream to the victim.

2.3 Statistics of Threats

Quite regularly (quarterly or annually) a number of top companies in the field of information security publish reports and analytical reviews with results of their research [1, 18, 19, 22–25, 44]. Comparing reviews about DDoS attacks by periods and countries we have defined the following statistically significant dependencies and trends:

1) China, South Korea and the United States are leading in the number of attacks, the number of targets and command and control servers (see Table 1).
2) The number of DDoS attacks approximately doubles every year.
3) The number of simple attacks at the application level is reducing, it gives way to attacks at the level of network protocols and mixed types. This increases the number of multi-vector attacks at the application level, taking into account the specificity of a particular organization resources. The number of vectors in the attacks can reach 5 or more (see Figure 2).
4) There is an increasing demand on the DDoS as a service, the most popular are attacks aimed at putting pressure on the security service rather than causing real harm to the company. The number of attacks for blackmail is growing rapidly and exceeds at least 18% of the total.

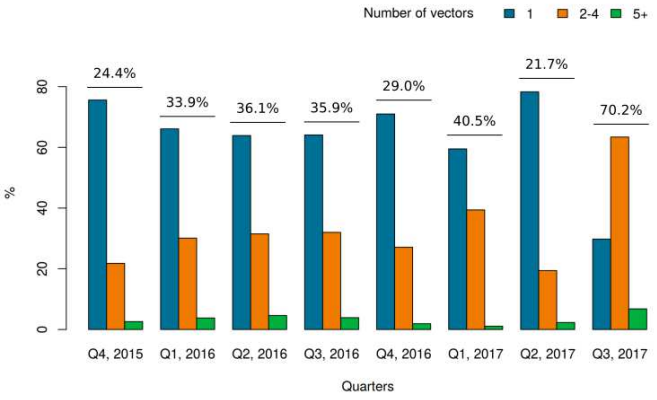

Figure 2: Number of vectors in DDoS attacks for the last two years. Percents of multivector attacks are given on the top of bars. Data were taken from Incapsula reports [18, 19]

5) In the last two years there were a few peak attacks with volume from 400 Gbit/s to 1200 Gbit/s. The average volume of DDoS attacks to major information resources is close to 100 Gbit/s.
6) The maximum duration of attacks is gradually increasing with records of 291 hours of continuous attack (IV quarter of 2016) and 277 hours (II quarter of 2017). However, the average time of attacks remains at a fairly low level — about 3 hours. Short-term attacks account for about 75% of all attacks.
7) A new approach called Pulse Wave technology has been developed. It is capable of increasing the power of a DDoS attack by use of vulnerabilities in hybrid and cloud technologies. Pulse Wave technology implies series of powerful but short duration attacks in the small period of time.
8) Cybercriminals primarily create botnets on the basis of Linux-devices included in the IoT — the share of the networks increased reaching 75%.
9) Botnets participating in DDoS attacks become more sophisticated. Some advanced bots are able to emulate browser behavior, for example, they are able to store cookies and handle JavaScript. The share of such bots reached 42% and tends to increase.
10) The number of attacks with encryption is growing.
11) In 2017 the most popular were SYN flood attacks, they took up to 60% from the total. TCP flood DDoS attacks became less frequent — the share of the attacks decreased from 28% to 12%. Conversely there is a growing demand for HTTP flood DDoS attacks — the share of the attacks increased from 5% to 11%.

Based on the analysis of reports it can be stated that the proportion of simple attacks (primitive to conduct)

Table 1: Percents of targets and command and control servers for DDoS attacks in various countries for the period from the IV quarter (Q4) of 2016 to the III quarter (Q3) of 2017

#	Country	Targets / Attacking servers			
		Q1	Q2	Q3	Q4
1	China	71.6% / 77.0%	47.8% / 55.1%	47.4% / 58.1%	**51.6% / 63.3%**
2	USA	9.1% / 7.3%	13.8% / 11.4%	18.6% / 14.0%	**17.3% / 13.0%**
3	South Korea	9.4% / 7.0%	26.6% / 22.4%	16.4% / 14.2%	**11.1% / 8.7%**
4	Russia	1.7% / 1.8%	1.6% / 1.6%	1.3% / 1.2%	**2.2% / 1.6%**
5	United Kingdom	0.5% / 0.3%	1.1% / 0.8%	2.1% / 1.4%	**2.0% / 1.4%**
6	Hong Kong	1.2% / 0.8%	1.6% / 1.4%	1.0% / 2.4%	**1.6% / 1.3%**
7	Germany	0.6% / 0.8%	0.8% / 0.6%	0.9% / 0.5%	**1.4% / 1.2%**
8	Other	6.0% / 5.3%	6.9% / 6.8%	12.2% / 8.2%	**12.8% / 9.6%**

is reducing. The growth of DDoS attacks complexity indicates that intruders are quick enough at identifying vulnerabilities of network devices and network protocols, they find new ways to exploit vulnerabilities for conducting multi-vector attacks and quickly master at applying new developing techniques (such as botnets based on IoT). It makes it possible to set new records on maximum volume and duration of DDoS attacks. At the same time, the absolute number of simple DDoS attacks does not decrease, as in the global network there are constantly appearing both special services and free tools for their organization. So ordering of simple DDoS attacks becomes available for everyone who is interested in it.

3 Countermeasures for DDoS Attacks

Over the last decade several books and major research works have been published on the subject. The book [2] recommends actions that can be taken before, during and after the attack. The author described the main steps in preparation and conducting of DDoS attacks and discussed how to anticipate attacks and provide protection for computers and networks, minimizing potential devastating consequences. In [37] authors specially paid attention to protection techniques applied in real time on high speed packet transmission with wide channel width. They described a set of possible options for managing web services during the DDoS attack. In the monograph [40] features of network protocols are considered from different points of view, under different conditions of use, including a large number of new scenarios. In [5] various types of DDoS attacks and their implementation are considered, the main stages and mechanisms of creating botnets are given. Particular attention is paid to the methods of statistical analysis and machine learning used to detect and prevent DDoS attacks. DDoS attacks and defences in cloud infrastructure are described in the detailed survey [6].

Various classifications of DDoS attacks protection mechanisms are used for assessment of performance and applicability. They can consider a number of factors, however the most common classifications are based on time of reaction, activity level, deployment location and cooperation degree [33,42]. For example, by time of reaction protection mechanisms can be divided into preventive (can prevent the fact of attack or significantly reduce its damage), real-time (identify the type of attack and filter traffic), and post factum (investigate the incident to improve the means of protection). Classification by deployment location includes protection mechanisms with outer, border and inner location in the network infrastructure.

Here we follow the classification of DDoS protection mechanisms based on "areas of responsibility", in other words we group approaches by party that takes responsibility for applying countermeasures against DDoS attacks. The classification includes:

- **Protection at the level of information resources management.** System administrators of an organization are responsible for countermeasures. The effectiveness and reliability of protection are fully determined by their professional level and network infrastructure capabilities.

- **Protection by specialized hardware and software products.** Responsibility lies with companies developing hardware and software solutions, and in this case, protection level can change only with purchasing new equipment or updating software and it is unlikely to be improved during the attack.

- **Protection by involving security services.** The company that provides security services is responsible for countermeasures. Due to the company's large resources it can vary the protection level according to the situation and use a wide range of protection measures, for example, the channel capacity can be increased with growing attack volume.

There is a brief description for each defence mechanism below; the most prominent business and academia solu-

tions are named. In Subsection 3.4 we discuss advantages and disadvantages of the mechanisms in general.

3.1 Protection at the Level of Information Resources Management

Protection at the level of information resources management includes the analysis of resources demand and bottleneck identification, carrying most of the traffic load in normal network state. Taking into account peculiarities of the server and/or network segment load it is possible to determine potential attack vectors and provide additional network resources for a client, *e.g.* extension of the communication channel bandwidth in advance, increase of server resources, and allocation of resources between several devices.

With the development of cloud technologies and hosting services usability, it is possible to conclude an agreement on providing a client with the necessary amount of resource depending on the load on the infrastructure. It can be a reaction, both to a temporary increase in the number of legitimate users, and to undesired malicious requests. Many providers implement a bandwidth cap, a restriction imposed on the transfer of data over the network, and only a certain type of traffic can consume resources over the time.

Rerouting is another solution that may be used by ISP providers. Most commonly the "black hole" option is used — after filtering malicious traffic is sent to a non-existent interface, which, in effect, leads to its removal. As a result server resources will not be overloaded, however, incoming traffic will still overload the communication channel [14, 20].

In terms of network equipment, many routers allow to configure access control lists (ACLs) to filter out unwanted traffic. The settings provide protection against simple and known DDoS attacks, for example, from ICMP flood attacks. Also, firewalls can be used as additional barriers and confine external networks from internal ones. However the direct protection from DDoS attacks is not included in their functionality.

3.2 Protection by Specialized Hardware and Software Products

Most specialized hardware and software solutions use the concept of protection from DDoS attack "clean pipes" developed by Cisco Systems. It includes the following steps:

- **Baseline Learning.** Traffic profiling with learning intrinsic traffic characteristics.
- **Detection.** Identification of attacks and anomalies.
- **Diversion.** Traffic redirection to the cleaning device.
- **Mitigation.** Filtering traffic to mitigate attacks.
- **Injection.** Entering traffic back into the network and sending to the client.

Cisco Systems used the technology in their products implemented as separate devices or modules.

The Cisco Intrusion Prevention System (IPS) module, deployed on a subnet, is able to eliminate the threat of DDoS attacks that occurs below the location of the sensor device. The system recognizes different signatures of flood attacks and then automatically implements countermeasures specified for them, such as resetting the connection, dropping packets so that they do not reach the target, modifying ACLs on the edge router or the switch next to the affected zone. IPS can also establish a rationing policy, *i.e.* limit the amount of data transferred per unit of time on the edge router.

The Cisco Guard, the product for DDoS attacks protection, consists of two components: a traffic anomaly detector (Cisco Traffic Anomaly Detector) and an anomaly protection tool (Cisco Anomaly Guard). Both components can be implemented as server applications, switch modules or "older" series of Cisco routers (7XXX and above). During the initial deployment, it is required to train the system to capture normal traffic parameters. Subsequently, the trained module is able to detect DDoS attacks by protocols and functionality, and transmit information to the Cisco Anomaly Guard in order to take further action. It should be noted that, although this solution is still on the market, Cisco Systems has stopped further development in this direction, relying on partner companies, and does not support the products since 2014.

Arbor Networks, also actively supporting the "clean pipes" concept, were developing their hardware and software solutions in parallel with the analogues from Cisco Systems. Due to withdraw of the main competitor from the market Arbor Networks significantly expanded the product line and took leading positions, both in development and in the production of solutions for DDoS attacks protection. Similarly to the Cisco Guard their products consists of two main modules:

- Peakflow SP CP is a platform for collecting and analyzing routing information. It differs from Cisco Detector by a feature to control the sampling frequency in analysis of information flows, which allows to use Peakflow SP CP in telecom operators networks and backbone channels.
- Peakflow SP TMS is a threat management system. It suppresses DDoS attacks by a multistage filtering procedure rest upon data received from Peakflow SP CP. Preliminary training of the system is carried out on the basis of statistical data prepared by the laboratory of ASERT, a subsidiary of Arbor Networks.

The Radware offers a comprehensive protection solution DefensePro — a device intended to deal with attacks in real-time including overloading of the Internet channel, attacks on authorization pages, CDN DDoS attacks and

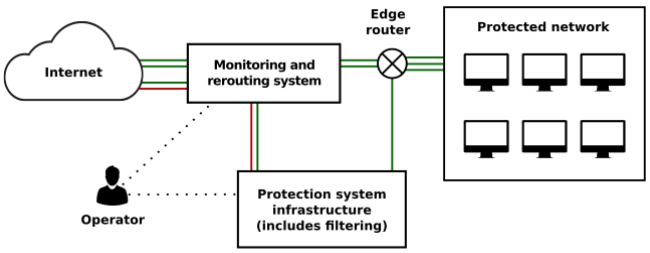

Figure 3: Principle scheme for the DDoS attack protection by involving security services

powerful attacks based on SSL. DefensePro uses a specially designed hardware platform based on OnDemand Switch from Radware with support for network bandwidths up to 40 Gbit/s. It has two hardware components built in:

1) The mechanism for massive DoS and DDoS attacks defence, as well as bulk attacks without affecting the legitimate traffic;

2) The mechanism aimed to accelerate the detection of signatures.

The software of the APSolute Vision device offers centralized management, monitoring and reporting on numerous DefensePro devices. The functions as intrusion detection, network behavior analysis, protection from DDoS, protection against SSL attacks are implemented.

3.3 Protection by Involving Security Services (SaaS Model)

SaaS model security services can be rendered only by large companies with a branched network infrastructure. Kaspersky Lab, one of the leaders in the market, offers the Kaspersky DDoS Prevention — a protecting complex against most types of DDoS attacks, that appears as distributed in the Internet infrastructure of data-clearing centers. The central element of the Kaspersky DDoS Prevention is a sensor installed in the immediate vicinity of the client's information infrastructure. The sensor comes as the software running on a standard x86 architecture server with Ubuntu operating system, it performs traffic analysis without redirecting/changing traffic and examining contents of packages. The statistics is then transferred to the cloud infrastructure of the Kaspersky DDoS Prevention, where customer-specific statistical "profiles" are created based on the collected metadata. The profiles reflect information exchange patterns that are typical for the client taking into account time and calendar fluctuations. Later, during traffic analysis deviations of current characteristics from the statistical profiles serve as indicators of a possible attack.

The second element of the Kaspersky DDoS Prevention is data-clearing centers connected to the largest Internet highways, they are geographically distributed with duplication of functionality in each region of presence. The data-clearing centers are integrated into the cloud infrastructure, however the traffic passing through them remains within the original region. If an attack is detected, the infrastructure allows to divide traffic over several threads decreasing the attack volume and processing each thread separately.

Another key mechanism of DDoS defence is traffic filtering on the provider side. The provider does not only provide an access to the Internet channel, but also filters out "junk" traffic with help of the Kaspersky DDoS Prevention, including traffic that is generated during most flood DDoS attacks. This also makes it difficult to merge DDoS flows into a single powerful attack and reduces the load on data-clearing centers.

If during monitoring of the current traffic deviations from the client's statistical profiles are observed, a warning signal is sent to the DDoS expert of Kaspersky Lab on duty. In case the expert confirms the fact of the attack, the client is notified and the malicious traffic is rerouting to data-clearing centers. Next, the type of attack is determined and type- and resource-specific clearing rules are applied. Traffic comes to servers of data-clearing centers, where filtering by a set of characteristics is applied, *e.g.*, filtering by blacklisting IP addresses, geography, according to statistical criteria or information from HTTP headers. During filtering the sensor continues to analyze client's incoming traffic and if signs of a DDoS attack are still observed, the sensor reports this to data-clearing centers, and the traffic become a subject to in-depth behavioral and signature filtering. Thus, especially complex attacks such as HTTP flood can be detected and neutralized during which the common actions of users on the site are simulated.

When the attack is over, the traffic is again redirected to the client's servers. The Kaspersky DDoS Prevention switches to the standby mode, and the client is provided with detailed report on the incident including a description of the attack progress, diagrams illustrating traffic dynamics, and geographical distribution of attack sources. Another company in the field is the Qrator Labs. The filtering nodes of Qrator Labs are connected to the channels of the largest backbone Internet providers in the USA, Russia, Western and Eastern Europe, and Southeast Asia. The network infrastructure is designed for extreme loads, and an attack on one of the resources should not affect the performance of other resources.

The filtering nodes use the BGP anycast technology to announce their IP addresses. If there is a need to protect client subnets, the corresponding client prefixes can be added to the BGP anycast. Traffic of clients constantly, regardless of the presence/absence of an attack, goes through the Qrator Labs network and is analyzed. "Clean" traffic is redirected to the protected site. This technology allows the filtration nodes to determine which traffic profiles are typical for each resource, and in the event of any deviations, respond immediately. All nodes

of the Qrator Labs network work independently, and if there is a failure of one of them, the traffic of the protected site will not be lost. It will automatically be redirected to the nearest filtering node.

3.4 Practical Aspects of Countermeasures Application

Companies choose defence strategies against DDoS attacks depending on the criticality of protected resources, available financial means, and company-specific security policies. There is no universal tool suitable for every organization. For some cases it will be fair enough to find a qualified stuff for information resources management and entrust network attack protection on it. Later on with business improvement or changes in security policies the protection level can be enforced by more convenient solutions. So, each of the proposed protection mechanisms has its advantages associated with flexibility of use, cost and quality of the staff, but also all of them have a number of substantial shortcomings.

Choosing a solution based on the protection at the level of information resources management one could experience its economic inexpediency, caused by spending money on processing traffic including malicious requests. In addition, legitimate and illegitimate traffic are treated the same, so useful traffic can also be rejected by mistake. Thus, protection by sustainable information resources management allows only to "absorb" DDoS-attacks of low intensity due to a well-designed infrastructure, but does not provide any countermeasures to serious threats. For example, if a DDoS attack is used as diversion for information stealing, there will be no proper actions to prevent data leaks.

Software and hardware solutions are less flexible than other protection systems in some aspects. They are highly dependent on updating and can easily become outdated for newly developed attacks. During a DDoS attack software and hardware products provide just few options to control defence mechanisms and if they fail to negate the attack there is no additional countermeasures. Also, for some companies the price for software and hardware solutions, their maintenance and updates is unaffordable.

Protection from DDoS involving security services is only suitable for very large companies, including providers. The efficiency of these solutions is achieved through the redistribution of computing resources involved in the overall system of protection. However there is no assurance that applied clearing algorithms are appropriate and optimal in each case.

4 In-depth Traffic Analysis and Intellectual Systems

Algorithms for in-depth traffic analysis and intellectual systems represent an advanced field of science and technology, they are developed exponentially and bring promising result for modern challenges in the network security. The methods often serve as mathematical basis for solutions offered by major IT-companies in the field. However they could be possibly used independently for network traffic monitoring and network infrastructure maintenance.

There are two distinct strategies for in-depth traffic analysis: comparison of network traffic characteristics with known templates of attacks (misuse detection systems) and tracing of deviations from common system states (anomaly detection systems). Currently, most studies are aimed at developing anomaly detection methods. Attackers by all means try to complicate cyberattacks detection and bypass security systems, for example, by adding random packets in malicious traffic or using special algorithms for botnets exploitation. Therefore, methods for misuse detection, and methods for anomaly detection require sophisticated intellectual algorithms. Both strategies are discussed in details below.

4.1 Misuse Detection Systems

For misuse detection it is required to determine some abnormal states of the network and describe their characteristics. For each type of attacks a specific pattern, so-called attack signature, is created taking into account the basic parameters of the attack. Any state of the system that does not match any of known patterns is considered normal.

Misuse detection systems have high speed and relatively high accuracy, however, in most cases they only able to detect already known attacks. So the relevance of the system training set is extremely important for good detection performance. If the attack is characterized by a previously unknown set of system parameters, in other words, does not correspond to any of specified signatures, then the attack will be missed. Another drawback of misuse detection systems — these methods require significant amounts of memory for storing signature databases.

As primary characteristics of traffic data streams, the number of packets from different sources, the amount of incoming traffic, the amount of incoming UDP traffic, the amount of incoming TCP traffic, *etc.*, can be used. Some works propose to apply the basic statistics, *i.e.* logical or algebraic functions of initial parameters, to form secondary characteristics. Well-known detection methods differ in approaches to the formation of a space of secondary characteristics that well describe the flows of telemetric traffic data, as well as measures of comparison of these characteristics. As a comparison measure for secondary characteristics, Shannon entropy variants, collision entropy or Renyi's quadratic entropy, Kulback-Leibler discrepancy, generalized entropy or information distance, Jeffreys divergence, squared Hellinger distance and Sibson's information radius are most often used [4, 27, 38, 49].

4.2 Anomaly Detection Systems

Anomaly detection systems try to establish the normal state of the system or its elements, for example, a specific user or a service. If a profile of normal network system functioning is determined, than any system state that is significantly different from the created profile will be defined as anomalous, and a warning for the administrator will be generated. The main advantage of anomaly detection systems is the ability to detect previously unknown DDoS attacks. There is no need to collect, describe and store all types attacks: every system behaviour deviating from common usual will be considered as unwanted and malicious.

However, in contrast to misuse detection systems anomaly detection techniques have worse performance: It shows less accuracy in detection and is memory-consuming, since there is a need to store statistics on large volumes of legitimate traffic. There are a set of possible normal system states if the traffic characteristics are distributed unequally over week, month or year (for example, e-shops traffic will be significantly different for periods of sales and after presentation of new collection than in ordinary days) and this information have to be properly saved and addressed in future. Also a problem may occur if the protected resource become extremely popular in a short period of time. Then detection systems by mistake can consider situation as potentially dangerous and block incoming traffic, as consequences legitime users will partly or totally lost the access to the resource. The effect is known as flash crowds. It is required to apply subtle sensitive algorithms to not confuse flash crowds with malicious traffic.

4.3 Algorithms for In-depth Traffic Analysis

Intelligent systems can be built on the basis of various methods of data mining and machine learning, both approaches specified in Subsections 4.1 and 4.2 are applied for them. The range of methods used is quite wide, to demonstrate the possible directions of intellectual systems development we name a number of works studied various techniques applied to the problem.

For traffic anomaly detection based on deviations from templates of normal system states many techniques have been applied, including principal component analysis [30], wavelets [43], histogram-based modelling [26], support vector machines [7, 48], detection of shifts in spatial-temporal traffic patterns [51]. For more in-depth analysis secondary characteristics are used, they are formed as logical [12], entropy [38], correlation [50] and structural [15] functions of primary traffic characteristics. Various probability measures and special metrics are used to differentiate DDoS attacks from legitimate traffic (including the effect of flash crowds) [8, 21].

Signature analysis, implemented for detecting DDoS attacks, requires to accumulate measurable amount of data for all diverse attacks types and is similar to analogous virus detection tools [33]. A compact and effective technique for formation of network protocols fingerprints was proposed in work [12], preliminary result demonstrated accurate traffic classification.

Artificial neural networks (ANN) are widely used as a part of complex DDoS detection and protection systems. The ability to identify hidden regularities in packets data and create accurate pattern recognition system make them attractive for researchers. However, the accuracy of ANN mainly relies on the relevance of the training set. Chen *et al.* [10] reported high accuracy for an algorithm judging legitime users behaviour from malicious traffic based on auto Turing test and ANN. In work [16] ANN were successfully applied for estimation of the attacking botnet size. Saied *et al.* [39] presented an ANN algorithm for TCP, UDP and ICMP protocols attacks detection based on characteristic traffic patterns. Packets headers were used for training process including source addresses, ID and sequence numbers coupled with source destination port numbers. The algorithm achieved 98% accuracy and performed well on unknown attacks: it failed to detect less than 5% of new attacks from the testing set.

Another approach is relying on the group-related anomalous behavior that botnet exhibits in contrary to normal random communication of ordinary resource users. Traffic source IPs [3] and packet IDs [46] deviations could be used for easy to implement and low cost DDoS detection methods. Chen & Lin [9] proposed a detection system that efficiently identifies anomalous traffic by patterns in hosts homogenous response and group activity. The system applies two-level correlation analysis to reveal sets of hosts with same communication pattern over a long duration, and it may detect malicious traffic produced by even small number of infected hosts. In works [2,13,31,45,47] different clustering techniques were used to group malicious traffic packets and detect bots.

It is challenging to find works describing algorithms for the formation of a space of secondary characteristics, corresponding to the dynamic nature of the network information channel. In the works mentioned above network traffic is considered as a set of static values (*e.g.*, packets per second) without taking into account the dynamic structure of network traffic. In fact, any information channels and their traffic conditions appear to be dynamical systems [28]. We believe, that for their adequate description it is necessary to consider the rates of change in packets flows, and not just the instantaneous values of their loads. Also algorithms allowing automatic adjustment of threshold values of secondary characteristics are rare implemented. It leads to the ongoing need of manual setting of these threshold values and, as a result, to errors in the identification of attack types. No work has been found with preset probabilities of type I and type II errors for identification of attack types.

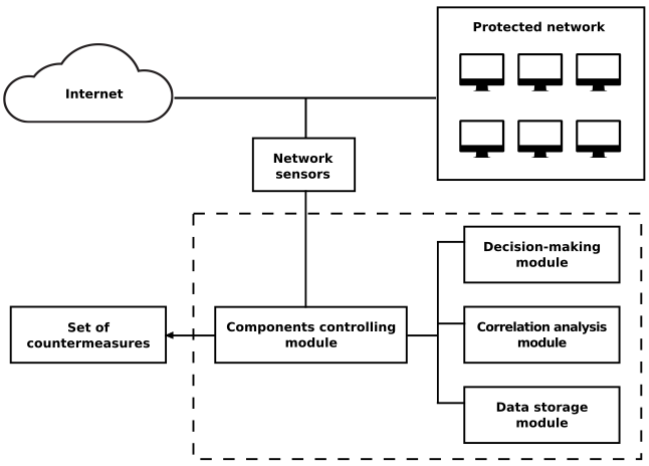

Figure 4: Principle scheme for application of intellectual algorithms in DDoS attack protection systems

4.4 Principle Scheme for Intellectual Methods Application

The intellectual methods discussed above can be implemented both in hardware and software solutions, and in the SaaS model security. Intellectual component can be introduced into the protection mechanism as a separate module. Most of these solutions are based on a similar generalized architecture which includes:

1) **Network sensors.** providing recording of traffic characteristics and revealing some of their patterns;

2) **Components controlling module.** providing interactions between all modules of the system, as well as being an element of interaction between systems for responding to emerging threats and an interface for the system operator;

3) **Decision-making module.** determining whether a package belongs to legitimate or malicious traffic based on identified features;

4) **Data storage module.** containing both signatures for legitimate and malicious traffic detected earlier;

5) **Correlation analysis module.** inspecting for significance newly detected network features, analysing data obtained earlier for current set of features from the decision-making module.

As a basis for decision-making modules and correlation analysis modules researchers use almost the entire spectrum of intellectual decision-making methods.

All of the intelligent algorithms discussed above can be used in various combinations within the overall detection complex. The entire architecture remains the same, but the decision module can be built both on the basis of parallel and sequential study of traffic for the presence of anomalies and their typing. It generally increases the accuracy of incoming information processing, however it may possibly affect the processing speed.

5 Conclusions

DDoS attacks are becoming more sophisticated and massive and cause significant damage to loyal users. The development of attacking techniques is very dynamic and does not keep up with the general pace of development in information technologies. The work aimed at analyzing recent years development of DDoS attacks in order to identify trends with most significant adverse effects to the network infrastructure.

Scientific articles studying DDoS attacks evolution and protection mechanisms against them may lag to some extent and do not reflect the current state of affairs. In addition, this problem is so extensive that research works has become narrowly focused: many articles are devoted to solving one specific problem that arises in a certain situation providing detailed techniques and their applications. To be up-to-date with the last trends in DDoS attacks development it is required to monitor research reports by top IT companies publishing recent statistics and key accidents quarterly or annually as well.

The number of devices connected to the Internet is growing day by day giving wider opportunities for intruders to create large botnets and conduct massive DDoS attacks. The main promising direction for development of DDoS attacks protection systems is their consistency and intellectualization. In this regard, it becomes urgent to develop methods and algorithms for filtering traffic based on in-depth analysis using intelligent systems allowing such analysis for large traffic volumes (more than 100 Gbit/s). Probably different approaches should be combined together for development of new-generation intellectual protection systems taking best from already existing solutions. It could be concluded from the analysis of research articles that there is a tendency to study network traffic as dynamical system with parameters changing in time. Most of the algorithms take in consideration only primary traffic characteristics, however, the study of secondary characteristics may assure DDoS attacks detection using less amount of data or shorter time intervals compared to classical approaches. This hypothesis requires additional research.

Acknowledgments

We thank our colleges A. Krasnov, E. Nadezhdin and D. Nikol'skii for their constructive feedback about the work and helpful comments that greatly improved the manuscript. The work was supported by the Ministry of Education and Science of Russia by lot code 2017-14-579-0002 on the topic: "The development of effective algorithms for detection network attacks based on identifying of deviations in the traffic of extremely large volumes arriving at the border routers of the data network and

creating a sample of software complex for detection and prevention of information security threats aimed at denial of service". The agreement No. 14.578.21.0261 on granting a subsidy at September, 26, 2017, a unique identifier of the work (project) is RFMEFI57817X0261.

References

[1] Kaspersky Security Bulletin 2016, "Review of the year: Overall statistics for 2016," 2016. (https://securelist.com/kaspersky-security-bulletin-2016-executive-summary/76858/)

[2] D. V. V. Sindhu Arumugam and M. V. P. Sumathi, "Detection of botnet using fuzzy c-means clustering by analysing the network traffic," *International Journal of Scientific and Engineering Research*, vol. 6, no. 4, pp. 475–479, 2015.

[3] R. C. Baishya, N. Hoque, and D. K. Bhattacharyya, "DDoS attack detection using unique source IP deviation," *International Journal of Network Security*, vol. 19, no. 6, pp. 929–939, 2017.

[4] D. Balamurugan, S. Chandrasekar, D. Jaya Prakash, and M. Usha, "Analysis of entropy based DDoS attack detection to detect UDP based DDoS attacks in IPv6 networks," *International Journal of Information and Computation Technology*, vol. 3, no. 10, pp. 25–28, 2013.

[5] Dhruba K. Bhattacharyya and Jugal K. Kalita, *DDoS Attacks. Evolution, Detection, Prevention, Reaction and Tolerance*, Boca Raton, USA: Taylor and Francis, 2016.

[6] A. Bonguet and M. Bellaiche, "A survey of denial-of-service and distributed denial of service attacks and defenses in cloud computing," *Future Internet*, vol. 9, no. 3, p. 43, 2017.

[7] C. A. Catania, F. Bromberg, and C. G. Garino, "An autonomous labeling approach to support vector machines algorithms for network traffic anomaly detection," *Expert Systems With Applications*, vol. 39, no. 2, pp. 1822–1829, 2012.

[8] S. Chawla, M. Sachdeva, and S. Behal, "Discrimination of DDoS attacks and flash events using Pearson's product moment correlation method," *International Journal of Computer Science and Information Security*, vol. 14, no. 10, pp. 382–389, 2016.

[9] C. M. Chen and H. C. Lin, "Detecting botnet by anomalous traffic," *Journal of information security and applications*, vol. 21, pp. 42–51, 2015.

[10] J. H. Chen, M. Zhong, F. J. Chen, and A. D. Zhang, "DDoS defense system with Turing test and neural network," in *IEEE International Conference on Granular Computing (GrC'12)*, pp. 38–43, Hangzhou, China, Aug. 2012.

[11] Aruba. Hewlett Packard Enterprise Company, "The Internet of Things: Today and tomorrow," 2016. (https://www.arubanetworks.com/assets/eo/HPE_Aruba_IoT_Research_Report.pdf)

[12] M. Crotti, M. Dusi, F. Gringoli, and L. Salgarelli, "Traffic classification through simple statistical fingerprinting," in *ACM SIGCOMM Computer Communication Review*, vol. 37, pp. 5–16, Kyoto, Japan, August 2007.

[13] C. J. Dietrich, C. Rossow, and N. Pohlmann, "CoCoSpot: clustering and recognizing botnet command and control channels using traffic analysis," *Computer Networks*, vol. 57, no. 2, pp. 475–486, 2013.

[14] C. Dietzel, A. Feldmann, and T. King, "Blackholing at ixps: On the effectiveness of ddos mitigation in the wild," in *International Conference on Passive and Active Network Measurement*, pp. 319–332, Heraklion, Crete, Greece, Mar. 2016.

[15] V. S. Galayev, A. E. Krasnov, D. N. Nikol'skii, and D. S. Repin, "The space of structural features for increasing the effectiveness of algorithms for detecting network attacks, based on the detection of deviations in traffic of extremely large volumes," *International Journal of Applied Engineering Research*, vol. 12, pp. 10781–10790, 2017.

[16] B. B. Gupta, R. C. Joshi, and M. Misra, "ANN based scheme to predict number of zombies in a DDoS attack," *International Journal of Network Security*, vol. 14, no. 2, pp. 61–70, 2012.

[17] Imperva, Inc, "Incapsula's 2014 DDoS impact report," 2014. (https://lp.incapsula.com/ddos-impact-report.html)

[18] Imperva, Inc, "Global DDoS threat landscapy," Q2 2017. (https://www.incapsula.com/ddos-report/ddos-report-q2-2017.html)

[19] Imperva, Inc, "Global DDoS threat landscapy," Q3 2017. (https://www.incapsula.com/ddos-report/ddos-report-q3-2017.html)

[20] K. Kalkan and F. Alagöz, "A distributed filtering mechanism against DDoS attacks: ScoreForCore," *Computer Networks*, vol. 108, pp. 199–209, 2016.

[21] L. Ke, Z. Wanlei, L. Ping, and L. Jianwen, "Distinguishing DDoS attacks from flash crowds using probability metrics," in *IEEE Third International Conference on Network and System Security*, pp. 9–17, Shanghai, China, Oct. 2009.

[22] A. Khalimonenko and O. Kupreev, "DDOS attacks in Q1 2017. kaspersky lab," 2017. (https://securelist.com/ddos-attacks-in-q1-2017/78285/)

[23] A. Khalimonenko, O. Kupreev, and T. Ibragimov, "DDoS attacks in Q2 2017. kaspersky lab," 2017. (https://securelist.com/ddos-attacks-in-q2-2017/79241/)

[24] A. Khalimonenko, O. Kupreev, and K. Ilganaev, "DDoS attacks in Q3 2017. kaspersky lab," 2017. (https://securelist.com/ddos-attacks-in-q3-2017/83041/)

[25] A. Khalimonenko, J. Strohschneider, and O. Kupreev, "DDOS attacks in Q4 2016. Kaspersky Lab," 2016. (https://securelist.com/ddos-attacks-in-q4-2016/77412/)

[26] A. Kind, M. P. Stoecklin, and X. Dimitropoulos, "Histogram-based traffic anomaly detection," *IEEE Transactions on Network and Service Management*, vol. 6, no. 2, pp. 110–121, 2009.

[27] A. Koay, A. Chen, I. Welch, and W. K. Seah, "A new multi classifier system using entropy-based features in DDoS attack detection," in *Information Networking (ICOIN), 2018 IEEE International Conference*, pp. 162–167, Chiang Mai, Thailand, Jan. 2018.

[28] A. E. Krasnov, E. N. Nadezhdin, V. S. Galayev, E. A. Zykova, D. N. Nikol'skii, and D. S. Repine, "DDoS attack detection based on network traffic phase coordinates analysis," *International Journal of Applied Engineering Research*, vol. 13, no. 8, pp. 5647–5654, 2018.

[29] V. Kuskov, M. Kuzin, Ya. Shmelev, D. Makrushin, and I. Grachev, "Honeypots and the Internet of Things. securelist. Kaspersky Lab.," 2017. (`https://securelist.com/honeypots-and-the-internet-of-things/78751/`)

[30] Y. Liu, L. Zhang, and Y. Guan, "Sketch-based streaming PCA algorithm for network-wide traffic anomaly detection," in *Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference*, pp. 807–816, Genova, Italy, June 2010.

[31] W. Lu, G. Rammidi, and A. A. Ghorbani, "Clustering botnet communication traffic based on n-gram feature selection," *Computer Communications*, vol. 34, no. 3, pp. 502–514, 2011.

[32] D. Makrushin, "The cost of launching a DDoS attack. securelist. Kaspersky Lab," 2017. (`https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/`)

[33] L. Malina, P. Dzurenda, and J. Hajny, "Testing of DDoS protection solutions," in *Security and Protection of Information*, pp. 113–128, Brno, Czech Republic, May 2015.

[34] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," in *ACM SIGCOMM Computer Communication Review*, vol. 34, pp. 39–53, Portland, USA, 2004.

[35] MIT, *The Internet of Things*, Business Reports, MIT Technology Review, Aug. 2014.

[36] Radware, "DDoS attack definitions — DDoSPedia: glossary that focuses on network and application security terms with many DDoS-related definitions," 2017. (`https://security.radware.com/ddos-knowledge-center/ddospedia/rudy-r-u-dead-yet/`)

[37] S. V. Raghavan and E. Dawson, eds., *An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks: Critical Information Infrastructure Protection*, India: Springer Science & Business Media, 2011.

[38] V. S. Reddy, K. D. Rao, and P. S. Lakshmi, "Efficient detection of DDoS attacks by entropy variation," *IOSR Journal of Computer Engineering*, vol. 7, no. 1, pp. 13–18, 2012.

[39] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDoS attacks using artificial neural networks," *Neurocomputing*, vol. 172, pp. 385–393, 2016.

[40] Chris Sanders, *Practical packet analysis: Using Wireshark to solve real-world network problems*, San Francisco: No Starch Press, 2017.

[41] A Neustar security solution exclusive report, "Worldwide DDoS attacks & cyber insights research report: Taking back the upper hand from attackers," 2017. (`https://hello.neustar.biz/201705-Security-Solutions-DDoS-SOC-Report-LP.html`)

[42] K. Singh, K. S. Dhindsa, and B. Bhushan, "Distributed defense: An edge over centralized defense against DDoS attacks," *International Journal of Computer Network and Information Security*, vol. 9, no. 3, pp. 36, 2017.

[43] V. Srihari and R. Anitha, "DDoS detection system using wavelet features and semi-supervised learning," in *Security in Computing and Communications. SSCC 2014. Communications in Computer and Information Science*, pp. 291–303, Delhi, India, Sept. 2014.

[44] Akamai Technologies, "Q3 2016 state of the internet: Security report," 2016. (`https://content.akamai.com/pg7407-soti-security-report-q3-en.html`)

[45] D. S. Terzi, R. Terzi, and S. Sagiroglu, "Big data analytics for network anomaly detection from netflow data," in *Computer Science and Engineering (UBMK), 2017 IEEE International Conference*, pp. 592–597, Antalya, Turkey, Oct. 2017.

[46] T. M. Thang and V. K. Nguyen, "Synflood spoof source DDoS attack defence based on packet ID anomaly detection — PIDAD," *Software Networking*, vol. 2017, no. 1, pp. 213–228, 2017.

[47] K. Wang, C.-Y. Huang, S.-J.Lin, and Y.-D. Lin, "A fuzzy pattern-based filtering algorithm for botnet detection," *Computer Networks*, vol. 55, no. 15, pp. 3275–3286, 2011.

[48] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, "A DDoS attack detection method based on SVM in software defined network," *Security and Communication Networks*, vol. 2018, pp. Article ID 9804061, 8 pages, 2018.

[49] S. Yu, W. Zhou, R. Doss, and W. Jia, "Traceback of DDoS attacks using entropy variations," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 3, pp. 412–425, 2011.

[50] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS attacks from flash crowds using flow correlation coefficient," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1073–1080, 2012.

[51] J. Yuan and K. Mills, "Monitoring the macroscopic effect of DDoS flooding attacks," *IEEE Transactions on Dependable and secure computing*, vol. 2, no. 4, pp. 324–335, 2005.

Biography

Vladimir Galyaev received his specialist's degree in Math and his Ph.D. degree in Information Technologies from Dagestan State University (Makhachkala, Russia) in 2000 and 2004, respectively. Since 2008 he is the Head of the Department of Information Technologies and Information Security of Dagestan State University of National Economy (Makhachkala, Russia). In 2013 he became an associate professor in Dagestan State University of National Economy, he gives lectures for students specialized in information security. Since 2017 he works as senior research fellow in State Institute of Information Technologies and Telecommunications. His research interests include network security, data protection, steganography and e-learning.

Evgenia Zykova received her specialist's degree in Biochemical Physics from Siberian Federal University (Krasnoyarsk, Russia) in 2011, and she received her Ph.D. degree in Biophysics from Institute of Cell Biophysics RAS (Pushchino, Russia) in 2016. She is a research fellow in State Institute of Information Technologies and Telecommunications. Her research interests include data statistical analysis, machine learning and data mining techniques.

Dmitry Repin graduated from Kaliningrad Higher Engineer School of Engineer Troops (Kaliningrad, Russia) in 1992 and from Moscow Power Engineering Institute in 2005, he have a major in computer networks and telecommunications. In 2008 he received his Ph.D. degree in Technical Sciences in Moscow State Mining University. In 2018 he graduated from the Academy of Information Systems by specialty of information security. He is a Deputy Director of State Institute of Information Technologies and Telecommunications. For many years Dr. Repin participated in federal projects devoted to development and implementation of advanced information technologies for high-performance data processing, storage and high-speed data transmission in computer telecommunications networks of Russian Ministry of Education and Science. His main areas of expertise are telecommunication technologies, network security, software-defined networking, National Research and Education Networks located in or connected to Russia.

Denis Bokov received his specialist's degree in Comprehensive information security of automated systems from Moscow Engineering Physics Institute in 2007, and he received his Ph.D. degree in Social Philosophy from Moscow State Regional University in 2011. Also he received a specialist's degree in Jurisprudence from Institute for Socio-Economic Forecasting and Modeling (Moscow, Russia) in 2006. He is the Director of State Institute of Information Technologies and Telecommunications. Dr. Bokov is managing a few federal programs aimed at development of the information infrastructure to ensure coordination of activities in the field of informatization of subordinate institutions of the Ministry of Education and Science of Russia. His main areas of expertise are technical, social and law aspects of higher education informatization, e-learning, data protection and National Research and Education Networks located in or connected to Russia.