Detection strategies for post-pandemic DDoS profiles

Péter Orosz, Balázs Nagy, and Pál Varga

Abstract—**The global pandemic lockdowns fostered the digital transition of companies worldwide since most of their employees worked from home using public or private cloud services. Accordingly, these services became the primary targets of the latest generation DDoS threats. While some features of current DDoS attack profiles appeared before the pandemic period, they became significant and reached their current complexity in the recent period. Besides applying novel methods and tools, the attacks' frequency, extent, and complexity also increased significantly. The combination of various attack vectors opened the way for multi-vector attacks incorporating a unique blend of L3-L7 attacking profiles. Unifying the hit-and-run method and the multi-vector approach contributed to the remarkable rise in success rate.**

The current paper has two focal points. First, it discusses the profiles of the latest DDoS attacks discovered in real data center infrastructures. To demonstrate and emphasize the changes in attack profile, we reference attack samples recently collected in various data center networks. Second, it provides a comprehensive survey of the state-of-the-art detection methods related to recent attacks. The paper especially focuses on the accuracy and speed of these, mostly networking-related detection approaches. Furthermore, we define features and quantitative and qualitative requirements to support detection methods handling the latest threat profiles.

Index Terms—**Intrusion detection and prevention, DDoS, Network security, Machine learning.**

I. Introduction

The pandemic lockdown fostered the ongoing digital transformation of society in many ways. Remote working and distance learning opened the way for new forms of group interactions. Online sale platforms were out for a more personal shopping experience for their customers. All of these transient shifts were supported by highly centralized cloud infrastructures that became the primary target of Distributed Denial of Service attacks. To improve the success rate, post-pandemic threats involve new methods and tools. A new set of protection methods should be developed and deployed to effectively improve the security level against high-complexity and high-intensity DDoS attacks. Our survey targets the presentation of post-pandemic DDoS attack profiles and their detection strategies, and goes beyond previous studies in highlighting technical depth. Moreover, we collected attack samples in a real data center and made them openly available (see related references in Section IV).

Many industrial stakeholders predict that DDoS attacks are becoming ”bigger” and more frequent in the coming years (according to Cisco [1], and Akamai [2]). Some recent DDoS attacks in 2020 already reached 2.3Tbps (AWS), and then 2.5Tbps (Google), which are much larger than the Mirai botnet attack against the DNS provider Dyn, estimated to reach as high as 1.5Tbps in 2016. A more sophisticated, multi-vector Mirai botnet variant attack reaching almost 2Tbps has also been captured at the end of 2021 by Cloudflare. These incidents dominated the most worrying global news. However, there are countless attack cases that may not hit the front page, although their *relative* impact on the given (less widely used) service or (less known) company could be much more pronounced.

How can we keep up with the adversaries? It is not only a matter of more machinery in the defense: detection methods need to be faster and more precise.

The exact methods to be used depend on the attack type; but detection time is a critical factors of success. Within the three main attack types – i.e., volumetric, protocol-based, and application-specific – the somewhat traditional attacker approach is brute force. However, the new breed of DDoS attacks has two typical types: massive volume amplification and/or volatile presence (Fig. 1).

There are numerous survey papers on the topic, although this current study of ours goes beyond their target in terms of timely presentation of new-generation DDoS attacks, as well as in technical depth. We focus on the accuracy and speed of threat detection. Among the many overviews, some of the suggested survey papers on the topic are the following. Peng, Leckie, and Ramamohanarao [3] surveyed ”network-based” defense mechanisms against DDoS attacks in 2007. Their paper already included many of the terms, architectures and mechanisms we use today as a basic reference point. Zargar, Joshi, and Tipper [4] provided one of the earliest comprehensive surveys on modern defense mechanisms against DDoS flooding attacks in 2013. Masdari and Jalali [5] provided a comprehensive-at-the-time taxonomy of DDoS attack types in 2016, extending the focus to cloud infrastructures as well. In the same year, Yan et. al [6] described DDoS attacks from the perspective of Software-Defined Networking (SDN) and highlighted research issues and challenges, some of which are still open to this day. In 2018-2019 the challenges described by Yan were still not solved, but many significant steps were taken to harden SDN against DDoS [7], [8], [9].

Department of Telecommunications and Media Informatics Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics, Budapest, Hungary
E-mail: orosz, bnagy, pvarga {@tmit.bme.hu}

DOI: 10.36244/ICJ.2023.4.4

Volumetric attacks have become more significant and use a broader set of methods than ever, especially for mixing various strategies. Devices and botnets have become rental objects; hence the group of users has also grown. These changes motivated the current article to go beyond previous overviews of the topic.

The contributions of the current paper are the following:

1) First, we define the main terms around DDoS analysis,
2) We provide a condensed comparison of the new breeds of DDoS attacks and discuss the related detection and mitigation methods,
3) We provide real-life captured DDoS traffic traces and analyze them in Section IV to help general comprehension.

The structure of the paper is the following. Section II provides basic definitions for the standard terms in the DDoS domain. Section III describes the new breed of DDoS attacks and the challenges raised by their existence, whereas Section IV provides a comprehensive and structured survey on the related detection methods. Section V surveys the modern methods for DDoS detection, including those based on artificial intelligence – especially machine learning – techniques. Finally, Section VI gives an outlook on DDoS trends in the future, and Section VII concludes the paper.

II. DEFINITIONS

This section provides brief definitions of terms that are commonly used in the domain of DDoS attacks, their detection and mitigation.

(D)DoS: The (Distributed) Denial of Service attack is a cyber threat that targets network segments or online services to deny access to certain resources and/or services. (D)DoS can be classified as an attack against the base of the CIA triad (availability). Since DDoS attacks are a lot more widespread now than DoS, we commonly refer to (D)DoS attacks as DDoS in this article.

IDS: The Intrusion Detection System monitors the network traffic for suspicious activity and issues alerts when such action is discovered. Intrusion detection systems are not designed to block attacks but to monitor the network and send alerts to system administrators if a potential threat is detected.

IPS: The Intrusion Prevention System supervises the access to an IT network and protect it from abuses and attacks. These systems are designed to monitor system data and take the necessary action to prevent an attack from developing.

IP spoofing: IP spoofing is the process of creating Internet Protocol (IP) packets that have a modified source address to either hide the identity of the sender, impersonate another computer system, or both. In theory, IP spoofing should not exist because ISPs are advised to implement source IP egress filtering. Still, in reality, many ISPs do not implement these filters. Spoofing is still very common in 2023.

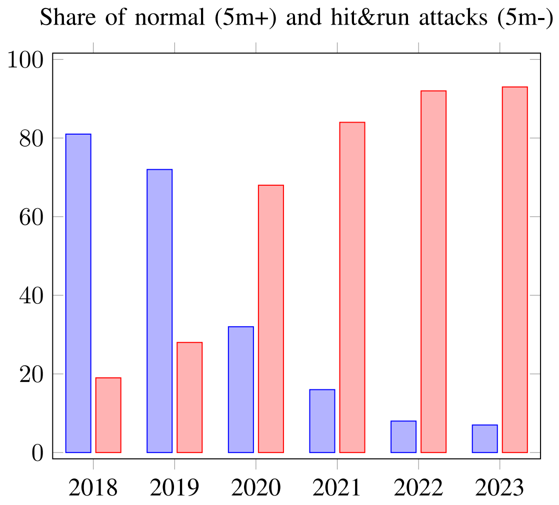


Fig. 1. Comparison of number of normal (longer than 5 minutes, blue) attacks and hit&run (shorter than 5 minutes, red) through 2018-2022 at the networks protected by AITIA SGA-NEDD

Volumetric DDoS attack (or Layer-3,-4 attack, flood attack): A DDoS attack that uses the sheer number (volume) of forged packets to achieve denial of service. Volumetric DDoS attacks primarily target network segments such as switches, routers, network processors, and data-links. This method of DDoS is by far the most popular among DDoS types because: a) the Internet is littered with poorly secured machines, IoT devices mainly, which can be organized into powerful botnets, and b) one botnet can be used to mount an effective attack against all targets.

Reflection DDoS attack: A volumetric DDoS attack that uses intermediary services of the Internet to amplify its attack throughput. It requires vulnerable Internet services – such as the NTP protocol – and the ability to inject packets into the network with spoofed source IP addresses. Reflection is a very effective and popular attack method: multi 100 Gbps attacks can be achieved with ease, and according to Akamai Inc., gives more than 50% of all DDoS attacks. The reasons are mainly the following: a) even 10000x amplification can be achieved, b) the attack's origin is obfuscated, and c) there is an abundance of widely used vulnerable services on the Internet.

Amplification DDoS attack: A DDoS attack that exploits a vulnerability related to asymmetric request-response volumes, where the response takes significantly more effort or contains considerably more data than the request. It is often used together with a reflection method. Hence, the attacker issues a ”tiny” request (in effort or volume) to the reflection nodes, which reflects its (relatively) massive amount of data response to the victim node (instead of addressing the attacker). It is implemented using IP spoofing.

Application layer DDoS attack (or Layer 7 attack): A DDoS attack that uses application vulnerabilities to achieve denial of service. Application layer DDoS attack primarily targets computational resources like server processors and memory.

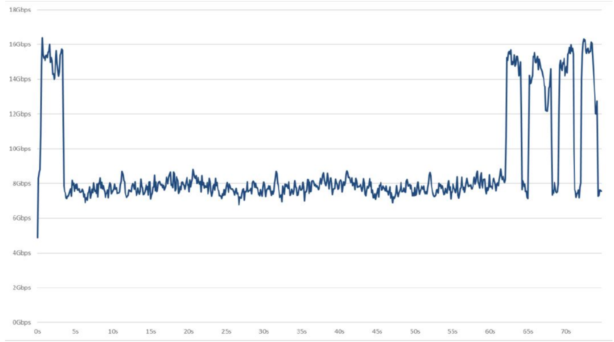


Fig. 2. An example of hit-and-run attack. This attack was captured by the authors of this paper in the network of KIFÜ (Hungarian Governmental Agency for IT Development). The x-axis represents time, and the y-axis shows measured throughput.

These attacks are tailored for their target, so each attack has a limited number of targets. This quality makes this kind of attack quite rare. These attacks are extremely different from volumetric attacks in the method of attack and the mitigation. This paper does not focus on application layer attacks; it instead aims to provide a detailed overview of volumetric attacks.

Hit-and-Run Attack: Volumetric DDoS attack that uses short bursts of attacking traffic to achieve its goals (Fig. 2). This attack is becoming increasingly popular because i) IDSs have problems detecting these kinds of attacks, and ii) it can achieve a lasting impact on the network through congestion control mechanics, such as TCP congestion control.

False positive detection rate: The portion of traffic identified falsely as a DDoS attack – although that was genuinely legitimate traffic. It is calculated as the ”number of packets falsely identified as belonging to the DDoS attack” divided by the ”number of all packets” that arrived in the time period.

False negative detection rate: The portion of traffic identified falsely as legitimate – although that was truly a DDoS attack. It is calculated as the ”number of packets falsely identified as legitimate” divided by the ”number of all packets” that arrived in the time period.

Detection time of a DDoS attack: The time span between the arrival time of the first packet of the attack and the decision at the IDS. Commonly also referred to as detection lag.

North-South attack: An attack where malicious traffic originates from outside the data-center hosting the under-attack service.

East-West attack: An attack where the malicious traffic originates from the data-center hosting the targeted service. Method to circumvent the main-defensive lines of the DCN, east-west (internal) routes are almost always less protected than north-south routes.

III. New profiles of DDoS attacks: methods, tools, and challenges

As a generic definition for Denial-of-Service (DoS) attack, it is a particular type of malicious traffic that attempts to make an online service unavailable for normal service users. Its distributed version (Distributed-DoS) enhances the threat's effectiveness by concurrently generating malicious traffic from many contributing sources (usually many thousands or even more) to a single target. The traffic distribution enables a much larger traffic volume (nowadays, it may well exceed the Terabit order) to be developed and directed toward the targeted host or service. In the last decade, we could face a new wave of DDoS methods and attacks that have become the most common threats on the Internet due to their relatively easy and automated execution (see Table I). DDoS attempts usually target the resources of service and cloud providers. The new breed of DDoS threats may involve key novelties: i) vulnerable IoT devices as their security suites often miss even the basic protecting tools, ii) shorty living and pulsating volatile traffic patterns to be under the radar even for state-of-the-arts IDS/IPS systems, iii) very high volume of cumulative traffic generated by various amplification techniques, and iv) composite malicious traffic by combining various DDoS types (so-called vectors) to construct a multi-vector attack.

Typically, we distinguish three main categories of DDoS attacks: volumetric, protocol-based, and application-specific. While volumetric attacks focus on saturating bandwidth on the server's local network, protocol-based variants target the exhaustion of server-side hardware resources, i.e., system memory, CPU, and IO bus. From the complexity perspective, application-specific attacks have significantly more sophisticated operations, specifically targeting a web service or other application.

Here, we provide reasons and arguments for the appearance of multi-vector attacks during the pandemic.

A. New methods and tools

The post-pandemic DDoS threats' major novelty over the more conventional DDoS operational patterns is the development and amalgamation of two previously existing techniques: massive volume amplification and volatile presence. Moreover, applying this blend of techniques in multiple attack vectors challenges the security systems of data centers and cloud services and calls for a new generation of DDoS detection methods and implementations. Using the latest techniques, an attacker does not even require to access large-scale botnet resources and gain control over them to achieve a substantial attack volume. Instead, new attack techniques make one or many public service hosts send a response message to a spoofed destination address, i.e., to the targeted server host's address. An alternative way to amplify malicious traffic is to send a small-sized request message to the targeted host with a spoofed source address, which triggers a large response message to that address. This asymmetry between request and response messages results in low resource utilization on the attacker-side and may sink all resources on the server-side.

Amplification/reflection: By sending spoofed requests, the attacker triggers responses from a group of open DNS or NTP servers back to the victim's address (Fig. 3). Since the reply is typically more extensive than the request, the cumulative traffic

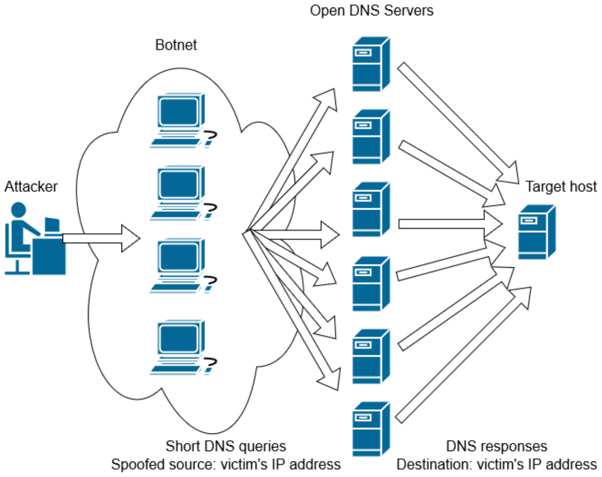


Fig. 3. Attack amplification/reflection mechanism

of the targeted response messages can saturate the network path between the attacked host and the Internet.

Volatile (hit-and-run) attack: In contrast to conventional DDoS threats, volatile attacks apply a periodic on/off strategy for controlling their presence on the network (see Fig. 2). In this case, the ON period is concise, typically lasting from milliseconds to minutes only, followed by an extended OFF period. This behavior is often successful since most IDS/IPS systems today have a detection time in the second range. Thus, these malicious traffic transients can reach the target host under the detection radar.

Multi-vector attack: It combines multiple methods and techniques to over-consume the resources of the target system in various ways. Mitigating these attacks can be challenging and often requires a multi-layer mitigation strategy. An efficient way to make an attack successful is to generate a complex traffic pattern that is easy to blend with regular traffic. Thus, multi-vector attacks may increase the probability of false positive detection that can block out an indefinite portion of user traffic along with the malicious one. The most popular component vectors are DNS reflection/amplification, TCP-Syn, TCP-Ack, TCP-Syn/Ack, TCP-Rst, and ICMP flood.

B. New generation botnets

The primary sources of DDoS attacks are botnets of various scales and feature sets. While a typical botnet is based on desktop computers, the security suites (including firewalls, virus, and intrusion detection systems) designed for desktop computers have evolved dynamically in the last decade. Accordingly, it became more challenging for hackers to infect a large number of computers with malicious codes. State-of-the-art desktop security suites typically incorporate a broad spectrum of protection features: anti-virus, web, email, user data, anti-hacking, and payment protections. Additionally, the processing power of the popular desktop processors enables to run of these detection features in real-time. Subsequently, there is a shift in the target of hackers towards alternative equipment with a lower security level, i.e., home, mobile, and IoT devices. In the last couple of years, numerous volumetric DDoS attacks approached or even exceeded the terabit-scale and originated from IoT botnets (Mirai-based botnets, as recent examples).

1) IoT-based botnets: The security protection of IoT devices is often overlooked by their developers due to strict delivery deadlines, lack of technical security background, or hardware cost. Moreover, the operating system of these devices is typically a stripped-down Linux distribution, omitting even the basic security subsystem. In addition, the generic Linux-based runtime environment enables attackers to effectively compile their malware codes to a broad spectrum of IoT devices. Considering IoT security, we should also focus on network-level defense beyond device-level security. From the networking perspective, IoT nodes like CCTV cameras routinely access the Internet with no rate limiting, which is an appealing feature for attackers. Since the IoT development life-cycle is relatively short, developers may reuse firmware codes or even web certificates and SSH keys. On the user-side, IoT equipment requires low maintenance, and they are considered deploy-and-forget devices. Thus, access passwords are often unchanged from the factory-default. These device-level shortcomings can be eliminated by setting up a strict network-level security and password policy specifically tailored to the deployed IoT device pool.

Ali et al. in [10] "Systematic Literature Review on IoT-Based Botnet Attack" performed a systematic literature review including the state-of-the-art of IoT-based botnet attacks. This review paper revealed that research in this domain is gaining momentum, particularly in the last 3 years.

N. Koroniotis et al. in [11] "Forensics and Deep Learning Mechanisms for Botnets in Internet of Things: A Survey of Challenges and Solutions" discusses the origin of botnets, overview the network forensic methods and focus on deep learning mechanisms and their roles in network forensics. Forensics of DDoS attacks is still a widely researched subject today; no standard method has been found, and most stakeholders are not interested in it. The main criterion of forensic research usefulness is how easy it is to deploy the system over the current Internet. Shi et al. and Ding et al. [12], [13] give a good overview of the current challenges and state-of-the-art.

T. S. Gopal et al. in [14] "Mitigating Mirai Malware Spreading in IoT Environment" analyzed the Mirai malware in detail and presented its exploitation techniques. They proposed a white-listing method to prevent an IoT-based botnet from spreading.

H. -V. Le and Q. -D. Ngo in [15] "V-Sandbox for Dynamic Analysis IoT Botnet" discuss the importance of sandbox environments in collecting behavior data from botnets in a secure way. They overview the limitations of the existing sandbox solutions and introduces the V-sandbox method for a dynamic analysis of IoT botnets. This proposal enables IoT botnet samples to reveal all of their malicious properties.

W. Li et al. in [16] "Analysis of Botnet Domain Names for IoT Cybersecurity" discusses the role of the global DNS service in supporting botnets to connect bots to C&C servers. To avoid tracking the C&C through the DNS information, botnets use sophisticated schemes such as fast-flux. Authors performed an in-depth analysis of the activities of Rustock botnet domain names, which use the fast-flux as the connection method between bots and C&C server.

R. Vinayakumar et al. in [17] ”A Visualized Botnet Detection System Based Deep Learning for the Internet of Things Networks of Smart Cities” proposes a botnet detection system based on a two-level deep learning framework for semantically discriminating botnets and legitimate behaviors at the application layer of the domain name system (DNS) services. In the first level of the framework, the similarity measures of DNS queries are estimated using siamese networks based on a predefined threshold for selecting the most frequent DNS information across Ethernet connections. In the second level of the framework, a domain generation algorithm based on deep learning architectures is suggested for categorizing normal and abnormal domain names.

Y. Jia et al. in [18] ”FlowGuard: An Intelligent Edge Defense Mechanism Against IoT DDoS Attacks” propose an edge-centric IoT defense scheme called FlowGuard for the detection, identification, classification, and mitigation of IoT DDoS attacks. They present a new DDoS attack detection algorithm based on traffic variations and design two machine learning models for DDoS identification and classification.

N. Ravi et al. in [19] ”Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture” present a security scheme that leverages the cloud and software-defined network (SDN) paradigm to mitigate DDoS attacks on IoT servers. They have proposed a novel mechanism named learning-driven detection mitigation (LEDEM) that identifies DDoS using a semi-supervised machine-learning algorithm and mitigates DDoS. Authors tested LEDEM in the testbed, emulated topology, and compared the results with state-of-the-art solutions. They achieved an improved accuracy rate of 96.28% in detecting DDoS attacks.

2) Mobile-based botnets: Smart mobile phones can be considered as handheld computers with ever-increasing processing power and network bandwidth. An LTE or 5G mobile network enables the transmission of multiple 100 Mbps of data from a single mobile device. M. Eslahi et al. in [20] ”MoBots: A new generation of botnets on mobile devices and networks” present an overview of mobile botnets, including studies on the new command and control mechanisms, actual examples, and malicious activities. N. Hoque et al. in [21] ”Botnet in DDoS Attacks: Trends and Challenges” present a comprehensive overview of DDoS attacks, their causes, types with a taxonomy, and technical details of various attack launching tools. Authors give a detailed discussion of several botnet architectures and tools developed using botnet architectures. Moreover, the dominant Android mobile operating system has an approx. 72% market-share worldwide. The combination of high processing and networking capacities and a single highly prevalent OS platform made a mobile device an appealing target for hackers for many malicious purposes. Primarily, due to the less sophisticated security suites, attackers can remotely install malware codes to the mobile device. Mobile botnets are a group of unrelated mobile devices infected by a common botnet malware. The operational scheme is similar to that of the desktop-based variant; the botnet master remotely manages the botnet by a command and control mechanism to initiate a DDoS attack towards a target victim. Z. Lu et al. in [22] ”On the Evolution and Impact of Mobile Botnets in Wireless Networks” adopt a stochastic approach to study the evolution and impact of mobile botnets. Authors find that node mobility can be a trigger to botnet propagation storms. They also reveal that mobile botnets can propagate at the fastest rate of quadratic growth in size, which is substantially slower than the exponential growth of Internet botnets. A. A. Santos et al. in [23] ”A Stochastic Adaptive Model to Explore Mobile Botnet Dynamics” propose a stochastic adaptive model for the dynamics and the self-organized and self-adaptive behavior of mobile botnets to perform DDoS attacks.

Beyond the legacy command and control protocols (e.g., IRC, HTTP, and P2P), mobile-specific control mechanisms such as SMS-, MMS-, or Bluetooth-based variants have also emerged. The most challenging mobile botnet is the SMS- and P2P-based architecture in terms of detection complexity. E. Johnson and I. Traore in [24] ”SMS Botnet Detection for Android Devices through Intent Capture and Modeling” investigated mobile botnets focusing on the Android operating system. Authors discuss a short messaging service (SMS) botnet structure and investigate a new detection model using the concept of intents. They show that transparent control can be achieved by a remote endpoint yet also detected by the proposed intent detection model.

C. Today’s challenges

Increasing traffic volume requires ever more protective network resources. Volumetric attacks can quickly exhaust even the most considerable amount of Internet access capacity.

Shared botnets (many available for hiring): Hiring a botnet is a viable business option for botnet masters. In this model, hired resources are often accounted and paid for on a time basis. A major economic challenge here is a significant asymmetry in the expense of the attack and the defense. Renting botnet resources for a 10-minute attack costs as low as 35 cents [25].

Linux-based DDoS malware: The latest Windows versions enable running a complete Linux run-time environment on a Windows-based laptop or desktop computer. This feature opened the possibility for malware authors to cross-compile botnet code to run on both Windows and Linux systems. This option raises crucial challenges in the defense strategy: i) a high number of IoT devices with common security vulnerabilities run a Linux-based operating system, ii) Linux-based datacenter servers possess a high amount of computational and bandwidth resources to execute a heavy-hitter DDoS attack.

Launching attacks by non-technical users: Volumetric attacks can be initiated with dedicated control programs and scripts available on the darknet or offered to the attacker by the bot master of the rented botnet. These tools are easy to use; therefore, even a non-technical user can initiate and control a powerful attack.

Attack from mobile and IoT equipment: The increasing computational power of handheld devices and the transmission capacity of 4G and 5G networks open the way to deliver a wide range of botnet malware to mobile devices. Moreover, mobile security suites typically have a lower level of defense against malware deployment. Thus, handheld devices may become the next target of the bot master (a person who owns the botnet). Reputation-based detection is inefficient for identifying infected mobile devices since user equipment's IP addresses frequently change in mobile communication networks.

Hit-and-run and multi-vector attacks continue to evolve. H-a-R is still popular due to its low cost and ease of deployment. At the same time, multi-vector variants are very effective in bypassing traditional mitigation strategies. Recently, we have seen a significant rise in the popularity of multi-vector attacks incorporating 15 or more vectors. Combining the hit-and-run and multi-vector strategies resulted in a shorter attack duration with an increased success rate. Since attackers often rent a shared botnet to execute the DDoS attack, their ambition to reduce the duration is reasonable. Moreover, the shortened attack has a higher probability of bypassing security systems with a larger detection window.

Browser-based bot attacks: Websites are attractive platforms to deliver malware to a high number of user devices via popular web browsers. Javascript-based codes do not depend on the operating systems and exploit the web browsers' vulnerabilities. While these codes stop running as the user quits the browser application, they are re-downloaded and re-initialized as one re-visits the compromised web page.

Emerging encrypted attacks. TLS- and ESP-based attacks have two key advantages: i) they consume extra CPU resources to perform encryption and decryption, ii) many DDoS detection systems do not support the inspection of TLS- and ESP-encrypted traffic.

Distributed targets: From the infrastructural perspective, popular cloud-based services are distributed across many physical servers, and many of them are often located in dedicated IP subnets. Instead of attacking a single IP node, this type of DDoS threat increases the success rate by targeting an entire IP subnet incorporating a set of servicing nodes.

Application-specific attacks: The majority of application-specific attacks target a specific service and not a service type in general, e.g., developed to attack a specific streaming service. It means that no attack is capable of targeting streaming services universally. Meanwhile, a recent method called mimicked user browsing is very effective for a large-scale of web applications. It is a web-based application-specific attack type developed to imitate the behavior of real user interaction with the service provider nodes. The major challenge is its low false rate detection since its traffic pattern is identical to that of a real user. Due to the similarity property, it can easily maintain its success rate even using a large number of participating botnet nodes.

D. Lessons learned in DDoS challenges

Recent research works propose several methods and tools for effectively detecting the new-generation DDoS attack types (see Section IV). However, a new breed of attack techniques (especially the combination of hit-and-run and multi-vector attacks) still challenges protection systems with a more sophisticated traffic pattern combined with a large traffic volume within a very short time period. Besides the new types of network layer attacks, the mimicked user browsing attack targets a specific service with a high success rate. Moreover, shared low-cost botnets create a high resource and economic imbalance between the expense of the attack and the defense. In Section IV, we discuss the major scientific works for detecting the presented threat types.

IV. DETECTION OF NEW GENERATION DDOS THREATS

A. Hit-and-run

The so-called hit-and-run (or shrew) DDoS attacks are attacks that operate with multiple high throughput short bursts, [26], [27]. These attacks are dangerous because: i.) They cause significant quality of service degradation through TCP congestion control, ii.) many DDoS detection engines cannot identify them, iii.) even if they are detected if there is a human operator in the decision-loop, for her, the number of signals can be overwhelming. i.) Network equipment has relatively small intermediary buffers that can be saturated in less than an ms. Saturated buffers imply packet loss. After the initial packet loss(es), the TCP connection's congestion control throttles the connection speed. After this event, the TCP connection will need seconds to recover to the pre-loss throughput. This kind of QoS drop was very hard to quantify in the past, so operators ignored unconventional hit-and-run attacks. Aleksandar Kuzmanovic and Edward W. Knightly did the first research on this subject; they published their results in ”Low-Rate TCP-Targeted Denial of Service Attacks: The Shrew vs. the Mice and Elephants” [28]. In this paper, they proved that a DDoS attack that delivers its payload in short bursts significantly affects the throughput of TCP flows. Kuzmanovic's method was relatively complex and had a high margin of error; thus, it wasn't used much. Since then, this kind of DDoS have become the most researched subject in the field because it lacks the throughput footprint of regular DDoS [29], [30], [31]. In ”A Way to Estimate TCP Throughput under Low-Rate DDoS Attacks: One TCP Flow” [32] Kieu et al. propose a precise and straightforward method to quantify the damage caused by unconventional low-throughput or hit-and-run attacks. Kieu proves that their method is accurate using the NS-2 simulator. ii.) The detection time of the DDoS detector is in the range of seconds, which is longer than the time required to disrupt TCP flows. If the IDS doesn't have detection times in the ms range, it will always lag after the effect of the attack. iii.) The human-in-the-loop is a multiple way inadequate to deal with hit-and-run attacks. The time needed to make a human decision is multiple orders of magnitude longer than the duration of a DDoS burst that can successfully disrupt the TCP

TABLE I
OVERVIEW: THE NEW BREED OF DDOS ATTACKS

Attack type	Key characteristics	Special features
Amplification/Reflection	Spoofed request to a set of public servers triggers responses toward the targeted system	Cumulative response traffic can saturate the network path of the vicim host
Hit-and-Run (Volatile)	Periodic On/Off strategy	Short On period (form milliseconds to minutes) followed by an extended Off period
Multi-vector	Combines multiple methods and attack types (most popular are: DNS reflection, TCP smart attacks and ICMP flood) into a single attack	Challenging mitigation: complex traffic pattern blended easily to normal traffic
Linux-based botnet	Cross compiled botnet code to run in Linux systems	Infection targets: IoT devices and data center servers
Mobile botnet	With 72% of market share, Android devices are in the focus of botnet malware. Key method is remotely install the malware code.	Increasing processing power and network bandwidth of mobile devices
Browser-based	Exploits vulnerability of web browsers to deploy malware JavaScript codes	Code stops running as user quit the browser application and therefore it requires a re-visit of the compromised site.
Distributed targets	Attack targets a set of server nodes within a subnet	Physical servers behind a cloud-base service are typically located in a dedicated data center subnet. Attacking a set of servers increases the success rate.
Mimicked user browsing	An application-specific attack aiming to replicate the behavior of real user interaction with the service provider nodes	Detection is challenging even when a large number of botnet nodes are participating in the attack

flows. If the attack changes some parameters (IP/port/protocol) between bursts, each burst will generate a discrete detection signal. Authors identified attacks that operated with changing parameters by generating more than 2000 signals per day for weeks. Such a high number of signals cannot be efficiently processed and validated by a human operator.

To successfully mitigate the effect of hit-and-run attacks, the network has to be changed, or the IDS has to: a.) detect and mitigate attacks within milliseconds, b.) have an acceptably low false detection rate to work without human validation.

There is a relatively small number of research results on this subject.

In ”Low-rate TCP DDoS Attack Model in the Southbound Channel of Software Defined Networks” [33], Balarezo et al. showcase how low-rate DDoS attacks can exploit TCP congestion control to cause significant QoS drop in SDN networks. They propose a method to model the attacks and their effects in SDN.

In ”On a Mathematical Model for Low-Rate Shrew DDoS” [34], Luo et al. present a new, more accurate analytical method to model the effect of a wide variety of hit-and-run attack patterns. This method aims to be significantly more accurate than current state-of-the-art methods. It reduces the average margin of error from 69% to 10% for most network environments and attack patterns. By making accurate models and understanding how network environments and attack patterns determine the effect of attacks, they managed to build a novel defense method against hit-and-run attacks. The proposal significantly reduces the impact of the attack.

In ”Stability of TCP/AQM Networks Under DDoS Attacks With Design” [35], Tan et al. propose a method to tweak TCP active queue management to mitigate the effect of hit-and-run attacks on TCP congestion control. The results of this research are promising since they prove that TCP throughput can be stabilized at an acceptable level during an attack without sacrificing anything else or adding new network components.

In ”A new network flow grouping method for preventing periodic shrew DDoS attacks in cloud computing” [36], Liu et al. propose a new method to extend the usability of the BIRTH algorithm in detecting shrew (hit-and-run) attacks. The primary deficiency of BIRTH is its long detection time, which makes it hardly usable against hit-and-run attacks. By clustering and re-merging traffic using flow-level frequency domain characteristics, this method appears to significantly improve the detection time of the BIRTH algorithm.

In ”An optimized design of reconfigurable PSD accelerator for online shrew DDoS attacks detection” [37] Chen et al. propose the idea of abandoning the time-domain approach in favor of frequency domain analysis. It is a logical step because the main difficulty of detecting hit-and-run threats is the short length of the attacks, e.g., the detection window in the time-domain is short. Meanwhile, in the frequency domain, the energy of the attack is unmaskable. They use FPGA hardware to implement a DFT (Discrete Fourier Transformation) algorithm complemented by their auto-correlation algorithm. This approach proves to be significantly more efficient than the regular approach.

In ”Low-Rate DoS Attack Detection Using PSD Based Entropy and Machine Learning” [38], Zhang et al. propose a novel method using supervised learning on frequency domain data. This appears to be an efficient approach because the time-domain problem can be eliminated completely, and ML provides a robust framework to detect a wide variety of attacks.

The future of detecting hit-and-run attacks seems to be in the frequency domain. The need for ms range detection is eliminated by performing frequency domain analysis.

B. Distributed targets- carpet bombing attacks

There is a new trend of attacking distributed cloud services by not just attacking the public-facing IP but all the physical servers of the service. This makes attacks more challenging to mitigate since multiple attacks have to be handled in the same time. Apart from this difference, the mitigation of these attacks is identical to the mitigation of regular attacks. There is no research on this subject because the mentioned difference is not a scientific but an engineering challenge, and still only relatively few services are out there worth being attacked distributively.

C. QUIC-based DDoS

QUIC-based DDoS attacks represent a significant evolution in the landscape of distributed denial-of-service threats, leveraging the unique characteristics of the QUIC (Quick UDP Internet Connections) protocol. Developed as an alternative to the traditional TCP/IP model, QUIC offers faster and more secure data transmission over the Internet. In a QUIC-based DDoS attack, attackers exploit these properties to overwhelm target servers with a high volume of encrypted requests, making detection and mitigation challenging. The encryption masks the malicious traffic, blending it with legitimate requests. One can examine the currently publicly available QUIC-based attack tools at [39]. The effects and prevention of QUIC DDoS are not yet a very well-researched subject. There are only researches studying the difference between QUIC and TCP/TLS-based attacks [40], [41], [42].

D. Application

The detection (and mitigation) of application-based attacks mostly rely on the application developer instead of a universal security solution provider. The main reason for this is that application-based attacks do not follow any universal rules, which can be observed through a wide variety of attack types because application attacks exploit very specific application-related vulnerabilities. The detailed problems, challenges, and solutions of app DDoS are described in this survey [43]. There are proposed universal methods detecting these attacks [44], [45]. These methods mainly utilize machine learning or entropy-based methods. With the help of security professionals, these vulnerabilities can be eliminated or at least mitigated by the app developer. The mimicked user browsing attack is the newest ”widespread” (still very uncommon compared to universal volumetric attack types) application-based attack. For mimicked user browsing, a victim can take two routes: i) use universal anti-bot services like Google capcha or ii) use machine learning to profile their traffic and identify irregular attack traffic. Recently, a novel attack type called DNS Water Torture [46] appeared in the toolkit of adversaries. It is an application layer attack that overloads the targeted DNS servers with a high volume of fraudulent domain request messages. Often, DNS water torture attacks are combined with more common DDoS attacks. By overshadowing the application layer attack, mitigating with first-line security defense is more challenging.

E. Browser-based bot attacks

The dominant browser-related threat is a malware packed into a browser extension [47]. The main benefit of using the extension framework to execute malicious codes is twofold: i) one-time download, ii) JavaScript-based portable code. In contrast to malware downloaded via compromised websites, extension-based variants reload to the system memory each time the user starts the browser. These benefits make the browsers an appealing target for criminals. Often, while the malware function runs silently in the background, the extension also provides a valuable function to the users. The primary concern is that an extension may have a privilege to access and manipulate the DOM (Document Object Model) of a web page, user’s browsing history, bookmarks, or even files on the local storage system. Meanwhile, browser developers have a constant effort to make extension APIs stricter and more secure.

F. Multi-vector

A multi-vector attack combines multiple techniques shown in Fig. 4 to increase its success rate. Furthermore, the incorporating vectors may have unique timing properties to switch on and off or rise and fall the traffic volume. This feature enables to construct a wide variety of attack scenarios that are easy to re-organize by the attackers. The benefit of applying multiple vectors are two-fold [48]: i) the traffic volume of the individual vectors is additive, ii) the generated traffic pattern can reach higher complexity and, thus, is more effectively blended to the regular user traffic. The most popular vectors are volumetric type, i.e., DNS/NTP amplification, UDP flood, Chargen, and SSDP. Often, TCP Syn or application-specific vectors are also added to the vector mix, [49], [50], [51], [52]. Besides being automated, the most sophisticated attacks dynamically adjust the parameters of the individual vectors in response to the applied mitigation strategy. The intelligent control of the vectors allows attackers to tailor attacks to be shorter (typically in the 10-minute order) and yet more effective.

G. Lessons learned in DDoS detection

The emergence of new DDoS threats provides new challenges for both researchers and solution providers. The most concerning new trend is the emergence of encrypted attacks, including QUIC-based threats, which are very hard to detect. Application-based attacks became very sophisticated; the detection and mitigation of these attacks relied mostly on payload inspection, which becomes impossible with encryption. Likely, aggregated metadata inspection will become more prevalent in this field. Multi-vector and volatile attacks are not as novel as encrypted attacks. Still, their maturity and real-world share are very concerning.

For attacks that apply the hit-and-run method, detection algorithms should focus on short-time high-intensity bursts combined with an on-off traffic pattern. The novel time-domain behavior claims for algorithms with low false rate without human validation. The scope of potential botnet sources is

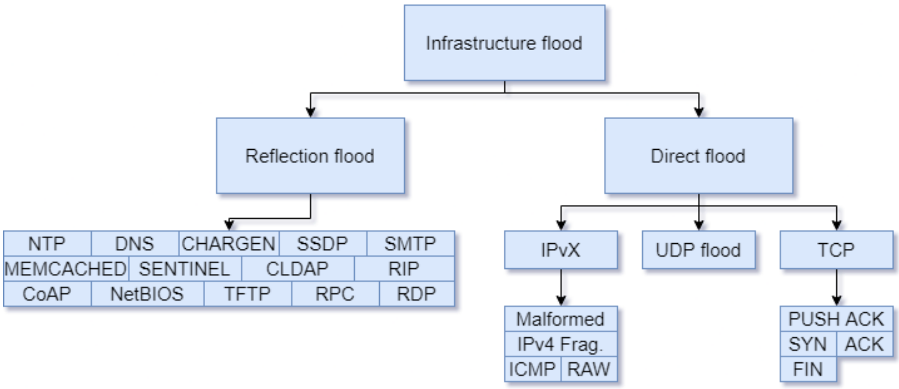


Fig. 4. The taxonomy of flood-based DDoS attacks

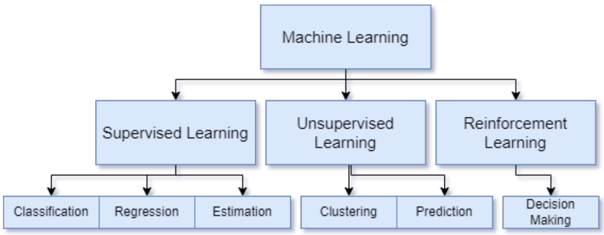


Fig. 5. The high level breakdown of machine learning methods

also significantly extended with a large number of IoT and mobile devices. These new types of botnets incorporate novel infection and attack strategies as well. The latest research works focus on the potential of deep learning to adapt to the new attack patterns (see Table II). Furthermore, in the last couple of years, we have seen a significant rise in the popularity of multi-vector attacks incorporating 10+ vectors. The primary protection challenge is that each incorporating vector should be individually detected and mitigated.

V. Supporting DDoS detection with ML

The detection of DDoS attacks is traditionally done by rule-based or heuristic software running on CPUs. Machine Learning (ML) is quite a broad subject; it is categorized into three main categories (see Fig. 5): supervised learning, where the machine is taught with inputs for which the correct output is known, unsupervised learning, where there is only input data, no information about the expected outcomes, reinforcement learning, where reward function is known. ML-supported DDoS detection became a viral subject for researchers in the past decade because ML has the potential to solve two major research-development gaps that are hard-to-impossible to solve using rule-based or heuristic detection methods: 1.) Detecting novel zero-day attacks automatically, 2.) Detect non-malicious anomalous network events (not-scope of this paper). While machine learning holds the promise to build a universal so-called ”Silver Bullet” system, there are significant challenges. The major drawback of machine learning is false positive detection. False positive detection is a serious issue because blocking the traffic of paying customers has more severe consequences than letting an attack pass through. For this reason, ML-based detection has not achieved major industrial success yet.

DDoS detection was most studied from the ML perspective in the past three years (see Table III). There is a plethora of research from this perspective. This section only draws a broad picture of how ML accelerates DDoS detection and mitigation while focusing on the two mentioned research gaps.

A. *Detecting novel attacks with ML*

Scaranti et al., in ”Artificial Immune Systems and Fuzzy Logic to Detect Flooding Attacks in Software-Defined Networks” [53], propose a novel AIS-based defense architecture for SDN systems. This system can detect and mitigate multiple types of DDoS attacks with minimal false detection (less than 1%). Scaranti et al. concept and results are imposing because they solved the issue of a high false detection rate while being able to detect previously unknown attacks, and they verified their system on publicly available datasets.

Poongodi et al., in ”DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET” [54], propose a novel method to segregate DDoS attackers. This method is based on trust and clustering. This method has two main benefits: 1.) It is resource efficient, 2.) It can be scaled very well. Their system is benchmarked against the AODV protocol and Firecol technique. The method developed by Poongodi et al. is significantly better in the achieved goodput, latency, and energy consumption than the other two state-of-the-art methods.

Nezhad et al. in ”A Novel DoS and DDoS Attacks Detection Algorithm Using ARIMA Time Series Model and Chaotic System in Computer Networks” [55] propose a novel method (TNA) to amend the main backdraw of ARIMA (auto-regression). They combine multiple previously known methods, including Box-Cox, Lyapunov, and chaotic error detection, to increase the detection rate. They successfully enhance the detection rate on large data sets to 99.5%, which is 1.1% higher than the previous best-known algorithm.

TABLE II
CURATED OVERVIEW OF ARTICLES ON THE TOPIC OF NEW GENERATION DDOS THREATS

Author(s)	Reference	Threat type	Novelty	Results
Ali et. al.	[10] in III-B1	IoT-based botnet attack	Systematic literature review	Focusing on research works of the recent years
N. Koroniotis et. al.	[11] in III-B1	IoT-based botnets	A survey of forensics and deep learning mechanisms	Overviews deep learning-based network forensic methods
M. Eslahi et. al.	[20] in III-B2	Mobile botnet	Overview of the novel command and control mechanisms and their malicious activities	Reviews the limitations of botnet detection in mobile environment
N. Hoque et. al.	[21] in III-B2	Mobile botnet	A survey of various botnet architectures and tools	Pros and cons analysis
Z. Lu et. al.	[22] in III-B2	Mobile botnet	Impact of mobile botnets on wireless networks	Node mobility can trigger a botnet propagation storm. Mobility range over a threshold enables the botnet to growth quadratically (theoretical maximum). Comparing to the exponentially expanding Internet botnets, it is significantly slower mechanism.
Kuzmanovic et. al.	[28] in IV-A	Hit&Run	Analysis of Hit&Run	Demonstration of distruptiveness of hit&run attacks
Kieu et. al.	[32] in IV-A	Hit&Run	Analysis and simulation of Hit&Run	Demonstration of distruptiveness of hit&run attacks
Balarezo et. al.	[33] in IV-A	Hit&Run	Congestion analysis	Demonstration of distruptiveness of hit&run attacks
Luo et. al.	[34] in IV-A	Hit&Run	Mathematical model of Hit&Run attacks	Very high precision model for wide variety of attacks
Tan et. al.	[35] in IV-A	Hit&Run	TCP congestion control algorithm	Resilient congestion control algorithm
Teyssier et. al.	[40] in IV-C	QUIC	Attack evaluation	Attack effectiveness against QUIC evaluation method
Balaji et. al.	[41] in IV-C	QUIC	Attack method	Showcase of novel QUIC-based attack
Wang et. al.	[44] in IV-D	Application	Detection method	Novel universal entropy-based L7 detection method
Yadev et. al.	[45] in IV-D	Application	Detection method	Novel universal ML-based L7 detection method
Perotta et. al.	[47] in IV-E	Browser based	Case study	Study of the detection challenges of attacks originating from browsers
Dimolianis et. al.	[48] in IV-F	Multi-vector	Mitigation method	Novel method to mitigate and detect multi-vector attacks

Simpson et al., in ”Per-Host DDoS Mitigation by Direct-Control Reinforcement Learning” [56], propose a new mitigation method based on reinforced machine learning (RL). Regular machine learning has a hard time keeping up with the constantly changing patterns of DDoS attacks. By monitoring the result of the mitigation and using it to reinforce the per-flow decision-making, they achieve increased goodput compared to the state-of-the-art.

These four papers illustrate well how ML can be used to detect previously unknown attacks. This is the single most significant achievement of ML in this field from the industrial point of view.

B. ML detection on a small footprint

The scope of this paper is to discuss the DDoS attacks threatening DCN and ISP networks. Still, there is relevant research outside the DCN scope that can and should be applied to this subject as well. One of the main problems of ML-based DDoS detection is its relatively high resource utilization. This problem becomes a vital issue, even in DCNs, when detection is extended to east-west routes. In this subsection, we will showcase ML methods from resource-sensitive fields (IoT, VANET) where these methods have been implemented with a minimal footprint.

Kim et al. in ”Intelligent Application Protection Mechanism for Transportation in V2C Environment” [57] proposes a novel image-based system resource monitoring AI for DDoS detection in Vechile-to-cloud (V2C) systems. V2C systems are not safety-critical, but there has been no previous research on the safety of these systems. This kind of AI can be a great fit for IoT or distributed systems because this AI does not sample the traffic but the system’s resource utilization. This approach is extremely resource-efficient, but a significant detection lag exists. By combining the memory, CPU, and network utilization, they managed to achieve a 7.36% false detection rate.

Gao et al. in ”A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network” [59] propose a novel massively-scalable DDoS detection system for vehicular ad-hoc networks (VANET). The system proposed by Gao is partitioned into subsystems: 1.) Real-time traffic collection subsystem, 2.) Spark-based attack detection subsystem. The detection system was moved into the cloud to access computing resources and aggregate the traffic of detected attacks. This approach solves the cost-sensitive nature of VANET nodes (Vehicles), and by using Big-data resources, it can approach very low (0.05%-1%) false detection ratios.

Yang et al. in ”Adaptive Measurements Using One Elastic Sketch” [58] propose a novel method, called Elastic Sketch, to measure the network during attacks. The main advantage of using Elastic Sketch is that it can adapt very well to rapidly changing network conditions. Elastic sketch has a 50 times shorter measuring speed than the current state-of-the-art sketch and a much lower error rate.

Xiao et al. in ”IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?” [60] identify IoT attack models and propose defense methods

TABLE III
OVERVIEW OF ARTICLES ON THE TOPIC OF ML ACCELERATION

Author(s)	Reference	Accelerator	Novelty	Results
Scaranti et. al.	[53]	ML	AIS-based method	Less-than 1% false detection, ability to detect zero-day attacks
Kim et. al.	[57]	ML	Image-based method	Extremly low resource usage, on a large data-set
Nezhad et. al.	[55]	ML	Auto-regression-based method	Very-low false detection
Yang et. al.	[58]	ML	New algorithm	50 times shorter detection time, than SOTA sketch

against them. They showcase how ML must meet unique challenges if applied in the IoT security scene.

C. Lessons learned

There is a growing demand from users to integrate ML into DDoS protection systems, which has not been done so far by most industrial solution providers. The reason for this is threefold i.) validating security systems is a very resource-intensive task (why should a provider spend immense resources on a method that is not proven to be effective on an industrial scale), ii.) establishing causality links between decisions and data is crucial for any security system not solved on the research level (eXplainable AI, root cause analysis, etc.), iii.) patching false detections is not an easy task in an ML pipeline.

The authors of this paper believe that the integration of ML into industrial DDoS detection will not be quick but inevitable. We predict that the first ML-based DDoS detection will be utilized to detect zero-day attacks, and eventually, more and more traditional algorithms will be superseded by ML-based methods.

VI. THE FUTURE OF DDOS

This section summarizes what we, as researchers and industrial solution providers, experience about the latest DDoS trends and the solutions to these new challenges, and we try to predict the future direction of this topic. We also looked into what global security solution providers see and forecast for the future [61] [62]. We found that our observations and predictions match their reported trends. In previous sections, we demonstrated that DDoS attacks are evolving at an unprecedented speed, with the following main characteristics:

TABLE IV
THE MOST PREVALENT CURRENT DDOS TRENDS AND THEIR EXPECTED FUTURE RELEVANCE. THE CURRENT RELEVANCE WAS MEASURED BY THE AUTHORS IN PROTECTED DCNS. A TWO-YEAR LONG CONTINUOUS MEASUREMENT PERIOD IS THE BASIS OF OUR ESTIMATION FOR THE FUTURE.

Trend nr.	Share 2022	Expected Share 2024	Challenge
I.	60%	90%	Engineering
II.	75%	85%	Engineering
III.	3%	20%	Engineering
IV.	3%	15%	Research
V.	1%	10%	Research

I.) The attacks' duration and ramp-up period become shorter and shorter while the peak throughput of the same attacks increases. **Solution:** The mitigation process has to be fully automated. Per-packet analysis has to be used for detection. The human reaction time is not fast enough to mitigate DDoS attacks reliably in under two minutes. Solution providers must provide highly reliable solutions that can be trusted as active devices. NetFlow and other flow aggregation-based DDoS detection methods have an aggregation period of a few minutes, which induces an intolerable mitigation lag. In contrast, per-packet traffic analysis can provide highly detailed attack insight in ms-s.

II.) Multi-vector attacks became the new norm. **Solution:** Multi-vector attacks can be mitigated with black-hole routing. Suppose we want a little bit more sophisticated mitigation, which can protect the user as well as the network. In that case, every attack vector must be analyzed and mitigated separately. So we need algorithms that not only detect attacks, but classify them on a vector-level resolution.

III.) One of the scientifically most exciting frontiers of DDoS research is the protection of IoT networks. The adoption of 5G networks boosts the number and significance of IoT devices; critical infrastructures adopt the IoT approach, like vehicular networks, thus making the protection of IoT more critical than ever. Meanwhile, IoT devices still do not have the resources necessary for straightforward DDoS protection. Currently, researchers are working on two tracks, developing alternative methods like [63], [64], [65], or extending protection at the 5G packet gateway, like [66], [67].

IV.) User/application mimicking DDoS attacks became a measurable (1-5%) share of all attacks. **Solution:** New methods of attack detection have to be developed by researchers, which can detect attacks and use the historical context of the end-points' regular traffic to detect these new smart attacks. In this field, per-endpoint-based unsupervised learning shows the greatest promise, but no industrial-grade solutions have been provided.

V.) The East-West attacks became a measurable (0.5-1%) share of all attacks. Most DDoS detection solutions monitor only the north-south links of the DCN. The current most common application architectures can not be scaled to cover every possible route between tenants. A very conservative estimate for the protecting cost of a 1000MW DCN on every east-west route with an industry-standard active inline DDoS mitigation device would be 1-2 billion USD annually. **Solution:** New data-collection schemes have to be devised by researchers to collect data, which could be used to feed the next generation of DDoS detection systems.

After reading this, one could ask themselves: What does the future hold in the next few years? Our guess is, according to Table IV, that Trend III and Trend IV will become much more prevalent (5-15%), making these challenges unavoidable by the SotA providers. Trend I and Trend II became the normal method of DDoS attacks making up 80+% of all attacks.

VII. CONCLUSIONS

In this survey, we discussed how DDoS attacks prove to be continuously evolving prevalent threats. First, we defined the basic terminology to navigate the landscape of post-pandemic DDoS. We presented how little the DDoS attack scene of the post-Covid world resembles the attacks of 5 years ago, providing examples of novel attacks, methods, and tools. We provided a survey of attack profiles prevalent in the network of Hungarian ISPs. After this, we discussed state-of-the-art research considering the detection of DDoS attacks. As part of this, we summarized the research considering acceleration schemes and discussed the rich literature on machine learning-based methods, their benefits, and their challenges.

The key lesson to be learned through this paper is that DDoS attacks might be considered old brute-force methods, but plenty of new threats are worthy of research. With the increasingly widespread QoS-sensitive applications, the multivector *ephemeral* – short and high volume – attacks became the new norm, making human-in-the-loop systems nearly obsolete.

The research has been partially funded by the Hungarian government's National Security Cooperative PhD program.

REFERENCES

[1] Cisco White Paper, "Cisco annual internet report (2018–2023) white paper," https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html, 2020, accessed: 10-01-2023.

[2] Akamai, "2021: Volumetric ddos attacks rising fast," https://www.akamai.com/blog/security/2021-volumetric-ddos-attacks-rising-fast, 2021, accessed: 10-01-2023.

[3] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the dos and ddos problems," vol. 39, no. 1, 2007. [Online]. Available: DOI: 10.1145/1216370.1216373

[4] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks," *IEEE Communications Surveys Tutorials*, vol. 15, No. 4, pp. 2046–2069, 2013. [Online]. Available: DOI: 10.1109/surv.2013.031413.00127

[5] M. Masdari and M. Jalali, "A survey and taxonomy of dos attacks in cloud computing," *Security and Communication Networks*, vol. 9, no. 16, pp. 3724–3751, 2016. [Online]. Available: DOI: 10.1002/sec.1539

[6] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (sdn) and distributed denial of service (ddos) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 602–622, 2016. [Online]. Available: DOI: 10.1109/comst.2015.2487361

[7] K. Kalkan, L. Altay, G. Gür, and F. Alagöz, "Jess: Joint entropy-based ddos defense scheme in sdn," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 10, pp. 2358–2372, 2018. [Online]. Available: DOI: 10.1109/JSAC.2018.2869997

[8] S. Dong, K. Abbas, and R. Jain, "A survey on distributed denial of service (ddos) attacks in sdn and cloud computing environments," *IEEE Access*, vol. 7, pp. 80 813–80 828, 2019. [Online]. Available: DOI: 10.1109/ACCESS.2019.2922196

[9] J. Zheng, Q. Li, G. Gu, J. Cao, D. K. Y. Yau, and J. Wu, "Realtime ddos defense using cots sdn switches via adaptive correlation analysis," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1838–1853, 2018. [Online]. Available: DOI: 10.1109/TIFS.2018.2805600

[10] I. Ali, A. I. A. Ahmed, A. Almogren, M. A. Raza, S. A. Shah, A. Khan, and A. Gani, "Systematic literature review on iot-based botnet attack," *IEEE Access*, vol. 8, pp. 212 220–212 232, 2020. [Online]. Available: DOI: 10.1109/ACCESS.2020.3039985

[11] N. Koroniotis, N. Moustafa, and E. Sitnikova, "Forensics and deep learning mechanisms for botnets in internet of things: A survey of challenges and solutions," *IEEE Access*, vol. 7, pp. 61 764–61 785, 2019. [Online]. Available: DOI: 10.1109/ACCESS.2019.2916717

[12] L. Shi, J. Li, M. Zhang, and P. Reiher, "On capturing ddos traffic footprints on the internet," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 4, pp. 2755–2770, 2022. [Online]. Available: DOI: 10.1109/TDSC.2021.3074086

[13] D. Ding, M. Savi, and D. Siracusa, "Tracking normalized network traffic entropy to detect ddos attacks in p4," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 6, pp. 4019–4031, 2022. [Online]. Available: DOI: 10.1109/TDSC.2021.3116345

[14] T. S. Gopal, M. Meerolla, G. Jyostna, P. Reddy Lakshmi Eswari, and E. Magesh, "Mitigating mirai malware spreading in iot environment," in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2018, pp. 2226–2230. [Online]. Available: DOI: 10.1109/ICACCI.2018.8554643

[15] H.-V. Le and Q.-D. Ngo, "V-sandbox for dynamic analysis iot botnet," *IEEE Access*, vol. 8, pp. 145 768–145 786, 2020. [Online]. Available: DOI: 10.1109/ACCESS.2020.3014891

[16] W. Li, J. Jin, and J.-H. Lee, "Analysis of botnet domain names for iot cybersecurity," *IEEE Access*, vol. 7, pp. 94 658–94 665, 2019. [Online]. Available: DOI: 10.1109/ACCESS.2019.2927355

[17] R. Vinayakumar, M. Alazab, S. Srinivasan, Q.-V. Pham, S. K. Padannayil, and K. Simran, "A visualized botnet detection system based deep learning for the internet of things networks of smart cities," *IEEE Transactions on Industry Applications*, vol. 56, no. 4, pp. 4436–4456, 2020. [Online]. Available: DOI: 10.1109/TIA.2020.2971952

[18] Y. Jia, F. Zhong, A. Alrawais, B. Gong, and X. Cheng, "Flowguard: An intelligent edge defense mechanism against iot ddos attacks," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9552–9562, 2020. [Online]. Available: DOI: 10.1109/JIOT.2020.2993782

[19] N. Ravi and S. M. Shalinie, "Learning-driven detection and mitigation of ddos attack in iot via sdn-cloud architecture," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3559–3570, 2020. [Online]. Available: DOI: 10.1109/JIOT.2020.2973176

[20] M. Eslahi, R. Salleh, and N. B. Anuar, "Mobots: A new generation of botnets on mobile devices and networks," in *2012 International Symposium on Computer Applications and Industrial Electronics (ISCAIE)*, 2012, pp. 262–266. [Online]. Available: DOI: 10.1109/ISCAIE.2012.6482109

[21] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "Botnet in ddos attacks: Trends and challenges," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2242–2270, 2015. [Online]. Available: DOI: 10.1109/COMST.2015.2457491

[22] Z. Lu, W. Wang, and C. Wang, "On the evolution and impact of mobile botnets in wireless networks," *IEEE Transactions on Mobile Computing*, vol. 15, no. 9, pp. 2304–2316, 2016. [Online]. Available: DOI: 10.1109/TMC.2015.2492545

[23] A. A. Santos, M. Nogueira, and J. M. F. Moura, "A stochastic adaptive model to explore mobile botnet dynamics," *IEEE Communications Letters*, vol. 21, no. 4, pp. 753–756, 2017. [Online]. Available: DOI: 10.1109/LCOMM.2016.2637367

[24] E. Johnson and I. Traore, "Sms botnet detection for android devices through intent capture and modeling," in *2015 IEEE 34th Symposium on Reliable Distributed Systems Workshop (SRDSW)*, 2015, pp. 36–41. [Online]. Available: DOI: 10.1109/SRDSW.2015.21

[25] NETSCOUT, "Netscout threat intelligence report," vol. 5, 2020. [Online]. Available: https://www.netscout.com/

[26] B. Nagy, "Chargen udpfrag tcp syn multivector ddos attack," Oct 2021. https://zenodo.org/record/5578700.

[27] ——, "Encrypted traffic with esp and tls," Oct 2021. https://zenodo.org/record/5578676.

[28] A. Kuzmanovic and E. W. Knightly, “Low-rate tcp-targeted denial of service attacks: The shrew vs. the mice and elephants,” in *Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, ser. SIGCOMM ’03. New York, NY, USA: Association for Computing Machinery, 2003, pp. 75–86. [Online]. Available: **doi**: 10.1145/863955.863966

[29] K. Hong, Y. Kim, H. Choi, and J. Park, “Sdn-assisted slow http ddos attack defense method,” *IEEE Communications Letters*, vol. 22, no. 4, pp. 688–691, 2018. [Online]. Available: **doi**: 10.1109/LCOMM.2017.2766636

[30] J. A. Pérez-Díaz, I. A. Valdovinos, K.-K. R. Choo, and D. Zhu, “A flexible sdn-based architecture for identifying and mitigating low-rate ddos attacks using machine learning,” *IEEE Access*, vol. 8, pp. 155 859–155 872, 2020. [Online]. Available: **doi**: 10.1109/ACCESS.2020.3019330

[31] A. Praseed and P. S. Thilagam, “Multiplexed asymmetric attacks: Next- generation ddos on http/2 servers,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1790–1800, 2020. [Online]. Available: **doi**: 10.1109/TIFS.2019.2950121

[32] M. V. Kieu, D. T. Nguyen, and T. T. Nguyen, “A way to estimate tcp throughput under low-rate ddos attacks: One tcp flow,” in *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)*, 2020, pp. 1–8. [Online]. Available: **doi**: 10.1109/RIVF48685.2020.9140777

[33] J. F. Balarezo, S. Wang, K. G. Chavez, A. Al-Hourani, J. Fu, and K. Sithamparanathan, “Low-rate tcp ddos attack model in the southbound channel of software defined networks,” in *2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS)*, 2020, pp. 1–10. [Online]. Available: **doi**: 10.1109/ICSPCS50536.2020.9310040

[34] J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, “On a mathematical model for low-rate shrew ddos,” *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1069–1083, 2014. [Online]. Available: **doi**: 10.1109/TIFS.2014.2321034

[35] L. Tan, K. Huang, G. Peng, and G. Chen, “Stability of tcp/aqm networks under ddos attacks with design,” *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 3042–3056, 2020. [Online]. Available: **doi**: 10.1109/TNSE.2020.3012002

[36] Z. Liu, X. Yin, and H. J. Lee, “A new network flow grouping method for preventing periodic shrew ddos attacks in cloud computing,” in *2016 18th International Conference on Advanced Communication Technology (ICACT)*, 2016, pp. 66–69. [Online]. Available: **doi**: 10.1109/ICACT.2016.7423276

[37] H. Chen, Y. Chen, D. H. Summerville, and Z. Su, “An optimized design of reconfigurable psd accelerator for online shrew ddos attacks detection,” in *2013 Proceedings IEEE INFOCOM*, 2013, pp. 1780–1787. [Online]. Available: **doi**: 10.1109/INFCOM.2013.6566976

[38] N. Zhang, F. Jaafar, and Y. Malik, “Low-rate dos attack detection using psd based entropy and machine learning,” in *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 2019, pp. 59–62. [Online]. Available: **doi**: 10.1109/CSCloud/EdgeCom.2019.00020

[39] @efchatz, “Quic-attacks,” https://github.com/efchatz/QUIC-attacks, 2023.

[40] B. Teyssier, Y. A. Joarder, and C. Fung, “An empirical approach to evaluate the resilience of quic protocol against handshake flood attacks,” in *2023 19th International Conference on Network and Service Management (CNSM)*, 2023, pp. 1–9. [Online]. Available: **doi**: 10.23919/CNSM59352.2023.10327907

[41] A. S. Balaji, V. Anil Kumar, P. P. Amritha, and M. Sethumadhavan, “Quicloris: A slow denial-of-service attack on the quic protocol,” in *Advanced IoT Sensors, Networks and Systems*, A. K. Dubey, V. Sugumaran, and P. H. J. Chong, Eds. Singapore: Springer Nature Singapore, 2023, pp. 85–94. [Online]. Available: **doi**: 10.1007/978-981-99-1312-1_7

[42] V. V. Tong, S. Souihi, H.-A. Tran, and A. Mellouk, State of the Art on Network Troubleshooting, 2023, pp. 1–23. [Online]. Available: **doi**: 10.1002/9781394236664.ch1

[43] A. Praseed and P. S. Thilagam, “Ddos attacks at the application layer: Challenges and research perspectives for safeguarding web applications,” *IEEE Communications Surveys Tutorials*, vol. 21, no. 1, pp. 661–685, 2019. [Online]. Available: **doi**: 10.1109/COMST.2018.2870658

[44] J. Wang, X. Yang, and K. Long, “A new relative entropy based app-ddos detection method,” in *The IEEE symposium on Computers and Communications*, 2010, pp. 966–968. [Online]. Available: **doi**: 10.1109/ISCC.2010.5546587

[45] S. Yadav and S. Subramanian, “Detection of application layer ddos attack by feature learning using stacked autoencoder,” in *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, 2016, pp. 361–366. [Online]. Available: **doi**: 10.1109/ICCTICT.2016.7514608

[46] K. Hasegawa, D. Kondo, and H. Tode, “Fqdn-based whitelist filter on a dns cache server against the dns water torture attack,” in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2021, pp. 628–632. [Online]. Available: **doi**: 10.1109/tnsm.2023.3277880

[47] R. Perrotta and F. Hao, “Botnet in the browser: Understanding threats caused by malicious browser extensions,” *IEEE Security Privacy*, vol. 16, no. 4, pp. 66–81, 2018. [Online]. Available: **doi**: 10.1109/MSP.2018.3111249

[48] M. Dimolianis, A. Pavlidis, D. Kalogeras, and V. Maglaris, “Mitigation of multi-vector network attacks via orchestration of distributed rule placement,” in *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 2019, pp. 162–170.

[49] B. Nagy, “Cldap dns multivector ddos attack,” Oct 2021. https://zenodo.org/record/5572097.

[50] ——, “Udp flood attack sample with short payload,” Oct 2021. https://zenodo.org/record/5578727.

[51] ——, “Udp flood attack sample,” Oct 2021. https://zenodo.org/record/5578712.

[52] ——, “Icmp, udp, tcp syn multivector ddos attack,” Oct 2021. https://zenodo.org/record/5578703.

[53] G. F. Scaranti, L. F. Carvalho, S. Barbon, and M. L. Proença, “Artificial immune systems and fuzzy logic to detect flooding attacks in software-defined networks,” *IEEE Access*, vol. 8, no. 10.1109/access.2020.2997939, pp. 100 172–100 184, 2020. [Online]. Available: **doi**: 10.1109/access.2020.2991273

[54] M. Poongodi, M. Hamdi, A. Sharma, M. Ma, and P. K. Singh, “Ddos detection mechanism using trust-based evaluation system in vanet,” IEEE Access, vol. 7, pp. 183 532–183 544, 2019. [Online]. Available: **doi**: 10.1109/access.2019.2960367

[55] S. M. Tabatabaie Nezhad, M. Nazari, and E. A. Gharavol, “A novel dos and ddos attacks detection algorithm using arima time series model and chaotic system in computer networks,” *IEEE Communications Letters*, vol. 20, no. 4, pp. 700–703, 2016. [Online]. Available: **doi**: 10.1109/lcomm.2016.2517622

[56] K. A. Simpson, S. Rogers, and D. P. Pezaros, “Per-host ddos mitigation by direct-control reinforcement learning,” *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 103–117, 2020. [Online]. Available: **doi**: 10.1109/TNSM.2019.2960202

[57] H. Kim, S. Hong, J. Kim, and J. Ryou, “Intelligent application protection mechanism for transportation in v2c environment,” *IEEE Access*, vol. 8, pp. 86 777–86 787, 2020. [Online]. Available: **doi**: 10.1109/access.2020.2991273

[58] T. Yang, J. Jiang, P. Liu, Q. Huang, J. Gong, Y. Zhou, R. Miao, X. Li, and S. Uhlig, “Adaptive measurements using one elastic sketch,” *IEEE/ACM Transactions on Networking*, vol. 27, no. 6, pp. 2236–2251, 2019. [Online]. Available: **doi**: 10.1109/tnet.2019.2943939

[59] Y. Gao, H. Wu, B. Song, Y. Jin, X. Luo, and X. Zeng, “A distributed network intrusion detection system for distributed denial of service attacks in vehicular ad hoc network,” *IEEE Access*, vol. 7, pp. 154 560–154 571, 2019. [Online]. Available: **doi**: 10.1109/access.2019.2948382

[60] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, “Iot security techniques based on machine learning: How do iot devices use ai to enhance security?” *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41–49, 2018. [Online]. Available: **doi**: 10.1109/msp.2018.2825478

[61] Corero, "Corero ddos threat intelligence report 2021," https://go.corero.com/ddos-threat-intelligence-report-2021-ty, 2021, accessed: 10-01-2023.

[62] Netscout, "Netscout threat intelligence report 2021 q2," https://www.netscout.com/sites/default/files/2022-03/ThreatReport_2H2021_WEB.pdf, 2021, accessed: 10-01-2023.

[63] T.-C. Huang, C.-Y. Huang, and Y.-C. Chen, "Real-time ddos detection and alleviation in software-defined in-vehicle networks," *IEEE Sensors Letters*, vol. 6, no. 9, pp. 1–4, 2022. [Online]. Available: DOI: 10.1109/LSENS.2022.3202301

[64] Z. Li, Y. Kong, C. Wang, and C. Jiang, "Ddos mitigation based on space-time flow regularities in iov: A feature adaption reinforcement learning approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 3, pp. 2262–2278, 2022. [Online]. Available: DOI: 10.1109/TITS.2021.3066404

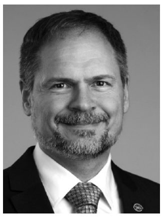
[65] X. Chen, L. Xiao, W. Feng, N. Ge, and X. Wang, "Ddos defense for iot: A stackelberg game model-enabled collaborative framework," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9659–9674, 2022. [Online]. Available: DOI: 10.1109/JIOT.2021.3138094

[66] X. Chen, Y. Chen, W. Feng, L. Xiao, X. Li, J. Zhang, and N. Ge, "Real-time ddos defense in 5g-enabled iot: A multidomain collaboration perspective," *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 4490–4505, 2023. [Online]. Available: DOI: 10.1109/JIOT.2022.3218728

[67] Y. Liu, K.-F. Tsang, C. K. Wu, Y. Wei, H. Wang, and H. Zhu, "Ieee p2668-compliant multi-layer iot-ddos defense system using deep reinforcement learning," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 1, pp. 49–64, 2023. [Online]. Available: DOI: 10.1109/TCE.2022.3213872

Péter Orosz is an associate professor and the head of Smart Communications Laboratory at the Department of Telecommunications and Media Informatics, BME Hungary. He received his Computer Science master's degree in software engineering (2003) and Ph.D. in infocommunication systems (2010) at the University of Debrecen, Hungary. His research interests cover communication networks, network and service management, QoS-QoE managed networks, online QoE prediction for media services, and acceleration of network functions.

Balázs Nagy is a PhD student at the Smart Communications Laboratory (Department of Telecommunications and Media Informatics), BME Hungary. He received his electrical engineering master's degree in embedded systems (2019). Currently, he is working as a project manager at AITIA International. His research interests cover communication networks, network security, service management, and acceleration of network functions.



Pál Varga is the Head of Department of Telecommunications and Media Informatics at the Budapest University of Technology and Economics. His main research interests include communication systems, Cyber-Physical Systems and Industrial Internet of Things, network traffic analysis, end-to-end QoS and SLA issues – for which he is keen to apply hard-ware acceleration and artificial intelligence, machine learning techniques as well. Besides being a member of HTE, he is a senior member of IEEE, where he is active both in the IEEE ComSoc (Communication Society) and IEEE IES (Industrial Electronics Society) communities. He is Editorial Board member in many journals, Associate Editor in IEEE Transactions on Network and Service Management, and the Editor-in-Chief of the Infocommunications Journal.