The Cooperative DDoS Signaling based on a Blockchain-based System

Bruno Rodrigues, Burkhard Stiller
Communication Systems Group CSG, Department of Informatics IfI, University of Zürich UZH
Binzmühlestrasse 14, CH—8050 Zürich, Switzerland
E-mail: [rodrigues|stiller]@ifi.uzh.ch

***Abstract*—Driven by challenges imposed by a cooperative network defense, the Blockchain Signaling System (BloSS) is presented as an effective and alternative solution for security management, especially cooperative defenses, by exploiting Blockchains (BC) and Software-Defined Networks (SDN) for sharing attack information, an exchange of incentives, and tracking of reputation in a fully distributed and automated fashion. BloSS was prototyped and evaluated through local and global experiments, without the burden to maintain, design, and develop special registries and gossip protocols.**

Those evaluation results based on the local and global prototyping of BloSS highlight its effectiveness in signaling information of large-scale DDoS attacks. The world-wide scale evaluation experimenting with the interaction between Autonomous Systems' (AS) victims of a DDoS attack and ASes acting as mitigators, presented an average of 97 seconds to complete all eleven possible outcomes of the BloSS protocol, fully determining the spectrum of possible options. The reputation assessment showed that BloSS is capable of punishing malicious providers and benefiting providers by acting honestly.

I. Introduction

As the number of connected devices (portable and stationary) increases, the complexity of systems providing content for these devices and the communication infrastructure increased in a similar proportion to support the growing volume of traffic [1]. As a consequence, these complex distributed systems are subject to several types of failures and threats that can compromise, for example, entire societies whose Critical Infrastructures (CI) are connected to the Internet [5]. Among the various threats to the Internet and its underlying systems, Distributed Denial-of-Service (DDoS) attacks are one of the biggest threats to the availability of services on the Internet.

Behind these various reasons that motivate a DDoS attack is the increasing number of, often insecure, devices connected to the Internet. As observed in Figure 1, the number of IoT devices is surpassing the number of non-IoT devices (*e.g.*, mobile phones, laptops, computers, and others), wherein such devices range from small sensors to baby cameras and home gateways, and are the main target of software that systematically exploits vulnerabilities to infect thousands of such devices.

Different detection and mitigation methods are available to prevent or reduce DDoS attack damage. A typical implementation is called on-premises defense, which is implemented by the target system based on dedicated ASIC-based

978-3-903176-32-4 © 2021 IFIP

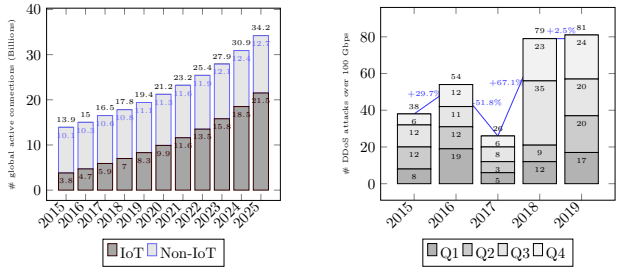

Fig. 1: Number of IoT-connected Devices [per Year] (left), Registered Large-scale DDoS Attacks [Accumulated Quarters/Year] (right) [9], [1]

(Application-specific Integrated Circuit) appliances to analyze flow records exported from edge routers and to filter malicious traffic or perform load balancing. Alternatively, *off-premises* protection services that can be distributed (mostly cloud-based) or decentralized (cooperative). While the former serves as a proxy receiving, analyzing, and redirecting traffic to the target, which delegates detection and mitigation tasks to the protection provider (*e.g.*, Akamai [1] or CloudFlare [3]), the latter is a decentralized approach, typically implemented as a cooperative overlay network.

As DDoS attacks are rapidly evolving in terms of traffic volume and sophistication, cooperation becomes a logical way to counter distributed and coordinated attacks. It allows to combine detection and mitigation capabilities of different domains, reducing the overhead at a single point, and to block malicious traffic near its source. However, there is still no widespread deployment of such cooperative defense systems. As identified by [27], [17], the main challenges of existing approaches include: (1) high complexity of operation and coordination; (2) need for trusted and secure communication; (3) lack of incentives for the service providers to cooperate; and (4) understand how operations of these systems are affected by different legislation, regions, and countries.

This paper is structured as follows. Section II presents key research questions of BloSS. Section III analyzes existing cooperative defenses concerning the aforementioned challenges. While Section IV offers design details, Section V discusses evaluations. Lastly, conclusions are drawn in Section VI.

II. Research Questions

Based on the challenges mentioned at Section 1, the following Research Questions (RQ) drive BloSS's design. This reinforces the opportunity for the proposal of coping solutions with the challenges of collaborative defenses. Henceforth, the main goal of BloSS is to provide a cooperative defense approach providing a technical answer for each of these categories combined into a single system (*cf.* Figure 2).

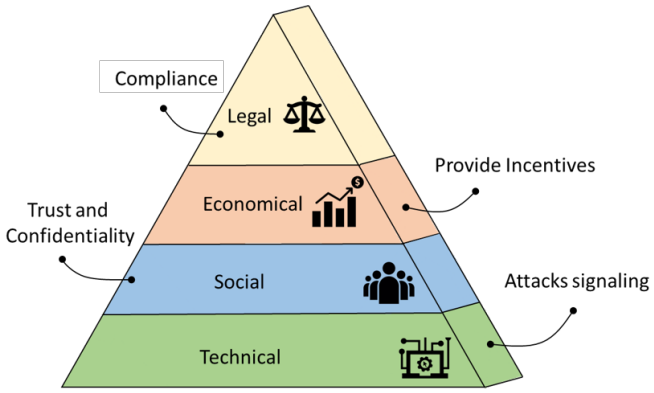

Fig. 2: BloSS Challenges

RQ1: Can a BC-based cooperative system reduce operation and deployment complexities? The proposed approach shall be simple to deploy and operate, aiming to avoid extra hardware or software requirements on the underlying network infrastructure.

RQ2: How to balance transparency and privacy in a cooperative system, increasing trust among cooperative members? In RQ2, the proposed solution shall punish malicious behavior of its members, preventing false-reporting and free-riding (*i.e.*, service providers that only request defense without contributing).

RQ3: How to provide financial incentives to foster cooperative behavior among its members? RQ3 concerns the economic impact and how to provide the necessary incentives to cover capital and operational expenses. Thus, the proposed method should provide a platform based on BC, enabling the exchange of incentives to boost cooperative behavior.

RQ4: How to ensure compliance across different jurisdictions? RQ4 refers to enabling or disabling its operation in certain regions or the interaction with selected participants to comply with organizational/legal obligations.

To answer the posed questions, a referenced research method is used to: (a) overview the core concepts on which this thesis is based, (b) analyze the state-of-the-art concerning cooperative defenses, listing their characteristics and proposals, as well as differentiating them from what is proposed in this thesis. Then, the applied research consists of the design, prototyping, and validation of BloSS in order to verify whether the proposed system satisfied the research questions.

III. Analysis of Cooperative Defenses

As a response to the increasing number of DDoS attacks, many proposals counter DDoS attacks based on centralized and distributed (cooperative) perspectives [19]. As presented above, different ways to classify DDoS defenses exist, whereas the most popular is according to the point in the network where mitigation occurs [13]. Table I[1] presents a comparison of how characteristics perform according to challenges.

TABLE I: Overview of Cooperative DDoS Defense Work

Related Work	Cooperative Defense Challenges				Capabilities
	Technical	Social	Economical	Legal	
DefCOM [15]	◐	✗	✗	◐	Signaling
SOS [10]	◐	✗	✗	◐	Signaling
COSSACK [16]	◐	✗	✗	◐	Signaling Mitigation
Zhang *et al.* [28]	◐	✗	✗	✗	Signaling
Pushback [8]	◐	✗	✗	◐	Signaling Mitigation
Steinberger *et al.* [25]	◐	✗	✗	◐	Signaling Mitigation
Sahay *et al.* [21]	●	✗	✗	◐	Signaling Mitigation
Velauthapillai *et al.* [26]	◐	✗	✗	◐	Signaling Mitigation
Bohatei [4]	●	✗	✗	◐	Signaling Mitigation
CoFence [18]	●	✗	✗	◐	Signaling Mitigation
IETF-DOTS [14]	◐	◐	✗	◐	Signaling
BloSS	●	●	●	●	Signaling

● = provides property; ◐ = partially provides property;
✗ = does not provide property

Secure Overlay Services (SOS) [10], Pushback [8] COSSACK [16], and DefCOM [15] paved the way for cooperative defenses in the early 2000s. While SOS focused on identifying legitimate sources for time-sensitive networks (*i.e.*, requiring peers to authenticate to the overlay network), Pushback, COSSACK, and DefCOM based their approach on detection and enforcement points in access networks. However, these approaches required changes in routers or require sources to be registered, thus, presenting a high complexity of operation.

SDN-based solutions allow greater agility to enforce decisions that require a global network view. Bohatei [4] demonstrates the scalability and performance advantages of using SDN in conjunction with VNF to build a DDoS defense system on top of proven, existing mitigation components. However, although the combination of SDN and NFV simplifies the technological aspect, the solution does not include cooperative other aspects of the mitigation, such as how cooperative mitigation requests can impact operational expenses (economic) or the potential damages to the public image of a domain in cases of information leaks (social).

Figure 3 extends Table I presenting details on the percentage in which the hybrid mechanisms fulfill the challenges. This emphasizes the need for hybrid mechanisms able to provide technical responses in these dimensions. Technical challenge is the main one faced by these mechanisms considering since it reflects on the system design which is the platform where social, economical, and legal challenges are implemented.

[1] A full list of related work summarized in Table I is provided in the thesis.

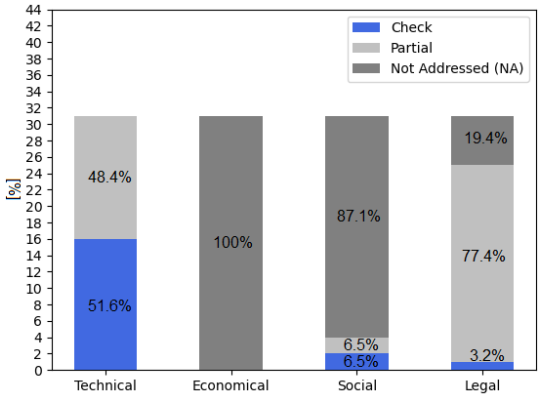

Fig. 3: Percentage of Challenges Addressed by Cooperative DDoS Defense Mechanisms

The technical dimension depicted in Figure 3 encompasses this vision with all mechanisms providing solutions with different approaches and characteristics. The distinction between Check (51.6%) and Partial (48.4%) implies how to implement these mechanisms, imposing a greater or lesser need for hardware changes on the peers involved in the collaborative defense. However, challenges in dimensions such as economic and social, are not adequately addressed. In case of economic challenges (*i.e.*, whether there is an approach to provide incentives that can cover detection costs or collaborative mitigation), 100% of the mechanisms do not address the challenge.

Another challenge of fundamental importance is the social one, in which most approaches consider as a premise that all participants are trusted. Thus, security details such as confidentiality and integrity of information exchanged in the overlay are not addressed by most works (87.1%). Concerning the legal aspect, most mechanisms deal partially (77.4%) based on the premise of participation by trusted members. However, even among trusted members, it is necessary to understand and react upon the differences in each region or country's legal aspects, which can influence the cooperation among members. BloSS encompasses the support for incentives based on Blockchain (BC) [23] that can be safely and reliably distributed among participants and that legal/conformity options can be selected to restrict operation to specific regions/countries or members.

Therefore, cooperative defenses can benefits from BC in different dimensions. While BC can *(i)* reduce the complexity of operation and coordination by using existing infrastructure to distribute rules without specialized registries or protocols, it also can foster a *(ii)* trusted cooperation due to its transparency and decentralized characteristics. Also, it can provide *(iii)* financial incentives which foster the cooperative behavior among service providers [20].

IV. Design

BloSS is structured into two parts:

- **On-chain**: include the processes of integrated payment and reputation ranking, being based on a sequence of defined steps mapped as states whereas each step's outcome is transparent and verifiable. Confidential information pertaining to collaboration between pairs is sent off-chain.
- **Off-chain**: includes the dApp with interface to the network management system and the deployed on-chain protocol. BloSS dApp stores individual settings related to when and how to request or accept mitigation services including legal aspects.

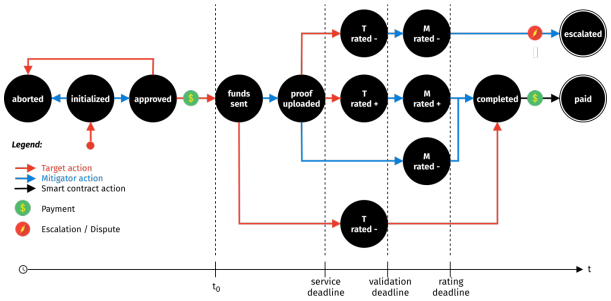

Fig. 4: On-chain Cooperative Signaling Protocol

A. On-chain BloSS Protocol

The use of a BC platform allows not only the full replication of attack information, but also the creation of a market of DDoS mitigation services as a fundamental pillar to foster cooperation between the service providers. BloSS is based on Ethereum, which is one of the most used BC platforms, and implemented as a dApp (Decentralized Application) providing REST interfaces for a network management system to interact with the cooperative system by requesting or offering mitigation services. An AS under attack (*i.e.*, Target AS) may request mitigation services (on-chain) by submitting transactions to members in the alliance, whose purpose is to offer mitigation services (and have the infrastructure available to influence attacking traffic). An AS whose purpose is to offer mitigation services (*i.e.*, Mitigator AS) may define in terms of financial incentives what is necessary to deliver services expressing these terms in their Smart Contracts (SC). Once a mitigation service is accepted, black-listed addresses are encrypted and sent off-chain in a separate data channel to the mitigator.

An overview of the BloSS workflow (*cf.* Figure 4) shows that once a mitigation service is accepted, a deadline to upload an evidence of completion is started (t0). Data exchange is done off-chain exchanging the encrypted data (*e.g.*, blacklisted addresses) via the Inter Planetary File System (IPFS) [2] ensuring the confidentiality and the integrity of the attack information based on a per-message signature bundled with the attack information. The Mitigator can act rationally and upload a evidence or miss the upload by expiring the validation deadline [12]. A Target can rate the service of the Mitigator and based on this rating funds initially locked in the SC are released to the Mitigator [7]. When there is no feedback (*i.e.*, Target is selfish), a rational Mitigator is allowed to rate negatively.

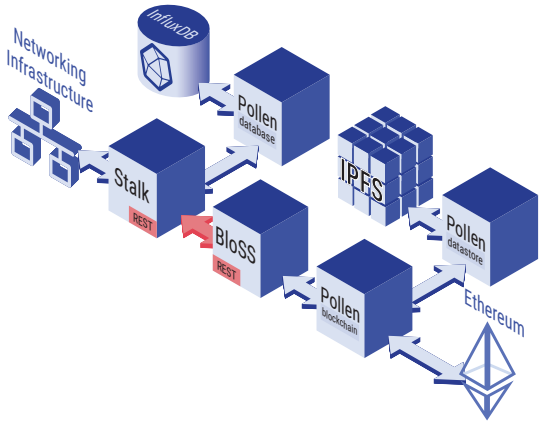

Fig. 5: BloSS Architecture

B. Off-chain BloSS dApp

An overview of the *BloSS* Decentralized Application (dAPP) (*cf.* Figure 5) details connections between its modules. The *BloSS* is the component, where each service provider taking part in the cooperative defense can post information about an ongoing attack to Ethereum, *i.e.*, the connector to on-chain contracts. It uses a REST interface to facilitate the isolation of the *BloSS*module, encapsulating the entire module together with Pollen BC and Pollen data store as SDN applications and, possibly, as a VNF running on commodity hardware [6]. The goal is not to impose restrictions on the underlying networking hardware, further simplifying the interaction with the *BloSS* and its modules via REST interfaces.

Data exchange is accomplished with the "Pollen" set of modules, and the "Stalk" module handles network-related tasks. Pollen is divided into dedicated modules for the specific data exchange duties of the *BloSS*, which includes a BC module for access to the Ethereum, a data storage module managing information on the IPFS. Attack information posted to the BC is not directly stored on the BC due to limited block sizes and to maintain the information confidential. For this purpose, IPFS is a decentralized and highly scalable storage solution to hold attack information. Each service provider running the *BloSS* also maintains an IPFS node to enable the decentralized storage. Whenever a new set of attack information is posted, the data is first stored in IPFS, and only the hash as a unique identifier of the storage location within IPFS is stored in a block on the Ethereum.

The Pollen data store also includes an encryption component. The encryption of attack information posted to IPFS ensures the confidentiality and the integrity of the attack information based on a per-message signature bundled with the attack information. Confidentiality is an essential attribute of the data exchange between service providers since the attack information can be sensitive to implicating individuals both as victims of an ongoing DDoS attack.

Verifying the integrity of attack information allows for holding each service provider accountable for the information posted to the BC and makes forgery of attack information impossible. The integrity-check is enabled through a public key published by each service provider to the BC and available to providers participating in the *BloSS* defense alliance. Without this measure, forgery of attack information would allow a malevolent party to indicate specific IP addresses as being the source of an ongoing attack and block flows from these addresses to the T address specified in the attack information.

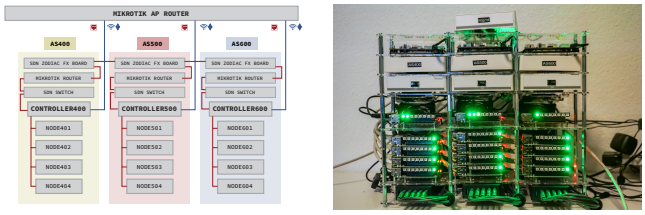

Fig. 6: BloSS Schematic View and Hardware Prototype

V. Evaluation

Several evaluations were performed during the development and refinement of the system to achieve the version presented in this thesis. This Section outlines their specific goals toward reaching the overall thesis goals.

A *BloSS* Functionality and Correctness: evaluations performed at the local prototype and deployed in the cluster depicted in Figure 6 to evaluate overall correctness and functionality (*e.g.*, signaling addresses, mitigating attacks, interaction with Ethereum).

B Signaling Protocol Latency: evaluation performed both locally and globally, in which the goal was to evaluate the performance in terms of latency of the off-chain communication channel based on an encrypted channel.

A. BloSS Functionality and Correctness

BloSS was deployed on a physical single-board computer cluster (*cf.* Figure 6). Three isolated and identically configured ASes were built: AS 400, AS 500, and AS 600 with each AS consisting of four host nodes used to initiate the attack traffic, and two controllers, which host the BloSS as well as the Ethereum BC and IPFS [2] nodes. Hosts are based on Raspberry Pi Model B (RPi), and controllers use ASUS Tinker Board devices, which provide greater computational capacity than RPIs.

BloSS has been evaluated by utilizing the iperf network bandwidth measurement tool [11]. An instance of iperf is installed on the last compute node of AS 600 with IP address 192.168.30.18 and is listening for incoming iperf connections on UDP port 5000. Table II shows delays recorded for 4 different bandwidths and over 10 attacks for each bandwidth. The bandwidth is set per compute node, which means at a bandwidth of 10 Mbit/s, a total attack volume of 80 Mbit/s is created and routed toward the target compute node.

It is important to note that one of the most significant contributing factors to the delay is the block period of 5 s. After sending an attack report, 5 s pass until the attack

TABLE II: Delay Until Attacks with Different Bandwidths are Blocked

[Mbit/s]	10 Runs [s]										Avg [s]
10	34	34	28	20	28	27	26	37	23	19	27.6
20	32	18	34	18	28	31	32	31	16	32	27.2
40	34	25	39	24	31	35	25	29	31	24	29.7
100	34	26	40	29	29	24	35	28	36	35	31.6

report becomes available to all BloSS instances. Since attack reports are based on subnetworks, a minimum of two reports need to be sent out to cover the two attacking subnetworks 192.168.10.0/24 and 192.168.20.0/24. If one of the attacking hosts is detected with a delay, another attack reports need to be filed, which consumes another 5 s. The average mitigation time of around 29 s overall experiments shows that the BloSS is a fast-acting mitigation solution capable of quickly diminishing even high-bandwidth threats.

B. Signaling Protocol Latency

The BloSS evaluation was based on Amazon Web Service (AWS) instances deployed in Ohio, Tokyo, and São Paulo. All instances were synchronized with the Ethereum Rinkeby BC in order to enable the separation of the Target T and Mitigator M. Each location was tested separately between the target in Zürich and São Paulo and the mitigator set to Ohio and Tokyo, respectively (*cf.* Figure 7: AWS instances deployed).

By running the target script on an AWS instance in Ohio and a M script on a node in Zürich (both synchronized to the Rinkeby network), the average global Rinkeby processing time with $n = 20$ is 96.950 s and the average standard deviation is 1.146 s (*cf.* Table III). Since the control condition has been tested and evaluated, similar results in terms of average processing time and average standard deviation are expected. However, similar results were reached as shown in Tables III, while the nodes were not synchronized at all times due to timeouts, *i.e.*, missed deadlines. This is due to full nodes, which are geographically in close proximity of these two AWS instances in Tokyo and São Paulo, but not being synchronized at all times.

For both global averages, average times measured show a similar result, with a slight difference in the average processing time of 0.668 s representing the difference of approximately

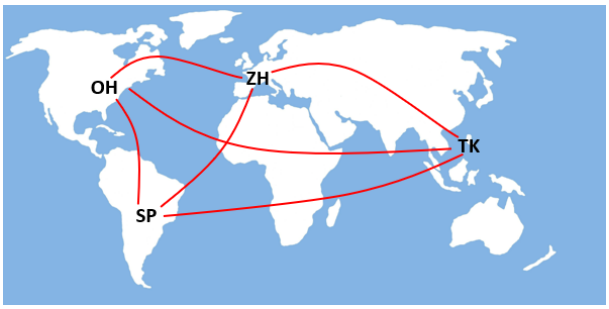

Fig. 7: AWS Instances Used in the Experiment. Acronyms: OH - Ohio, TK - Tokyo, SP - São Paulo, ZH - Zürich

TABLE III: *BloSS* Global Rinkeby Processing Times [s] (Zürich-Ohio)

Scenario	Average Time [s]	Standard Deviation [s]
1	88.938	3.025
2	88.616	1.099
3	87.973	2.110
4	104.090	0.509
5	88.006	1.361
6	104.358	1.340
7	118.900	0.442
8	103.932	0.458
9	89.265	0.711
10	103.331	1.038
11	88.956	0.509
Average	96.950	1.146

0.7%. By reaching these similar results in both global Rinkeby tests and removing the corresponding RTT the difference in average processing times for the scenarios is only 0.5171 s. It should be noted that 20 test runs per case may not lead to exact average values. Also, every test on the global Rinkeby network was tested with varying (not precise) average block times of 15 s.

VI. Conclusions, and Future Research

Conclusions. BloSS contributes to the modern security management for DDoS mitigation approaches with a cooperative defense logic and prototype as a proof-of-concept (available in [20]). It enables a flexible and efficient DDoS mitigation solution across multiple domains based on a permissioned PoA Ethereum [24], [22], in which only pre-selected operators participate in the cooperative defense. Therefore, based on recently validated technical tools, such as Blockchain (BCs) and Software-Defined Network (SDNs), it became possible to provide a practically deployable, collaborative defense mechanism capable of overcoming the main challenges as stated above and in [27].

The BC-based approach does not only enable the cooperative signaling of attacks, but also provides for an immutable and transparent platform allowing for incentives to be exchanged for mitigation services as well as tracking reputation. To the best of the author's knowledge, this is the first work that combines in a cooperative DDoS signaling system attacks BC concepts to provide incentives and reputation management in this context. Henceforth, the main contribution of this thesis was the conception of architecture and a system as a proof of concept showing that, while it is possible to simplify the deployment and operation of collaborative defenses, it is also possible to include aspects related to incentives, confidentiality, and legal aspects within the same system.

Furthermore, execution times and costs of *BloSS* as presented are based on the worst-case scenario, *i.e.*, a public BC infrastructure. For example, Target and Mitigators were configured to react to requests close to the deadlines configured in the contract. Therefore, it has to be noted that a

PoA-based deployment of *BloSS* will reach a much lower, almost neglectable cost basis and an even further reduced block creation time. This was shown for the case of simulated and local Rinkeby deployments.

Overall, the main achievement and advantages reached with the design and prototypical implementation as well as the evaluation of *BloSS* include *(a)* the use of an existing public and distributed infrastructure, the BC, to flare white- or blacklisted IP addresses and to distribute incentives related to the mitigation activities requested. Furthermore, it provides a proof-of-concept for *(b)* a cooperative, operational, and efficient decentralization of DDoS mitigation services, and *(c)* a compatibility of *BloSS* with existing networking infrastructures, such as SDN and BC.

Future Research. Based on an even further increase in traffic and the frequency of DDoS attacks, it is expected that future network and service management operations will also have to encounter alternatives equally distributed. While existing cooperative approaches present operational challenges, future work for *BloSS* involves the analysis of how actors (especially targets and mitigators) *(a)* would interact based on different profiles (*e.g.*, with malicious or honest properties) and *(b)* are impacted by different incentive values required to perform a mitigation service and, thus, simulating a DDoS protection market. Also, instead of storing raw names and strings in the *BloSS* register, hashes of data or even hashes of the storage address could be persisted within the BC, since transparency has to be taken into account.

REFERENCES

[1] Akamai, "The State of the Internet," 2020. [Online]. Available: https://www.akamai.com/us/en/resources/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp

[2] J. Benet, "IPFS-Content Addressed, Versioned, P2P File System," *arXiv preprint arXiv:1407.3561*, 2014. [Online]. Available: https://arxiv.org/abs/1407.3561

[3] CloudFare, "CloudFlare Advanced DDoS Protection," 2020. [Online]. Available: https://www.cloudflare.com/static/media/pdf/cloudflare-whitepaper-ddos.pdf

[4] S. K. Fayaz, Y. Tobioka, V. Sekar, and M. Bailey, "Bohatei: Flexible and Elastic DDoS Defense," in *24th USENIX Security Symposium (USENIX Security 15)*, Anaheim, California, USA, April 2015, pp. 817–832.

[5] M. Felici, N. Wainwright, S. Cavallini, and F. Bisogni, "What's New in the Economics of Cybersecurity?" *IEEE Security and Privacy,*, Vol. vol. 14, pp. pp. 11–13, may 2016.

[6] M. Franco, B. Rodrigues, and B. Stiller, "MENTOR: The Design and Evaluation of a Protection Services Recommender System," in *15th International Conference on Network and Service Management (IEEE CNSM 2019)*, Halifax, Canada, October 2019, pp. 1–7.

[7] A. Gruhler, B. Rodrigues, and B. Stiller, "A Reputation Scheme for a Blockchain-based Network Cooperative Defense," in *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM 2019)*, April 2019, pp. 71–79, washington, United States of America (USA).

[8] J. Ioannidis and S. M. Bellovin, "Implementing PushBack: Router-based Defense Against DDoS Attacks," 2002. [Online]. Available: https://www.cs.columbia.edu/~smb/papers/pushback-impl.pdf

[9] iotanalytics, "State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating," Fev 2018. [Online]. Available: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

[10] A. D. Keromytis, V. Misra, and D. Rubenstein, "SOS: Secure Overlay Services," *ACM SIGCOMM Computer Communication Review (ACM/CCR)*, Vol. 32, No. 4, pp. pp. 61–72, 2002.

[11] C. Killer, B. Rodrigues, and B. Stiller, "Security Management and Visualization in a Blockchain-based Collaborative Defense," in *ICBC 2019*. Seoul, South Korea: IEEE, May 2019, pp. 108–111. [Online]. Available: https://files.ifi.uzh.ch/CSG/staff/rodrigues/extern/publications/ICBC19_CK.pdf

[12] S. Mannhart, "Mitigation as a Service in a Cooperative Network Defense," Master's thesis, University of Zürich, Binzmuehlestrasse 14, 8050 Zürich, Switzerland, July 2018.

[13] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS attack and DDoS Defense Mechanisms," *ACM SIGCOMM Computer Communication Review (ACM/CCR)*, Vol. 34, No. 2, pp. 39–53, 2004.

[14] A. Mortensen, F. Andreasen, T. Reddy, C. Gray, R. Compton, and N. Teague, "Distributed-Denial-of-Service Open Threat Signaling (DOTS) Architecture," Internet Engineering Task Force, Internet-Draft draft-ietf-dots-architecture-06, Mar. 2018, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-dots-architecture-06.

[15] G. Oikonomou, J. Mirkovic, P. Reiher, and M. Robinson, "A Framework for a Collaborative DDoS Defense," in *2006 22nd Annual Computer Security Applications Conference (ACSAC'06)*. Miami Beach, Florida, USA: IEEE, December 2006, pp. 33–42.

[16] C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, and R. Govindan, "COSSACK: Coordinated Suppression of Simultaneous Attacks," in *DARPA Information Survivability Conference and Exposition*, Vol. 1. Washington, DC, USA: IEEE, April 2003, pp. 2–13.

[17] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems," *ACM Computing Surveys (CSUR)*, Vol. 39, No. 1, pp. pp. 03–15, 2007.

[18] B. Rashidi and C. Fung, "CoFence: A Collaborative DDoS Defence Using Network Function Virtualization," in *12th International Conference on Network and Service Management (CNSM 16)*, Montreal, Canada, November 2016.

[19] B. Rodrigues, E. J. Scheid, C. Killer, M. Franco, and B. Stiller, "Blockchain Signaling System (BloSS): Cooperative Signaling of Distributed Denial-of-Service Attacks," *Journal of Network and Systems Management*, Vol. 28, No. 3, pp. 1–27, August 2020. [Online]. Available: https://doi.org/10.1007/s10922-020-09559-4

[20] B. Rodrigues and B. Stiller, "Cooperative Signaling of DDoS Attacks in a Blockchain-based Network," in *The ACM SIGCOMM 2019 Conference Posters and Demos*, ser. SIGCOMM Posters and Demos '19. New York, NY, USA: ACM, 2019, pp. 39–41. [Online]. Available: http://doi.acm.org/10.1145/3342280.3342300

[21] R. Sahay, G. Blanc, Z. Zhang, and H. Debar, "Towards Autonomic DDoS Mitigation Using Software Defined Networking," in *SENT 2015: NDSS Workshop on Security of Emerging Networking Technologies*. San Diego, California. USA: Internet Society, February 2015.

[22] E. Scheid, T. Hegnauer, B. Rodrigues, and B. Stiller, "Bifröst: a Modular Blockchain Interoperability API," in *IEEE Conference on Local Computer Networks (LCN 2019)*, Osnabrück, Germany, October 2019, pp. 332–339.

[23] E. Scheid, B. Rodrigues, and B. Stiller, "Toward a Policy-based Blockchain Agnostic Framework," in *IFIP/IEEE Symposium on Integrated Network and Service Management (IM 2019)*, Washington - DC, USA, April 2019, pp. 609–613.

[24] E. J. Scheid, D. Lakic, B. B. Rodrigues, and B. Stiller, "PleBeuS: a Policy-based Blockchain Selection Framework," in *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2020, pp. 1–8.

[25] J. Steinberger, B. Kuhnert, A. Sperotto, H. Baier, and A. Pras, "Collaborative DDoS Defense Using Flow-based Security Event Information," in *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, Istanbul, Turkey, April 2016, pp. 516–522.

[26] T. Velauthapillai, A. Harwood, and S. Karunasekera, "Global Detection of Flooding-based DDoS Attacks Using a Cooperative Overlay Network," in *Network and System Security (NSS), 2010 4th International Conference on*. Melbourne, Australia: IEEE, September 2010, pp. pp. 357–364.

[27] 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. pp. 2046–2069, 2013.

[28] G. Zhang and M. Parashar, "Cooperative Defence Against DDoS Attacks," *Journal of Research and Practice in Information Technology*, Vol. 38, No. 1, pp. pp. 69–84, 2006.