SC-FLARE: Cooperative DDoS Signaling based on Smart Contracts

Bruno Rodrigues, Spasen Trendafilov, Eder Scheid, Burkhard Stiller
Communication Systems Group CSG, Department of Informatics IfI, University of Zurich UZH
Binzmühlestrasse 14, CH-8050 Zürich
E-mail: [rodrigues,scheid,stiller]@ifi.uzh.ch
spasen.trendafilov@uzh.ch

***Abstract*—Distributed Denial-of-Service (DDoS) attacks remains as one of the major causes of concerns for service providers around the world. This paper introduces *SC-FLARE*, a Smart Contract (SC) based cooperative signaling protocol built on top of a Ethereum Proof-of-Authority Blockchain (BC) for the sharing of attack information, the exchange of incentives, and the tracking of reputation in a fully distributed and automated fashion. By making use of BC and SC, *SC-FLARE* provide the required collaborative platform without the burden to maintain, design, and develop special registries and gossip protocols for a cooperative defense.**

I. Introduction

The growing number of insecure devices inflated Distributed Denial-of-Service (DDoS) statistics to unprecedented levels. Recent attacks demonstrated their power with new records in the volume of traffic and greater attack frequency [1]. While 2018 registered the largest ever DDoS attack in terms of traffic volume, the frequency of DDoS attacks also increased more than 2.5 times between 2014 and 2017 [2]. Botnets (*e.g.*, Mirai [3]) taking advantage of insecure devices ranging from small sensors to baby cameras and home gateways connected to the Internet are the main reason behind the escalation.

The distributed nature of DDoS attacks suggests that an ideal defense would be equally distributed. Advantages of cooperative defenses have been widely recognized in literature [4], [5]. It expands the detection and mitigation capabilities over the network, it also enables to block malicious traffic near its source. While our previous work [6] presented the initial structure of a collaborative defense based on Blockchain (BC) and Smart Contracts (SC), the SC design had no mechanisms to ensure the provision of incentives for mitigation services, nor assess the reputations of the actors involved.

SC-FLARE proposes a cooperative defense providing incentives and reputation tracking capabilities based on a permissioned Proof-of-Authority (PoA) Ethereum Blockchain. The main advantages are the deployment of existing public and distributed infrastructure to flare white or blacklisted IP addresses and to distribute incentives related to the requested mitigation activities. This work is structured as follows. Section II present related work. Section III presents the design and implementation. Evaluation is presented in Section IV and considerations and future work, in Section V.

978-1-7281-6680-3/20$31.00

II. Related Work

The literature contains a number of industry and academia proposals to detect and mitigate DDoS attacks, being categorized as *in-house* or *off-house* approaches [4]. While *in-house* defenses are based on resources available locally (*e.g.*, firewall, load balancer, intrusion detection/prevention systems) to protect a single target or network, an *off-house* defense involves a third-party to detect and/or mitigate the attack. In this regard, an off-house defense can be cloud-based or cooperative [5]. While the former serves as a proxy receiving, analyzing and redirecting traffic to the target, which delegate detection and mitigation tasks to the protection provider (*e.g.*, Akamai [1] or CloudFlare [7]), the latter is a decentralized approach typically implemented as an overlay network.

Secure Overlay Services (SOS) [8], COSSACK [9], and DefCOM [10] paved the way for cooperative defenses in the early 2000s. While SOS's approach focused on identifying legitimate sources for time-sensitive networks (*i.e.*, requiring peers to authenticate to the overlay network), COSSACK and DefCOM based their approach on detection and enforcement points in access networks. However, despite pioneering the decentralization of detection and mitigation points in the network, these approaches present a high complexity of coordination and operation, often requiring changes in routers [10], [9], or requiring the sources to be registered [8].

Approaches such as CoFence [11] and Bohatei [12] are based on relatively new technologies, respectively NFV (Network Function Virtualization) and SDN (Software-Defined Networking) to reduce the complexity of coordination and operation. However, other challenges such as economic, and social are not fully addressed, as pointed by [4], [5]. Thus, a technical solution based on BC should not only avoid additional hardware and software costs but also be simple to deploy and operate [13]. Also, *SC-FLARE* encompasses the support for incentives that can be safely distributed among participants and that legal/conformity options can be selected to, for example, restrict operation to specific regions/countries or members. While BC can reduce the complexity of operation and coordination by using existing infrastructure to distribute rules without specialized registries or protocols, it also can foster trusted cooperation due to its transparency and decentralized characteristics.

III. *SC-FLARE* Design

SC-FLARE protocol is deployed as a Smart Contract in a permissioned Proof-of-Authority (PoA) Blockchain involving two parties, Target (T) and Mitigator (M). *SC-FLARE* starts when *T* initiates a contract with *M*'s address, *cf.*, first step from left to right in Figure 1. The first step contains important variables (*e.g.*, network information, deadline interval, or minimal amount of funds), which are not changed during the following process until the *SC-FLARE* is reused through initializing or reinitializing.

M may decide whether to be cooperative or not, followed by *T* which can still abort the request or send the incentives required by *M*. If the request is accepted, a service deadline starts (denoted by t0), which is the deadline for *M* to upload a proof of completion of the mitigation task.

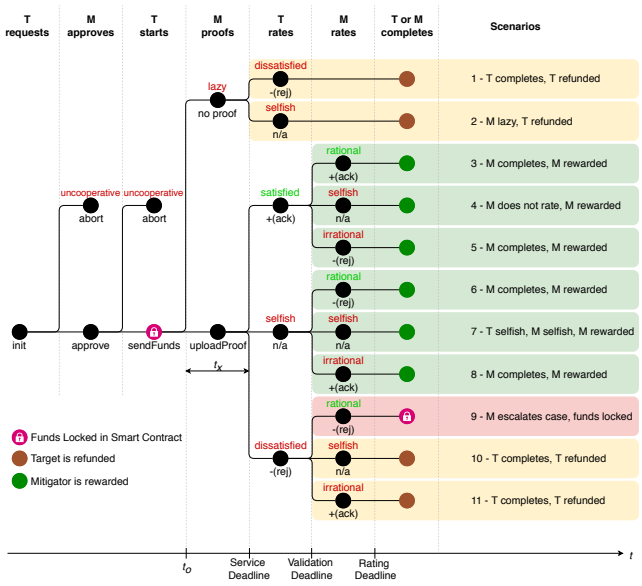

Fig. 1: *SC-FLARE* contract for a collaborative, on-chain signaling

M can act rationally and upload a proof or miss the upload. However, it is not possible verify the truthfulness or the quality of the (proof of) service performed by *M* [14]. Even if the BC preserve a transparent audit trail for all transactions, it cannot compensate for a lack of ground-truth. This holds for the uploaded proof of service as well as for user-defined, subjective ratings, in which there is no automated way to fully determine the truthfulness of a proof or rating.

If a proof is uploaded, the rating process of *T* and *M* begins [15]. During the rating, only the case where both actors are dissatisfied leads to the *Escalate* end-state, where a decision cannot be automated in *SC-FLARE* and proofs have to be verified externally. Other rating combinations, lead to the end-state *Complete*. When *Complete* is reached, locked funds are released and transferred either to *T* or *M*, depending on missed deadlines and ratings.

IV. Preliminary Evaluation

SC-FLARE was evaluated using the Truffle framework for the deployment of the contracts, as well as running the scenarios evaluating the performance (in terms of latency) to reach all possible final states, and more importantly, the correctness of *SC-FLARE* code. The *SC-FLARE* performance evaluation involves the scenarios described in Section 1 to measure their completion time, *i.e.*, time required for complete execution of each scenario. The simulation scenarios for Ganache were executed 20 times, simulating the permissioned PoA blockchain with a block-time of 5 seconds. The averaged times of each scenario are listed in Table I.

TABLE I: Ganache Completion Times [s]

End Scenario	Avg. Completion Time [s]	Std. deviation [s]
1	30.095	0.220
2	32.072	0.398
3	30.093	0.384
4	35.117	0.096
5	29.966	0.434
6	35.032	0.401
7	40.018	0.484
8	35.051	0.398
9	30.033	0.402
10	35.059	0.312
11	30.092	0.350
Average	32.783	0.353

When a missed deadline is simulated in order to evaluate scenarios 2, 7, and 10, an action by *T* or *M* can only be taken after the interval is expired. Such expiration deadlines were configured in 6 seconds considering a 5 seconds block-time, in order to wait for at least an additional block. More precisely, when a missed deadline is simulated, a predefined timeout occurs such that the initialized deadline interval is missed by introducing a wait, which waits longer than the defined deadline interval. Also, as Ganache is a simulated environment, an important aspect that can impact deadlines is not considered, the propagation delays of underlying network infrastructure. Thus, an important aspect evaluated in the experiments is the correctness and feasibility of *SC-FLARE*, counting on the provision of incentives and evaluations of actions taken by *T* and *M*.

V. Considerations and Future Work

This paper presented *SC-FLARE*, an approach enabling the signaling of attacks and an immutable and transparent platform that allows incentives to be exchanged for mitigation services, as well as tracking reputation. Future work involves the deployment of *SC-FLARE* in a real network (*i.e.*, Rinkeby testnet) and the evaluation of different thresholds.

Acknowledgements. This paper was supported partially by *(a)* the University of Zürich UZH, Switzerland and *(b)* the European Union's Horizon 2020 Research and Innovation Program under Grant Agreement No. 830927, the CONCORDIA project.

REFERENCES

[1] Akamai, "How to Protect Against DDoS Attacks - Stop Denial of Service." [Online]: https://www.akamai.com/us/en/resources/protect-against-ddos-attacks.jsp

[2] S. D. Kotey, E. T. Tchao, and J. D. Gadze, "On Distributed Denial of Service Current Defense Schemes," *Technologies*, Vol. 7, No. 1, p. 19, 2019.

[3] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, "Understanding the Mirai Botnet," *26th USENIX Security Symposium (USENIX Security 17)*, 2017, pp. 1093–1110.

[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.

[5] 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.

[6] B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, "A Blockchain-based Architecture for Collaborative DDoS Mitigation with Smart Contracts," *IFIP International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2017). Lecture Notes in Computer Science Vol. 10356*. Springer, 2017, pp. pp. 16–29, zurich, Switzerland.

[7] CloudFare, "CloudFlare Advanced DDoS Protection," 2016. [Online]: https://www.cloudflare.com/static/media/pdf/cloudflare-whitepaper-ddos.pdf

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

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

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

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

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

[13] B. Rodrigues, T. Bocek, and B. Stiller, "The Use of Blockchains: Application-driven Analysis of Applicability," *Advances in Computers*. Elsevier, 2018, Vol. 111, pp. 163–198.

[14] S. Mannhart, B. Rodrigues, E. Scheid, S. S. Kanhere, and B. Stiller, "Toward Mitigation-as-a-Service in Cooperative Network Defenses," *2018 IEEE 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (CyberSciTech 2018)*, Aug 2018, pp. pp. 362–367, Athens, Greece.

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