

Blockchain Signaling System

A Distributed Defense Against Distributed Attacks

Bruno Rodrigues



Department of Informatics

Blockchain Signaling System (BloSS)

Dissertation submitted to the Faculty of Business,
Economics and Informatics
of the University of Zurich

to obtain the degree of
DOKTOR DER WISSENSCHAFTEN, DR. SC.
(corresponds to DOCTOR OF SCIENCE, PHD)

presented by
BRUNO BASTOS RODRIGUES
from
BRASÍLIA, DISTRITO FEDERAL, BRAZIL

approved in FEBRUARY 2021

accepted at the request of
PROF. DR. BURKHARD STILLER
PROF. RADU STATE, PHD

The Faculty of Business, Economics and Informatics of the University of Zurich hereby authorizes the printing of this dissertation, without indicating an opinion of the views expressed in the work.

ZÜRICH, FEBRUARY 17, 2021

The chairman of the Doctoral Board: PROF. THOMAS FRITZ, PHD

Berichte aus der Informatik

Bruno Rodrigues

Blockchain Signaling System

(Diss. Universität Zürich)

Shaker Verlag
Düren 2021

Bibliographic information published by the Deutsche Nationalbibliothek

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at <http://dnb.d-nb.de>.

Zugl.: Zürich, Univ., Diss., 2020

Copyright Shaker Verlag 2021

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publishers.

Printed in Germany.

ISBN 978-3-8440-7956-2

ISSN 0945-0807

Shaker Verlag GmbH • Am Langen Graben 15a • 52353 Düren

Phone: 0049/2421/99011-0 • Telefax: 0049/2421/99011-9

Internet: www.shaker.de • e-mail: info@shaker.de

ABSTRACT

Distributed Denial-of-Service (DDoS) attacks are one of the major causes of concerns for communication service providers. When an attack is highly sophisticated and no countermeasures are available directly, sharing hardware and defense capabilities become a compelling alternative. Future network and service management can base its operations on equally distributed systems to neutralize highly distributed DDoS attacks. A cooperative defense allows for the combination of detection and mitigation capabilities, the reduction of overhead at a single point, and the blockage of malicious traffic near its source.

Cooperative defense systems face many challenges, such as deployment complexity due to high coordination overhead, reliance on trusted and stable channels for communication and the need for effective incentives to bolster cooperation among all involved parties. These challenges impairing the widespread deployment of existing cooperative defense are: *(a)* high complexity of operation and coordination, *(b)* need for trusted and secure communications, *(c)* lack of incentives for service providers to cooperate, and *(d)* determination on how operations of these systems are affected by different legislation, regions, and countries.

Driven by challenges imposed in a cooperative network defense, 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. Therefore, BloSS was prototyped and evaluated through local and global experiments, without the burden to maintain, design, and develop special registries and gossip protocols.

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 the interaction between Autonomous Systems (AS) victim of DDoS attack and ASes acting as mit-

igators, presented an average of 97 seconds to complete all eleven possible outcomes of the BloSS protocol. The reputation assessment, based on the transparency of actions carried out on BC using Beta reputation and individual thresholds of trust for each member, showed that the defined protocol is capable of punishing malicious providers and benefiting providers by acting honestly.

The definition of contracts in BloSS stipulates the cooperative logic based on BCs and allows for the increase of trust among cooperative operators due to their transparent exchange of selected information and respective incentives on a per request basis. Overall, the main achievement and advantages reached with the design, prototypical implementation, and evaluation of BloSS include (a) the use of an existing 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 Software-Defined Networking (SDN) and BC.

KURZFASSUNG

Distributed Denial-of-Service (DDoS)-Angriffe sind eine der Hauptbedrohungen für Anbieter von Kommunikationsdienstleistungen. Wenn ein Angriff technisch ausgereift ist und keine direkten Gegenmaßnahmen zur Verfügung stehen, wird die gemeinsame Nutzung von Hardware und Verteidigungsfähigkeiten zu einer zwingenden Alternative. Das zukünftige Netzwerk- und Dienstmanagement kann seine Operationen auf vollständig verteilte Systeme stützen, um hochgradig verteilte DDoS-Angriffe zu neutralisieren. Eine kooperative Verteidigung ermöglicht die Kombination von Erkennungs- und Abwehrfähigkeiten, die Reduzierung des Overheads an einem einzigen Punkt und die Blockierung bösartigen Datenverkehrs in der Nähe seiner Quelle.

Kooperative Verteidigungssysteme sind mit vielen Herausforderungen konfrontiert, wie z.B. der Komplexität des Einsatzes aufgrund des hohen Koordinationsaufwands, der Abhängigkeit von vertrauenswürdigen und stabilen Kommunikationskanälen und der Notwendigkeit wirksamer Anreize zur Förderung der Zusammenarbeit zwischen allen beteiligten Parteien. Diese Herausforderungen beeinträchtigen den weit verbreiteten Einsatz bestehender kooperativer Verteidigung: (a) hohe Komplexität von Einsatz und Koordination, (b) Notwendigkeit einer vertrauenswürdigen und sicheren Kommunikation, (c) Mangel an Anreizen für die Anbieter von Dienstleistungen zur Zusammenarbeit und (d) Feststellung, wie der Betrieb dieser Systeme durch unterschiedliche Gesetze, Regionen und Länder beeinflusst wird.

Von denjenigen Herausforderungen bestimmt, die durch eine kooperative Netzwerkverteidigung entstehen, wird das Blockchain Signaling System (BloSS) als eine effektive und alternative Lösung für das Sicherheitsmanagement, insbesondere für die kooperative Verteidigung, vorgestellt, indem Blockchains (BC) und Software-Defined Networks (SDN) für den Austausch von Angriffsinformationen, den Austausch von Anreizen und die Verfolgung der Reputation auf vollständig verteilte und automatisierte Weise genutzt werden. BloSS prototypisch entwickelt und durch lokale und glob-

ale Experimente evaluiert, ohne die Notwendigkeit, Betriebskosten spezieller Register bzw. Datenbanken und Gossip-Protokolle vorsehen zu müssen.

Die Evaluierungsergebnisse auf der Grundlage der lokalen und globalen Prototypisierung von BloSS unterstreichen seine Wirksamkeit bei der Signalisierung von Informationen über groß angelegte DDoS-Angriffe. Die weltweite Auswertung, bei der die Interaktion zwischen Autonomen Systemen (AS), welche typischerweise Opfer von DDoS-Angriffen sind, und AS, die als Mittelsman fungieren, getestet wurde, ergab einen Durchschnitt von 97 Sekunden, um alle elf möglichen Endzustände des BloSS-Protokolls zu erreichen. Die Reputationsbewertung, die auf der Transparenz der auf den BCs durchgeführten Aktionen unter Verwendung der Beta-Reputation und individueller Vertrauensschwellen für jedes Mitglied basierte, zeigte, dass das definierte Protokoll in der Lage ist, böswillige Anbieter zu bestrafen und Anbieter durch ehrliches Handeln zu begünstigen.

Die kooperative Logik auf der Grundlage von BCs erlaubt die Definition von Verträgen in BloSS und ermöglicht die Stärkung des Vertrauens zwischen den kooperativen Akteuren aufgrund ihres transparenten Austauschs ausgewählter Informationen und entsprechender Anreize auf einer Pro-Anfrage-Basis. Insgesamt gesehen gehören zu den wichtigsten Errungenschaften und Vorteilen, die mit dem Entwurf, der prototypischen Implementierung und der Evaluierung des BloSS erreicht wurden, die Nutzung einer bestehenden verteilten Infrastruktur, der BCs, dem Eintrag von IP-Adressen in White- bzw. Black-Listen und zur Verteilung von Anreizen in Zusammenhang mit Gegenmaßnahmen. Darüber hinaus erlaubt es den Nachweis des einsatzfähigen Konzeptes für eine kooperative, betriebsbereite und effiziente Dezentralisierung von DDoS-Mitigaton-Diensten und eine Kompatibilität mit bestehenden Netzwerkinfrastrukturen auf der Basis von Software-Defined Networking (SDN) und BCs.

Acknowledgments

First of all, I would like to thank God for being able to do what I love. I thank all my family who provided me with all the necessary support before entering academic life, and friends that I could always count on in my free time to talk and share beers and coffees.

Thanks to my advisor Prof. Dr. Burkhard Stiller, who guided me during all the doctorate stages involving the entire scope of tasks (*i.e.*, teaching, presentations, guiding students) performed during the period, offering advice and freedom to suggest ideas and research paths. I would also like to thank my advisors of the master's, Prof. Dr. Tereza Cristina Melo de Brito Carvalho, and bachelor's degrees, Prof. Dr. Charles Christian Miers, who provided me with the necessary background and support to keep following the academic path.

I am very grateful to many people who have helped me directly or indirectly with my thesis work. All the CSG members that helped my work with many suggestions and discussions on how to improve the various specific parts, ranging from helping to build a cluster of Raspberry Pi's to how to run many of the experiments in the thesis. Also, I want to thank the many students who contributed to this thesis conducting and extending experiments, and proposing improvements to my initial BloSS prototype, which was gracefully ported to virtual machines enabling world-wide experiments.

Contents

| | | |
|----------|--|-----------|
| 1 | INTRODUCTION | 1 |
| 1.1 | Cooperative Network Defenses | 4 |
| 1.2 | Blockchain-based Cooperative Defense | 5 |
| 1.3 | Research Questions | 6 |
| 1.4 | Methodology | 7 |
| 1.5 | Research Methods | 8 |
| 1.6 | Thesis Contributions | 9 |
| 1.7 | Thesis Outline | 10 |
| 2 | THEORETICAL FOUNDATIONS | 12 |
| 2.1 | Distributed Denial-of-Service Attacks | 12 |
| 2.2 | Distributed Denial-of-Service Defense | 23 |
| 2.3 | The IETF DOTS Standard | 26 |
| 2.4 | Blockchains and Consensus Mechanisms | 28 |
| 2.5 | Blockchain as an Enabler of Trust in a Cooperative Defense | 46 |
| 2.6 | Reputation Tracking and Management | 48 |
| 2.7 | Security Basics and Blockchain Security | 57 |
| 2.8 | Key Observations | 63 |
| 3 | STATE-OF-THE-ART OF COOPERATIVE NETWORK DEFENSES | 65 |
| 3.1 | Classification of DDoS Defense Mechanisms | 65 |
| 3.2 | Source-based DDoS Mechanisms | 67 |
| 3.3 | Destination-based DDoS Mechanisms | 69 |
| 3.4 | Network-Based DDoS Mechanisms | 72 |
| 3.5 | Hybrid DDoS Defense Mechanisms | 74 |

| | | |
|-------------------|---|------------|
| 3.6 | Analysis of Cooperative Defenses Characteristics and Challenges | 79 |
| 3.7 | Key Observations | 84 |
| 4 | DESIGN OF THE COOPERATIVE SIGNALING PROTOCOL | 86 |
| 4.1 | Design Considerations | 87 |
| 4.2 | Cooperative Signaling Protocol | 92 |
| 4.3 | Reputation Tracking | 100 |
| 4.4 | Key Observations | 105 |
| 5 | DESIGN OF THE BLOCKCHAIN SIGNALING SYSTEM | 106 |
| 5.1 | Architecture | 107 |
| 5.2 | Defense Scenario | 114 |
| 5.3 | Off-chain Data Exchange | 117 |
| 5.4 | BloSS Management Dashboard | 119 |
| 5.5 | Key Observations | 124 |
| 6 | EVALUATION | 126 |
| 6.1 | Roadmap of BloSS Evaluations | 127 |
| 6.2 | BloSS Functionality and Correctness | 128 |
| 6.3 | Dashboard Usability | 131 |
| 6.4 | Off-chain Signaling Latency | 135 |
| 6.5 | Reputation Scores | 145 |
| 6.6 | Cooperative Signaling Protocol Latency | 151 |
| 6.7 | Smart Contract's Vulnerabilities | 159 |
| 6.8 | Key Observations | 165 |
| 7 | SUMMARY, CONCLUSIONS, AND FUTURE RESEARCH | 168 |
| 7.1 | Summary | 168 |
| 7.2 | Conclusions | 173 |
| 7.3 | Future Research | 174 |
| REFERENCES | | 198 |
| A | DESCRIPTION OF DDoS COOPERATIVE MECHANISMS | 199 |
| A.1 | Source-based DDoS Mechanisms | 199 |
| A.2 | Destination-based DDoS Mechanisms | 202 |

| | | |
|----------|--|------------|
| A.3 | Network-Based DDoS Mechanisms | 205 |
| A.4 | Hybrid DDoS Defense Mechanisms | 207 |
| B | BLOSS SMART CONTRACTS | 220 |
| B.1 | Register Contract | 220 |
| B.2 | Cooperative Signaling Protocol | 222 |
| C | COOPERATIVE SIGNALING GLOBAL LATENCY EVALUATIONS | 224 |
| D | REPUTATION IN ACCEPTANCE MODE | 227 |
| E | DESCRIPTION OF SMART CONTRACT'S VULNERABILITIES | 231 |
| F | PUBLICATIONS | 236 |
| F.1 | Contribution of Own Publications Within Chapters | 236 |
| F.2 | List of Publications | 239 |