

**SECURITY AND RELIABILITY OF RATIONAL  
PLAYERS IN DISTRIBUTED CONSENSUS**

Kehelwala Gamaralalage Janani Hansika Kehelwala

189329L

Degree of Master of Science

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

May 2021

# **SECURITY AND RELIABILITY OF RATIONAL PLAYERS IN DISTRIBUTED CONSENSUS**

Kehelwala Gamaralalage Janani Hansika Kehelwala

189329L

Dissertation submitted in partial fulfillment of the requirements for the degree of MSc  
in Computer Science specializing in Security Engineering

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

May 2021

## **DECLARATION**

### **Candidate:**

I declare that this is my own work and this dissertation does not incorporate, without acknowledgment, any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief, it does not contain any material previously published or written by another person except where the acknowledgment is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

.....  
K. G. J. H. Kehelwala

.....  
Date

### **Supervisor:**

The above candidate has carried out research for the Masters Dissertation under my supervision.

.....  
Dr. C. D. Gamage

.....  
Date

## ABSTRACT

Distributed ledgers and their applications in solving centralization problems in both financial and non-financial domains has been in the forefront of information security research since the emergence and the subsequent popularity of Blockchain. While the Proof of Work protocol has been successfully utilized for cryptocurrencies, the requirement for higher throughputs in non-financial domain based distributed ledgers favor alternate protocols whose consensus assumptions usually come with thresholds of Byzantine agents (faulty inputs) the consensus can withstand. Proof of Work is designed so that financial gain from conducting a successful attack is less than what honest participation would provide, eliminating any motivation an adversary might have to attack (within the context of direct gain). This assumption fails for non-financial solutions since resourceful malicious participants may exist where their gain may lie in manipulation of the distributed ledger or the order in which the transactions are recorded. A resourceful attacker could selectively convert rational agents to byzantine agents until the tolerance threshold is exceeded. Therefore, we propose that completeness assurance, and the overall reliability of distributed consensus requires rational and foresighted players to be sufficiently incentivized in affording costs of self-protection. We present a dynamic, complete, and imperfect information game to study the relationships between individual costs and utilities, tolerance threshold of the protocol and environment volatility in terms of exogenous attack probabilities, and observe conditions under which a mixed strategy equilibrium that preserves completeness would be stable. Our research extends existing literature by obtaining realistic resilience measures when considering rational player behavior in volatile environments, and provide a better understanding of mandatory security requirements that need to be implemented by a protocol designer for security in distributed consensus. We evaluate our proposed model using efficiency measurement concepts such as Price of Anarchy and Price of Malice, alongside learning methodologies such as regret matching and bounded rationality for extended insight. Our evaluations follow the theoretical predictions of the proposed model. Our results confirm reputation optimization to be capable of completeness assurance when the benefits are carefully assigned with consideration to tolerance threshold of the network. Our experiments also indicate that reputation optimization has attractive stability and convergence properties that are absent in other learning methodologies considered for evaluation.

**Keywords:** Incentive Compatibility, Mixed Strategy Equilibria, Social Trust Network, Bounded Rationality, Price of Malice, Game Theory, Distributed Consensus, Mechanism Design

## **DEDICATION**

This dissertation is dedicated to my grandfather, Captain John Jayapala.

I hope there is peace. I hope you have found it.

## **ACKNOWLEDGMENTS**

My gratitude goes to my supervisor, Dr. Chandana Gamage for providing continuous guidance throughout this endeavor. The expertise, resources and supervision provided by him were invaluable to the successful completion of this research. I would also like to thank Dr. Charith Chitraranjan and Dr. Indika Perera for the resources and guidance they provided in assessment and reviewing of literature.

Finally, my gratitude extends to my friends and family, whose support and patience has been a driving force throughout the duration of this effort.

## TABLE OF CONTENTS

Declaration .....	i
Abstract .....	ii
Dedication .....	iii
Acknowledgments .....	iv
Table of Contents .....	v
List of Figures .....	viii
List of Tables .....	x
List of Abbreviations .....	xi
List of Appendices .....	xii
1 Introduction .....	1
1.1 Background .....	1
1.2 Motivation .....	3
1.3 Problem .....	4
1.3.1 Definitions .....	4
1.3.2 Problem Statement .....	8
1.4 Research Objective .....	8
1.5 Summary .....	9
2 Literature Review .....	10
2.1 Introduction .....	10
2.2 Blockchain Applications Beyond Financial Sector .....	10
2.2.1 Intellectual Property .....	10
2.2.2 Internet of Things .....	15
2.2.3 Healthcare .....	17
2.2.4 Governance .....	18
2.2.5 Influence of Resourceful Adversaries .....	19
2.3 Consensus Algorithms in Blockchain .....	19
2.3.1 Proof of Work .....	20
2.3.2 Incentive Incompatibility .....	22
2.3.3 Selfish-mining .....	23
2.3.4 Fair Mining .....	25
2.3.5 Propagation Incentive .....	27
2.4 Byzantine Fault Tolerance .....	29
2.4.1 Byzantine Generals Problem .....	29
2.4.2 Practical Byzantine Fault Tolerance .....	32

2.5	Derived Consensus Protocols .....	35
2.5.1	Mining Based Protocols .....	35
2.5.2	Voting Based Protocols .....	39
2.5.3	Scalability of Consensus Protocols .....	43
2.6	Game Theory as a Solution Concept .....	45
2.6.1	Noise and Game Theory .....	47
2.6.2	Internet and Game Theory .....	50
2.7	Game Theory in Information Security .....	51
2.8	Game Theory in Distributed Systems Security .....	58
2.8.1	System Reliability in Game Theory .....	58
2.8.2	Service differentiation on peer contribution .....	61
2.8.3	Affording costs of self-protection .....	63
2.8.4	Reputation based service differentiation .....	66
2.8.5	Future Utility Optimization .....	68
2.9	Learning Of Equilibria .....	70
2.9.1	Reputation Optimization .....	70
2.9.2	Regret Matching .....	71
2.9.3	Bounded Rationality .....	72
2.10	Evaluation of Game Theoretical Models .....	73
2.10.1	Multi-Agent Based Simulation .....	73
2.10.2	Simulating networks of proactive agents .....	75
2.11	Summary .....	76
3	Methodology .....	78
3.1	Introduction .....	78
3.1.1	Contributions .....	78
3.1.2	Design And Analysis .....	79
3.2	Standard Notation and Definitions .....	80
3.2.1	Nash Equilibrium .....	80
3.2.2	Properties of Mixed Strategy Equilibria .....	80
3.2.3	Social Welfare of an Attacker vs Network game .....	81
3.3	Game of peers .....	82
3.3.1	Specific Notations .....	82
3.3.2	Reputation modifier functions $R$ .....	83
3.3.3	Utilities .....	86
3.3.4	Pure Strategy Equilibria .....	87
3.3.5	Mixed Strategy Equilibria .....	92



3.4	Equilibrium Efficiency Measurements . . . . .	98
3.4.1	Social Optimum Welfare . . . . .	98
3.4.2	Price of Anarchy . . . . .	99
3.4.3	Price of Malice and Fear Factor . . . . .	100
3.5	Evaluation Strategy . . . . .	103
3.5.1	Evaluating effects of Noise . . . . .	103
3.5.2	Evaluating Efficiency . . . . .	104
3.6	Summary . . . . .	104
4	Implementation and Evaluation . . . . .	106
4.1	Simulation Design . . . . .	106
4.2	Peer-based simulation design . . . . .	107
4.2.1	Design . . . . .	107
4.2.2	Implementation . . . . .	109
4.2.3	Limitations . . . . .	109
4.3	Server-based simulation design . . . . .	110
4.3.1	Design . . . . .	110
4.3.2	Implementation . . . . .	112
4.3.3	Limitations . . . . .	112
4.4	Learning-based simulation design . . . . .	113
4.4.1	Design . . . . .	113
4.4.2	Implementation . . . . .	115
4.4.3	Limitations . . . . .	115
4.5	Design constraints and System Level Limitations . . . . .	116
4.5.1	Evaluating influence of varying parameters . . . . .	117
4.6	Simulation Results . . . . .	117
4.6.1	Effects of Noise . . . . .	118
4.6.2	Efficiency of Learning Strategies . . . . .	125
4.7	Summary . . . . .	131
5	Conclusion and Future Works . . . . .	132
5.1	Summary . . . . .	132
5.2	Future Work . . . . .	133
	Reference List . . . . .	135
	Appendix A Game Theoretic Definitions . . . . .	139
	Appendix B Additional Simulation Results . . . . .	142
	Appendix C Digital Document and Simulation Code . . . . .	151

## LIST OF FIGURES

	Page
Figure 1.1 Byzantine Fault Tolerant Consensus .....	5
Figure 1.2 Selective interference .....	6
Figure 2.1 Selfish Mining Rewards .....	24
Figure 2.2 Fruitchains .....	26
Figure 2.3 A d-ary tree with a duplicating node .....	28
Figure 2.4 PFBT Client, Primary and Replica interactions .....	33
Figure 2.5 Keynes Beauty Contest Game .....	49
Figure 2.6 Payoffs for the Prisoner's Dilemma .....	64
Figure 3.1 Payoffs for Network vs Attacker .....	81
Figure 3.2 Scaled reputations for average availability values against differing attack probabilities .....	85
Figure 3.3 Upper limits of benefit for <i>passive</i> action being the best response .....	89
Figure 3.4 Lower limits of benefit for <i>active</i> action being the best response	90
Figure 3.5 Lower limits of benefit for <i>active</i> action being the best response with minimum attack probability .....	91
Figure 3.6 Active protection probability for varying environmental condi- tions .....	93
Figure 3.7 Maximum benefits feasible for various tolerance thresholds ...	96
Figure 3.8 Utilities for different actions in Mixed Strategy Equilibria ....	98
Figure 3.9 Price of Malice and Fear Factor .....	102
Figure 3.10 Fear Factor .....	103
Figure 4.1 Peer-based simulation design .....	108
Figure 4.2 Peer-based simulation implementation .....	109
Figure 4.3 Server-based simulation design .....	111
Figure 4.4 Server-based simulation implementation .....	112
Figure 4.5 Learning-based simulation design .....	114
Figure 4.6 Learning-based simulation implementation .....	115
Figure 4.7 NetLogo Interface .....	117
Figure 4.8 Homogenous peer behavior at Benefit per unit of cost 3 .....	118
Figure 4.9 Homogenous peer behavior at Benefit per unit of cost 1.5 (top) and 4 (bottom) .....	118

Figure 4.10	Homogenous peer behavior at varying Minimum Attack Probabilities .....	119
Figure 4.11	Homogenous peer behavior at varying Timeout values .....	120
Figure 4.12	Homogenous peer behavior at differing number of peers .....	120
Figure 4.13	Heterogenous peer behavior .....	121
Figure 4.14	Heterogenous peer behavior for larger range of costs .....	121
Figure 4.15	Homogenous peer behavior at differing tolerance thresholds ..	122
Figure 4.16	Peer reputations at differing tolerance thresholds .....	122
Figure 4.17	Convergence for tolerance thresholds 33.4% when benefit per unit of cost 1.5 .....	123
Figure 4.18	Convergence for tolerance thresholds 20% when benefit per unit of cost 1.2 .....	123
Figure 4.19	Peer reputations at differing tolerance thresholds .....	123
Figure 4.20	Convergence for tolerance thresholds 20% at differing attack probabilities .....	124
Figure 4.21	Reputation Optimization Learning Strategy execution for 20 rounds .....	125
Figure 4.22	Regret Matching Learning Strategy execution for 20 rounds ..	126
Figure 4.23	Regret Matching Learning Strategy (with History) execution for 20 rounds .....	126
Figure 4.24	Regret Matching Learning Strategy execution for differing benefits .....	127
Figure 4.25	Bounded Rationality Learning Strategy execution .....	128
Figure 4.26	Bounded Rationality Learning Strategy execution for differing benefits .....	128
Figure 4.27	Reputation Optimization Learning Strategy Utilities for 20 rounds	129
Figure 4.28	Regret Matching Learning Strategy Utilities for 20 rounds .....	129
Figure 4.29	Regret Matching Learning Strategy Utilities for differing benefits	129
Figure 4.30	Bounded Rationality Learning Strategy Utilities for 20 rounds	129
Figure 4.31	Bounded Rationality Learning Strategy Utilities for differing benefits .....	130

## LIST OF TABLES

	Page
Table 2.1 Desirable Security and Operational Properties of Blockchain Protocols . . . . .	46
Table 2.2 Game Theory Applications in Network Security . . . . .	53
Table 2.3 Game Theoretic Applications in Different Domains of Information Security . . . . .	55
Table 3.1 Benefits and costs of network and attacker . . . . .	81

## LIST OF ABBREVIATIONS

Abbreviation	Description
ABS	Agent Based Simulation
BFT	Byzantine fault tolerance
BGP	Byzantine Generals Problem
DES	Discrete Event Simulation
DMS	Dynamic Micro Simulation
DoS	Denial of Service
EFBP	El Farol Bar Problem
IDS	Intrusion Detection Systems
IoT	Internet of Things
IP	Intellectual Property
MABS	Multi Agent Based Simulation
NFT	Non-fungible tokens
OOS	Object Oriented Simulation
PBFT	Practical Byzantine fault tolerance
PoA	Price of Anarchy
PoM	Price of Malice
PoW	Proof of Work
UNL	Unique Node List

## LIST OF APPENDICES

Appendix	Description	Page
Appendix A	Game Theoretic Definitions .....	139
Appendix B	Additional Simulation Results .....	142
Appendix C	Digital Document and Simulation Code .....	151