UTILIZING A GAME THEORETICAL APPROACH TO PREVENT COLLUSION AND INCENTIVIZE COOPERATION IN CYBERSECURITY CONTEXTS

by

Arash Golchubian

A Thesis Submitted to the Faculty of

The College of Engineering and Computer Science

in Partial Fulfillment of the Requirements for the Degree of

Master of Science

Florida Atlantic University

Boca Raton, FL

December 2017

Copyright 2017 by Arash Golchubian

UTILIZING A GAME THEORETICAL APPROACH TO PREVENT COLLUSION AND INCENTIVIZE COOPERATION IN CYBERSECURITY CONTEXTS

by

Arash Golchubian

This thesis was prepared under the direction of the candidate's thesis advisor, Dr. Mehrdad Nojoumian, Department of Computer & Electrical Engineering and Computer Science, and has been approved by the members of his supervisory committee. It was submitted to the faculty of the College of Engineering and Computer Science and was accepted in partial fulfillment of the requirements for the degree of Master of Science.

SUPERVISORY COMMITTEE:

Dec 11, 2017

Mehrdad Nojoumian, Ph.D.
Thesis Advisor

Reza Azarderakhsh, Ph.D.

Nurgun Erdol, Ph.D.
Chair, Department of Computer & Electrical Engineering and Computer Science

Elias Bou-Harb, Ph.D.

Stella N. Batalama, Ph.D.
Dean, The College of Engineering and Computer Science

Deborah L. Floyd, Ed.D.
Dean, Graduate College

December 12 2017
Date

ACKNOWLEDGEMENTS

I would first and foremost like to express my deepest gratitude to my thesis advisor Dr. Mehrdad Nojoumian whose support and insightful counsel has guided me through my Master's studies at Florida Atlantic University. I am grateful for all of the hours Mehrdad has spent on this thesis, for helping me through the difficult challenges of my research, and for the interesting lectures which made understanding cryptography, secret sharing, and game theory easy and interesting. I am forever in his debt for everything he has taught me.

I would like to take this opportunity to send my thanks to Dr. Reza Azarderakhsh and Dr. Elias Bou-Harb who accepted to review my work as defense committee members. I would also like to extend my appreciation to all of the teachers and professors who have been a source of inspiration and whose encouragement and positive attitude motivated me to follow this path of higher education. I am forever grateful to all of them, for I would not have been where I am today without their guidance.

My deep appreciation goes to Mike O'Connor, my manager and colleague at Motorola Solutions Inc. He has been supportive and encouraging throughout both my professional and academic careers. He has allowed me the freedom to pursue my academic ambitions and given me opportunities to grow and follow my interests at work. He is more than my manager and colleague, I am lucky to have his friendship.

I am highly thankful for the wonderful staff of Florida Atlantic University for helping to guide me through the process and procedures of the university. Your friendly attitude and general willingness to help, made my experience an enjoyable and positive memory.

Finally, I would like to thank my family and friends. My amazing wife, Sanaz Imen, for the love and support she has given me throughout this experience and for encouraging me to pursue my graduate studies. I could not have done this without her. My mother, Mina

Ellini, for the deep and unconditional love she has given me and for teaching me to never give up. My brother, Kurosh Golchubian, for always being supportive and encouraging. My best friends, Felix and Lissette Redensky, for always being there whenever I need them. I consider myself fortunate to have such wonderful people in my life. I would have been lost without them.

The results of this research appear in the following publications:

[1] Arash Golchubian and Mehrdad Nojoumian. “A Survey of Game Theoretic Network Security”. Submitted to the International Journal of Game Theory (IJGT), 18 pages, Nov 07, 2017. (Under Review).

[2] Mehrdad Nojoumian, Arash Golchubian, Laurent Njilla, Kevin Kwiat, and Charles Kamhoua. “Incentivizing Blockchain Miners to Avoid Dishonest Mining Strategies By a Reputation-Based Paradigm”. In: To appear in IEEE Computing Conference (CC). London, UK: IEEE, 2018. (Accepted To Be Published).

[3] Mehrdad Nojoumian, Arash Golchubian, Nico Saputro, and Kemal Akkaya. “Preventing Collusion Between SDN Defenders and Attackers Using a Game Theoretical Approach”. In: Infocom: Adv in Software Defined & Context Aware Cognitive Radio Net. Atlanta, USA: IEEE, 2017, 6 pages. (Accepted To Be Published).

ABSTRACT

Author:	Arash Golchubian
Title:	Utilizing a Game Theoretical Approach to Prevent Collusion and Incentivize Cooperation in Cybersecurity Contexts
Institution:	Florida Atlantic University
Thesis Advisor:	Dr. Mehrdad Nojoumian
Degree:	Master of Science
Year:	2017

In this research, a new reputation-based model is utilized to disincentivize collusion of defenders and attackers in Software Defined Networks (SDN), and also, to disincentivize dishonest mining strategies in Blockchain. In the context of SDN, the model uses the reputation values assigned to each entity to disincentivize collusion with an attacker. Our analysis shows that *not-colluding* actions become Nash Equilibrium using the reputation-based model within a repeated game setting. In the context of Blockchain and mining, we illustrate that by using the same socio-rational model, miners not only are incentivized to conduct honest mining but also disincentivized to commit to any malicious activities against other mining pools. We therefore show that *honest mining* strategies become Nash Equilibrium in our setting.

This thesis is laid out in the following manner. In chapter 2 an introduction to game theory is provided followed by a survey of previous works in game theoretic network security, in chapter 3 a new reputation-based model is introduced to be used within the context of a Software Defined Network (SDN), in chapter 4 a reputation-based solution concept is introduced to force cooperation by each mining entity in Blockchain, and finally, in chapter 5, the concluding remarks and future works are presented.

To:

My loving wife, Sanaz. You inspire me to better myself.

and

My mother, Mina. You showed me that nothing is impossible.

UTILIZING A GAME THEORETICAL APPROACH TO PREVENT COLLUSION AND INCENTIVIZE COOPERATION IN CYBERSECURITY CONTEXTS

List of Tables xii

List of Figures xiii

1 Introduction 1

1.1 An Introduction to Game Theory 3

1.1.1 The Prisoner's Dilemma 4

1.1.2 Game Theory Preliminaries 5

1.1.3 Classifications 7

2 Survey of Game Theoretic Network Security 9

2.1 Game Theory as Applied to Network Security 9

2.1.1 Intrusion Detection 10

2.1.2 Sensor Networks 12

2.1.3 Attacks on Network Infrastructure 13

2.1.4 Attacker Defender Models 14

2.1.5 Coalitions 15

2.1.6 Risk Assessment 15

2.2 Previous Surveys 17

2.3 Summary of reviewed works 19

3 Disincentivizing Collusion Between SDN Defenders and Attackers 20

3.1 Introduction 20

3.2 Literature Review 22
3.2.1 Game-Theoretical Approaches to SDN Security 22
3.2.2 SDN-Based MTD 23
3.3 Game-Theoretical Construction 25
3.3.1 Model Description 25
3.3.2 Our Solution in a Nutshell 26
3.3.3 Formalizing Our Solution 28
3.3.4 Utility Assumptions 29
3.3.5 Utility Function and Mathematical Analysis 30
3.4 Conclusion 34

4 Incentivizing Honest Mining in Blockchain 35
4.1 Introduction 35
4.2 Preliminaries 37
4.2.1 Digital Currencies: Terminologies and Mechanics 37
4.3 Literature Review 39
4.4 Reputation-Based Mining Model and Setting 41
4.5 Mining in Our Reputation-Based Model 44
4.5.1 Prevention of the Re-Entry Attack 44
4.5.2 Technical Discussion on Detection Mechanisms 45
4.5.3 Colluding Miner's Dilemma 47
4.5.4 Repeated Mining Game 49
4.5.5 Colluding Miners' Preferences 50
4.5.6 Colluding Miners' Utilities 51
4.6 Game-Theoretical Analyses of Our Model 51
4.7 Conclusion 53

5 Concluding Remarks and Future Directions 54

5.1 Future Directions 55
5.2 An Expansion of Reputation-Based Repeated Games 55

LIST OF TABLES

1.1 Prisoner's Dilemma - Payoff Matrix 5

1.2 Prisoner's Dilemma - Perspectives 5

1.3 Prisoner's Dilemma - Dominant Strategy 6

2.1 Summary of Literature 19

3.1 Two Defenders Who Intend to Collude With the Attacker 27

3.2 Collusion Game Between Two Defenders in the Socio-Rational Model . . . 32

4.1 Payoff in Colluding Miner's Dilemma 48

4.2 Game Between Two Miners 52

LIST OF FIGURES

1.1 Zero-Day Vulnerabilities by Year [8] 2

2.1 Information Warfare Game Model [25] 10

2.2 Classification of Research 11

2.3 Classification of game theory proposed by [61] 16

2.4 Taxonomy Based on Game Theory for Wireless Sensor Networks (WSNs) Security [63] 17

2.5 Relationship among game theory application in network security [64] . . . 18

4.1 Blockchain and Mining 38

4.2 Architecture of Our Reputation-Based Setting 42

ACRONYMS

AOAR Automatic or Administrator Response. 11

CERT United States Computer Emergency Response Team. 1, 20

DDoS Distributed Denial of Service. 1, 20, 21, 25, 26, 36, 39, 41, 45, 47

DNS Domain Name Servers. 1, 24

DoS Denial of Service. 13, 14, 18, 22

IDS intrusion detection system. 11–13

IoT Internet-of-Things. 1, 12

IRMA Interference Mitigation Risk Aware. 12

MAD Mutualy Assured Destruction. 7

MTD Moving Target Defense. 20–23, 25

NAT Network Address Translation. 23

NFC Near Field Communication. 12

NFV Network Function Virtualization. 20

RAD Routing Around Decoys. 14

RFID Radio Frequency Identification. 12

SDN Software-Defined Networking. 2, 20–25, 27, 28, 30, 33, 34, 56

SIS Secure Implicit Sampling. 13

SMT Satisfiability Module Theories. 23, 24

SSG Stackelberg security game. 15

WSN Wireless Sensor Network. xi, 13, 17, 18

CHAPTER 1

INTRODUCTION

Network security is essential in today's age of constant threat from hackers all around the world. As our world has become more connected through the advent of Internet connected devices and the introduction of the Internet-of-Things (IoT), the avenues of attack which are exploitable by a malicious player have increased as well. The damage that these attackers cause to the systems we use each and every day have an extremely high cost and that cost is often unrecoverable. The recent high profile Equifax breach, where the private financial data of at least 143 million Americans was compromised [4], is one example of a loss which will have years of impact on the lives of those that were affected. There are numerous organizations that work around the clock to combat these attacks including government agencies like the United States Computer Emergency Response Team (CERT), and private companies such as Symantec, McAfee, and Kaspersky. It is through the efforts of such organizations that society is able to enjoy the benefits of a connected world. Juniper Research estimated the annual cost of criminal data breaches will reach a mind bending two trillion dollars by 2019 [5]. Some government entities are reporting equally astonishing numbers; the state of Utah's government has reported that the facilities operated by the government in the state experience upwards of 300 million attacks per day.

These attacks do not stop at attempts to steal information, in October of 2016 a large scale Distributed Denial of Service (DDoS) attack on the Dyn Domain Name Servers (DNS) cause the United States' east coast to temporarily loose access to major websites such as Twitter and Reddit [6]. This attack was aimed at the infrastructure of the Internet and took advantage of security flaws which existed in some IoT devices such as video recorders and digital cameras [7].

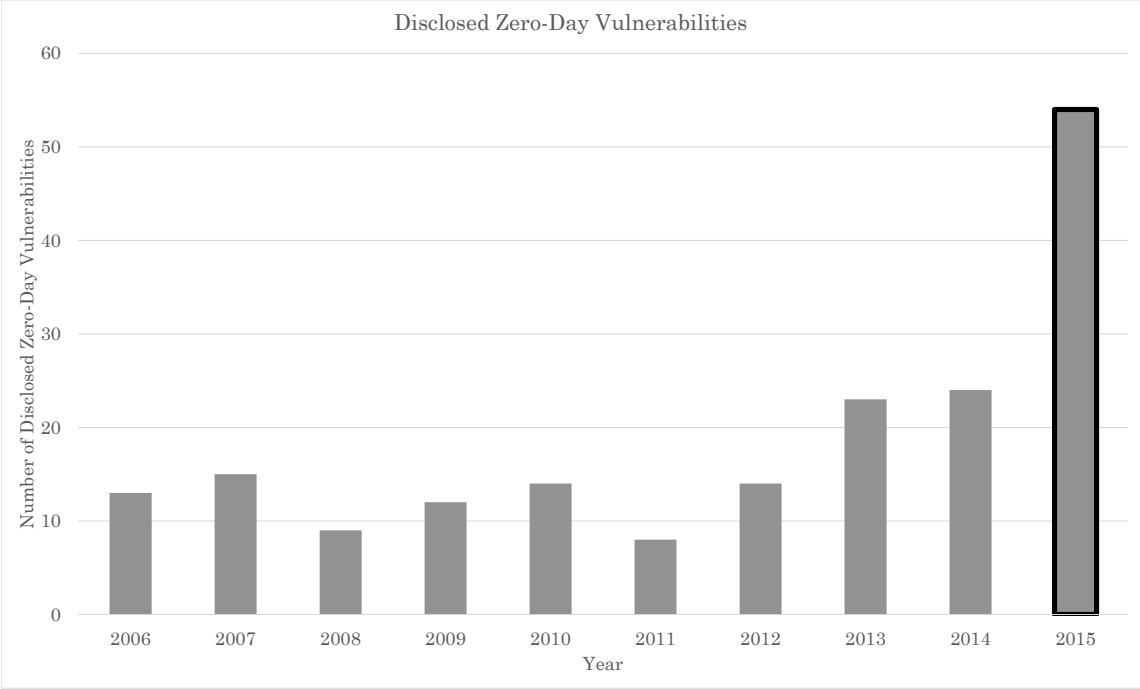


Figure 1.1: Zero-Day Vulnerabilities by Year [8]

The endless struggle between the security research teams and engineers who patch the software and the hackers that are becoming more clever with every attack has not been going well for the defenders. By 2015, the number of Zero-Day exploits used by hackers had reached fifty four [8]. In more recent years, the use of zero-day vulnerabilities has become less common with more attacks hiding in plain site [9].

As the challenges in keeping a network secure have become ever greater in the face of an increasing number of attempted hacks, the field of network security has begun to turn its attention to game theoretic approaches to provide a mathematical framework for the quantitative analysis of the inherent security within network systems. These methods are helpful in quickly analyzing thousands of different strategies to mitigate on going attacks. Additionally, and perhaps more importantly, game theoretic methods are being used to modify the strategies employed to lower the benefits an attacker may get from successfully breaching a network reducing the incentive for network attacks.

In this thesis two collusion problems will be studied by utilizing game theoretic tech-

niques. The first is collusion between Software-Defined Networking (SDN) defenders and attackers, and the second is collusion between miners in a Bitcoin mining pool. Both of these problems are studied and a reputation based, game theoretic model is applied to force cooperation amongst players.

The rest of this thesis is organized as follows. In section 1.1 a survey of previous works in game theoretic network security is presented. Chapter 3 introduces a solution to defender and attacker collusion problems within the context of an SDN. Chapter 4 shows how to incentivize honest mining in Blockchain by using a reputation-based trust model. Chapter 5 contains concluding remarks and ideas for future study.

1.1 AN INTRODUCTION TO GAME THEORY

Game theory is a branch of mathematics concerned with the study of mathematical models used for competitive and cooperative games when the players involved are rational. These games are commonly used to discuss many different subjects such as politics, economics, and military situations. The use of game theoretic games to model strategies are older than the modern day mathematical field by centuries. The earliest reference to such a mathematical analysis can be traced to Waldegrave's Problem originally known as Problme de la Poulle or the Problem of the Pool [10]. This was originally published by Pierre Rmond de Montmort in 1713 [11] where he discusses corresponding with a gentleman named Waldegrave about two probability problems involving card games. This is the first appearance of a mixed strategy solution to a two player game. In a 1787 essay, *Vices of the Political System of the United States*, Madison [12] discusses the political and tax system of the united states by using rational arguments and games which are similar to those found in modern day game theory.

Modern Day Game theory did not exist as a unique branch of mathematics until a publication by John Von Neumann in 1928 [13] formalized the idea of a game and provided a proof for the famous Minimax theorem. He later expanded on these ideas in his book

Theory of games and economic behavior [14] which he co-authored with the German economist Oskar Morgenstern. This book set the fundamental framework for analyzing and solving two-person zero-sum games. However, the work done by Von Neumann and Morgenstern was only sufficient for analysis of cooperative games.

In his PhD dissertation [15], John Nash introduced the equilibrium ideas which are general enough to handle both cooperative and non-cooperative games. This equilibrium theory is now known as the Nash equilibrium and is central to almost all cooperative and non-cooperative game theoretical analyses. Nash further expanded on his ideas in several publications between 1950 and 1953 [16, 17, 18].

1.1.1 The Prisoner's Dilemma

The most basic academic case that is studied in game theory is the prisoners dilemma; first framed and discussed by Merrill Flood and Melvin Dresher while working for the Rand Corporation. This research was in an attempt to use game theory in setting a global nuclear strategy [19]. In this game we imagine that there are two suspects who are assumed to be partners in a crime. The police separate the two suspects and give both of them the same choices. If one confesses and the other does not, then the person who confesses is set free, while the other is sent to jail for three years. If both players stay silent then they will both go to jail for one year. If they both confess, then each will serve 2 years. The game theoretic approach to solving for what is known as a dominant strategy is to place the outcomes into a matrix and calculate the utility of each choice given different conditions. We set the utility for being set free at +1, a one year sentence will be given a utility of 0, a two year sentence will be given a utility of -1, and a three year sentence will be given a utility of -2.

The game is now analyzed from the perspective of prisoner 1 and keep in mind that prisoner 2 would have an equivalent outcome since this game is symmetrical. Prisoner 1 will think about what prisoner 2 could do. 1) prisoner 2 confesses. According to the above matrix, prisoner 1 would be better off confessing since that will result in a 1 year sentence.

P_2 / P_1	$\mathscr{C}$: Quiet	$\mathscr{D}$: Confess
$\mathscr{C}$: Quiet	$(0,0)$	$(-2,+1)$
$\mathscr{D}$: Confess	$(+1,-2)$	$(-1,-1)$

Table 1.1: Prisoner's Dilemma - Payoff Matrix

2) prisoner 2 stays silent. Again according to the matrix it would be better for prisoner 1 to confess since that would set him free. What prisoner 1 discovered is that it doesn't matter what prisoner 2 does because it is always better to confess. This is known as a dominant strategy and it along with Nash equilibrium are fundamental principals when discussing and analyzing games of strategy.

Player 1's Best Choice

P_2 / P_1	$\mathscr{C}$: Quiet	$\mathscr{D}$: Confess
$\mathscr{C}$: Quiet	$(0,0)$	$(-2,+1)$
$\mathscr{D}$: Confess	$(+1,-2)$	$(-1,-1)$

Player 2's Best Choice

P_2 / P_1	$\mathscr{C}$: Quiet	$\mathscr{D}$: Confess
$\mathscr{C}$: Quiet	$(0,0)$	$(-2,+1)$
$\mathscr{D}$: Confess	$(+1,-2)$	$(-1,-1)$

Table 1.2: Prisoner's Dilemma - Perspectives

1.1.2 Game Theory Preliminaries

A *game* consists of a set of *players*, a set of *actions* and *strategies* (that is, the way of selecting actions in different rounds of the game), and finally, a *pay-off function* which is used by players to calculate their utilities. In *cooperative games*, the players collaborate and

P_1 \ P_2	$\mathscr{C}$: Quiet	$\mathscr{D}$: Confess
$\mathscr{C}$: Quiet	$(0,0)$	$(-2,+1)$
$\mathscr{D}$: Confess	$(+1,-2)$	$(-1,-1)$

Table 1.3: Prisoner's Dilemma - Dominant Strategy

split the total utility among themselves. In other words, cooperation is always enforced by agreements among players. However, in *non-cooperative games*, the players cannot reach an agreement to coordinate their behavior, that is, any cooperation must be self-enforcing. Next, some game-theoretic definitions are briefly reviewed [20] for our further technical discussions.

Definition 1 *Let* $A \stackrel{\text{def}}{=} A_1 \times \cdots \times A_n$ *be an action profile for n players, where* A_i *denotes the set of possible actions for player* S_i*. A* game $\Gamma = (A_i, u_i)$ *for* $1 \leq i \leq n$*, consists of* A_i *and a utility function* $u_i : A \mapsto \mathbb{R}$ *for each player* S_i*. An* outcome of the game *is then a vector of actions* $\vec{a} = (a_1, \ldots, a_n) \in A$*.*

Definition 2 *The* utility function u_i *illustrates the preferences of player* S_i *over different outcomes. We say player* S_i prefers *outcome* $\vec{a}$ *over* $\vec{a}'$ *iff* $u_i(\vec{a}) > u_i(\vec{a}')$*, and he* weakly prefers *outcome* $\vec{a}$ *over* $\vec{a}'$ *if* $u_i(\vec{a}) \geq u_i(\vec{a}')$*.*

In order to allow the players S_i *to follow randomized strategies (where the strategy is the way of choosing actions), we define* σ_i *as a probability distribution over* A_i *for a player* S_i*. This means that he samples* $a_i \in A_i$ *according to* σ_i*. A strategy is said to be a pure-strategy if each* σ_i *assigns probability* 1 *to a certain action, otherwise, it is said to be a mixed-strategy. Let* $\vec{\sigma} = (\sigma_1, \ldots, \sigma_n)$ *be the vector of players' strategies, and let* $(\sigma_i', \vec{\sigma}_{-i}) \stackrel{\text{def}}{=} (\sigma_1, \ldots, \sigma_{i-1}, \sigma_i', \sigma_{i+1}, \ldots, \sigma_n)$*, where player* S_i *replaces* σ_i *by* σ_i' *and all the*

other players' strategies remain unchanged. Therefore, $u_i(\vec{\sigma})$ denotes the expected utility of S_i under the strategy vector $\vec{\sigma}$. A player's goal is to maximize $u_i(\vec{\sigma})$. In the following definition, one can substitute an action $a_i \in A_i$ with its probability distribution σ_i or vice versa.

Definition 3 *A vector of strategies $\vec{\sigma}$ is a* Nash Equilibrium *if, for all i and any $\sigma_i' \neq \sigma_i$, it holds that $u_i(\sigma_i', \vec{\sigma}_{-i}) \leq u_i(\vec{\sigma})$. This means no one gains any advantage by deviating from the protocol as long as the others follow the protocol.*

Definition 4 *Let $\mathscr{S}_{-i} \stackrel{\text{def}}{=} \mathscr{S}_1 \times \cdots \times \mathscr{S}_{i-1} \times \mathscr{S}_{i+1} \times \cdots \times \mathscr{S}_n$. A strategy $\sigma_i \in \mathscr{S}_i$ (or an action) is* weakly dominated *by $\sigma_i' \in \mathscr{S}_i$ (or another action) with respect to $\mathscr{S}_{-i}$ if:*

1. *For all $\vec{\sigma}_{-i} \in \mathscr{S}_{-i}$, it holds that $u_i(\sigma_i, \vec{\sigma}_{-i}) \leq u_i(\sigma_i', \vec{\sigma}_{-i})$.*
2. *There exists a $\vec{\sigma}_{-i} \in \mathscr{S}_{-i}$ s.t. $u_i(\sigma_i, \vec{\sigma}_{-i}) < u_i(\sigma_i', \vec{\sigma}_{-i})$.*

This means player P_i can never improve its utility by playing σ_i, and he can sometimes improve it by not playing σ_i. A strategy $\sigma_i \in \mathscr{S}_i$ is strictly dominated *if player P_i can always improve its utility by not playing σ_i.*

1.1.3 Classifications

Games are split into two main groups. The fist is a non-cooperative game where there are no binding agreements; the second is a cooperative game where binding agreements are allowed. This section will discuss the differences between these two top level types.

Non-Cooperative Games

Non-cooperative games are those in which there are no external forces or authorities to ensure that players remain honest. Instead these games rely upon ensuring that players have the proper incentive to remain honest, and the disincentive to keep them from defecting. These games are often solved by finding the Nash equilibrium where the players cannot

force a better outcome by changing only his/her own strategy. An example of such a game is the doctrine of Mutualy Assured Destruction (MAD). The name and acronym are credited to John Von Neumann who was a cold war strategist and known as the father of game theory [21]. The MAD doctrine states that because the Soviet Union and the United States both had enough nuclear weapons to completely annihilate each other, neither side had any reason to either disarm, or to escalate the standoff because if one were to fire, the other had no choice but to fire causing ones own demise.

Cooperative Games

Cooperative games have an external enforcer which ensures that players cooperate. The majority of cooperative games have a goal of predicting the coalitions which would be formed rather than the individual actions of players as is the goal with non-cooperative games [22, 23]. Cooperative games are not commonly used in field of security research and hence have a very limited scope within this survey.

CHAPTER 2

SURVEY OF GAME THEORETIC NETWORK SECURITY

In this chapter a survey of previous works concerning the application of game theory to the field of network security is provided. This chapter categorizes the publications into six categories: Intrusion Detection, Sensor Networks, Attacks on Network Infrastructure, Attacker Defender Models, Coalitions, and Risk Assessment. The results of this chapter appear in [1].

2.1 GAME THEORY AS APPLIED TO NETWORK SECURITY

Network security has been thoroughly studied since the dawn of the computer age. The first network worm was released in 1987, before the popularization of computers and the Internet[24]. The first introduction of game theoretic methods to the analysis of computer and information security was made by the thesis of David A. Burke [25]. By expanding on the works of game theorists and nuclear strategists, Burke created a basic framework for applying game theory to the field of information warfare. The pyramid presented in Figure 2.1 illustrates the breakdown of Burke's classifications.

While Burke's efforts laid the foundation of applying game theory to information security over the Internet, it was not directly towards the analysis of network security. The Application of game theoretic approaches to this effort did not occur until 2002 when Akella et al. [26] introduced game theoretic approaches to the analysis of TCP. In this publication, the authors explored the effects of selfish behavior of network end-points on the stability of the Internet. It was suggested that while the older Internet technologies, at that time, are largely unaffected by selfish players, the newer Internet technologies and routers are

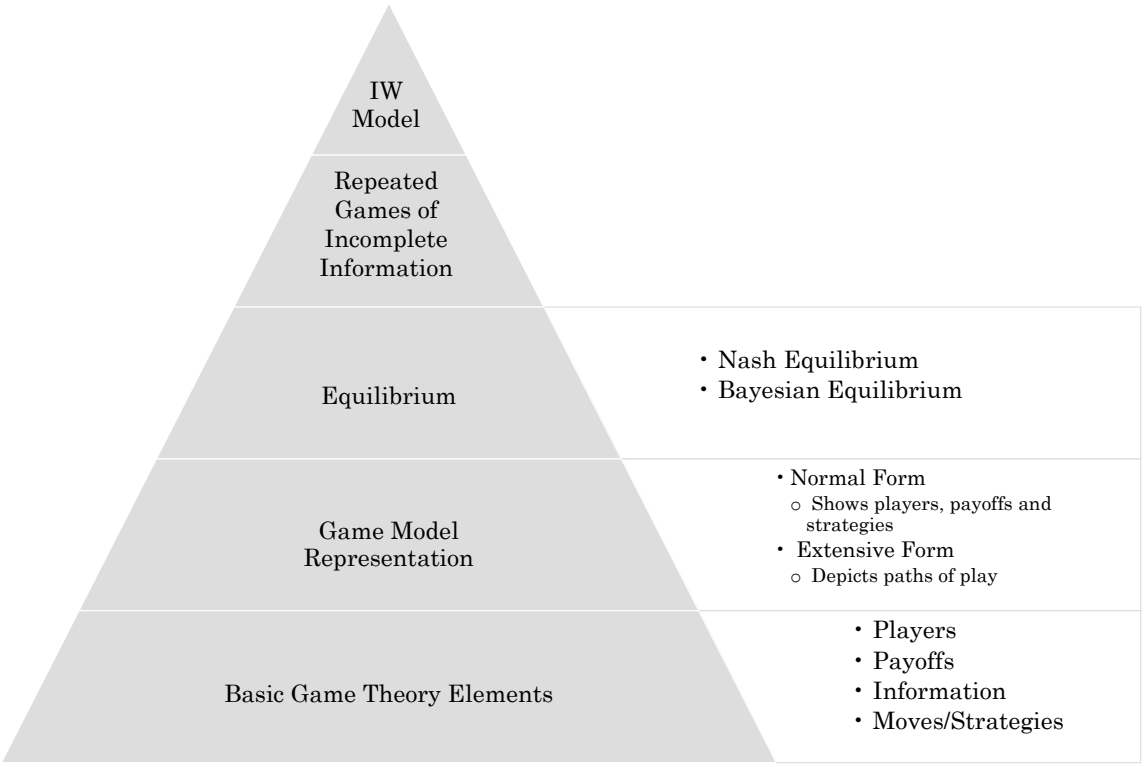


Figure 2.1: Information Warfare Game Model [25]

susceptible to these types of attacks and would be negatively impacted by selfish nodes.

The current network security related research which involves game theory can be broken down into six categories: Intrusion Detection, Sensor Networks, Attacks on Network Infrastructure, Attacker Defender Models, Coalitions, and Risk Assessment. The majority of current research is on non-cooperative zero-sum games, however there are very interesting topics being pursued by various researchers which use Markov, Bayesian, Stackelberg, and Cooperative games.

2.1.1 Intrusion Detection

Alpcan and Basar [27] produced an intrusion detection system (IDS), in a network of sensors, by using game theory to model the IDS behavior in a two person, nonzero-sum game. This work was further expanded upon by the same authors in 2004 [28], where they used the previously introduced framework to produce a game theoretic approach to intrusion

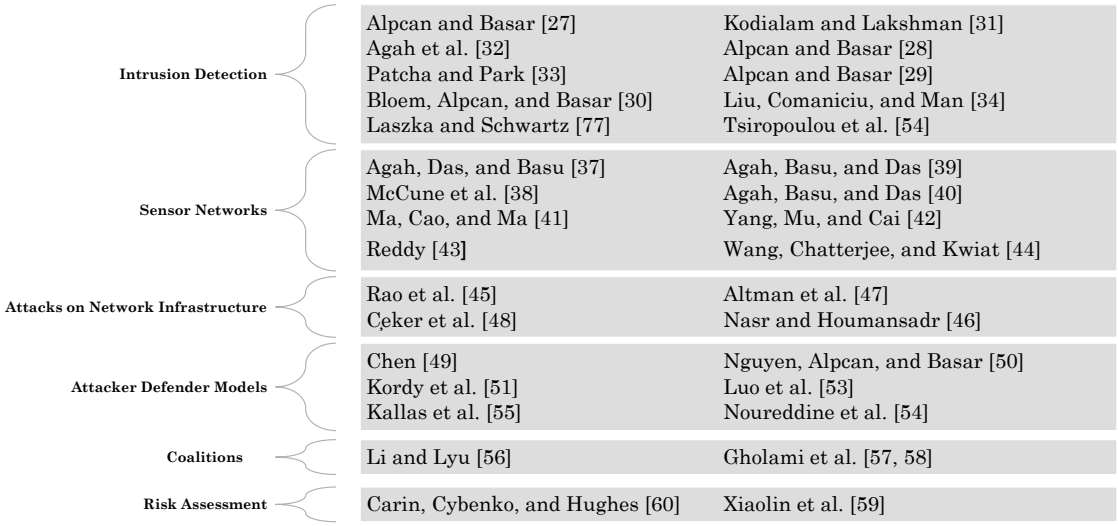


Figure 2.2: Classification of Research

detection in access control systems using both finite and continuous-kernel non-cooperative games. They further expanded on these works by using a 2-player zero-sum stochastic security game to extend this framework to a stochastic and dynamic one [29]. In 2006, Bloem, Alpcan, and Basar [30] arrived at the Automatic or Administrator Response (AOAR) algorithm by modeling the interactions between attackers and the IDS. It was also shown that the IDS performed better with the AOAR algorithm under all tested conditions. The authors did not provide a formal framework for this work and only presented the implementation.

There are several works which focus on the application of game theoretic models for the improvement of existing IDSs or to create specialized IDS for particular applications. Kodialam and Lakshman [31] used a game theoretic framework to optimize the attack strategy for injecting packets into a network and then optimized a sampling scheme using a game theoretic framework to maximize the chances of detecting the intruding packets while minimizing the sampling rate. Agah et al. [32] compared a game theoretic approach to a Markov Decision Process and a metric driven method. The authors show that the game theoretic approach significantly increases the odds of detecting an intrusion. Patcha and Park [33] introduced an IDS for use in Mobile Ad-hoc Networks by using a game theoretic model based on Bayesian games. Liu, Comaniciu, and Man [34] used Bayesian game theory

to produce an IDS for wireless Ad-hoc networks which minimized the power consumption while maximizing the detection rate. Laszka and Schwartz [35] presented a game theoretic model used for calculating security-breach probabilities and then shows that if all users are homogeneous there exists an equilibrium at which all honest players choose the same security level. This equilibrium is also shown to be unique for a fixed number of malicious players. The authors further showed that the security level is a decreasing function of the total number of malicious users.

IoT and the emergence of low powered connected devices such as Radio Frequency Identification (RFID) and Near Field Communication (NFC) have created a new and exciting avenue of research for security researchers. There is little research performed on the application of game theoretic models to RFID networks. Tsiropoulou et al. [36] uses a game theoretic approach to incentivize intruder nodes to behave in a more social manner. The authors used the theory of supermodular games to optimize the game and find the Nash equilibrium point of the Interference Mitigation Risk Aware (IRMA) problem discussed in the paper.

2.1.2 Sensor Networks

Securing a sensor network requires the application of a different set of techniques due to limitations in processing power, battery capacity, memory, and other resources [37]. The application of game theory to this field has been in an effort to produce more effective means of securing sensor networks while working within the constraints of the limited resources. In 2004, Agah, Das, and Basu [37] introduced a new method for clustering sensor nodes based on cooperative game theory. The proposed method is able to reduce the number of clusters and message passings compared with distance based clustering approaches. McCune et al. [38] presents a new method for broadcasting base stations to detect the failure of a node in receiving a message. The authors called this newly introduced method the Secure Implicit Sampling (SIS) and used a game theoretic approach in evaluating the scheme against an

optimized attacker.

Agah, Basu, and Das [39] presents a game theoretic framework for the prevention of Denial of Service (DoS) attacks by using an intrusion detection mechanism and forcing cooperation by imposing punishment on malicious nodes. In 2006, Agah, Basu, and Das [40], proposed two new game theoretic schemes for the prevention of DoS attacks. Ma, Cao, and Ma [41] used a non-cooperative game theoretic framework to enable a cluster head node to make the decision of activating the IDS. This is in an attempt to make the system more efficient by turning on the IDS only when needed and hence making it's application more suitable for WSNs. Improving upon the ideas introduced by Agah, Basu, and Das [40], Yang, Mu, and Cai [42] produced a new security scheme in which compromised nodes are considered to be rational and the payoff strategy is designed to force cooperation. Reddy [43] proposed a new framework for the detection of malicious nodes in the forward data path using a zero-sum game. Wang, Chatterjee, and Kwiat [44] employs a game theoretic approach to show that malicious nodes and regular nodes can co-exist if the malicious nodes cause less damage than they are contributing.

2.1.3 Attacks on Network Infrastructure

In Rao et al. [45] the authors examine attacks on both cyber components such as servers, routers, and switches as well as attacks focused on the physical infrastructure needed to maintain the cyber infrastructure functioning such as cooling and power systems. The authors analyze the attack-defense model using a Boolean attack-defense model. In this Boolean model, the attacker chooses to attack either the cyber components, or the physical components but not both. This is regardless of the attacker having knowledge that both parts are necessary to maintain the cyber physical system functioning. The authors further explore the game-theoretic scenarios by taking the probabilities of an attack on each part and its chances of success into account. These however only provided a basic analysis of cyber infrastructure and the authors suggest that they be extended by 1) explicitly modeling the

cyber and physical components, 2) bounding the total costs of reinforcements and attacks.

In Nasr and Houmansadr [46] the authors investigate the usefulness and effectiveness of decoy routing and Routing Around Decoys (RAD) attack. This publication examines two real-world models of decoy routing deployments. The first model is a central model much like Tor and a distributed deployment in which decoy deployment is decided upon by the autonomous systems based on economic interests. They examine the use of decoy routing by optimizing the placement of decoys through the use of game-theoretic modeling and finding optimal censorship actions for each case. Altman et al. [47] studied a parallel link network in which the controller is malicious. The authors used a game theoretic framework and show that there are not any saddle points since the cost is convex for both the minimizer and maximizer. The max-min problem is then solved using a water-filling algorithm and a new algorithm, which the authors name water-distributed algorithm, is proposed for finding a solution to the min-max problem.

DoS attacks are a amongst some of the older, and most common, types of attacks on network and cyber infrastructure. DoS attacks are launched with the aim of blocking legitimate traffic from getting to and from a server. Çeker et al. [48] uses a signaling game with Perfect Bayesian equilibrium to study the strategies that can be used to mitigate DoS attacks.

2.1.4 Attacker Defender Models

In his 2007 thesis, Chen [49], used game theory to optimize the strategy an administrator should use when defending against an importance scanning worm. Nguyen, Alpcan, and Basar [50] introduced models for the analysis of attack and defense strategies in situations where there is imperfect information. Kordy et al. [51] showed that attack-defense trees, an expansion of attack trees which was popularized by Schneier [52], and two-player binary zero-sum extensive form games are equivalent and can be used interchangeably. Luo et al. [53] produced a multi-stage intrusion defense system by optimizing the classical attack tree

approach at each stage. This produced an improvement in the total loss the system suffered from each attack. Noureddine et al. [54] used game theory to produce a response engine to respond to an attacker moving laterally through an enterprise network in an effort to prevent the breach of sensitive network nodes. In Kallas et al. [55], the authors develop an optimized consensus algorithm which is capable of making a correct detection even in the presence of corrupted measurements. The publication also addresses scenarios in which the attacker knows what the defender's strategy is and will attempt to stay below the detection threshold.

2.1.5 Coalitions

Li and Lyu [56] presents a new game theoretic framework for the application of coalition games to wireless network security. The authors also provide an algorithm for coalition formation and show that the convergence to coalition formation is achieved very quickly and that the coalitions can be of significant size. In Gholami et al. [57, 58] a social Stackelberg security game (SSG) is observed by using Amazon's Mechanical Turk. SSGs are games where the defender is in a leadership position and the attacker is a follower of the defending player. In other words, the defender makes the first move and then the attacker makes a move based on the leaders action. While this social defender/attacker scenario is not directly related to the field of networking, the results are quite interesting in that they reveal a method for disincentivizing collusion through the introduction of an imbalance in defense resources. The authors are able to show that when an imbalance is introduced into the defense strategy, it will disincentivize the attackers from forming collusive attacks because it places one attacker into a better position than the other attackers and hence the attacker refuses to collude.

2.1.6 Risk Assessment

The assessment of security threats on a network is of great importance and has been thoroughly studied in the field of cyber security research. However, the application of

game theory to this field is rare and the field could benefit from further research. In 2008, Xiaolin et al. [59] proposed a model for risk assessment on a systemic basis by using Markov game theory. The authors provided a method to provide remediation schemes to minimize the total risk of the system. While this publication provides a basic framework for the application of game theory to risk assessment in network security, it does not provide any specifics for different types of security risks such as worms, viruses, Trojans, etc. Another aspect which can be considered is the economics of cyber security. Carin, Cybenko, and Hughes [60] used game theory in conjunction with a Markov decision process to produce a new method for cyber security risk assessment called Quantitative Evaluation of Risk for Investment Efficient Strategies. The authors were mainly concerned with defining strategies for protection investment of intellectual property within complex systems.

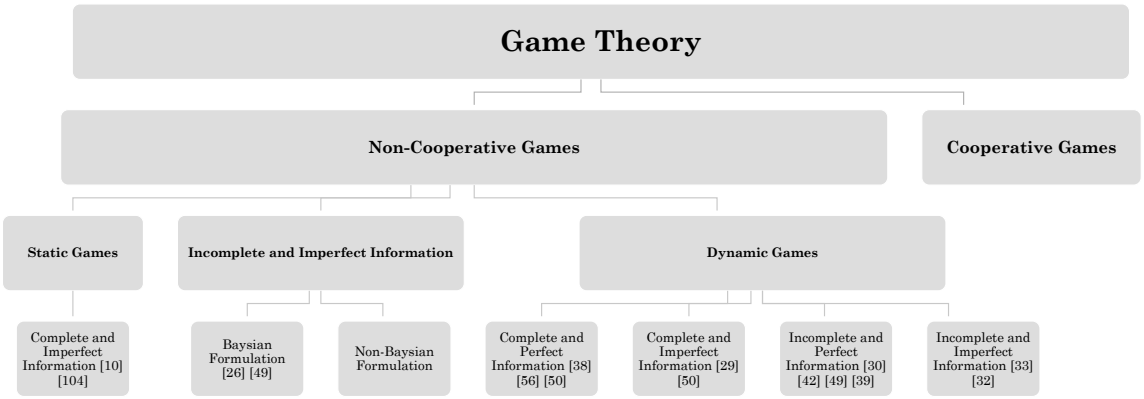


Figure 2.3: Classification of game theory proposed by [61]

2.2 PREVIOUS SURVEYS

Hamilton et al. [62] identified the areas of game theory relevant to information warfare, and presented an example of these techniques in action. Roy et al. [61] reviewed the existing game theoretic solutions which are designed to enhance network security and presented a taxonomy for classifying the proposed solutions. Their proposed classification is shown in Figure 2.3. Some of the limitation of the research in that time was: (a) the stochastic game models at that time only consider perfect information and assume that the defender is always able to detect attacks; (b) the stochastic game models at that time assume that the state transition probabilities are fixed before the game starts and these probabilities can be computed from the domain knowledge and past statistics; (c) the game models at that time assume that the player's actions are synchronous, which is not always realistic; (d) Most models were not scalable with the size and complexity of the system under consideration.

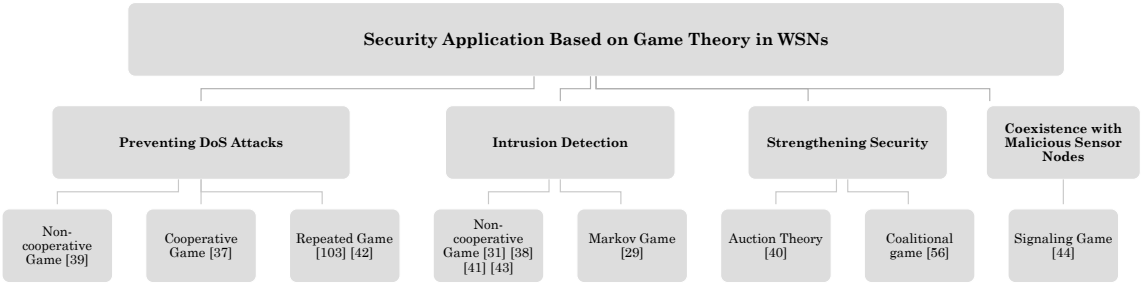


Figure 2.4: Taxonomy Based on Game Theory for WSNs Security [63]

Shen et al. [63] presented a survey of security approaches based on game theory in WSNs. According to different applications, they proposed a taxonomy, which divides current existing typical game-theoretic approaches for WSNs security into four categories: preventing DoS attacks, intrusion detection, strengthening security, and coexistence with malicious sensor nodes.

Liang and Xiao [64] classified the applications of game theory in network security into two categories: (1) Applications for analysis of network attack-defense, (2) applications

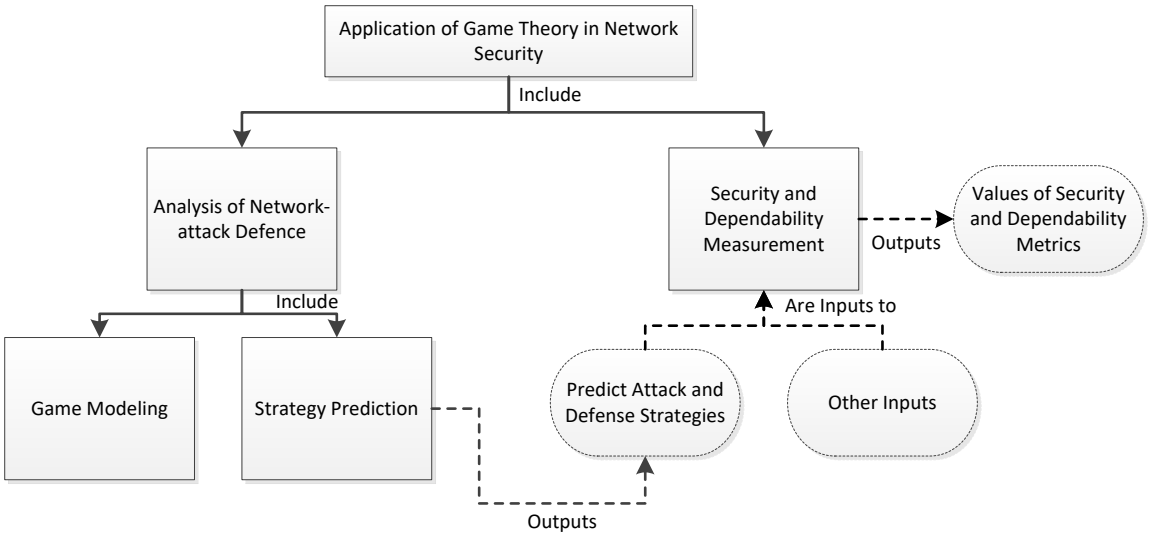


Figure 2.5: Relationship among game theory application in network security [64]

for network security and dependability measurement. They also classified the modeling of game theoretic approaches to network security into two categories including cooperative and non-cooperative games and discussed the limitations of existing game theoretic approaches.

2.3 SUMMARY OF REVIEWED WORKS

The following table summarizes the classification of publications reviewed in this survey.

	Papers	Categories	Non-Zero Sum	Zero Sum	Stochastic	Bayesian	Complete Information	Perfect Information
Cooperative	[37] [56]	Sensor Networks, Coalitions						
Non-cooperative	[41] [42] [45]	Sensor Networks, Attacks on Network Infrastructure	✓	✓				
	[65]	Attacker Defender Models, Moving Target Defense	✓		✓			
	[53]	Attacker Defender Models	✓		✓		✓	✓
	[33] [30]	Intrusion Detection	✓			✓		✓
	[34]	Intrusion Detection	✓			✓		
	[27] [32] [28] [39] [40] [53] [46] [36] [35]	Intrusion Detection, Sensor Networks, Attacks on Network Infrastructure	✓					
	[59]	Risk Assessment		✓	✓		✓	✓
	[29]	Intrusion Detection		✓	✓			
	[43]	Sensor Networks		✓		✓		
	[31]	Intrusion Detection		✓			✓	✓
	[49]	Attacker Defender Models		✓				✓
	[60]	Risk Assessment		✓			✓	
	[38] [47] [51] [55] [54] [58] [57]	Sensor Networks, Attacks on Network Infrastructure, Attacker Defender Models, Coalitions		✓				
	[44] [48]	Sensor Networks, Attacks on Network Infrastructure				✓		

Table 2.1: Summary of Literature

CHAPTER 3

DISINCENTIVIZING COLLUSION BETWEEN SDN DEFENDERS AND ATTACKERS

In this chapter the concept of a reputation-based trust model is applied to the problem of attacks within SDNs where the network switches are taken over by an adversary and used to disrupt network flow by colluding with the attackers and not following the instructions of the controller. We show that by employing a socio-rational model within a repeated game setting the defenders (switches) are incentivized not to collude with attackers. The results of this chapter appear in [3].

3.1 INTRODUCTION

SDN has enjoyed tremendous popularity growth in the last few years. Everyday, more networks are migrated to use the SDN instead of traditional networking technologies because of its numerous advantages such as manageability, flexibility in network design and scalability [66]. This is partially driven by the demand for better, faster and more complex content delivery for today's advanced web applications. More importantly, the SDN has started to be used for securing the networks by integrating ideas from Moving Target Defense (MTD) and Network Function Virtualization (NFV) paradigms [67]. The MTD provides a different perspective to secure the networks, which is one of the major issues in today's highly connected cyberspace. For this reason, government organizations such as CERT as well as private security companies, such as Symantec, McAfee and Kaspersky, spend hundreds of thousands of man-hours researching and mitigating security vulnerabilities in Internet-connected devices. A recent projection by Juniper Research estimates that the

annual cost of data breaches will reach to two trillion dollars per year by 2019 [5].

The MTD paradigm simply applies continuous changes to the underlying network infrastructure in order to make it harder for the attackers to launch attacks. It heavily relies on the capabilities of the SDN. Furthermore, it utilizes the SDN controller and switches to apply certain changes such as route mutation, port and address mutation, service relocation, and configuration updates [68, 69]. Using such mechanisms, the MTD can be an effective means to thwart the DDoS attack, which is very difficult to be handled by traditional techniques. In all these approaches, the SDN controller and switches are assumed to be trusted and not to be compromised by the attackers. It is important to note that within the context of SDN, the term "route" is not reserved to routers as it is in a traditional network. In SDN, the term route refers to the control flow operation that is ordered by the SDN controller to determine the route packets take through the network and a route mutation refers to an order issued by the SDN controller to change the flow of packets to a different node of the network.

However, the assumption that the controller and switches are trusted may not be true in many cases. One threat vector of importance is the exploitation of weaknesses in the security of switches [70]. If compromised, a single switch can help the attacker to control the flow of traffic on the entire network by modifying the behavior of the switch. As a result, the switch will not respond (in an expected manner) to the instructions that are sent by the SDN controller. This can be exploited by the attacker to bring the network to a crawling halt. In particular, these types of vulnerabilities can be used to disrupt or inhibit the defense mechanisms against DDoS attacks such as Crossfire attacks that target a network area for taking down the network links [71, 72].

Moreover, the attacker can use vulnerabilities within a switch to change the control flow procedures. The affected switch would be reprogrammed by the attacker to ignore route mutation orders issued by the controller. As a result, the attacker can find permanent links. This can be further exploited to redirect the switch traffic to particular destinations with the

aim of aiding the attacker in pursuing the DDoS attack. In our setting, these actions are referred to as collusion of the SDN elements with the attackers.

With the aim of mitigating the effects of such attacks and fully enjoying the benefits of SDN-based MTD approaches, we propose a game-theoretical solution concept in which the defenders (switches) are incentivized not to collude with the attackers. We first illustrate our model and its components. Subsequently, we utilize a socio-rational approach [73, 74] to provide a new anti-collusion solution that shows cooperation with the SDN controller is always Nash Equilibrium.

The rest of this chapter is organized as follows. Section 3.2 briefly reviews the literature of game-theoretical approaches to SDN security. Section 3.3 illustrates our game-theoretical solution with its assumptions and analysis. Finally, Section 3.4 provides concluding remarks and future works.

3.2 LITERATURE REVIEW

3.2.1 Game-Theoretical Approaches to SDN Security

Recently, several game-theoretical approaches have been proposed for SDN security with emphasis on the SDN controller assignment [75, 76, 77] as well as the MTD [78]. Wang et. al. [75] proposed a novel two-phase dynamic SDN controller assignment mechanism to minimize the average response time of the control plane. The assignment between controllers (with various capacities to serve requests) and switches (with different request demands) is considered as the stable matching problem in the first phase. The solution quality from the first phase (the mapping between switches and controllers that guarantees the worst-case response time for each switch) is then improved by leveraging the coalitional game theory. A group of switches that are assigned to a controller can be seen as a coalition and they can negotiate to change their coalitions to improve the response time.

In [76], Chen et. al. proposed a zero-sum game-theoretical solution for the controller load-balancing. In this model, controllers are the players and SDN switches are the com-

modities that are traded among the players who intend to maximize their profits (e.g., by load balancing). An overloaded controller selects a switch and then sends an announcement (i.e., the existing load of the selected switch) to its nearby controllers so that they can compete to be the new master controller of the selected switch.

In [77], an optimal multi-controllers placement is considered as a multi-objective optimization problem that minimizes the latency and communication overhead between switches and a controller. It also ensures the load balancing among controllers. A cooperative Nash bargaining game theory is used to find the trade-off between two conflicting objectives. These two objectives are considered in order to find a unique solution that satisfies the Pareto efficiency between both players.

Finally, in [78], Jafarian et. al. model the interaction between a defender (that proactively defends against DoS attacks through a random route mutation mechanism) and a DoS attacker as a static game of complete information. In this model, an attacker is aware of the flow properties (for instance, source and destination, size and duration, transmission starting time) and its strategy is to attack a number of routes during the flow transmission. The defender's strategy is to use a number of routes for the flow transmission. The aim of each player (that is, defender and attacker) is to determine its Nash Equilibrium strategy by taking into account the opponent strategy and the cost of its own strategy.

3.2.2 SDN-Based MTD

The static nature of existing network attributes (e.g., IP address and route to certain network hosts) enables attackers to perform the network reconnaissance without any time constraint. The network-based MTD has been intensively studied to obfuscate attackers' reconnaissance efforts by changing the network attributes randomly and periodically in order to make it harder for the attackers to collect useful information, that is, to increase the attackers' overheads significantly while minimizing the legitimate users' overheads. The emerging SDN has been employed for efficient and cost-effective network-based MTD operations [68,

69, 79, 72, 78, 80, 81]. However, the roles of the SDN switch and SDN controller are varied among the proposed SDN-based MTD approaches.

In proactive MTD-based address mutation approaches (in which the real address of a moving target network host remains untouched and a short-lived virtual address is associated to that host dynamically [68, 69, 79]), the SDN switch can be used as the address translator between these real and virtual addresses [69, 79]. On the other hand, the SDN controller has more complex tasks. In [68], while there is no additional function for the SDN switch, the SDN controller acts as a generator of the synthetic MAC and IP addresses, and also, informs the server application to create Network Address Translation (NAT) rule to map the synthetic and real addresses. In [69], the SDN controller has the following roles: coordinating mutation across the SDN switches, determining the optimal set of new virtual addresses for hosts using Satisfiability Module Theories (SMT) solver, and finally, handling the DNS updates. In [79], besides proactive and reactive IP-address randomizations, the SDN controller is responsible to learn the topology and also assign a random flow to the traffic because the IP-address randomization is still prone to traffic analysis.

Proactively modifying the traffic flow through route mutation is also performed in [78, 72]. Besides performing route mutation, the SDN controller in [78] is responsible to determine the optimal defender strategy by finding the Nash Equilibrium of the game and also the qualified routes for this strategy by using the SMT solver. In [72], route mutation is utilized to increase the attacker's cost of finding persistent links. The SDN controller is used to create traceroute profiles by monitoring the ICMP traffic, and performs route mutation in response to the identified traceroute accordingly. In [80], the SDN is employed to monitor the transport layer traffic (e.g., TCP) and generate random TCP responses and payloads for the illegitimate TCP scanning traffic to prevent operating system fingerprinting. In [81], the SDN is employed to modify the detected network scanning traffic flow to a shadow network that provides a response to this network scanning attempt.

In all of these approaches, the SDN controller and switches are assumed to be trusted

and no collusion is considered between the SDN elements and the attackers. In this chapter, we will drop such an assumption to propose a game-theoretical model to address collusion between the switches and attackers.

3.3 GAME-THEORETICAL CONSTRUCTION

Game-theoretical paradigms are mostly used to model interaction between attackers and defenders [82, 64]. In these models, a two-player game is proposed in which attackers and defenders try to maximize the utility that they can gain. For instance, the defenders can provide value to the system and, as a result, gain utility by enabling features, shifting the attack surface, and reducing the attack surface measurement. On the other hand, the attackers can benefit if features are disabled or the attack surface measurement is increased.

In majority of existing models, an attacker and a defender play the game by selecting different actions from their action profiles in each round of the game (for instance, the defender can modify the system in order to shift the attack surface or the attacker can manipulate the system in order to disable some features). After each selection, the system moves to a new state and the players receive their rewards based on a reward function, also known as utility function.

3.3.1 Model Description

Our model is constructed upon the SDN-based MTD [72] that strives to provide route mutation defense against the link-map creation at the reconnaissance stage of the crossfire attack [71]. It is a powerful attack that degrades and cuts off network connections of selected server targets, e.g., a link-flooding DDoS that attacks links surrounding a target. Reconnaissance phase is the first and the longest step in which the attacker strives to find persistent links that can be candidates for the targeted link-flooding DDoS attacks. The persistent link is a link that always presents whenever an attacker performs the reconnaissance, as opposed to transient links. By performing the route mutation, when a suspected reconnaissance attempt

is detected, an attacker is expected to receive a transient link instead of a persistent link.

Our model consists of an SDN controller that assigns a flow rule to every switch based on the selected route mutation strategy and n switches that act as defenders. On the other hand, we have a group of attackers that try to collude with switches so that the following actions are considered as defection in our setting:

1. They do not perform the route mutation; therefore, the attacker can find persistent links.

2. They send their traffic to certain links in order to help the attacker to launch the DDoS attack.

The following two scenarios are considered for collusion: a single switch is not trusted and colludes with the attacker, or multiple switches are not trusted and form collusion with an attacker. We consider the later case as it is the general case of the first scenario. Note that game-theoretical paradigms are usually used to model *interaction* between defenders and attackers. Here, we specifically intend to model *collusion* between defenders and attackers.

In our new game-theoretical model, we first consider a 2-player game between two defenders (i.e., switches) that may/may not collude with an attacker by not performing the route mutation or sending the traffic to certain links. These two actions are part of the players' action profiles and they will be considered as defection, denoted by $\mathscr{D}$. As such, cooperative actions, denoted by $\mathscr{C}$, are considered to be performing the route mutation or sending the traffic to different links.

3.3.2 Our Solution in a Nutshell

We consider the following payoff function for two switches similar to the prisoners' dilemma, shown in Table 3.3.2. Note that this model can be easily extended to a model with n switches.

S_1 \ S_2	$\mathscr{C}$: Not Collude	$\mathscr{D}$: Collude
$\mathscr{C}$: Not Collude	$(0,0)$	$(0,2)$
$\mathscr{D}$: Collude	$(2,0)$	$(1,1)$

Table 3.1: Two Defenders Who Intend to Collude With the Attacker

This model illustrates, if both switches collude with the attacker, they each gain, e.g., \$1 utility (i.e., attacker's \$2 budget will be shared between both switches) but if one switch colludes but the other one doesn't collude, the colluder will receive \$2 from the attacker. As a result, collusion is Nash Equilibrium meaning that switches always collude because it's in their best interest to do so. This is a realistic scenario in which an attacker with a limited budget tries to compromise components of a network by colluding with defenders.

We tackle the aforementioned problem by considering a socio-rational model [73, 74] (that is, a repeated game among rational players who have public reputation values where these values affect players' utilities overtime) in which:

1. The SDN controller selects a group of switches (a subset of switches based on their trust values using a non-uniform probability distribution) to protect the targeted system against potential attacks.

2. The attacker utilizes his budget in order to collude with switches, and consequently, compromise the system.

In our setting, if a switch colludes with the attacker, it can gain some utility in the current game (e.g., \$1), however, that switch has less chance (lower probability) to be selected by the SDN controller in the future games due to the reduction of his reputation value, see [83,

84] for a trust/reputation management system. Therefore, it would be in the best interest of switches not to collude with the attacker because a non-cooperative switch will lose his reputation, and consequently, he will lose many future games (e.g., $-\$3$).

3.3.3 Formalizing Our Solution

We utilize a trust management scheme in a repeated two-player game between "two defenders" who try to maximize their utilities through collusion with the attackers. We show that, by using proper strategies, cooperation (i.e., not-colluding with the attackers) is always Nash Equilibrium because of a long-term utility that we consider in our game-theoretical setting. We not only consider a reward function but also use a function to penalize colluders. We also consider two classes of actions, that is, *collude* as non-cooperative actions and *not collude* as cooperative actions. E.g., disabling features and increasing the attack surface are actions from the first class.

Our game is repeatedly played for an unknown number of rounds. Each network switch S_i has a public reputation value $\mathscr{R}_i$, where the initial value is zero, i.e., $\mathscr{R}_i(0) = 0$, and it is bounded as follows $-1 \leq \mathscr{R}_i(p) \leq +1$; note that $p = 0, 1, 2, \ldots$ denotes subsequent rounds of the game. Moreover, each switch's action $a_i \in \{\mathscr{C}, \mathscr{D}, \perp\}$, where $\mathscr{C}$ and $\mathscr{D}$ denote *cooperation* and *defection* respectively, and $\perp$ denotes S_i has not been chosen by the SDN controller in the current game. Finally, each switch calculates two utility functions to decide whether he should collude with the attacker or not, i.e., a long-term utility function u_i and an actual utility function u_i'. Each round of the game consists of the following steps:

1. Let Ψ be a non-uniform probability distribution over types of switches, i.e., good/non-colluding, bad/colluding and new switches. The SDN controller selects m out of n switches, where $m \leq n$, based on this probability distribution in each round of the game.

2. Each switch S_i computes his long-term utility function $u_i : A \times \mathscr{R}_i \mapsto \mathbb{R}$, and then

selects an action from the action profile A, i.e., whether to collude with the attacker or not.

3. Each player S_i receives his utility $u_i' : A \mapsto \mathbb{R}$ (that is, the real utility that each switch can gain) at the end of each round of the game according to the outcome.

4. The reputation values $\mathscr{R}_i$ of all the chosen switches are publicly updated based on each switch's behavior using a reputation system. Note that the SDN controller doesn't know if a switch has colluded with the attacker at each round of the game, however, if a switch deviates from the SDN controller's instructions (e.g., it does not perform the rout mutation or sends the traffic to certain links), it will be assumed that it has colluded with the attacker.

3.3.4 Utility Assumptions

Let $u_i(\vec{a})$ denote S_i's long-term utility in outcome $\vec{a}$ by considering current and future games, let $u_i'(\vec{a})$ denote S_i's short-term utility in outcome $\vec{a}$ in the current game, let $c_i(\vec{a}) \in \{0,1\}$ denote if S_i has colluded with the attacker in the current game, and define $\Delta(\vec{a}) = \sum_i c_i(\vec{a})$, that is, the number of switches/defenders who have colluded with the attacker. Let $\mathscr{R}_i^{\vec{a}}(p)$ denote the reputation of S_i after outcome $\vec{a}$ in period p; note that $\vec{a}$ and $\vec{a}'$ are two different outcomes of the game. The following preferences are considered in our setting:

- $c_i(\vec{a}) = c_i(\vec{a}')$ and $\mathscr{R}_i^{\vec{a}}(p) > \mathscr{R}_i^{\vec{a}'}(p) \Rightarrow u_i(\vec{a}) > u_i(\vec{a}')$.

- $c_i(\vec{a}) > c_i(\vec{a}') \Rightarrow u_i'(\vec{a}) > u_i'(\vec{a}')$.

- $c_i(\vec{a}) > c_i(\vec{a}')$ and $\Delta(\vec{a}) < \Delta(\vec{a}') \Rightarrow u_i'(\vec{a}) > u_i'(\vec{a}')$.

The first assumption states that each switch S_i prefers to sustain a high reputation value overtime despite of colluding or not colluding with the attacker as he can potentially gain a

higher long-term utility. The second assumption expresses that if a switch S_i colludes with the attacker, he gains a short-term utility. Finally, the third assumptions illustrates that if a switch S_i colludes with the attacker and the total number of colluding parties in $\vec{a}$ is less than the total number of colluding parties in $\vec{a}'$, he gains a higher short-term utility in outcome $\vec{a}$.

3.3.5 Utility Function and Mathematical Analysis

The long-term utility function $u_i : A \times \mathscr{R}_i \mapsto \mathbb{R}$ calculates the utility that each switch S_i potentially gains or loses by taking into account both current and future games (based on all three utility assumptions), whereas the short-term utility function $u_i' : A \mapsto \mathbb{R}$ only calculates the current gain or loss in a given period (based on the last two utility assumptions). Note that A is the action profile.

Let ϕ_i be the reward coefficient that is defined by the SDN controller based on the reputation value of each switch S_i, and let $\delta_i(\vec{a}) = \mathscr{R}_i^{\vec{a}}(p) - \mathscr{R}_i^{\vec{a}}(p-1)$ be the difference of two consecutive reputation values. Note that $\tau_i = |\delta_i(\vec{a})| / \delta_i(\vec{a})$ is positive if the selected action in period p is $\mathscr{C}$ and it is negative, if it is $\mathscr{D}$. Also, let $\Omega > 0$ be a unit of utility, e.g., \$100. To satisfy the stated assumptions in Section 3.3.4, we have the following equations:

$$\frac{|\delta_i(\vec{a})|}{\delta_i(\vec{a})} \times \phi_i \times \Omega \tag{3.1}$$

$$c_i(\vec{a}) \times \Omega \tag{3.2}$$

$$\frac{c_i(\vec{a})}{\Delta(\vec{a}) + 1} \times \Omega \tag{3.3}$$

- Eqn (1) means S_i gains or loses ϕ_i units of utility Ω in the future games due to his behavior as reflected in $\mathscr{R}_i$.

- Eqn (2) illustrates that S_i gains one unit of utility if he colludes with the attacker in the current game and he loses this opportunity, otherwise.

- Eqn (3) results in almost one unit of utility to be divided among all the colluders.

The linear combination of these terms defines the long-term utility function $u_i(\vec{a})$, however, actual utility $u_i'(\vec{a})$ only consists of the linear combination of equations (2) and (3).

$$u_i(\vec{a}) \quad = \quad \Omega\left(\frac{|\delta_i(\vec{a})|}{\delta_i(\vec{a})} \times \phi_i + c_i(\vec{a}) + \frac{c_i(\vec{a})}{\Delta(\vec{a})+1}\right).$$

Theorem-1: *In a* $(2,2)$*-socio-rational collusion game,* $\mathscr{C}$ *strictly dominates* $\mathscr{D}$ *when we use our utility function.*

Proof: We compute the utility of each outcome for S_i. Let S_j be the other defender.

1. If both defenders don't collude/cooperate, then δ_i is positive, $c_i = 0$, and $\Delta = 0$:

$$\big(\delta_i > 0, c_i = 0, \Delta = 0\big) \Rightarrow u_i^{(\mathscr{C},\mathscr{C})} = \Omega\,\phi_i.$$

2. If only S_i cooperates, then δ_i is positive, $c_i = 0$ since S_i has not colluded, and $\Delta = 1$ because only switch S_j has colluded with the attacker:

$$\big(\delta_i > 0, c_i = 0, \Delta = 1\big) \Rightarrow u_i^{(\mathscr{C},\mathscr{D})} = \Omega\,\phi_i.$$

3. If only S_j cooperates, then δ_i is negative, $c_i = 1$ since S_i has colluded, and $\Delta = 1$:

$$\big(\delta_i < 0, c_i = 1, \Delta = 1\big) \Rightarrow u_i^{(\mathscr{D},\mathscr{C})} = \Omega\Big(-\phi_i + 1.50\Big).$$

4. If both switches defect, then δ_i is negative, $c_i = 1$, and $\Delta = 2$ because both switches have colluded:

$$\big(\delta_i < 0, c_i = 1, \Delta = 2\big) \Rightarrow u_i^{(\mathscr{D},\mathscr{D})} = \Omega\Big(-\phi_i + 1.33\Big).$$

If reward factor $\phi_i \geq 1.5$, we will have the following payoff inequalities that proves our theorem:

$$\overbrace{u_i^{(\mathscr{C},\mathscr{C})}(\vec{a}) = u_i^{(\mathscr{C},\mathscr{D})}(\vec{a})}^{S_i \text{ cooperates}} > \overbrace{u_i^{(\mathscr{D},\mathscr{C})}(\vec{a}) > u_i^{(\mathscr{D},\mathscr{D})}(\vec{a})}^{S_i \text{ defects}} \quad \square$$

If we assume the reward factor ϕ_i is at least 1.5 (note that the minimum value of this constant is defined based on the model's parameters), the payoff matrix is as follows, Table 3.3.5:

S_1 \ S_2	$\mathscr{C}$: Not Collude	$\mathscr{D}$: Collude
$\mathscr{C}$: Not Collude	$(1.5, 1.5)$	$(1.5, 0)$
$\mathscr{D}$: Collude	$(0, 1.5)$	$(-0.17, -0.17)$

Table 3.2: Collusion Game Between Two Defenders in the Socio-Rational Model

As you can see, cooperation is always Nash Equilibrium. To expand our proof to a case with n switches/defenders, let $\mathscr{C}_i$ (or $\mathscr{D}_i$) denote that S_i cooperates (or defects), and let $\mathscr{C}_{-i}$ (or $\mathscr{D}_{-i}$) denote that, excluding S_i, all the other defenders cooperate (or defect), and finally, let $\mathscr{M}_{-i}$ denote that, excluding S_i, some defenders cooperate and some of them defect.

Theorem-2: *In a (n,n)-socio-rational collusion game, $\mathscr{C}$ strictly dominates $\mathscr{D}$ when we use our utility function.*

Proof: We compute the utility of each outcome in six different scenarios. Let $n > k \geq 2$.

1. If all the defenders cooperate, or S_i and $k-1$ defenders cooperate, or only S_i cooper-

ates, as a result, δ_i is positive, $c_i = 0$, and $\Delta \in \{0, n-k, n-1\}$:

$$\big(\delta_i > 0, c_i = 0, \Delta \in \{0, n-k, n-1\}\big) \Rightarrow$$
$$u_i^{(\mathscr{C}_i, \mathscr{C}_{-i})} = u_i^{(\mathscr{C}_i, \mathscr{M}_{-i})} = u_i^{(\mathscr{C}_i, \mathscr{D}_{-i})} = \Omega\, \phi_i.$$

2. If only S_i defects, δ_i is negative, $c_i = 1$ and $\Delta = 1$:

$$\big(\delta_i < 0, c_i = 1, \Delta = 1\big) \Rightarrow u_i^{(\mathscr{D}_i, \mathscr{C}_{-i})} = \Omega\Big(-\phi_i + 1.5\Big).$$

3. If S_i as well as $k-1$ defenders defect, and the rest of them cooperate:

$$\big(\delta_i < 0, c_i = 1, \Delta = k\big) \Rightarrow u_i^{(\mathscr{D}_i, \mathscr{M}_{-i})} = \Omega\Big(-\phi_i + \frac{k+2}{k+1}\Big).$$

4. If all the defenders defect, δ_i is negative, $c_i = 1$, and $\delta = n$ because no one has cooperated:

$$\big(\delta_i < 0, c_i = 1, \Delta = n\big) \Rightarrow u_i^{(\mathscr{D}_i, \mathscr{D}_{-i})} = \Omega\Big(-\phi_i + \frac{n+2}{n+1}\Big).$$

We simply analyze these scenarios as follows. Let $*_{-i}$ be $\mathscr{C}_{-i}$ or $\mathscr{M}_{-i}$ or $\mathscr{D}_{-i}$. It is easy to show that:

$$1.5 > \frac{k+2}{k+1} > \frac{n+2}{n+1} \text{ when } n > k \geq 2.$$

Similarly, if we assume the reward factor ϕ_i is at least 1.5, cooperation (i.e., not colluding with the SDN controller) is always Nash Equilibrium. As a result, it is always in S_i's best interest to cooperate no matter what other parties do:

$$u_i^{(\mathscr{C}_i, *_{-i})}(\vec{a}) > u_i^{(\mathscr{D}_i, *_{-i})}(\vec{a}) \qquad \square$$

3.4 CONCLUSION

We showed that a game-theoretical solution concept can be utilized to tackle the collusion attack in a SDN-based framework. In our proposed setting, the defenders (i.e., switches) were incentivized not to collude with the attackers in a repeated-game setting that utilizes a reputation system. We first illustrated our model and its components. We then used a socio-rational approach to provide a new anti-collusion solution that shows cooperation with the SDN controller is always Nash Equilibrium due to the existence of a long-term utility function in our model.

CHAPTER 4

INCENTIVIZING HONEST MINING IN BLOCKCHAIN

In this chapter the reputation-based trust model is applied to the problem of dishonest mining in Blockchain. We show that by applying a trust score to each miner or mining group we can create a disincentive for selfish behavior and incentivize honest mining practices. The results of this chapter appear in [1].

4.1 INTRODUCTION

Security games are mainly designed and utilized to model interaction between attackers and defenders [82, 64]. In these models, two-player games (extendable to any number of players) are proposed in which both attackers and defenders try to maximize the utility that each can gain. For instance, the defenders will be able to provide value to the system and, as a result, gain utility by enabling features, shifting the attack surface, and reducing the attack surface measurement. Likewise, the attackers will be able to gain utility if features are disabled or the attack surface measurement is increased.

In the majority of existing security games, attackers and defenders play the game by choosing various actions from the action profiles based on their strategies in each round of the game. For instance, the defenders can modify the setting of the targeted system in order to shift the attack surface whereas the attackers can manipulate the system in order to disable some features. After each round of the game, the game moves to a new state and the players receive their rewards based on some utility functions.

One of the fascinating research areas where the security games can be utilized is the verification of transactions in the context of digital currencies, e.g., Bitcoin [85], or similar

paradigms. The mining operation is very resource intensive. As a result, players form different coalitions in order to verify every single block of transactions in return for a reward. This leads to intense competitions among competitors because only the first coalition that accomplishes the mining process will be rewarded.

To address what issues this competition may cause, different strategies are analyzed in the literature. Rosenfeld [86] introduces the *block withholding attack* where a dishonest player only reveals a partial solution of the verification problem whenever he has the complete solution to act in favor of another competing coalition. As a result, the dishonest miner shares the revenue obtained by the entire coalition without any contribution. Eyal and Sirer [87] introduce *selfish mining* where the players of a coalition keep their discovered blocks private and continue to verify more blocks privately until they get a sub-chain that its length is threatened. As a result, selfish players receive the reward. Johnson et. al. [88] look at the malicious activity of the players from another perspective. The authors compare an honest approach with a dishonest strategy, i.e., players of a coalition can invest to acquire additional computing resources, or launch ***DDoS*** attacks against other competing coalitions. The authors provide game-theoretical analyses by exploring the trade-off between these two strategies when two groups of varying sizes are involved. Recently, more attacks were introduced, e.g., *eclipse attack* [89] that makes a node invisible in the Bitcoin network, or *stubborn mining* as a generalization of the selfish mining [90].

We therefore propose a new reputation-based framework in which miners not only are incentivized to conduct honest mining but also disincentivized to commit to any malicious activities against other mining pools, such as block withholding attack, selfish mining, eclipse attack and stubborn mining, to name a few. We first illustrate the architecture of our reputation-based paradigm, explain how miners are rewarded or penalized in our model, and subsequently provide game theoretical analyses to show how this new framework encourages the miners to avoid dishonest mining strategies.

The rest of this chapter is organized as follows. Section 4.2 provides some preliminary

materials on digital currencies and game theory. Section 4.3 briefly reviews the existing digital currency literature where game theory is utilized. Section 4.4 illustrates our model. Section 4.5 explains how our reputation-based scheme works. It also provides the game theoretical analysis of our model. Finally, Section 4.7 concludes with final remarks.

4.2 PRELIMINARIES

Now preliminary materials regarding Blockchain and game theory are briefly reviewed.

4.2.1 Digital Currencies: Terminologies and Mechanics

In the digital currency frameworks, specifically Bitcoin, transactions are grouped in blocks in order to be verified by a subset of nodes in the network, known as *miners*. The mining process, named *proof-of-work*, is computationally intensive with a specific difficulty factor that is increased overtime as the computational power of hardware systems grows. Therefore, nodes form *mining pools* under the supervision of *pool managers* to accomplish the mining task. In some technical articles, the mining process of the Bitcoin (or even other digital currencies) is referred to as the miners' *mathematical puzzle*.

The first mining pool that accomplishes the proof-of-work is rewarded a certain amount of freshly mined Bitcoins as an incentive for miners' works. That is why this process is also known as *mining*. As soon as a block is verified, it is attached to the list of existing verified blocks, known as *Blockchain*. Immediately after that, all miners stop the mining process of the already verified block and start working on the next block.

The high-level idea of the proof-of-work/verification/mining is shown in Figure 4.1. Each block consists of a block number, a nonce value, list of transactions, the hash value of the previous block (address of the previous block), and the hash value of the next block (address of the next block). During the mining process, the miners try to generate a valid hash value of a block that is less than a threshold (i.e., it starts with a certain number of zeros). They will conduct this process by trying different nonce values. It's clear that

generating a hash value that starts with, say 5 zeros, is harder than a hash value that begins with 4 zeros; this is what we call the *difficulty factor* of mining.

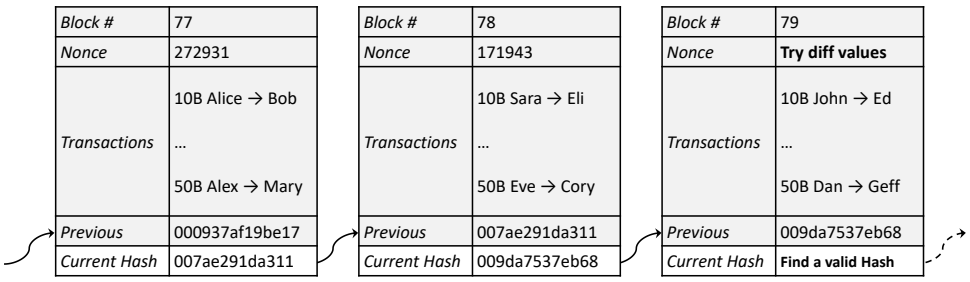


Figure 4.1: Blockchain and Mining

The hashing rate h_r (also known as *mining power*) is the total number of hashes that a miner can calculate during a specific time interval. Therefore, the average time to find a valid hash value (also known as *full* proof-of-work) correlates to a miner's hashing rate. In fact, the pool manager sends different templates of the current block to his miners so that they can find a valid hash value by changing the nonce value. If a miner accomplishes the full proof-of-work, he will then send it to his pool manager. Consequently, the pool manager publishes the legitimate block on behalf of the entire pool. He will then distribute the revenue among miners based on their mining powers. Note that new coins are put explicitly in the block by the miner(s) who created it.

To estimate each miner's power, the pool manager determines a *partial target* for each miner, much easier than the actual target of the system. For instance, instead of calculating a hash value that starts with, say 5 zeros, a hash value with a single zero is sufficient. Note that this is just a simple example for the sake of clarification. Therefore, each miner is instructed to send a valid hash value according to the partial target. This partial target is defined in such a way that a partial solution can be calculated frequently enough so that the manager can fairly estimate the miners' powers because, as we stated earlier, the revenue is distributed based on the miners' powers.

4.3 LITERATURE REVIEW

Even though the concept of Blockchain is relatively new, introduced by an unknown author or authors in 2008 [85], it has gained considerable attention from the computer science and economics communities because of its unique approach in decentralizing verification of transactions related to a digital currency, and its inherent security because of this decentralized nature. However, the body of work that is focused on the study of Blockchain through the use of game theoretic methods is limited. In this section, related research works to game theory and Blockchain are reviewed.

Johnson et. al. [88] study the incentives for a mining pool to carry out a DDoS attack against another mining pool. The authors scrutinize this problem from an economic point of view where the incentive for an attack is to increase one's own probability of successfully verifying the next block of transactions, and hence, earning the Bitcoin rewards from this mining operation. They conclude that there is a greater incentive to attack a large mining pool rather than a small pool. The authors point out that this finding is consistent with statistics reported by [91] that shows 17.1% of small mining pools suffered DDoS attacks where as 62.5% of large pools were affected by such attacks. The authors make two other interesting observations as well, the first being that the ability to mitigate the DDoS attacks will increase the market threshold for the size at which a pool becomes vulnerable to the DDoS attack. This makes intuitive sense since the ability to mitigate such attacks will decrease the utility to the attacker. Secondly, the cost of these attacks will keep small players out of the DDoS market since the incentive for attacking such a player is relatively low.

Babaioff et. al. [92] look at a different problem that is present in the Bitcoin protocol. In fact, this problem will intensify once the mining reward is ended in the Bitcoin. In the current design, the nodes that authorize a transaction are rewarded through two separate methods. The first is through the generation of new Bitcoins for every new block that is added to the Blockchain, and the second method is through a transaction fee. The maximum number of Bitcoins is limited to about 21 Million [93] and the creation of new Bitcoins

becomes exponentially smaller until the maximum limit is reached. The transaction fee will be the only resource to incentivize the miners when the maximum threshold is reached. At this point, miners are incentivized to keep the information of a possible transaction secret as there are no new Bitcoins to be mined from the efforts of reversing a hash, i.e., there is only the transaction fee that is given to the authorizer of the transaction. This incentive to keep information secret can potentially cripple the Bitcoin system as the time for confirming a transaction will be long when there is only one node attempting to authorize the transaction.

Kroll et. al. [94] study Bitcoin as a consensus game and consider the economics of Bitcoin from the mining perspective to determine whether there exists any incentive for rational players to defect from the mining protocol. The authors show that there is a Nash equilibrium for which all players cooperate with the Bitcoin reference implementation. However, there are infinitely many equilibria where the players can behave otherwise. The authors show that a motivated adversary may be capable of crashing the currency, as a result, governance structures will be necessary.

Even though the authors in [95] don't refer to any game theoretic models, they detail several possible vulnerabilities within the Blockchain protocol that are great candidates for game theoretic study such as deflationary spiral, the History-Revision attack, and delayed transaction confirmation. Carlsten et. al. [96] study the issues of Bitcoin and Blockchain when the last block reward is collected. The authors show that once the consistency of the block reward is removed from the protocol, leaving only the transaction fees, the incentive for defection increases.

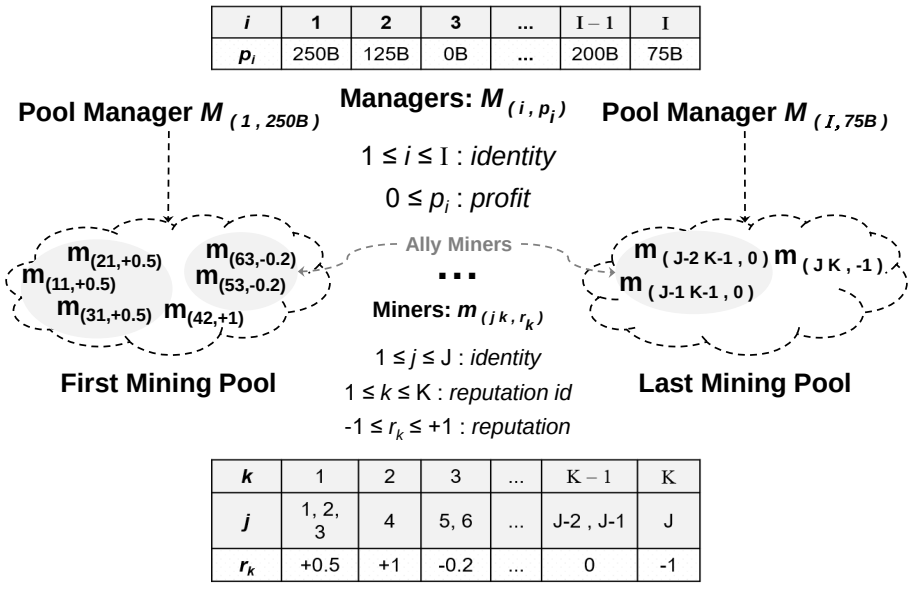
Luu et. al. [97] scrutinize the block withholding attack on mining pools, introduced by Rosenfeld [86]. They show that the attack always has incentive when looking at a long term operation but may not be profitable for short term duration. Eyal [98] studies the same subject and concludes that when two pools attack each other, it results in a version of the prisoner's dilemma, named the *Miner's Dilemma*. Lewenberg et. al. [99] introduce a modification to the Blockchain protocol to allow for inclusion of forked blocks with the

aim of increasing the rate of operation. The authors then provide a game theoretic model of the competition for fees between the nodes under the new protocol. Rosenfeld [100], and Sompolinsky and Zohar [101], as well as the original publication by Satoshi Nakamoto [85] have considered the probability of a successful double-spending attack in the non-inclusive protocol. Lewenberg et. al. [99] further analyze the inclusive protocol and determine that it is as secure as the non-inclusive form.

4.4 REPUTATION-BASED MINING MODEL AND SETTING

As illustrated in Figure 4.2, our model consists of a set of pool managers $M_{(i,p_i)}$ who form coalitions for the proof-of-work computations, for $1 \leq i \leq I$, where $0 \leq p_i$ denote profits that pool managers have so far accumulated; a set of miners/ally miners $m_{(jk,r_k)}$ who perform proof-of-works, for $1 \leq j \leq J$ and $1 \leq k \leq K$, where $-1 \leq r_k \leq +1$ denotes the reputation value of a miner/ally miners. In our model, miners/ally minors may commit to malicious activities through direct attacks (e.g., DDoS attack) or collusion attacks (e.g., block withholding) to disrupt the proof-of-work computations of certain mining pools. As such, two actions are considered in the miners' action profile, i.e., commit to malicious activity to disrupt computations of mining pools, denoted by $\mathscr{D}$: *dishonest mining*, or conduct the proof-of-work honestly, denoted by $\mathscr{H}$: *honest mining*.

Note that, in the current setting of digital currencies, each miner is defined by a unique identity j, however, in our proposed framework, each miner is also assigned a public reputation value r_k, where k is the index of this value. In fact, the reputation value reflects how well the miner has so far performed in the system in terms of mining performance as well as honest or malicious activities (i.e., a history of behaviors). This public reputation value r_k is updated after a specific period of time based on different criteria, e.g., the ratio of full proof-of-work over partial proof-of-work, detection of any malicious activity such as collusion with other miners, selfish-mining, or contribution to a DDoS attack. Moreover, each pool managers i is also assigned a parameter p_i that defines the profit that he has so far



i	1	2	3	...	I – 1	I
p_i	250B	125B	0B	...	200B	75B

k	1	2	3	...	K – 1	K
j	1, 2, 3	4	5, 6	...	J-2 , J-1	J
r_k	+0.5	+1	-0.2	...	0	-1

Figure 4.2: Architecture of Our Reputation-Based Setting

accumulated through his pool. As p_i reflects how well a manager is performing, it can be interpreted as his reputation.

In our setting, a subset of miners who highly trust each other (due to partnerships, personal relationships, common nationality, or even geographical proximity) can form an alliance, named *ally miners*, and request a single reputation value r_k even though they each have a separate identity j. This means, while members of a coalition can build reputation all together through r_k by collaborations overtime, they are all responsible for malicious activities triggered even by a single member of their coalition.

This leads to the notion of *neighborhood-watch* meaning that each member of an alliance is incentivized to monitor his allies. For instance, members can agree to execute a randomized algorithm to monitor each other through various methods, that is, cybersecurity detection techniques or transparency policies to make sure no one has ever received any *bribe* from other mining pools due to any sort of collusion attacks. As a result, the pool manager doesn't need to have any concern for every single member of his mining pool. Furthermore, if a member decides to launch an attack, he may need to convince all his

coalition members or act solo, which might be caught by his allies through randomized monitoring before it can even affect the mining procedure.

Once in a while, the pool managers rearrange their groups to form new coalitions for the proof-of-work. They send invitations (invitation-based) to miners/ally miners based on a non-uniform probability distribution that is defined by the reputation values r_k. In other words, the miners/ally miners who are more reputable, have a higher chance to be invited to the mining pools and those who are not trustworthy have a lower chance to get invitations. The miners/ally miners can also chose to whom they would like to join if they receive multiple invitations, that is, a mutual *merit-based* setting for both miners and managers.

As this public reputation system is sustained over time, as a result, it will be in the best interests of the miners/ally miners to become reputable (or sustain their high reputation) to maximize their long-term utility. This will incentivized the miners/ally miners to avoid any dishonest behavior even if it has short-term utility. Note that the underlying reputation system must be immune against re-entry attack (i.e., cheat and come back to the scheme with a new identity j). We utilize the proposed idea of rational trust modeling [102] to make sure our setting is not vulnerable to these sorts of attacks against reputation systems.

Furthermore, in our proposed model, while ally miners are incentivized to form larger coalitions to gain/sustain a high reputation value and consequently more revenue, they are not incentivized to admit any new miner to their alliance unless they fully trust the newcomer. This is due to the fact that a single miner can harm the entire coalition. Moreover, it is worth mentioning that, although ally miners only have a single reputation identity r_k, a miner cannot commit to malicious activities in a set and then simply joins another alliance because each miner still has a unique identifier j.

Our proposed model can be seen as a *global* community where each mining pool represents a *federal* authority and each alliance represent a *state* authority. Therefore, each alliance is responsible to detect malicious activities inside the coalition in a smaller scale. In addition, each alliance can be changed in size and also move to a new mining pool

when the rearrangement is occurred periodically. This approach not only leads to less managerial overheads for the pool managers but also it creates a framework where practical implementations of preventive and detective protocols become possible.

4.5 MINING IN OUR REPUTATION-BASED MODEL

Since our approach is designed using a reputation-based paradigm, it's necessary to utilize a reputation/trust model that is resistant to the well-known *re-entry attack*, that is, corrupted players return to the scheme using new identities. Otherwise, our approach cannot be utilized properly. We will discuss this in the next section.

4.5.1 Prevention of the Re-Entry Attack

To deal with the re-entry attack in our reputation-based scheme, we utilize the proposed approach of *rational trust modeling* [102]. We provide a high-level description as how this modeling technique works. Suppose there exist two trust functions as follows. The first function $f_1(\mathscr{T}_i^{p-1}, \alpha_i)$ has two inputs, i.e., trust value $\mathscr{T}_i^{p-1}$ of player P_i in period $p-1$ and action α_i (cooperation or defection) selected by player P_i in period $p-1$. This function computes the updated trust value $\mathscr{T}_i^{p}$ of player P_i for the next round p based on these two inputs. However, the second function $f_2(\mathscr{T}_i^{p-1}, \alpha_i, \ell_i)$ has an extra input value that defines the player's lifetime, denoted by ℓ_i. This extra input determines how long a player with a reasonable number of interactions exists in a reputation-based scheme, for instance, our proposed reputation-based mining framework.

Using the second function, the reputation-based scheme should then be designed in a way that a player with a longer lifetime can be rewarded (penalized) more (less) than a player with a shorter lifetime assuming that the other two inputs (i.e., current trust value and the action) are the same. In this setting, "reward" means gaining a higher trust value/becoming more trustworthy, and consequently, receiving a higher utility, and "penalty" means otherwise. In other words, if two players P_i and P_j both cooperate $\alpha_i = \alpha_j = \mathscr{C}$ and their current trust

values are equal $\mathscr{T}_i^{p-1} = \mathscr{T}_j^{p-1}$ but their lifetime parameters are different, say $\ell_i > \ell_j$, the player with a higher lifetime parameter, gains a higher trust value for the next round, i.e., $\mathscr{T}_i^p > \mathscr{T}_j^p$. This helps player P_i to accumulate more utility/revenue in the targeted reputation-based framework.

To exemplify, consider a situation in which sellers in a reputation-based e-commerce setting have options to sell the "defective" versions of an item with more revenue or the "non-defective" versions of the same item with less revenue. If the first sample function f_1 is utilized in the scheme, it might be tempting for a seller to sell the defective items with more revenue and then returns to the e-commerce framework with a new identity (i.e., re-entry attack). However, if the second sample trust function f_2 is utilized, it's no longer in a seller's best interest to sell the defective items because if he returns to the community with a new identity, his lifetime indicator becomes zero and he loses all the credits that he has accumulated overtime. Consequently, he loses a huge potential revenue that he could gain because of his lifetime parameter, i.e., buyers always prefer a seller with a longer lifetime (longer existence with a reasonable number of transactions) over a seller who is a newcomer.

We emphasize that this is just an example of a rational trust modeling. In fact, the second sample function uses the lifetime parameter ℓ_i to enforce trustworthiness and prevent the re-entry attack. Note that different parameters can be incorporated into trust functions or reputation systems based on the context (e-commerce, mining in Blockchain, or whatsoever), and consequently, different attacks can be prevented.

4.5.2 Technical Discussion on Detection Mechanisms

Detection mechanisms are required to reward or penalize miners in our reputation-based setting. In the next part, we provide some discussions and mechanisms by which non-cooperative actions by miners (e.g., block withholding, selfish mining, DDoS attack, eclipse attack, stubborn mining, or upcoming attacks that are unknown) can be detected.

A mining pool can detect if is under a block withholding attack with a relatively high

accuracy. In fact, calculation of the partial proof-of-work is much easier than calculation of the full proof-of-work. Therefore, a mining pool can simply estimate its expected mining power in addition to its actual mining power. As a result, any difference between the expected and actual mining powers, which is above a certain threshold, can be an indication of a block withholding attack.

To determine which registered miner is the perpetrator, there are two possibilities. First, if the mining power of a miner/ally miners is high enough, the ratio of the full proof-of-work over the partial proof-of-work can indicate whether the miner/alliance is committing to the block withholding attack. Second, if the mining power is not high, the frequency of success to find the full proof-of-work is very low, and statistically, we may not be able to define if a miner is really committing to the block withholding attack. However, the latter case has a negligible (close to zero) impact on the mining process and can be simply ignored, i.e., block withholding attack by a single miner/miners with a low mining power cannot negatively affect the fair mining process.

As suggested by Eyal and Sirer [87] who initially introduced the selfish mining, an increase in the number of orphaned blocks can be an indication of selfish mining in the Blockchain. Furthermore, the amount of time taken to release consecutive blocks in the Blockchain can potentially provide evidence of selfish mining. This issue has been investigated by several researchers through experimental analysis [1]. In other words, two blocks in close succession should be a very rare incident when miners are honest, and this is more common when a miner/a group of miners quickly releases selfishly mined blocks to overcome the honest miners. As a result, it's not hard to detect which miners are committing to the selfish mining.

As stated in [89], the eclipse attack has several signatures and properties that make it detectable, e.g., a flurry of short-lived incoming TCP connections from diverse IP addresses. Moreover, an attacker that suddenly connects a large number of nodes to the Bitcoin network

[1] http://scienceblogs.com/builtonfacts/2014/01/11/is-bitcoin-currently-experiencing-a-selfish-miner-attack/

could also be detected. Therefore, anomaly detection software systems that look for similar behaviors can be helpful to detect the attacker. Likewise, there are many other techniques in the security literature that can be utilized to detect the DDoS attack, stubborn mining, etc.

Besides, other methods might be used to detect bribes and illegal money exchanges among registered miners in the transparent network of Bitcoin (unless they exchange bribes outside of the Bitcoin network). This is how the government agencies usually detect money laundering/illegal money exchanges in the traditional banking system. In other words, detection of these bribes might be an indication of collusion; why miners from two competing pools should frequently exchange money with a certain amount. This is just another candidate solution outside of the scope of this thesis.

4.5.3 Colluding Miner's Dilemma

In this section, we consider a scenario in which two miners (independent or from two different alliances) have to decide whether to collude with an attacker to disrupt another mining pool's effort or not. Two collusion scenarios can be considered, i.e., a single miner colludes with the attacker, or multiple miners form a coalition with the attacker. We consider the latter case as it is the general case of the first scenario. It is worth mentioning that game-theoretical paradigms are usually utilized to analyze interaction between honest parties and attackers. However, we intend to model collusion between miners and an attacker in the context of Blockchain's proof-of-work. In our setting, we initially consider a 2-miner game, named *colluding miner's dilemma*, that may/may not collude with the attacker to disrupt the mining efforts of a targeted mining pool. We further extend this scenario to a n-miner game that is played repeatedly among all the miners of the Blockchain network for an unknown number of rounds.

In the 2-miner setting, shown in Table 4.5.3, if both miners collude with the attacker, they each gain one unit of utility. In other words, the attacker's budget will be equally shared between both miners. However, if one miner colludes with the attacker but the other one

acts honestly, the colluding miner will receive two units of utility from the attacker. As a result of this dilemma, collusion is a Nash Equilibrium meaning that miners always collude because it's in their best interest to gain a higher utility. This is a realistic assumption where an attacker with a limited budget tries to disrupts the proof-of-work computation of a mining pool in favor of another alliance. Note that the budget is limited because mining reward is fixed in the Blockchain network.

$m_{(j'k',r'_k)}$ / $m_{(jk,r_k)}$	$\mathscr{H}$: Honest Mining	$\mathscr{D}$: Dishonest Mining
$\mathscr{H}$: Honest Mining	$(\text{₿}0, \text{₿}0)$	$(\text{₿}0, \text{₿}\Omega)$
$\mathscr{D}$: Dishonest Mining	$(\text{₿}\Omega, \text{₿}0)$	$(\text{₿}\frac{\Omega}{2}, \text{₿}\frac{\Omega}{2})$

Table 4.1: Payoff in Colluding Miner's Dilemma

We approach the colluding miner's dilemma by setting a socio-rational model [73, 74] (that is, a repeated game among rational foresighted players with public reputation values where these values directly affect players' utilities overtime) in which:

1. Each pool manager sends invitations to miners to form his mining pool for the proof-of-work computation. He not only tries to maximize his pool's revenue but also intends to protect his pool against any malicious activity. These invitations are defined based on miners' trust values using a non-uniform probability distribution.

2. On the other hand, the attacker uses his limited budget to collude with the miners, and consequently, compromise the proof-of-work computation of a targeted pool.

In this setting, if a miner colludes with the attacker, he may gain some utility in the current round of the game, however, that miner will be selected by the pool managers with a lower probability in the future if his malicious activity is detected. This is due to the

reduction of his reputation value, see [83, 84] for a trust/reputation management system. Therefore, it will be in the best interest of the miners not to collude with the attacker because a malicious miner will lose his public reputation, and consequently, he will lose many future mining opportunities with a much larger gain.

4.5.4 Repeated Mining Game

We use a trust model that is resistant to the re-entry attack in a repeated game setting. The miners try to maximize their utilities through the proof-of work computation as well as collusion with the attacker, or any dishonest mining strategies. We show that, by using our proposed model, cooperation (not-colluding with the attacker or committing to any malicious activity) is always a Nash Equilibrium because of a *long-term utility* function that we consider in our model in addition to a *short-term utility* function. Our model not only rewards honest miners but also penalizes colluding/dishonest miners. For the sake of simplicity and without loss of generality, two classes of actions are defined in our setting, i.e., *dishonest/collude* as a non-cooperative action and *honest/not collude* as a cooperative action, similar to [3].

The mining game is repeatedly played for an unknown number of rounds. Each miner $m_{(jk,r_k)}$ has a public reputation value r_k, where the initial value is zero, and it is bounded as follows: $-1 \leq r_k \leq +1$. In addition, each miner's action $\alpha_j \in \{\mathscr{H}, \mathscr{D}, \perp\}$, where $\mathscr{H}$ and $\mathscr{D}$ denote *honest mining* and *dishonest mining* respectively, and $\perp$ denotes miner $m_{(jk,r_k)}$ has not been selected by any pool manager $M_{(i,p_i)}$ in the current round. Finally, each miner calculates two utility functions to select his action, i.e., a long-term utility function u_j and an actual utility function u'_j. Note that each round of the game consists of a sequence of block verification, for instance, after verifying a constant number of blocks or after a certain amount of time.

1. Suppose we have a non-uniform probability distribution over types of miners, i.e., honest, dishonest and new miners. Each pool manager $M_{(i,p_i)}$ sends invitations to a

subset of miners based on this probability distribution in each round of the game.

2. Each miner $m_{(jk,r_k)}$ computes his long-term utility u_j, and then selects a new action from the action profile, i.e., employ honest or dishonest mining strategies.

3. Each $m_{(jk,r_k)}$ receives his short-term utility u'_j, i.e., the actual reward that each miner gains, at the end of each round of the game based on the proof-of-works' outcomes.

4. The reputation values r_k of the selected miners/ally miners are publicly updated based on each miner's/alliance's behavior using a reputation system.

4.5.5 Colluding Miners' Preferences

Let $u_j(\vec{a})$ denote $m_{(jk,r_k)}$'s long-term utility in outcome $\vec{a}$ by taking into account the current and future games, and let $u'_j(\vec{a})$ denote $m_{(jk,r_k)}$'s short-term utility in outcome $\vec{a}$ of the current game. Also, let $d_j(\vec{a}) \in \{0,1\}$ denote if miner $m_{(jk,r_k)}$ has employed dishonest mining strategies in the current game, and define $\Delta(\vec{a}) = \sum_i d_j(\vec{a})$, that is, the total number of miners who have utilized dishonest mining strategies. Let $r_k^{\vec{a}}(p)$ denote the reputation of $m_{(jk,r_k)}$ after outcome $\vec{a}$ in period p; note that $\vec{a}$ and $\vec{a}'$ are two different outcomes of our repeated game.

Here are the miners' preferences: $d_i(\vec{a}) = d_i(\vec{a}')$ & $r_k^{\vec{a}}(p) > r_k^{\vec{a}'}(p) \Rightarrow u_j(\vec{a}) > u_j(\vec{a}')$, that is, each miner $m_{(jk,r_k)}$ prefers to sustain a high reputation value overtime despite of employing honest or dishonest mining strategies as he can potentially gain a higher long-term utility; $d_i(\vec{a}) > d_i(\vec{a}') \Rightarrow u'_j(\vec{a}) > u'_j(\vec{a}')$, that is, if a miner $m_{(jk,r_k)}$ utilizes a dishonest mining strategy, he gains a short-term utility from the attacker, and finally; $d_i(\vec{a}) > d_i(\vec{a}')$ & $\Delta(\vec{a}) < \Delta(\vec{a}') \Rightarrow u'_j(\vec{a}) > u'_j(\vec{a}')$, that is, if $m_{(jk,r_k)}$ employs dishonest mining strategies and the total number of dishonest miners in $\vec{a}$ is less than the total number of dishonest miners in $\vec{a}'$, the miner gains a higher short-term utility in $\vec{a}$.

4.5.6 Colluding Miners' Utilities

In our setting, the long-term utility function u_i is computed based on the utility that each miner $m_{(jk,r_k)}$ potentially gains or loses by considering both current and future games, i.e., taking into account all stated utility preferences. However, the short-term utility function u_i' is only calculated based on the current gain or loss in a given time interval, i.e., taking into account the last two utility preferences, as mentioned in Section 4.5.5.

Let φ_j be the reward factor that is determined by each pool manager $M_{(i,p_i)}$ based on r_k of each miner $m_{(jk,r_k)}$, and let $\delta_j(\vec{a}) = r_k^{\vec{a}}(p) - r_k^{\vec{a}}(p-1)$ be the difference of two consecutive reputation values. Note that $\tau_j = \left|\delta_j(\vec{a})\right| / \delta_j(\vec{a})$ is positive if the selected action in period p is $\mathscr{H}$: *honest mining*, and it is negative, if it is $\mathscr{D}$: *dishonest mining*. Also, let $\Omega > 0$ be a unit of utility, for instance, ฿50. To satisfy the miners' preferences, we compute the long-term utility $u_j(\vec{a})$ through the following linear combination:

$$u_j(\vec{a}) \;\; = \;\; \Omega\Big(\tau_j \varphi_j + d_j(\vec{a}) + \frac{d_j(\vec{a})}{\Delta(\vec{a})+1}\Big). \tag{4.1}$$

Note that the actual utility $u_j'(\vec{a})$ only consists of the second and third terms, that is, $u_j'(\vec{a}) = \Omega(d_j(\vec{a}) + d_j(\vec{a})/(\Delta(\vec{a})+1))$. The first term of the utility function denotes miner $m_{(jk,r_k)}$ gains or loses φ_i units of utility in the future games due to his behavior as reflected in r_k. This is due to τ_j that depends on the miner's reputation value r_k. The second term illustrates miner $m_{(jk,r_k)}$ gains one unit of utility if he employs dishonest mining strategies or colludes with the attacker in the current game and he loses this opportunity, otherwise. Finally, the last term results in almost one unit of utility to be shared among all the dishonest miners.

4.6 GAME-THEORETICAL ANALYSES OF OUR MODEL

In this section, we use game theory to analyze our proposed reputation-based mining paradigm. We first consider a $(2,2)$-game that is played between two miners in order to show honest mining always dominates dishonest mining in our setting. We further extend

this analysis to a (n,n)-game that is played among n miners.

Theorem 1 *In a $(2,2)$-game between two miners, honest mining $\mathscr{H}$ strictly dominates dishonest mining $\mathscr{D}$ when we use utility function $u_j(\vec{a})$, as defined in Eqn (4.1).*

The proof for this theorem is similar to the analysis in chapter 3.

Likewise, if we assume φ_i is at least 1.5 (note that the minimum value is defined based on the model's parameters), the payoff matrix is as follows, Table 4.6:

$m_{(jk,r_k)}$ \ $m_{(j'k',r'_k)}$	$\mathscr{H}$: Honest Mining	$\mathscr{D}$: Dishonest Mining
$\mathscr{H}$: Honest Mining	(฿1.5, ฿1.5)	(฿1.5, ฿0)
$\mathscr{D}$: Dishonest Mining	(฿0, ฿1.5)	(฿ − 0.17, ฿ − 0.17)

Table 4.2: Game Between Two Miners

As shown, honest mining is always a Nash Equilibrium in our reputation-based mining paradigm. To expand our proof to a case with n miners, let $\mathscr{H}_j$ (or $\mathscr{D}_j$) denote $m_{(jk,r_k)}$ employs honest mining strategies (or dishonest mining strategies), and let $\mathscr{H}_{-j}$ (or $\mathscr{D}_{-j}$) denote, excluding $m_{(jk,r_k)}$, all other miners utilize honest mining strategies (or dishonest mining strategies), and finally, let $\mathscr{M}_{-j}$ denote, excluding $m_{(jk,r_k)}$, some miners employ honest mining strategies and some of them utilize dishonest mining strategies.

Theorem 2 *In a (n,n)-game among n miners, honest mining $\mathscr{H}$ strictly dominates dishonest mining $\mathscr{D}$ when we use the utility function $u_j(\vec{a})$, as defined in Eqn (4.1).*

The proof for this theorem is similar to the analysis in chapter 3.

4.7 CONCLUSION

In this chapter, we proposed a new reputation-based mining paradigm for the proof-of-work computation of Blockchain. We first illustrated the problem of dishonest mining, demonstrated our proposed model, and subsequently, we provided a candidate solution concept to the aforementioned problem. Note that, by dishonest mining, we refer to any malicious activity against other mining pools or competitors, such as *block withholding attack, selfish mining, eclipse attack* and *stubborn mining*, to name a few.

Our proposed mining game is repeatedly played among a set of pool managers and miners where the reputation value of each miner or mining ally is continuously measured by a trust management scheme that is resistant to the re-entry attack. At each round of the game, pool managers send invitations only to a subset of miners based on a non-uniform probability distribution defined by the miners' reputations. It is worth mentioning that each round of the game consists of a sequence of block verification, for instance, after verifying a constant number of blocks or after a certain amount of time.

We showed that, by using our proposed solution concept, honest mining becomes a Nash Equilibrium in our setting. In other words, it will not be in the best interest of the miners to disrupt the proof-of-work computation or commit to dishonest mining even by gaining a short-term utility. This is due to the consideration of a long-term utility function in our model and its impact on the miners' utilities overtime.

CHAPTER 5

CONCLUDING REMARKS AND FUTURE DIRECTIONS

In this thesis two new game theoretic models were introduced based on the notion of reputation-based trust within a repeated game. In chapter 3 we introduced a game-theoretical solution concept that can be used to tackle collusion attacks in SDN based networks. In our solution, a repeated-game setting utilizing a reputation system was used to incentivize the defenders to not collude with the attackers. We illustrated the proposed model and it's components, and then we provided a new anti-collusion solution using a socio-rational approach. We showed that cooperation with the SDN controller is always Nash Equilibrium because of the long-term utility function of our model.

In chapter 4 we proposed a new reputation-based mining paradigm for use in the proof-of-work computation in Blockchain. We discussed several problems that exist within the Blockchain mining scheme when players are dishonest and proposed a solution to those problems. In our proposed solution, we setup a repeated game where pool managers and miners are observed and a trust management scheme which is resistant to the re-entry attack is used to continuously measure the reputation value of each miner. In our repeated game setup each round consists of a sequence of block verifications. As in chapter 3, we showed that using the proposed solution, honest mining becomes a Nash Equilibrium meaning that it will not be in the best interest of the miners to be dishonest by not adhering to the proof-of-work computation protocol even though there may be some short term utility in doing so.

While these methods do not necessarily prevent an attack from being successful, the rules can be changed to disincentivize such attacks. Each and every attack has a cost, and there is an expected return for a successful attack. By using our model the expected return is

reduced to a level which make the return on investment of the attack negative, meaning that it will cost more to perform the attack than the profit gained.

5.1 FUTURE DIRECTIONS

In the context of Bitcoin/Blockchain we are interested in implementing our proposed game through a simulation-based approach using real data from the Bitcoin network.

Within the context of SDNs, we are interested in constructing new game-theoretical paradigms to model cyber deception and collusion risks in SDN-based platforms. Similarly, we will consider a SDN controller, a set of switches that act as defenders, and a group of attackers who intend to compromise different parts of the network. The defenders' goal will be the protection of the targeted network by utilizing appropriate deceptive as well as anti-collusion strategies. Subsequently, the defenders will gain utility if they select proper actions from the action profile in order to deceive the attackers. We intend to provide new solution concepts in which the attackers are incentivized by extra utility in order to act according to the defenders' strategies (i.e., deception). We will construct a two-player game between "two attackers" and show that, in our model, selection of the deceptive action(s) is Nash Equilibrium. We will further extend this two-player game to a game with any number of attackers. In other words, in our future framework, the SDN controller and defenders deceive the attackers by choosing a certain class of actions that have a higher short-term payoff. Note that, in the presented work here, we considered a two-player game between "two defenders" who may/may not collude with the attackers.

5.2 AN EXPANSION OF REPUTATION-BASED REPEATED GAMES

We would like to expand the notion of reputation-based repeated games to analyze and improve other areas of network security such as WSNs, and wireless Ad-hoc networks. Using the framework introduced here we could assign trust values to nodes within these wireless networks to incentivize them to cooperate with the established protocols.

Another related area of study is state sponsored cyberwarfare. The notion of a reputation-based repeated game can be adapted to disincentivize these attacks by making the maximum reward gained by the attack as little as possible.

BIBLIOGRAPHY

[1] Arash Golchubian and Merhrdad Nojoumian. “A Survey of Game Theoretic Network Security”. Submitted to the International Journal of Game Theory (IJGT), 18 pages, Nov 07, 2017. (Under Review).

[2] Mehrdad Nojoumian, Arash Golchubian, Laurent Njilla, Kevin Kwiat, and Charles Kamhoua. “Incentivizing Blockchain Miners to Avoid Dishonest Mining Strategies By a Reputation-Based Paradigm”. In: *To appear in IEEE Computing Conference (CC)*. London, UK: IEEE, 2018. (Accepted To Be Published).

[3] Mehrdad Nojoumian, Arash Golchubian, Nico Saputro, and Kemal Akkaya. “Preventing Collusion Between SDN Defenders and Attackers Using a Game Theoretical Approach”. In: *Infocom: Adv in Software Defined & Context Aware Cognitive Radio Net*. Atlanta, USA: IEEE, 2017, 6 pages. (Accepted To Be Published).

[4] Seena Gressin. *The Equifax Data Breach*. 2017. URL: `https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do`.

[5] James Moar. *Cybercrime and the Internet of Threats*. Tech. rep. Juniper Research, 2015.

[6] Kate Conger Darrell Etherington. “Large DDoS attacks cause outages at Twitter, Spotify, and other sites”. In: *TechCrunch* (2016).

[7] Nicky Wolf. “DDoS attack that disrupted internet was largest of its kind in history, experts say”. In: *The Guardian* (2016).

[8] Paul Wood, ed. *Internet Security Threat Report (ISTR)*. Apr. 2016. URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

[9] *Internet Security Threat Report (ISTR)*. Apr. 2017. URL: https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8.pdf?aid=elq_.

[10] David Bellhouse. "The problem of Waldegrave". In: *Electronic Journal for the History of Probability and Statistics* 3.2 (2007), pp. 1–12.

[11] Quillau, Jacques 1702-1729?, et al. *Essay d'analyse sur les jeux de hazard*. chez Jacque Quillau, imprimeur-juré-libraire de l'Université, rue Galande, 1713.

[12] James Madison. "Vices of the political system of the United States". In: *The Founders' Constitution* (1787).

[13] John Von Neumann. "Zur Theorie der Gesellschaftsspiele". English. Trans. by A.W. Tucker and R.D. Luce. In: *Mathematische Annalen* 100 (1928), pp. 295–320.

[14] J von Neumann, Oskar Morgenstern, et al. *Theory of games and economic behavior*. Vol. 60. Princeton university press Princeton, 1944.

[15] John Nash. "Non-cooperative games". In: *Annals of mathematics* (1951), pp. 286–295.

[16] John F Nash Jr. "The bargaining problem". In: *Econometrica: Journal of the Econometric Society* (1950), pp. 155–162.

[17] John F Nash et al. "Equilibrium points in n-person games". In: *Proc. Nat. Acad. Sci. USA* 36.1 (1950), pp. 48–49.

[18] John Nash. "Two-person cooperative games". In: *Econometrica: Journal of the Econometric Society* (1953), pp. 128–140.

[19] Steven Kuhn. *Prisoner's Dilemma*. In: *Standford Encyclopedia of Philosophy*. Ed. by Edward N. Zalta. 2014. URL: http://plato.stanford.edu/archives/fall2014/entries/prisoner-dilemma/ (visited on 2016).

[20] Martin J Osborne and Ariel Rubinstein. *A course in game theory*. MIT press, 1994.

[21] Steve J. Heims. *John von Neumann and Norbert Wiener: From Mathematics to the Technologies of Life and De*. MIT Press, 1980.

[22] Adam Brandenburger. "Cooperative game theory". In: *Teaching Materials at New York University* (2007).

[23] Robert J Aumann. "Game theory". In: *Game Theory*. Springer, 1989, pp. 1–53.

[24] Peter G Capek, David M Chess, Steve R White, and Alan Fedeli. "Merry christma: an early network worm". In: *IEEE security & privacy* 1.5 (2003), pp. 26–34.

[25] David A Burke. *Towards a game theory model of information warfare*. Tech. rep. DTIC Document, 1999.

[26] Aditya Akella, Srinivasan Seshan, Richard Karp, Scott Shenker, and Christos Papadimitriou. "Selfish behavior and stability of the internet:: a game-theoretic analysis of TCP". In: *ACM SIGCOMM Computer Communication Review*. Vol. 32. 4. ACM. 2002, pp. 117–130.

[27] Tansu Alpcan and Tamer Basar. "A game theoretic approach to decision and analysis in network intrusion detection". In: *Decision and Control, 2003. Proceedings. 42nd IEEE Conference on*. Vol. 3. IEEE. 2003, pp. 2595–2600.

[28] Tansu Alpcan and Tamer Basar. "A game theoretic analysis of intrusion detection in access control systems". In: *Decision and Control, 2004. CDC. 43rd IEEE Conference on*. Vol. 2. IEEE. 2004, pp. 1568–1573.

[29] Tansu Alpcan and Tamer Basar. "An intrusion detection game with limited observations". In: *12th Int. Symp. on Dynamic Games and Applications, Sophia Antipolis, France*. Vol. 26. 2006.

[30] Michael Bloem, Tansu Alpcan, and Tamer Basar. “Intrusion response as a resource allocation problem”. In: *Proceedings of the 45th IEEE Conference on Decision and Control*. IEEE. 2006, pp. 6283–6288.

[31] Murali Kodialam and TV Lakshman. “Detecting network intrusions via sampling: a game theoretic approach”. In: *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*. Vol. 3. IEEE. 2003, pp. 1880–1889.

[32] Afrand Agah, Sajal K Das, Kalyan Basu, and Mehran Asadi. “Intrusion detection in sensor networks: A non-cooperative game approach”. In: *Network Computing and Applications, 2004.(NCA 2004). Proceedings. Third IEEE International Symposium on*. IEEE. 2004, pp. 343–346.

[33] Animesh Patcha and J-M Park. “A game theoretic approach to modeling intrusion detection in mobile ad hoc networks”. In: *Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC*. IEEE. 2004, pp. 280–284.

[34] Yu Liu, Cristina Comaniciu, and Hong Man. “A Bayesian game approach for intrusion detection in wireless ad hoc networks”. In: *Proceeding from the 2006 workshop on Game theory for communications and networks*. ACM. 2006, p. 4.

[35] Aron Laszka and Galina Schwartz. “Becoming Cybercriminals: Incentives in Networks with Interdependent Security”. In: *International Conference on Decision and Game Theory for Security*. Springer. 2016, pp. 349–369.

[36] Eirini Eleni Tsiropoulou, John S Baras, Symeon Papavassiliou, and Gang Qu. “On the Mitigation of Interference Imposed by Intruders in Passive RFID Networks”. In: *International Conference on Decision and Game Theory for Security*. Springer. 2016, pp. 62–80.

[37] Afrand Agah, Sajal K Das, and Kalyan Basu. “A game theory based approach for security in wireless sensor networks”. In: *Performance, Computing, and Communications, 2004 IEEE International Conference on*. IEEE. 2004, pp. 259–263.

[38] Jonathan M McCune, Elaine Shi, Adrian Perrig, and Michael K Reiter. “Detection of denial-of-message attacks on sensor network broadcasts”. In: *2005 IEEE Symposium on Security and Privacy (S&P’05)*. IEEE. 2005, pp. 64–78.

[39] Afrand Agah, Kalyan Basu, and Sajal K Das. “Preventing DoS attack in sensor networks: a game theoretic approach”. In: *IEEE International Conference on Communications, 2005. ICC 2005. 2005*. Vol. 5. IEEE. 2005, pp. 3218–3222.

[40] Afrand Agah, Kalyan Basu, and Sajal K Das. “Security enforcement in wireless sensor networks: A framework based on non-cooperative games”. In: *Pervasive and Mobile Computing* 2.2 (2006), pp. 137–158.

[41] Yizhong Ma, Hui Cao, and Jun Ma. “The intrusion detection method based on game theory in wireless sensor network”. In: *Ubi-Media Computing, 2008 First IEEE International Conference on*. IEEE. 2008, pp. 326–331.

[42] Libin Yang, Dejun Mu, and Xiaoyan Cai. “Preventing dropping packets attack in sensor networks: A game theory approach”. In: *Wuhan University Journal of Natural Sciences* 13.5 (2008), pp. 631–635.

[43] Yenumula B Reddy. “A game theory approach to detect malicious nodes in wireless sensor networks”. In: *Sensor Technologies and Applications, 2009. SENSORCOMM’09. Third International Conference on*. IEEE. 2009, pp. 462–468.

[44] Wenjing Wang, Mainak Chatterjee, and Kevin Kwiat. “Coexistence with malicious nodes: A game theoretic approach”. In: *Game Theory for Networks, 2009. GameNets’ 09. International Conference on*. IEEE. 2009, pp. 277–286.

[45] Nageswara SV Rao, Stephen W Poole, Chris YT Ma, Fei He, Jun Zhuang, and David KY Yau. “Defense of Cyber Infrastructures Against Cyber-Physical Attacks Using Game-Theoretic Models”. In: *Risk Analysis* (2015).

[46] Milad Nasr and Amir Houmansadr. “GAME OF DECOYS: Optimal Decoy Routing Through Game Theory”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM. 2016, pp. 1727–1738.

[47] Eitan Altman, Aniruddha Singhal, Corinne Touati, and Jie Li. “Resilience of routing in parallel link networks”. In: *International Conference on Decision and Game Theory for Security*. Springer. 2016, pp. 3–17.

[48] Hayreddin Çeker, Jun Zhuang, Shambhu Upadhyaya, Quang Duy La, and Boon-Hee Soong. “Deception-Based Game Theoretical Approach to Mitigate DoS Attacks”. In: *International Conference on Decision and Game Theory for Security*. Springer. 2016, pp. 18–38.

[49] Zesheng Chen. “Modeling and defending against internet worm attacks”. PhD thesis. Georgia Institute of Technology, 2007.

[50] Kien C Nguyen, Tansu Alpcan, and Tamer Basar. “Security games with incomplete information”. In: *2009 IEEE International Conference on Communications*. IEEE. 2009, pp. 1–6.

[51] Barbara Kordy, Sjouke Mauw, Matthijs Melissen, and Patrick Schweitzer. “Attack–defense trees and two-player binary zero-sum extensive form games are equivalent”. In: *International Conference on Decision and Game Theory for Security*. Springer. 2010, pp. 245–256.

[52] Bruce Schneier. “Attack trees”. In: *Dr. Dobb’s journal* 24.12 (1999), pp. 21–29.

[53] Yi Luo, Ferenc Szidarovszky, Youssif Al-Nashif, and Salim Hariri. “Game theory based network security”. In: *Journal of Information Security* 1.1 (2010), p. 41.

[54] Mohammad A Noureddine, Ahmed Fawaz, William H Sanders, and Tamer Başar. "A Game-Theoretic Approach to Respond to Attacker Lateral Movement". In: *International Conference on Decision and Game Theory for Security*. Springer. 2016, pp. 294–313.

[55] Kassem Kallas, Benedetta Tondi, Riccardo Lazzeretti, and Mauro Barni. "Consensus Algorithm with Censored Data for Distributed Detection with Corrupted Measurements: A Game-Theoretic Approach". In: *International Conference on Decision and Game Theory for Security*. Springer. 2016, pp. 455–466.

[56] Xiaoqi Li and Michael R Lyu. "A novel coalitional game model for security issues in wireless networks". In: *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*. IEEE. 2008, pp. 1–6.

[57] Shahrzad Gholami, Bryan Wilder, Matthew Brown, Arunesh Sinha, Nicole Sintov, and Milind Tambe. "A Game Theoretic Approach on Addressing Collusion among Human Adversaries". In: *Proceedings of the 15th International Conference on Autonomous Agents and Multiagent Systems*. 2016.

[58] Shahrzad Gholami, Bryan Wilder, Matthew Brown, Dana Thomas, Nicole Sintov, and Milind Tambe. "Divide to Defend: Collusive Security Games". In: *International Conference on Decision and Game Theory for Security*. Springer. 2016, pp. 272–293.

[59] Cui Xiaolin, Tan Xiaobin, Zhang Yong, and Xi Hongsheng. "A markov game theory-based risk assessment model for network information system". In: *Computer Science and Software Engineering, 2008 International Conference on*. Vol. 3. IEEE. 2008, pp. 1057–1061.

[60] Lawrence Carin, George Cybenko, and Jeff Hughes. "Cybersecurity strategies: The queries methodology". In: *Computer* 41.8 (2008), pp. 20–26.

[61] Sankardas Roy, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Vivek Shandilya, and Qishi Wu. “A Survey of Game Theory As Applied to Network Security”. In: *Proceedings of the 2010 43rd Hawaii International Conference on System Sciences*. HICSS ’10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 1–10. ISBN: 978-0-7695-3869-3. DOI: 10.1109/HICSS.2010.35. URL: http://dx.doi.org/10.1109/HICSS.2010.35.

[62] Samuel N Hamilton, Wendy L Miller, Allen Ott, and O Sami Saydjari. “The role of game theory in information warfare”. In: *4th Information survivability workshop (ISW-2001/2002), Vancouver, Canada*. 2002.

[63] Shigen Shen, Guangxue Yue, Qiying Cao, and Fei Yu. “A survey of game theory in wireless sensor networks security”. In: *Journal of Networks* 6.3 (2011), pp. 521–532.

[64] Xiannuan Liang and Yang Xiao. “Game theory for network security”. In: *IEEE Communications Surveys & Tutorials* 15.1 (2013), pp. 472–486.

[65] Xiaotao Feng, Zizhan Zheng, Prasant Mohapatra, and Derya Cansever. “A Stackelberg Game and Markov Modeling of Moving Target Defense”. In: ().

[66] R. JAIN and S. Paul. “Network virtualization and software defined networking for cloud computing: a survey”. In: *Communications Magazine, IEEE* 51.11 (Nov. 2013), pp. 24–31.

[67] S. Scott-Hayward, G. O’Callaghan, and S. Sezer. “SDN Security: A Survey”. In: *Future Networks and Services, 2013 IEEE SDN for*. Nov. 2013, pp. 1–7.

[68] Douglas C MacFarland and Craig A Shue. “The SDN Shuffle: Creating a Moving-Target Defense using Host-based Software-Defined Networking”. In: *Proceedings of the Second ACM Workshop on Moving Target Defense*. ACM. 2015, pp. 37–41.

[69] Jafar Haadi Jafarian, Ehab Al-Shaer, and Qi Duan. “Openflow Random Host Mutation: Transparent Moving Target Defense Using Software Defined Networking”.

In: *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*. Helsinki, Finland: ACM, 2012, pp. 127–132. ISBN: 978-1-4503-1477-0.

[70] Diego Kreutz, Fernando Ramos, and Paulo Verissimo. "Towards secure and dependable software-defined networks". In: *2nd SIGCOMM workshop on Hot topics in software defined networking*. ACM. 2013, pp. 55–60.

[71] Min Suk Kang, Soo Bum Lee, and Virgil D Gligor. "The crossfire attack". In: *Symposium on Security and Privacy (SP)*. IEEE. 2013, pp. 127–141.

[72] A. Aydeger, N. Saputro, K. Akkaya, and M. Rahman. "Mitigating Crossfire Attacks Using SDN-Based Moving Target Defense". In: *41st IEEE Conference on Local Computer Networks*. 2016, pp. 627–630.

[73] Mehrdad Nojoumian and Douglas R. Stinson. "Socio-Rational Secret Sharing as a New Direction in Rational Cryptography". In: *3rd International Conference on Decision and Game Theory for Security (GameSec)*. Vol. 7638. LNCS. Budapest, Hungary: Springer, 2012, pp. 18–37.

[74] Mehrdad Nojoumian. "Generalization of Socio-Rational Secret Sharing with a New Utility Function". In: *12th IEEE Annual Int Conf on Privacy, Security and Trust*. Toronto, Canada, 2014, pp. 338–341.

[75] T. Wang, F. Liu, J. Guo, and H. Xu. "Dynamic SDN controller assignment in data center networks: Stable matching with transfers". In: *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*. Apr. 2016, pp. 1–9.

[76] H. Chen, G. Cheng, and Z. Wang. "A game-theoretic approach to elastic control in software-defined networking". In: *China Communications* 13.5 (May 2016), pp. 103–109.

[77] A. Ksentini, M. Bagaa, T. Taleb, and I. Balasingham. “On using bargaining game for Optimal Placement of SDN controllers”. In: *IEEE International Conference on Communications*. May 2016, pp. 1–6.

[78] Jafar Haadi Jafarian, Ehab Al-Shaer, and Qi Duan. “Formal Approach for Route Agility against Persistent Attackers”. In: *Computer Security – ESORICS 2013: 18th European Symposium on Research in Computer Security, Egham, UK, September 9-13, 2013. Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 237–254.

[79] A. R. Chavez, W. M. S. Stout, and S. Peisert. “Techniques for the dynamic randomization of network attributes”. In: *International Carnahan Conference on Security Technology*. Sept. 2015, pp. 1–6.

[80] Panos Kampanakis, Harry Perros, and Tsegereda Beyene. “SDN-based solutions for Moving Target Defense network protection”. In: *15th IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks*. IEEE. 2014, pp. 1–6.

[81] Li Wang and Dinghao Wu. “Moving Target Defense Against Network Reconnaissance with Software Defined Networking”. In: *Information Security: 19th International Conference, ISC 2016, Honolulu, HI, USA, September 3-6, 2016. Proceedings*. Ed. by Matt Bishop and A. Anderson C. Nascimento. Springer International Publishing, 2016, pp. 203–217.

[82] Sankardas Roy, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Vivek Shandilya, and Qishi Wu. “A survey of game theory as applied to network security”. In: *43rd Hawaii International Conference on System Sciences (HICSS)*. IEEE. 2010, pp. 1–10.

[83] Mehrdad Nojoumian and Timothy C. Lethbridge. “A New Approach for the Trust Calculation in Social Networks”. In: *E-business and Telecommunication Networks:*

3rd International Conference on E-Business, Best Papers. Vol. 9. CCIS. Springer, 2008, pp. 64–77.

[84] Mehrdad Nojoumian. “Novel Secret Sharing and Commitment Schemes for Cryptographic Applications”. PhD thesis. Department of Computer Science, UWaterloo, Canada, 2012.

[85] Satoshi Nakamoto. “Bitcoin: A peer-to-peer electronic cash system”. In: *Bitcoin. org,[cit. 2014-11-13]. URL: https://bitcoin.org/bitcoin.pdf* (2008).

[86] Meni Rosenfeld. “Analysis of bitcoin pooled mining reward systems”. In: *arXiv preprint arXiv:1112.4980* (2011).

[87] Ittay Eyal and Emin Gün Sirer. “Majority is not enough: Bitcoin mining is vulnerable”. In: *Int. conf. on financial crypto and data security*. Springer. 2014, pp. 436–454.

[88] Benjamin Johnson, Aron Laszka, Jens Grossklags, Marie Vasek, and Tyler Moore. “Game-theoretic analysis of DDoS attacks against Bitcoin mining pools”. In: *International Conference on Financial Cryptography and Data Security*. Springer. 2014, pp. 72–86.

[89] Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. “Eclipse Attacks on Bitcoin’s Peer-to-Peer Network.” In: *USENIX Security Symposium*. 2015, pp. 129–144.

[90] Kartik Nayak, Srijan Kumar, Andrew Miller, and Elaine Shi. “Stubborn mining: Generalizing selfish mining and combining with an eclipse attack”. In: *European Symposium on Security and Privacy (EuroS&P)*. IEEE. 2016, pp. 305–320.

[91] Marie Vasek, Micah Thornton, and Tyler Moore. “Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem”. In: *International Conference on Financial Cryptography and Data Security*. Springer. 2014, pp. 57–71.

[92] Moshe Babaioff, Shahar Dobzinski, Sigal Oren, and Aviv Zohar. “On bitcoin and red balloons”. In: *13th ACM conference on electronic commerce*. ACM. 2012, pp. 56–73.

[93] Andreas M Antonopoulos. *Mastering Bitcoin: unlocking digital cryptocurrencies*. ” O’Reilly Media, Inc.”, 2014.

[94] Joshua A Kroll, Ian C Davey, and Edward W Felten. “The economics of Bitcoin mining, or Bitcoin in the presence of adversaries”. In: *Proceedings of WEIS*. Vol. 2013. 2013.

[95] Simon Barber, Xavier Boyen, Elaine Shi, and Ersin Uzun. “Bitter to better-how to make bitcoin a better currency”. In: *International Conference on Financial Crypto and Data Security*. Springer. 2012, pp. 399–414.

[96] Miles Carlsten, Harry Kalodner, S Matthew Weinberg, and Arvind Narayanan. “On the instability of bitcoin without the block reward”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM. 2016, pp. 154–167.

[97] Loi Luu, Ratul Saha, Inian Parameshwaran, Prateek Saxena, and Aquinas Hobor. “On power splitting games in distributed computation: The case of bitcoin pooled mining”. In: *Computer Security Foundations Symposium (CSF), 2015 IEEE 28th*. IEEE. 2015, pp. 397–411.

[98] Ittay Eyal. “The miner’s dilemma”. In: *Security and Privacy (SP), 2015 IEEE Symposium on*. IEEE. 2015, pp. 89–103.

[99] Yoad Lewenberg, Yonatan Sompolinsky, and Aviv Zohar. “Inclusive block chain protocols”. In: *Int. Conf. on Financial Crypto and Data Security*. Springer. 2015, pp. 528–547.

[100] Meni Rosenfeld. “Analysis of hashrate-based double spending”. In: *arXiv preprint arXiv:1402.2009* (2014).

[101] Yonatan Sompolinsky and Aviv Zohar. “Secure high-rate transaction processing in bitcoin”. In: *International Conference on Financial Cryptography and Data Security*. Springer. 2015, pp. 507–527.

[102] Mehrdad Nojoumian. “Rational Trust Modeling”. In: *https://arxiv.org/abs/1706.09861*. Arxiv, 2017, 12 pages.

[103] Afrand Agah and Sajal K Das. “Preventing DoS attacks in wireless sensor networks: A repeated game theory approach.” In: *IJ Network Security* 5.2 (2007), pp. 145–153.

[104] Jorma Jormakka and JVE Molsa. “Modelling information warfare as a game”. In: *Journal of information warfare* 4.2 (2005), pp. 12–25.

[105] Peng Liu, Wanyu Zang, and Meng Yu. “Incentive-based modeling and inference of attacker intent, objectives, and strategies”. In: *ACM Transactions on Information and System Security (TISSEC)* 8.1 (2005), pp. 78–118.

[106] Kong-wei Lye and Jeannette M Wing. “Game strategies in network security”. In: *International Journal of Information Security* 4.1-2 (2005), pp. 71–86.