9-9-2015

Modeling Security and Resource Allocation for Mobile Multi-hop Wireless Neworks Using Game Theory

Laurent L. Y. Njilla
Florida International University, lyame001@fiu.edu

DOI: 10.25148/etd.FIDC000182

FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

MODELING SECURITY AND RESOURCE ALLOCATION FOR MOBILE MULTI-HOP WIRELESS NETWORKS USING GAME THEORY

A dissertation submitted in partial fulfillment of

the requirements for the degree of

DOCTOR OF PHILOSOPHY

in

ELECTRICAL ENGINEERING

by

Laurent Lavoisier Yamen Njilla

2015

To: Interim Dean Ranu Jung
College of Engineering and Computing

This dissertation, written by Laurent Lavoisier Yamen Njilla, and entitled Modeling Security and Resource Allocation for Mobile Multi-Hop Wireless Networks Using Game Theory, having been approved in respect to style and intellectual content, is referred to you for judgment.

We have read this dissertation and recommend that it be approved.

Jean Andrian

Deng Pan

Kang Yen

Charles Alexandre Kamhoua

Niki Pissinou, Major Professor

Date of Defense: September 9, 2015

The dissertation of Laurent Lavoisier Yamen Njilla is approved.

Interim Dean Ranu Jung
College of Engineering and Computing

Dean Lakshmi N. Reddi
University Graduate School

Florida International University, 2015

DEDICATION

To the Njillas:

Isaac Njilla, Emilienne Njilla:

Honoré Njilla, Rostand Njilla, Hildegarde Njilla,

Eugenie Njilla, Herrick Njilla, Dieunedort Njilla, and Emilie C. Y. Njilla.

ACKNOWLEDGMENTS

There are numerous important milestones in our lives. The transition between these milestones may be smooth and mild; the end of a milestone is marked by an event. In the scientific life, one such event is the completion of a PhD dissertation. This document represents the outcome of more than four years of research efforts.

When glancing back, the outcome of this research has strongly been influenced by many people who accompanied me during the whole or part of the work in my academic and private life. Therefore, this is also the occasion to thank these people and to acknowledge their support.

I would express my gratitude to my advisor Dr. Niki Pissinou for her direction, advice and support throughout my PhD. studies at the Florida International University. I am deeply indebted to Dr. Niki Pissinou for showing me the excitement that can be found in collaborative academic research and for allowing me to work independently too. Her guidance has helped to mold me into a successful researcher and mentor and has equipped me with the tools necessary to be successful in the future of my career. I hope to be able to live up to her expectations.

I would also like to thank the members of my Ph.D. supervisory committee: Dr. Kang Yen, Dr. Deng Pan, Dr. Jean Andrian and Dr. Charles Kamhoua. Their constructive comments have improved the quality of this work. They have been helpful during the entire Ph.D. process. I would like to extend my thanks to Dr. Charles Kamhoua for his collaboration and all the discussions we had days and nights on game theory and the summer internship at the Air Force Research Laboratory (AFRL)

My frequent exchanges and co-authoring with Dr. Kia Makki have been reflective, all my gratitude. My appreciation to Dr. Kevin Kwiat of the Air Force Research Laboratory, CyberSecurity Division. Our initial conversation on agility, recovery and network security has been insightful. The work on Chapter 7: Cyber Security Resource Allocation: A Markov Decision Process Approach was conducted while in an intership at the Air Force Research Laboratory, Rome, NY site and it is included in the dissertation with the permission of Dr. Kevin Kwiat, Principal Computer Engineer.

I also thank Dr. Shekhar Bhansali and the excellent faculty members of the Electrical and Computer Engineering Department. Their lectures and class projects have been influential, and thank you to Ms. Maria Benincasa and Ms. Pat Brammer.

Because of their constant motivation, I would like to thank my fellow research lab mates. Likewise, I appreciate the comments and work of the undergraduate student Patricia Echual I have mentored in the NSF/REU program. Thanks to Bob, Darrius, Mark, Oscar, Rich, Ricky for the endless discussion we had at the City of Miami Beach, IT Department.

I am thankful to Jackie Genard, Christ'Ella Francis and Emilie for the stimulation and support they have provided me during this journey. Furthermore, words are not enough to express the love and blessings from my family members. I would like to appreciate all the devotion and sacrifice made by Emilie C. Yamen, my little daughter, for making this dissertation possible just by loving me.

Finally, I would like to acknowledge that my graduate studies have been partially

funded by the Department of Homeland Security (grant# 2008-ST-062-000012), the Air Force Office of Scientific Research (grant# FA9550-14-1-0299), the National Science Foundation (grant# 1263124) and the McKnight Foundation through the McKnight Doctoral Fellowship (MDF).

ABSTRACT OF THE DISSERTATION

MODELING SECURITY AND RESOURCE ALLOCATION FOR MOBILE MULTI-HOP WIRELESS NETWORKS USING GAME THEORY

by

Laurent Lavoisier Yamen Njilla

Florida International University, 2015

Miami, Florida

Professor Niki Pissinou, Major Professor

This dissertation presents novel approaches to modeling and analyzing security and resource allocation in mobile ad hoc networks (MANETs). The research involves the design, implementation and simulation of different models resulting in resource sharing and security's strengthening of the network among mobile devices. Because of the mobility, the network topology may change quickly and unpredictably over time. Moreover, data-information sent from a source to a designated destination node, which is not nearby, has to route its information with the need of intermediary mobile nodes. However, not all intermediary nodes in the network are willing to participate in data-packet transfer of other nodes. The unwillingness to participate in data forwarding is because a node is built on limited resources such as energy-power and data. Due to their limited resource, nodes may not want to participate in the overall network objectives by forwarding data-packets of others in fear of depleting their energy power.

To enforce cooperation among autonomous nodes, we design, implement and simulate new incentive mechanisms that used game theoretic concepts to analyze and model the strategic interactions among rationale nodes with conflicting interests. Since there is no central authority and the network is decentralized, to address the concerns of mobility of selfish nodes in MANETs, a model of security and trust relationship was designed and implemented to improve the impact of investment into trust mechanisms. A series of simulations was carried out that showed the strengthening of security in a network with selfish and malicious nodes. Our research involves bargaining for resources in a highly dynamic ad-hoc network. The design of a new arbitration mechanism for MANETs utilizes the Dirichlet distribution for fairness in allocating resources. Then, we investigated the problem of collusion nodes in mobile ad-hoc networks with an arbitrator. We model the collusion by having a group of nodes disrupting the bargaining process by not cooperating with the arbitrator. Finally, we investigated the resource allocation for a system between agility and recovery using the concept of Markov decision process. Simulation results showed that the proposed solutions may be helpful to decision-makers when allocating resources between separated teams.

TABLE OF CONTENTS

CHAPTER PAGE

LIST OF TABLES

TABLE PAGE

LIST OF FIGURES

FIGURE PAGE

CHAPTER 1

INTRODUCTION

The continuing advances in wireless communications and hardware design technology have led to the manufacturing of low-cost, low-maintenance and easy to deploy devices in order to create an ad-hoc network without relying on pre-existing infrastructure. The nurturing dream of building a pervasive and ubiquitous network is becoming highly plausible. A pervasive network by definition has the ability to offer spontaneous services created on-the-fly by autonomous mobile devices that interact with ad-hoc connections. Moreover, the ubiquitous network is the concept that provides available services in a network by giving users the ability to access services anytime and irrespective of their location. [1] [2].

To fulfill this vision of a network, it requires the participation of several devices or nodes, from multiple network domains with completely diverse objectives and preferences. With the rapid advances in computer and wireless communications, devices and all associated techniques and concepts, mobile sensor networks are becoming practical and attracting more research attention in recent years. The decentralized nature, minimal configuration and quick and easy deployment of wireless ad hoc networks make them suitable for emergency situations, such as natural disasters or military conflicts where there is no infrastructure or central nodes to depend on. Wireless ad hoc networks have emerged as an important information transmission paradigm in both military and commercial applications such as intrusion detection, battlefield surveillance, disaster rescue missions, hostile environment monitoring and target tracking. Flexibility, on the other hand, brings in many research challenges.

The mobility of the device is also a challenge due to the ubiquity of the network. By nature, wireless ad-hoc network is a highly dynamic self-organizing network with limited channels. Servicing mobile users brought a new prospective to an already dynamic network, the mobile ad-hoc networks (MANETs). A MANET is a self-organizing, self-configuring network of mobile hosts wirelessly interconnected. The mobile hosts or mobile nodes (MNs) are free to move randomly and organize themselves arbitrarily. Therefore, the network connectivity and topology could be dynamically changed rapidly and unpredictably [3]. A MANET can be operated in a stand alone, or connected to other networks. Moreover, a MANET can be quickly deployed in any area. Without the support of any fixed infrastructure, mobile nodes need to cooperate with each other to maintain the link and routing information. Each MN acts not only as a host, but also as a router for data forwarding between other MNs.

Network security and device autonomy, for example, are major issues in order to achieve robust and reliable communication in wireless ad hoc networks. The wireless communication between typically autonomous devices, where each device makes a decision whether and to what extent it wishes to be part of the network's main purpose, can become a challenge. In the pursuit of their own objectives, the participating devices in the network could therefore exhibit some misbehavior patterns – either by being selfish or by being malicious [4]. Because of their limited resources like battery power, low radio transmission range, memory spaces and computational power, a selfish node attempts to save its resources by not participating in any network task. As a consequence, each node will strive to save its limited supply while competing against needy nodes with a depleted supply to gain access to others' resources with the goal of maximizing their own capacity. A malicious node's main objective is to cause damage to the network. They use their available resources to launch various attacks, for example, Denial of service (DoS), selective forwarding, Sybil attack and sinkhole attack. The faulty node misbehaves in the network because of the default in its circuitry which may be due to a physical damage. The internal damage causes the node not to follow the protocol recommendations.

The security is the primary concern of an ad-hoc network deployed infrastructure-less. The network needs to guarantee a secure data transmission between different nodes and also, the confidentiality, the integrity and the availability of the data should be guaranteed. Henceforth, the primary issue that would arise with autonomous nodes in an ad hoc network would be packet forwarding. Moreover, here is a scenario, nodes are selfish and there is neither infrastructure nor a central authority. When the sender and the destination are not in transmission range, packets are sent through a multi-hop communication. Intermediary nodes are needed to facilitate packet forwarding. But, there is a transmission cost in battery power usage and bandwidth associated with forwarding packets and therefore, it is not in the best interest of an intermediate node to deplete its own resources to forward others's packets. Meanwhile, if all nodes behave the same way by refusing to forward packets for others, the network will collapse. However, no node is interested in a collapsed network as the outcome.

The network performance degradation can be attributed to node misbehavior. Therefore, proficient mechanisms need to be implemented to enforce node cooperation and strengthen network security at all layer levels. In fact, selfish behavior is a thorn in the side of networks without central authority. Selfishness and overall network objectives may be the cause of misbehaviors in other layers of the network with autonomous nodes. For instance, by looking at the different layers of the network, there is a tremendous impact that selfish nodes can cause. For example, at the physical layer, a node can selfishly decide to ignore the network protocol by increasing its power to transmit its packets at a successful rate after detecting failure. The general response of other selfish nodes in the vicinity would be to follow the actions generating the successful transmission rate. As for the result, the overall network performance will decrease and deteriorate tremendously which will cause the collapse of the network. At the link/MAC layer, some nodes may attempt to send more packets by ignoring the backoff period. While the backoff period occurs for other nodes to use the medium for transmission, so instead of waiting for other nodes to finish sending their packets, a selfish node may attempt to quickly send its own packets. As a consequence, an increase in packet collision would drastically affect the network performance because of selfish nodes. On the transport layer, the most widely used protocol in this layer is the User Datagram Protocol (UDP) and the Transmission Control Protocol (TCP) [5] [6]. The main reasons for TCP performance degradation in MANETs are contention between sharing terminals, hidden terminal problems, and packet losses in the MAC layer. Furthermore, path disconnections arising from mobility and exponential retransmission backoff in the TCP layer also exacerbate performance. A selfish node may be unwilling to decrease its window size during congestion to take full advantage of its own flow. Therefore, in the case that all nodes follow the same behavior, congestion and contention in the network will be worsened.

Security mechanisms in traditional wired networks rely on trusted systems like certificate authority (CA) to manage security operations. In the absence of such authority, nodes are required to integrate tools to auto-secure themselves and to rely (trust) on each other to secure the network and protect their privacy. Trust, in this circumstance, can be defined as the confidence a node in the network has about the appropriate participation of others in the security mechanism. Without trust, no rational node will participate in any security mechanism that involves the cooperation of numerous nodes to be successful. Therefore, several security mechanisms require some level of trust in their design and implementation [7]. Let us consider a provider with users to provide network services. Securing the network service in order to protect the users' privacy and personal information against cyberattacks or hackers is costly for the service providers. A provider would prefer to minimize its investment in upgrading the network infrastructure while financially increasing its bottom line with customers using the service or product. On the other hand, without regular upgrades to the network infrastructures from the provider, there are vulnerabilities generated from the software used or developed by programmers and components installed in the network; the upgrade of a vulnerability may open the system to other vulnerabilities. With the attackers always launching attacks, it is just a matter of time to breach the system due to an undetected or un-patched vulnerability. A breached system would have private information and privacy of the users compromised. One option available to unsatisfied users is to quit their service provider. Without any doubt, we are faced with a conflict of interest between a service provider and its users. The optimum behavior of the provider will be linked to the users' strategies.

Game theory is the unifying mathematical framework able to model the conflict of interests faced by different players in each circumstance above-mentioned and examine the possible solutions with a precise depiction of their properties [1]. Clearly, this is our justification of using game theory as the principal method employed in our research. It clearly shows that the realization of the ultimate of interconnection between any mobile devices, anytime, anywhere (ubiquitous) in life is not possible if the efficient connection and security mechanisms were not designed to stimulate nodes' participation or provide sufficient incentives to all network entities. Therefore, a network protocol at all layers must take into account the heterogeneity of sub-network components, interfacing between different MANETs and components and finally, the self-interest of autonomous nodes performing separate optimization. Cooperation among wireless multi-hop ad hoc nodes can also protect a network from malicious attacks. The absence of a central authority, trusted entity, new and different classes of distributed security mechanisms and privacy protections require cooperation among several mobile nodes to protect and secure a network from malicious attacks [8]. This dissertation addresses selfish and malicious nodes present in MANETs. The interconnection among highly mobile nodes, cooperation in resource sharing, and network security is studied and solutions are investigated.

1.1 RESEARCH OBJECTIVES

The evolvement from traditional wired to wireless networks has brought a shift in the primary concerns which need to be addressed for ad hoc wireless networks. Like their wired counterparts, wireless networks are interested in high throughput and low-cost design, network priorities will dictate a tradeoff for an increase in power efficiency and bandwidth optimization. The mobility of the node increases the primary concerns with the connectivity and moving patterns. The more confidently a node shares its resources with other nodes belonging to the same network; the more secure is the network and their applications. Our research stems from the recognition that mobile autonomous nodes with different intent will remain elusive unless a MANET with incentive mechanism is developed. The presence of selfish nodes in a mobile heterogeneous ad hoc network where autonomous put their own objectives ahead of the overall network objectives must be modified due to the fact that network protocols do not have a better control of the node mobility and the network operations. This dissertation involves the mechanism design, implementation, analysis and simulation evaluation of the resource allocation model and security strengthening model of strategic interactions in mobile ad hoc wireless multi-hop networks with selfish and malicious users using the game theoretic framework. Specifically, our investigative objective of this research is threefold:

1. Design distributed game theoretic algorithms using only local information to enforce nodes cooperation at the network routing layer and optimize network performance with autonomous nodes, and imperfect monitoring.
2. Investigate and propose satisfactory game theoretic solutions to the remarkable enhance in bandwidth demand and throughput due to an increase of the number of mobile devices.

3. Use game theory to analyze new security mechanisms for MANETs with autonomous nodes without a trusted authority or a central manager to strengthen the overall network.

Specially, our work focuses on:

- The study of various techniques for incorporating arbitration monitoring, incomplete information into the game model for networks using game theory.
- Evaluating the performance of models developed using game theory and investigating the underlying assumptions of those theories in the context of ad hoc networks with mobile nodes and dynamic change in the network topology.
- Designing a game theoretic algorithm for autonomous networks that achieve performance similar to those of cooperative networks with a central authority.
- Providing and detailing mathematical analysis of ad hoc network security models to capture in a general contest the equilibrium conditions in the MANET.
- Predicting the user and provider behaviors under diverse type of noise conditions.
- Simulating the designed models with known conventional software and tools that will allow any researcher to replicate the results if deem necessary.

1.2 SIGNIFICANCE

This research has an unprecedented impact in several areas. First, our work on cooperation enforcement at the routing layers provides significant insight into the problem of distributed decision-making, random mobility, random neighboring interactions, self-healing, self-organizing, and the resource proficiency needed to deal with rapid topology changes of the network. Our approach leads to a precise characterization of the properties of cooperation in MANETs.

Second, this research establishes solid frameworks for integrating practical network conditions into autonomous mobile network models. Practically, we mean incorporating random mobility, real arbitration monitoring, and private information into the model. Our research allows the self-interest of individual nodes to be in agreement with the overall interest network performance. Furthermore, as with traditional networks, autonomous networks need to be secured to authenticate the nodes, avoid exploitation, identify abnormality, and protect user's private data.

Our research provides novel concepts and fundamental knowledge concerning the modeling, mechanism design, analysis, and simulation of complex dynamic systems, including distributed autonomous network security. This work evaluates distributed security mechanism adequate for mobile ad hoc networks. Evidently, this research strengthens the interconnection of mobile autonomous devices in cyberspace for the peace of mind of each user.

1.3 ORGANIZATION AND CONTRIBUTION

The work in this dissertation is divided into several chapters. We have introduced the background, challenges, research objectives and approaches of this dissertation. The remainder of this dissertation is organized as follows. We review the comprehensive literature works related to mobile ad hoc networks and game theory that will provide an understanding and significant analysis of the tremendous contribution of the scientific world within the domain in chapter 2.

In chapter 3, we tackle the issue of dynamics of data delivery in MANETs using the bargaining game theoretic approach. The mobility of nodes makes it difficult to have a better timeframe when two nodes are in transmission range on top of the volatility of the wireless communication. The presence of selfish nodes in the path of routing to destination renders packet forwarding extremely weak. We model the dynamic packet forwarding problem as a modified Rubinstein-Ståhl bargaining game. In our model, a mobile player negotiates with the other mobile node to obtain an agreeable and respectable sharing rule of packet forwarding based on its own resource available, such that a node should not agree to forward packets without the energy or storage capacity to do so. We also consider finite horizon of the bargaining game because of the mobility of the nodes and the rupture of communication due to their velocity. The solution obtained from bargaining ensures that a mobile device always finds a peer to help forward packets in order to keep the network at flow.

In Chapter 4, the mobility that causes the topology changes provides to selfish nodes the ability to move around and not being participative to the overall network objectives. In order to incentivize in packet forwarding, an arbitrator is tasked to negotiate with nodes in need of data transfer. The arbitrator is considered like a temporary cluster head and the nodes in need of service are one hop away from the cluster head. The negotiation game is applied with one-way offer by the arbitrator and the players either accept or reject the offer. There is no alternating between players, only the arbitrator makes offers. The generate offers follows the Dirichlet distribution.

In chapter 5, security and trust are considered in cyberspace. Three types of entities are interacting in the game, the users, the service providers and the attackers. The attackers launch attacks on the service provider’s infrastructure in order to breach the system and compromise the users’ privacy and private information. On the other hand, the service provider needs to invest in security and protect users’ privacy and personal data and also provider’s private information. Users need to feel that their private information are not or will not be compromised by an insecure provider infrastructure in order to do business. A prisoner’s dilemma game (PDG) is implemented and equilibrium strategies are drawn. In Chapter 6, the mobility that causes the topology changes provides to selfish nodes the ability to move around and not being too participative to the overall network objectives. In order to incentivize nodes in packet forwarding, a selected arbitrator is tasked to negotiate with nodes in need of data transfer. Because of the collusion of selfish nodes may cause the drainage of energy power for any node bargaining against a colluder. The arbitrator has the difficult task based on historic data, to avoid node that has the pattern of rejecting offers. The negotiation game is also applied with one-way offer by the arbitrator and the players either accept or reject the offer. There are no alternating offers between players, only the arbitrator makes offers. Chapter 7 deals with resource allocation in cyberspace by using the Markov decision process (MDP) approach. The goal is to defend a system against cyber-attack using several independent methods. A two-way division is agility and recovery. Cyber agility pursues attack avoidance techniques such that cyber-attacks are rendered as ineffective; whereas cyber recovery seeks to fight-through successful attacks. Recovery should be an essential point during implementation because the frequency of attacks will degrade the system and a quick and fast recovery is necessary. However, there is not yet an optimum mechanism to allocate limited cyber security resources into the different layers.

Finally, in Chapter 8, we discuss our achievements, the limitations of the current outcomes including the simulation constraints, identify future research directions and conclude this dissertation.

CHAPTER 2:

RELATED WORK

A wireless ad hoc network is a self-organized network formed by peer nodes for common purpose without a pre-existing infrastructure as the backbone of such a network. Henceforth, data is exchanged between nodes by the sole effort of communicating nodes deployed with transmission capabilities. Nodes serve as routers to relay data in case the source and the destination are out of transmission range. The nature of no infrastructure communication in ad hoc networks requires nodes in the network to cooperate for the network to remain operational. However, some nodes may refrain from forwarding data packets of other nodes to preserve their limited energy resources. In addition to selfishness, other factors can degrade quality of cooperation. These factors include mobility and environmental obstructions. In this Chapter, we provide a brief survey of related research in the area. We review the research work on encouraging cooperation in mobile ad hoc networks (MANETs). We focus on research that aimed to overcome selfishness of autonomous nodes by providing incentives to participants for cooperating. We review the different cooperation approaches that have been proposed in the literature and focus on game theory as the domain of our contribution in this dissertation. Each approach is summarized and we identify their problems and limitations.

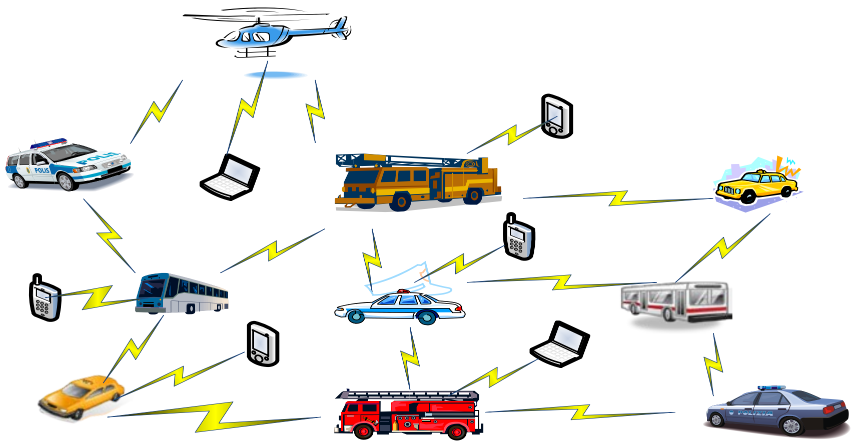


Figure 2.1: A Mobile Ad hoc Network (MANET).

2.1 MANETs Cooperation Schemes

Most of the literature review on encouraging, stimulating or enforcing cooperation in MANETs can be divided into two main categories: credit-based (a.k.a. price-based or virtual currency) [10] [11] [19] and reputation-based [3] [4] [12] [13]. The credit exchange in virtual currency systems, the distribution of reputation information and the reliability on promiscuous listening among neighboring nodes in reputation-based systems raise some issues regarding the scalability of the above approaches.

2.1.1 Credit-Based Schemes

In credit-based schemes, nodes use virtual currency to pay for packet forwarding services. Intermediate nodes charge for the relay service they are providing as a form of incentive for cooperation. The two most popular approaches using the virtual currency schemes as incentive are the Nuglet and Sprite. The authors in [10] proposed the Nuglets, a virtual currency to stimulate cooperation in self-organized MANETs. Two models are proposed to stimulate cooperation: the packet purse model and the packet trade model. For the packet trade model, the destination node pays for the packet-forwarding expenses. Moreover, each intermediate node along the path to destination buys and sells packets to be forwarded all the way to the destination. When a packet reaches its final destination, the destination node buys and owns the packet. Hence, there is an incentive to cooperate by intermediate nodes with a return on investment while spending their resources in packet forwarding. The limitations and issues of this approach are: the sender may not filter the type of message to send out and overloads the network, which may cause congestion. To solve the issue, the packet purse approach is modeled. In this model, the source node pays to send a packet to a destination node by loading some Nuglets in the "packet's purse". Each intermediate node along the path acquires some Nuglets from the packet before forwarding to the next hop or intermediary node. The packet is dropped from the network if there are not enough Nuglets for the service rendered. Tamper resistant software and hardware are required for both models to store the correct amount of Nuglets. Another issue includes the fact that at the moment of forwarding, a packet an intermediary (autonomous) node can decide to charge more, which will cause the packet not to have enough Nuglets to reach its destination.

The authors in [20] proposed Sprite. Sprite relies on a central authority: the Credit Clearance Service (CCS). Nodes keep a log (receipt) of all transactions they participate in. The logs are submitted to the CCS for clearance and to claim payment. The CCS determines the credit of each intermediate node and the cost to the sender. Sprite cautiously computes payment to prevent cheating and collusion among nodes. Unlike

Nuglets, Sprite does not require tamper proof hardware. However, the CCS as a central authority violates the premise of MANETs and may become a target for security threats.

2.1.2 Reputation Based Schemes

In reputation-based schemes, a node’s decision to cooperate with other nodes with packet forwarding impacts its own reputation. This decision is made by maintaining reputation information about other nodes in the network by tracking their behavior towards others. Reputation information is usually shared in the network using periodically exchanged messages. Unlike the credit-based scheme, which provides direct incentives to cooperating nodes, reputation-based instead punishes non-cooperating nodes. A non-cooperative node will have a bad reputation and nodes with good reputation will punish them by not forwarding their packets. Reputation information is collected at two levels: first-hand and second-hand. In the latter, second-hand reputation schemes [12] [13], nodes use direct and indirect observations to compute their reputation information bases. For indirect observations, information is conveyed to a node via its neighbors, it’s not collected by its own effort. We have promiscuous listening to neighbors' behavior, which is used to collect indirect reputation information, like in [3]. However, relying on information conveyed by others may not be completely accurate because of multiple factors, such as imperfect monitoring or hidden terminal issue. Although second-hand schemes incur an overhead in exchange of the reputation information collected, misbehavior report can be detected faster than first-hand systems. In first-hand schemes

[13], a node relies only on its own observations to evaluate the cooperation of other nodes and compute the reputation information.

Different systems have used the reputation model, in particular, the Beta reputation system [12] with a strong statistical background. A *watchdog* mechanism implemented on each node is used to monitor the behavior of its neighbors. After a packet is sent, the node equipped with an omnidirectional antenna listens and observes. If the packet has been forwarded by its neighbor or not, the result is recorded in a reputation table. Depending on the model implemented, models can share reputation information or not by applying the second hand information. Nevertheless, second-hand information improves the algorithm by accelerating its convergence time. However, second hand information overhead creates traffic load on the network. For different models implemented, there are also different weights assigned for new and old information. Assigning more weight to new information, cooperating nodes may lose their reputation in low network activity. Meanwhile, assigning more weight to old information, a malicious node may decide to accumulate a good reputation first, then start dropping packets without any punishment. Noted also, all packet loss is due to a node misbehavior. Thus, packet losses due to congestion in the network or noise in signal received are not taken into consideration. Michiardi and Molva in [4] developed CORE (COllaborative REputation). It’s a reputation mechanism for mobile ad hoc networks. Three types of reputation mechanism are used: we have a subjective reputation from first-hand information, then the indirect reputation from second-hand information, and third a functional reputation calculated in conjunction with different functions like forwarding and routing. The combination of reputation information is an issue in itself; reputation composite does not allow the mechanism to trust a node for one of its specific functions. The assigned weight to each function can be problematic. Moreover, to avoid a denial of service, only positive reputation information is propagated. However, a coalition of malicious nodes may propagate positive reputation of each other and gain longer access in the network. CORE is simulated using the Dynamic Source Routing (DSR) protocol and shows prominent performance results. Marti *et al* [22] proposed a combination system of a *watchdog* system and a *pathrather* that selects the best route to avoid malicious nodes. The system achieves an acceptable throughput in the presence of misbehaving nodes. However, this system does not get rid of misbehaving nodes. Malicious nodes can send their own packets in the network, even though they do not forward packets of other nodes. Buchegger *et al* [2] proposed Cooperation Of Nodes-Fairness In Dynamic Ad hoc NeTworks (CONFIDANT). CONFIDANT detects and quarantines misbehaving nodes. The CONFIDANT protocol is made of four components: the monitoring, the reputation, the path manager, and the trust manager. The monitoring is similar to the *watchdog* defined above, the reputation structure rates nodes, the trust manager issues Alarm messages on node behavior, and the path manager makes decisions when conflict occurs. CONFIDANT propagates only negative information. The authors' argument is that the malicious behavior is not the norm, but an exception. However, the protocol can allow misbehaving nodes to mount erroneous accusation attacks and cause the dismissal of cooperating nodes from the network.

The Reputation-based Framework for Sensor Networks (RFSN) is introduced in [13]. First and second-hand information are used for reputation. Only the first-hand information is propagated in the network as shared reputation. Moreover, to prevent misbehaving nodes to propagate false information (bad-mouthing attacks), only positive information is propagated. A combination of first-hand and second-hand information is used to obtain a new reputation value, Dempster-Shafer belief theory is used [13]. This takes into account the fact that reputation information from the most trusted nodes must have more weight. Nodes with low reputation are considered malicious and quarantined from the networks. Aging is used to give more weight to fresh information. Thus, cooperating nodes can lose their reputation in a network with low activity.

2.1.3 Other Schemes

To avoid the disadvantage of both credit-based and reputation-based system, researchers have exploited the fact that nodes in the network are autonomous and the device has limited resources. By combining both features in a node, there will always be a situation of conflict in interests. Some nodes in the network will always want to take advantage of the situation which is a rational behavior whenever there is no central authority in a group. The use of game theoretic modeling is convenient to analyze cooperation with incentives among nodes in the networks. In [1], the authors use game theory to analyze cooperation incentives provided by the type of cooperation schemes, and propose a hybrid system that offers strong incentives to encourage cooperation while ensuring quick and effective detection of selfish nodes.

Researchers in other work focus on horizontal improvements by enhancing features that are shared by most of the schemes in the literature. In [23], the proposed scheme avoids the need to maintain traces of past interactions. It permits to avoid tracking available credit and reputation information in credit-based and reputation-based systems, respectively.

The model aims to tag cooperative nodes in the network. Since cooperation between nodes will gain higher payoffs than selfish ones, the others will tend to join the cooperative group, with the assumption that nodes are rational. Subsequently, cooperative nodes will take over the population. In the next sections, we provide an introduction to basic concepts in game theory and their application to encourage cooperation in wireless networks. We, then, shed more light on bargaining game theory, and review the research work in the area of cooperation modeling in MANETs.

2.2 GAME THEORY

Game theory (GT) is a branch of applied mathematics that studies strategic interactions among rational players who look for best strategies to maximize their personal gain in response to others' strategies [1] [29] [30]. GT cannot be utilized to model irrational misbehavior of faulty components. Nonetheless, it is an adequate tool to analyze and mitigate selfish and malicious behaviors. Studying cooperation in MANETs using game theory provides a more comprehensive understanding of the process. In MANETs, the players are the nodes. Each node wants to maximize its own utility (payoff). In a game, a player decides whether to cooperate or not based on its evaluation of the prospective benefits and costs of cooperation and the expected strategies of other players in the network. Which means, send the most possible number of packets and forward the least number of packets while saving energy and bandwidth. A node's preferences are expressed in the form of a utility function that includes all factors that contribute to its satisfaction. The utility function reflects the node's objectives as it selects an action in response to the actions selected by other players. The main objective in a network is the convergence to a Pareto efficient Nash equilibrium. However, the challenge is that the allocations in the Nash equilibrium are not always Pareto efficient [31]. Here are some approaches that use game theory.

2.2.1 Cooperative Models

In cooperative games, players within the game cooperate to achieve common benefits. The most commonly used forms of cooperative games are coalitional games, in which nodes form coalitions that share benefits and follow common strategies. These coalitions compete with each others as opposed to individuals in non-cooperative games. Since coalition members follow agreed-on strategies to obtain shared benefits, there is an interest in the value of a coalition as an entity, which is the total amount of utility it can obtain as a whole, as compared to the payoff every member obtains by affiliating with a coalition [6]. The way the coalition value is divided among coalition members distinguishes transferable utility games (TU) from non-transferable utility games (NTU). In TU games, there is no restriction on the way utility can be divided among coalitional members. The clearest and simplest example of a unit of transfer for utility is money. Resource allocation in wireless networks is modeled as transferable utility game in [53], and grand coalition is shown to be stable in many cases. On the other hand, the payoff an individual player obtains in an NTU game depends on some factors, and among them is the coalition structure and formation sequence. In [31], the authors model cooperative spectrum sensing in cognitive radio networks as a non-transferable coalitional game, and use a simple merge and split algorithm to optimize coalition formation. We provide a more detailed discussion of features and solution concepts of coalitional game problems in the next section.

2.2.2 Non-Cooperative Models

In non-cooperative games, nodes strategically react individually to others' interactions based on the assessment of their own benefit. Jade *et al*. [32] combined credit-based and Stochastic Game Theory to formulate an optimal policy to forward packets towards route in peer-to-peer mobile networks. A source node requests data from the destination, each intermediate node that relays a packet is remunerated with a currency token. Their optimal policy is achieved based on cost, free bandwidth, and service capacity. The incentive-based routing protocol implemented shows a better performance when compared to the DSR protocol. Srinivasan *et al*. [21] motivated cooperation in a network by using Generous Tit For Tat (GTFT). The authors showed that GTFT is a Nash equilibrium (NE) of the forwarding game. However, each node must know all nodes in the network in order to compute the equilibrium of the game. For a MANET, the notion of each node to know all nodes available is a strong requirement for distributed networks.

Yan *et al*. [18] [19] proposed models for cooperation in wireless multi-hop networks by using the prisoners’ dilemma game (PDG) as the base of their model. The assumption is that, any two neighbors have a uniform network traffic demand that is not always the case in real network. The authors in [13] used game theory and graph theory to investigate and prove the conditions under which, cooperation among nodes can evolve in the network. The authors concluded that the probability to have all nodes in the network cooperating is very small. Nevertheless, local subsets of cooperating nodes may exist. The model relies on a dependency loop. Even though, each node is only aware of its neighbors as opposed to the full network topology. Obviously, dependency loop will not be common knowledge among nodes. To reach a Nash equilibrium point in a non-cooperative game could be desirable because it guarantees stability among rational players [30]. A non-cooperative game is said to be in a NE state if no single player can be better off by changing its own strategy while other players remain unchanged. However, if at least two players colluded, they might be better off by changing their strategies, but this is outside the scope of non-cooperative games. In [6], the authors investigated equilibrium conditions for packet forwarding strategies in wireless ad hoc networks, but they restrict their study to static configurations, i.e., no mobility is applied on the nodes.

Yu *et al* [17] proposed a game theoretic approach to a secure cooperation in ad hoc network. Comparably, a mechanism design has been used to enforce node cooperation and develop optimal and truthful routing mechanism. By definition, a mechanism design is a field of game theory that investigates how privately known preference of several strategic players can be aggregated toward a desirable outcome. The desirable outcome is sometimes the maximization of some utility function or to have strategic players truthfully reveal their private information.

2.3 BARGAINING GAME THEORY

Cooperative game theory abstracts from the procedures and details of reaching an outcome and focuses on the possibility of reaching an agreement. It studies the frictionless negotiations among rational players who can make binding agreements with or without the need to enforce by means of punishment on the rule of the game. Commitments are fully binding and enforceable.

The bargaining formal theory was introduced by John Nash in his research papers [33]. The final outcome is the main interest and it is often convenient to analyze the domain of all outcomes in order to uncover an efficient outcome. The desirable solution is expressible in terms of axioms, which ideally should incorporate some fairness and efficient features to the solution. A bargaining problem is represented as a pair *(S, d)* in the utility space. The point of disagreement represents the minimum utility level that players will obtain if negotiations fail. The set *S* must include points that dominate the disagreement point. However, there is a positive surplus to be divided among the players once their minimum requirements are reached. The main question to be asked usually is *"How the surplus should be divided?"*. The strategic bargaining describes what the outcome will be and the axiomatic bargaining emphasizes on how negotiations can evolve to reach an outcome.

In [29], strategic bargaining studies the exact specification of the negotiation procedure such as the periodicity of each exchange, the duration of communication between the players, the discount or threat each time an agreement is not reached. It helps identify the behavior of the players. As a strategic bargaining procedure, we have the Rubinstein-Ståhl's model of alternating offers [1] [29]. The negotiation is modeled very closely to a real-time game. Suppose there are two players bargaining over the division of a surplus of *1*. In the period *1*, Player *1* will make an offer on the division *(x, 1-x)*. Player *2* can either reject or accept the offer. If the offer is accepted, the bargaining game ends. If the offer is rejected, then Player *2* will make a proposal on the next period. Therefore, Player *1* will respond. The negotiation continues until an outcome is reached or the threat or discount factor brings the game to an end.

The axiomatic bargaining [30] assumes some desirable properties about the outcome of the negotiation process and then identifies process rules that will guarantee the outcome. The bargaining process is ignored completely. The Nash bargaining solution specifies four axioms [33], to be should satisfy:

i. ***Symmetry***: Two players bargaining for a better payoff with symmetric utilities get the same payoff. It ensures that the solution yields a fair outcome for any player.

ii. ***Pareto Optimality***: The solution is on the Pareto boundary. The axiom reflects the rationality of the players. Therefore, If players work together during the negotiations, they would not accept the disagreement point as the outcome when they can do better and reach an agreement.

iii. ***Invariance with respect to affine transformation***: In case the defined payoff functions are rescaled, the obtained solution should be rescaled the same way. For example, a change in valuation for the players' utility implies a change in the valuation of the outcome of the game.

iv. ***Independence of Irrelevant Alternatives (IIA):*** Let's suppose the solution for the bargaining problem *(S, d)* is *s**. By considering a new bargaining *(S', d),* where $S' \subseteq S$. Therefore, the solution of the new negotiation problem is also *s**. The solution obtained is independent of the "alternatives" that are deemed irrelevant because they were not chosen in *S*, so their absence should not alter the outcome.

Brahma *et al* [16] modeled the problem of dynamic spectrum access by a network of N nodes as a perfect information infinite horizon bargaining game. Players negotiate among themselves to agree upon a sharing rule of the channels. The authors investigated the subgame perfect equilibrium strategies of the bargaining game, each player can maximize its own throughput against other players. The impact of the discount factor is also taken into consideration. However, the authors do not consider the possibility of players bargaining with the intent of malice, a player does not willing to share equitably the resource. Hassan *et al* [34] showed that users can apply a brinkmanship technique to present credible threats to their provider by using an ultimatum bargaining game and therefore, constraint the provider to allocate more resources to users's services.

2.4 NETWORK SECURITY GAME

The use of game theory to address network security challenges has increased in recent years. Generally, the main objective of a rational attacker is to intelligently choose its strategy to maximize the damage to the network while the network administrator strategies are to minimize the damage to the network. The attacker's and the defender's objectives are diametrically opposed. Applying the zero-sum game to model network security [38], where by definition, the winning of a player generates the loss of its opponent. The game reaches the well known Nash equilibrium (NE) when, each player applies the best response to its opponent strategy. Neither the attacker nor the network administrator can unilaterally make a gainful deviation from the Nash equilibrium.

In the game presented in [8], strategies and payoffs are assumed to be common knowledge to all players. The network security game is known as a game of complete information. Otherwise, the game is an incomplete information which can be formulated as a Bayesian game as in [19]. The network security game can also be modeled as a static game [30], a repeated game or generally as a stochastic game [8]. A stochastic game is a generalization of a repeated game. In a repeated game, the game is played multiple times, players play the same stage game in all periods, whereas in a stochastic game, the stage game can randomly change from one period to the next. Game theory also provides a solid framework to model intrusion detection in a network [41]. A survey of game theory as applied to network security is provided in [42].

CHAPTER 3

DYNAMICS OF DATA DELIVERY IN MOBILE AD-HOC NETWORKS: A BARGAINING GAME APPROACH

In this chapter, we address the problem of dynamic packet forwarding with a set of wireless autonomous ad hoc network nodes, where each node acting in a selfish manner tries to use the resource of other nodes. We model the dynamic packet forwarding problem as a modified Rubinstein-Ståhl bargaining game. In our model, a mobile node (player) negotiates with the other mobile node to obtain an agreeable and respectable sharing rule of packet forwarding based on its own available resource, such that a node should not agree to forward packets without the energy or storage capacity to do so. We investigate and solve this bargaining process by finding the Subgame Perfect Nash Equilibrium (SPNE) strategies of the game. We consider finite horizon of the bargaining game and examine its SPNE. The solution obtained from bargaining ensures that a mobile device always finds a peer to help forward packets in order to keep the network at flow. Extensive simulations using OMNET++ simulation frameworks are conducted to evaluate how the level of participation of each mobile node may impact the overall network performance. Simulation results show that our proposed bargaining game scheme performs better than other resource shared algorithms, namely the technique for order preference by similarity to ideal solution (TOPSIS) and the bargaining game based access network selection for heterogeneous network.

3.1 INTRODUCTION

In mobile wireless heterogeneous networks such as mobile ad hoc networks (MANETs), the main focus is on cooperation among mobile nodes. Whereas, mobile nodes are mainly constrained by the limits of their energy power, computational and transmission range, and also selfish node that may not be willing to fully cooperate with the overall network. Specifically, the limited energy and transmission range of a node encourage not to forward another node's data packet given that the packet forwarding task consumes lots of energy. Unless, there is an incentive for greedy nodes to be participative in another node's packet forwarding. Therefore, it may be in the node's best interest to participate in order to extend the network lifetime. However, refusal to be part of another node packet forwarding will severely hinder overall network reliability and degrade the node's own performance. Hence, it is essential to implement a mechanism that will motivate packet forwarding among nodes.

The novel mechanism proposed in this chapter is a bargaining theoretical game between a mobile source node and its intermediary to provide resource in reaching an access point (AP). Whenever a mobile node generates packets to be forwarded to the nearest AP, the selected intermediary mobile node bargains and the transfer of data-packet occurs only if the splitting rule is agreed upon between players. Until the nodes agree upon the splitting rule, none of the mobile devices can start data transfer. Thus, this "delay" of the bargaining transaction also costs the node in terms of energy. Consideration of this cost is conducted by discounting future payoff of the node. The discount factor represents the perseverance of the node in waiting for the bargaining result to its favor.

The bargaining game is analyzed using backward induction and we investigated the SPNE strategies with the player in the game. The subgame perfect equilibrium (SPE) comprises a set of strategies such that, no player in a subgame can deviate from these strategies and gain a better payoff. The main contributions of this chapter are as follows:

- We model the splitting rule which is agreed upon by each player before any data communication starts and this is performed without the need of an arbitrator or central manager.
- We model the problem of dynamic data delivery, where mobile nodes need to agree on the splitting rule of data packet among themselves using the Rubinstein-Ståhl bargaining game while in movement with the optimism not to lose wireless communication.

Prior work in the area by researchers are summarized and limitations are also introduced. Rasheed *et al* [43] proposed a 3-tier security framework for authentication between mobile sinks and sensor nodes based on a polynomial pool-based key pre-distribution scheme. Improvements are also made in security performance against a stationary access node replication attack. Munir *et al.* [44] proposed a multi-tier architecture for mobile wireless sensor network (WSN) as a key element of the future ubiquitous computing paradigm. The mobile WSN is also discussed with integration into a pervasive network and an analysis of the impact of mobility on performance related issues. Ren *et al*. [xx] explored the impact of multiple mobile sinks on end-to-end packet delay and energy depletion. Tradeoffs are considered to optimize both packet delay and energy consumption. Purposely, deploying multiple sinks that are moving randomly, they investigated the impact of sink number, speed, sink transmission radius, and data routing on performance. Basagni *et al* [28] effectively improved the lifetime of a WSN. A mathematical model is defined to take into account realistic parameters.

Niyato *et al*. [45] proposed an evolutionary game theoretic approach to solve the access network selection problem in heterogeneous networks (HetNets). The handoff to another network is dynamically handled by the users. The mobility-based method presented in [6] can be categorized as mobile-sink and mobile-relay methods, depending on the type of the mobile entity. Mobile entities can gather the data from the nodes by using sensor short radio transmission range, which is an efficient way of communication with respect to energy.

The authors in[6] evaluated the use of Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) for ranking candidate access networks in heterogeneous networks. Liou *et al.* [24] proposed a bargaining game based access network selection scheme for call requests in HetNet. The bargaining game considered some parameters such as the preference of the candidate access network to the call request.

This chapter is organized as follows: Section *3.2* presents the system models. Section *3.3* presents the game formulation. Section *3.4* analyzes the bargaining for resource allocation. Section *3.5* presents the bargaining with N players. Performance evaluation results are presented in section *3.6*, while conclusions and future works are drawn in Section *3.7*.

3.2 SYSTEM MODELS

In this section, we present the system models including the problem description, the network model, and the mobility model.

3.2.1 Problem Description

We assume a MANET of *N* nodes indexed from *1* to *N* deployed in a wide area. A Node is mounted on a vehicle moving in a specific pattern. Each node can be a mobile router or a mobile broadcast access point. Since we have an infrastructureless network, communication between two distant nodes or an access point becomes a challenge. Nodes can be geographically isolated from other nodes, but they are within transmission range from one another. The packet-forwarding problem of selfish nodes is problematic. Incentive and reward are a motivation for greedy nodes to use their energy to relay the data of other nodes. Also, a gain maximization is obtained by always relaying data from many nodes and to allocate the limited resources (storage) to a maximum number of mobile nodes at the same time.

3.2.2 Network Model

As shown in Figure 3.1, the MANET consists of multiple wireless local area networks (WLANs) based on IEEE 802.11 standards and multiple access points (APs). A Transmission device mounted on a vehicle (bicycle, taxicab, car, police cruiser, fire truck, helicopter, etc.) is considered a mobile unit. APs are deployed all over the WLAN as a data repository for all data collected.

3.2.3 Mobility Model

The movement of mobile devices is seen as random on a 3-dimensional plane. To model the mobility, the commonly used random waypoint (RWP) [66] model is similar and close to reality. The mobile node moves randomly and freely without restrictions. The waypoints are random vectors uniformly distributed in the service area.

A mobile node maintains the same speed when moving between two random waypoints. In each time intervals the speeds are independently and identically distributed (IID). When a mobile device arrives at a waypoint, it may stop or change its velocity but, any change of speed is broadcasted to its neighbors.

3.3 GAME FORMULATION

We present in this section, the method and constraint used to select the best candidate among the neighbors for the bargaining game. The source node which is in need of data forwarding service broadcasts its request to all of its neighbors. Before any eventual candidate reply to the request, there are prerequisites such as the direction of the movement of the mobile device, the speed, and the available storage needed for packet forwarding.

3.3.1 Energy and Signal Strength Constraint

An intermediary node can volunteer its service only if it has the minimal resource requirements to carry out the work. Let us assume the source node s transmits its information to the destination node d with power P_d. and a minimum energy spent E_s. The intermediary node should guarantee at least the threshold needed in term of energy E_i ($E_s \leq E_i$) and a power P_i to transmit ($P_d \leq P_i$) data with a signal to noise ratio (SNR) held to a minimum.

3.3.2 Communication Traveling Time Constraint

Consider two mobile devices within a distance d that are in radio transmission range T_R, ($d \leq T_R$).

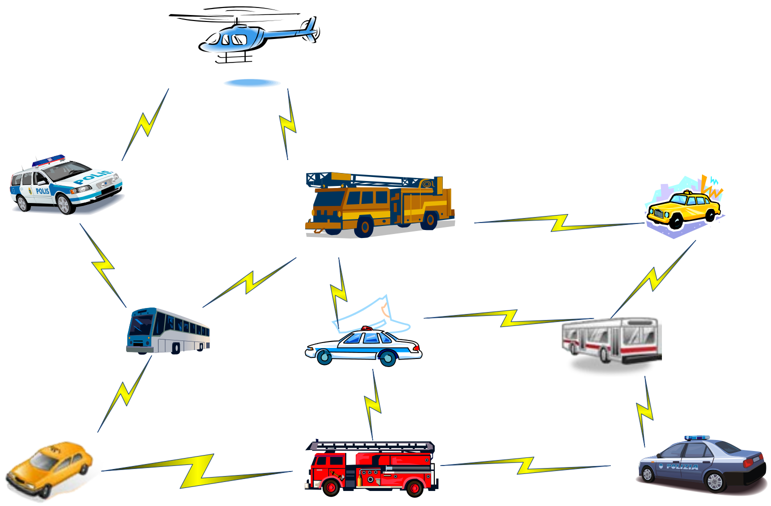
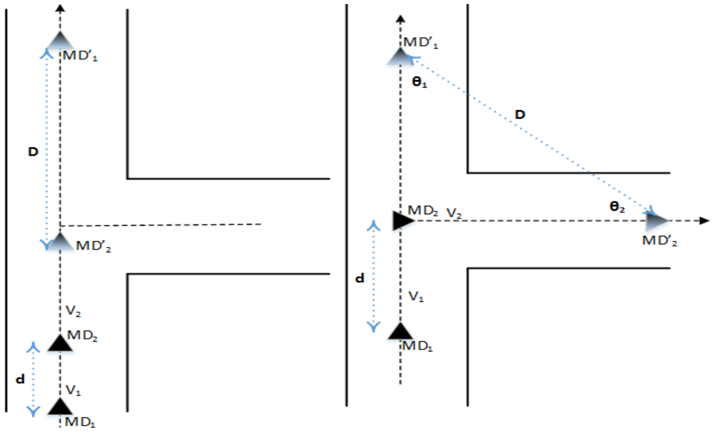


Figure 3.1: Example of mobile ad hoc network, nodes are mounted on vehicles. Source and access point (AP) need intermediary node to be reachable.

Let T_{eta} denotes the elapsed time of both mobile devices from their first communication to them before running out of transmission range. Let u be the vector that represents the trajectory of the mobile source device. Let v be the vector of point of origin for the source device and directed toward the destination device point represented by the intermediary mobile device. The inner product of two vectors denotes by $< u, v >$. Denote the norm of vector u by $\|u\|$ and norm of vector v by $\|v\|$. Let θ be the angle between vectors u and v. Following the base of linear algebra,

$$\cos(\theta) = \frac{< u, v >}{\| u \| * \| v \|} \text{ and } \sin(\theta) = \sqrt{1 - \cos^2(\theta)} \quad (3.1)$$

Define the handoff point to be the points in which both mobile devices are distant from each other of D ($D > T_R$).



(a) $V_1 \neq V_2$, θ={0, π}, same direction (b) θ≠{0, π}, perpendicular direction

Figure 3.2: The total travel distance of MDs before being out of range.

During the communication traveling time (T_{eta}), if a mobile device changes its speed, the overall time will be an arithmetic summation based on each segment of distance with constant and uniform speed, then Fig. 2 shows that T_{eta}, is calculated as

$$T_{eta} = \frac{D-d}{\|V_2\| - \|V_1\|},\ for V_2 > V_1$$
$$T_{eta} = \frac{D+d}{\|V_1\| - \|V_2\|},\ for V_1 > V_2 \tag{3.2}$$
$$T_{eta} = \frac{D\cos(\theta_1)+d}{\|V_1\|}, ...\vec{V}_1 \perp \vec{V}_2$$

Firstly, in traditional direct transmission, the sender transmits its information to the destination with power P_d. To achieve the minimal link quality γ, transmitted power has to be sufficiently large for the SNR that the destination received satisfies

$$SNR_d = \frac{P_d G_{s,d}}{\sigma} \geq \gamma \tag{3.3}$$

where σ is the noise level and $G_{s,d}$ is the path loss from source to destination, and γ is the SNR threshold of the destination.

Secondly, we consider the transmission case of a receiver on the move. While a source receives information from neighbors, the selection of the best candidate is based on all information received such as the location, speed/velocity, direction, and signal strength.

If the mobile device choice is always based on the mobile node moving to same direction and closest speed, then the large dwelling time implies more packets will be forwarded through the same mobile node. Thus, the network will experience higher throughput and the node will experience less delay in packet forwarding.

3.4 BARGAINING FOR RESOURCE ALLOCATION

A cooperative game in which players improve their payoffs through negotiation is also known as bargaining game [1]. We model the resource allocation problem as an infinite horizon Rubinstein- Ståhl bargaining game [29]. Both players must agree on the splitting rule before the data communication starts. In our model, player 1 has data packets to be forwarded to the AP. The requester prefers to obtain as much resources as possible in order to improve its QoS level; player *2* has the resource storage to forward the data packet but prefers to keep as much resource as possible in order to accept more requests from other mobile devices in need for data forwarding in the near future.

Periods	Offerer (Source Node)	Receiver (Mobile node)
1	$K\text{-}1$	1
2	$K\text{-}K\delta+\delta$	$K\delta\text{-}\delta$
3	$K\text{-}K\delta+K\delta^2\text{-}\delta^2$	$K\delta\text{-}K\delta^2+\delta^2$
4	$K\text{-}K\delta+K\delta^2\text{-}K\delta^3+\delta^3$	$K\delta\text{-}K\delta^2+K\delta^3\text{-}\delta^3$

…	…	…
p	$K\text{-}K\delta+K\delta^{2}\text{-}K\delta^{3}\text{-}\ldots+\delta^{p-1}$	$K\delta\text{-}K\delta^{2}+K\delta^{3}\text{-}\ldots+\delta^{p-1}$

Table 3.1: Subgame Perfect Equilibria: Horizontal lines represent the period of each session, then the splitting of player 1 and 3rd column is the part of the receiver (player 2).

The bargaining game proceeds in "time-periods" in which one player proposes a splitting rule to the other player who can "accept" or "reject" the offer. Let x be the amount of resources player *1* could obtain during the request of the bargaining game. Let y be the amount of resources available that player *2* could keep or spare by not offering them to the requester and available in near future to other requester. Denote K as the total amount of resource available to player 2, $K\text{-}x = y$. In periods $0, 2, 4, \ldots, 2k$ (where $p =0, 1, 2, \ldots$) player *1* proposes a splitting rule $(x, K\text{-}x)$ to player *2* whom can accept or reject. The game ends if an offer is accepted. In periods $2p+1$, player *2* makes an offer to player *1*. We have an infinite horizon game of perfect information.

3.4.1 Payoffs

Let consider that if $(x, K\text{-}x)$ is accepted by both players at period t, then the payoffs of player *1* and *2* are $\delta^{t}x$ and $\delta^{t}(K\text{-}x)$ respectively. $\delta \epsilon [0, 1]$ represents the discount factor of the players. The discount factor is also a representation of the delay cost for achieving a bargaining outcome for the players. There will be no data communication between players, unless there is an agreement on the splitting rule. The cost of not reaching an agreement is high for both players, because of the mobility of the players. There is a possibility for a mobile device to be out of transmission range and start the bargaining all over again with another mobile device. A player values a resource more now than it values the same resource in a future period. The decrease in value of the resource represents the disappointment of the players for being unable to start forwarding data right away. As the δ increases, the players become more anxious because of the volatility of the medium, and time delay between two bargaining periods decreases.

The payoff of player 2 is also based on the ratio of the resources allocated to the requester over the resource available to the receiver before the bargaining started, and the energy lost during long bargaining sessions.

3.4.2 Nash Equilibrium

There are many Nash equilibrium (NE) in this game. Any strategy profile in which player 1 splits its data load is a Nash equilibrium. Generally, splits of the overall K loads of player *1* between both players correspond to a NE strategy profile. However, not all profiles are a subgame perfect equilibrium (SPE). For example, if player *2* rejects first offer of player *1* during period $p=0$ and offers player *1* a share $x > \delta(K\text{-}1)$ in the following period, then that player should accept, because any share bigger than a previous rejected share based on the worthiness of the share at the period.

3.4.3 Solutions of the Bargaining Games

Table I shows the SPE of games in different periods [3]. The unique SPE in the last period or the period before the device goes out of range is for the player who makes the offer. From the table, the SPE shares demanded by the players in an increasingly larger period form a pattern. Depending on period p (odd or even), the SPE share demanded by player i:

- *p* is even: the SPE split offered by player *i* is:

$$K(1-\delta+\delta^{2}-...-\delta^{p-1})=\frac{K(1-\delta^{p})}{1+\delta}+\delta^{p-1} \tag{3.4}$$

Also, player *i* accepts any split equal to or less than:

$$\frac{K(1+\delta^{p-1})\delta}{1+\delta}-\delta^{p-1},\delta\in[0,1] \tag{3.5}$$

- *p* is odd: the SPE split demanded by player *i* is:

$$K(1-\delta+\delta^{2}-...+\delta^{p-1})=\frac{K(1+\delta^{p})}{1+\delta}-\delta^{p-1} \tag{3.6}$$

Also, player *i* accepts any split equal to or less than:

$$\frac{K(1-\delta^{k-1})\delta}{1+\delta}+\delta^{p-1},\delta\in[0,1] \tag{3.7}$$

Thus, the unique SPE solution of p periods (odd/even) is “Player *i* always offers a share of (3.4) respectively (3.6) for odd values of *p*, and he accepts any share greater than to (3.5) respectively (3.7) and rejects any smaller split.”

Let consider the case in which two mobile devices are in range for a longer period of time which mean period *p* tends to infinity.

$$\lim_{p\to\infty}\left[\frac{K[1-(-\delta)^{p}]}{1+\delta}-(-\delta)^{p-1}\right]\approx\frac{K}{1+\delta} \tag{3.8}$$

Player *i* will not reject any split greater than:

$$\lim_{p\to\infty}\left[\frac{K[1-(-\delta)^{p-1}]\delta}{1+\delta}+(-\delta)^{p-1}\right]\approx\frac{K\delta}{1+\delta} \tag{3.9}$$

3.4.4 Unicity of the SPE Solutions

According to the bargaining game theory [29], the safety payoff value of a player in a game is the guaranteed amount the player can get in the bargaining game. Let m_1 and M_1 be player *1*’s lowest and highest payoff values in any SPE where player *1* makes an offer. Denote n_1 and N_1 be the lowest and highest payoff values for player 1 game in which player 2 makes the offer.

Player *1* makes an offer to player *2*, player *2* will accept x such that his share of *K-x* exceeds δN_2, knowing that player *2* cannot expect more than M_2 in the continuation game following his refusal. Thus, we have,

$$m_1 \geq K- \delta M_2 \tag{3.10}$$

Player *1*will not reject a split of more than δM_1.

$$M_2 \geq K- \delta M_1 \tag{3.11}$$

Player *2* will never offer a share greater than δM_1. Thus, player 1's continued payoff when player *2* makes an offer is

$$N_1 \geq \delta M_1 \tag{3.12}$$

Since player *1* can obtain at least m_1 in the continuation game by rejecting player *2*'s offer, player *1* will reject any x such that x < δm_1. Thus, we have $n_1 \geq \delta m_1$

From [3], we can say that:

$$m_2 = M_2 = \frac{K}{1+\delta} \tag{3.13}$$

And similarly, we also have

$$n_2 = N_2 = \frac{K\delta}{1+\delta} \tag{3.14}$$

Thus, the subgame perfect equilibrium payoffs between player 1 and player 2 in the bargaining game are unique.

3.5 BARGAINING WITH N PLAYERS

With the intermediary device not willing to make available all of its resource to only one source device, we will investigate the game with *N* players. We have *N* players (mobile devices) which need to forward packets to the nearest AP. The intermediary node which carries the data acts like another player to have its share of the resources. Let P_i denote the player making an offer and let $P_{-i} = \{R_1, R_2, \dots, R_{N-1}\}$ be the players receiving offers.

To avoid data lost by collision, a token is implemented. Players communicate only when they are in possession of the token. A player P_i makes an offer by proposing a splitting rule ($x_1, x_2,\dots, x_{N-1}, x_N$), where x_i is the resource needs by player P_i and $x_N = K\text{-}\Sigma x_i$, $i=1..N-1$. P_N represents the intermediary mobile device. For example, the P_1 splitting rule is rejected by any P_{-1} players, then player P_2 is next to propose a splitting rule. In case all players P_{-i} accept their respective offers, the bargaining ends and the data transfer starts [16] [6]

```
Require: # player, N=2; Time period before out of range, T; Payload, Q;
time transferring a packet, t; Cost factor, $\delta$;
Initialization: Commitment level value for player 1 and 2 is $c_1$ and $c_2$
respectively;

 1:   $c_1 \leftarrow$ value; $c_2 \leftarrow$ value;
 2:   While $T > 0$ do
 3:     Player 1 proposes $z_1$ and $z_2 = Q - z_1$; $(z_1, z_2)$ with $z_1 \geq c_1$
 4:     Player 2, accept $\leftarrow$ ($z_2 \geq c_2$; True, False)
 5:     If !accept then
 6:       $T \leftarrow T - t$; $z_1 \leftarrow z_2\delta$; $z_2 \leftarrow Q - z_1$;
 7:       player 2 proposes $z_2$; $(z_1, z_2)$ with $z_2 \leq c_2$
 8:       player 1, accept $\leftarrow$ ($Q - z_2 \geq c_1$; True, False)
 9:       If !accept then $T \leftarrow T - t$; goto 4; Else Transfer Q; Break; End if
10:     Else  Transfer Q; Break; End if
```

```
    4: $z_1 \leftarrow z_2\delta$; $z_2 \leftarrow Q - z_1$
End While
```

Table 3.2: Algorithm for Bargaining

Let define the payoff of the players. For an offer x_i to be accepted in period t, the payoff of P_i is $\delta^t x_i$, $\delta\epsilon[0, 1]$ is known as the discount factor (delay cost in achieving the bargaining outcome).

3.5.1 Subgame Perfect Equilibrium (SPE)

Consider P_i, the player who makes the offer to players P_{-i}. The token is distributed following the round robin between all players. The SPE of the bargaining game; P_i demands of a split

$$\frac{K}{\sum_{j=1}^{N}\delta^{j}} \tag{15}$$

The receivers of the offers P_{-i} to share,

$$\frac{K\delta^{p}}{\sum_{j=1}^{N}\delta^{j}} \tag{16}$$

Equations (15) and (16) show that the SPE shares of a player is K/N as δ tends to 1. Since we are in a volatile environment with nodes moving randomly, there are chances for nodes to be out of range. There is no patience for all players; there is no need to be comfortable rejecting offers with hope for better. It may end up being a waste of precious energy. It is insightful to think that player P_N (carrier) gets a lesser fraction of the resource. In our game, all players are anxious to find themselves out of range, combine with the waste of energy. Therefore, players will aim for an equal distribution of the resources.

3.5.2 Resource Allocation Algorithm

The minimal acceptable share for a player is the only private information. Sharing information that may cause others to not offer anything better during the bargaining session. The algorithm in table II shows the resource allocation procedure players *1* and *2* will invoke when making an offer during bargaining.

3.6 SIMULATION RESULTS

We developed an OMNET++ [46] based simulation model for our proposed scheme. The OMNET++ is a discrete-event network simulation framework. The goal of this framework project is to develop a preferred and an open simulation environment for networking research. As shown in Fig. 3.1, the simulation environment is a grid where mobile nodes move following the north, south, east and west direction. The system parameters for this MANET are provided in table 3.3. The mobile device's speed is a random variable which is uniformly distributed. The device mobility is randomly and independently set from each other. The slot duration is set to be larger than packet duration in order to keep the nodes in the network time-synchronized. These guard bands are needed to compensate the arbitrary delays incurred by transmitted packets due to signal propagation delays or clock drifts.

The proposed bargaining game scheme in this chapter is compared quantitatively with the scheme of bargaining game based access network selection (BGANS) [24], and also with the TOPSIS scheme [16] [26]. With the TOPSIS scheme, only mobile devices with speeds lower than 2 m/s will see LANs as candidate access networks. In the BGANS approach, if the dwelling factors are larger, without taking into account the residual energy; then there is a high possibility of handoff because of lower energy for transmission.

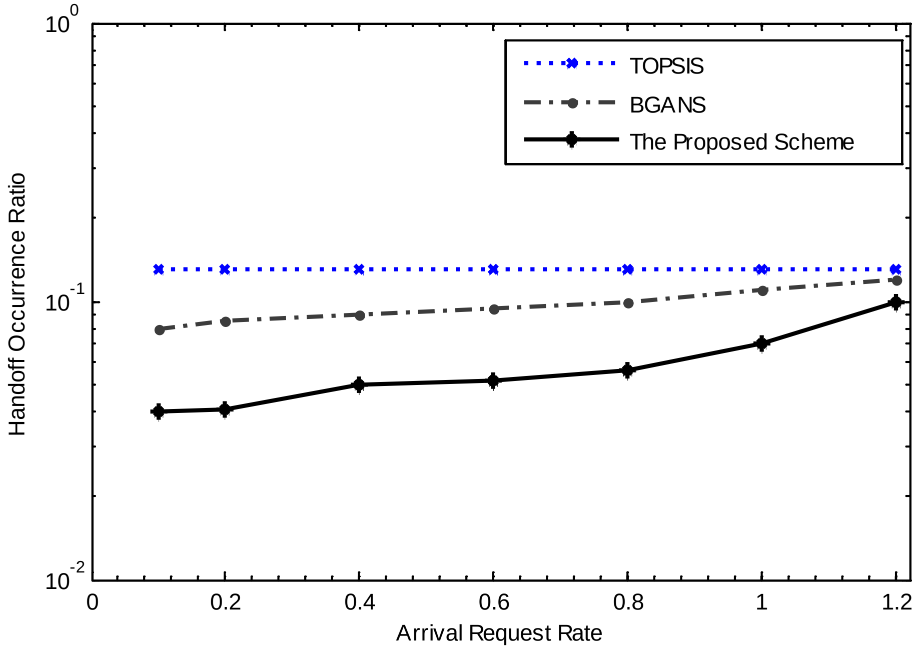


Figure 3.3. Handoff Occurrence Ratio

Figure 3.3 represents the handoff occurrence ratio. By definition, the handoff occurrence ratio is the average number of handoffs that a mobile device tried each time to connect. The proposed scheme has a better handoffs ratio compared to the TOPSIS and BGANS. The improvement is about 60% lower than the BGANS and the BGANS is about 40% lower than TOPSIS for an arrival rate of 0.1. The ratio improvement is due to that the bargaining game takes into consideration the devices' mobility, the time to remain connected and mainly the availability of the resource to be allocated. The receiver of a mobile device tends to allocate a portion of its resources based on section VI. A portion of a requested resource is always better than no resource at all. Meanwhile, the BGANS tends to allocate more resource to requests with larger dwelling factors.

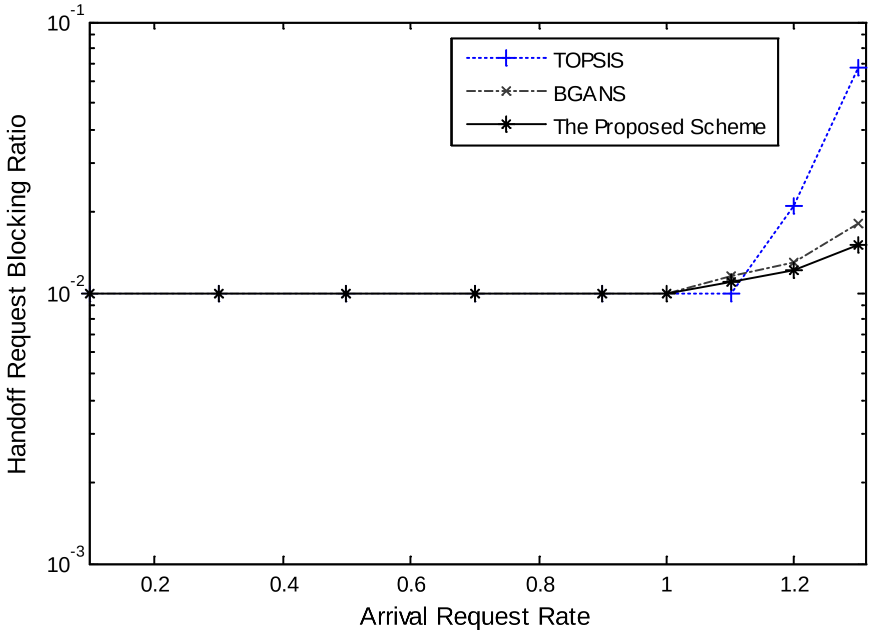


Figure 3.4: Handoff Request Blocking Ratio

Figure 3.4 shows the handoff request blocking probability, defined as the probability that a mobile device request for data communication fails to handoff to the intended mobile node. The performance improvement for handoff request blocking is lower compared the TOPSIS and BGANS schemes for about 25% for the BGANS scheme. Our proposed scheme uses the fact that a mobile device is not isolated or clustered. A receiver mobile device of the request has resources to allocate reason of the bargaining. Multiple requests from different mobile nodes may cause channel interference and block a request to the destination. The handoff request blocking ratio increases when the arrival rate goes over the value of *"1"*. Hence, the mobility and the bargaining game scheme lower the handoff blocking probability.

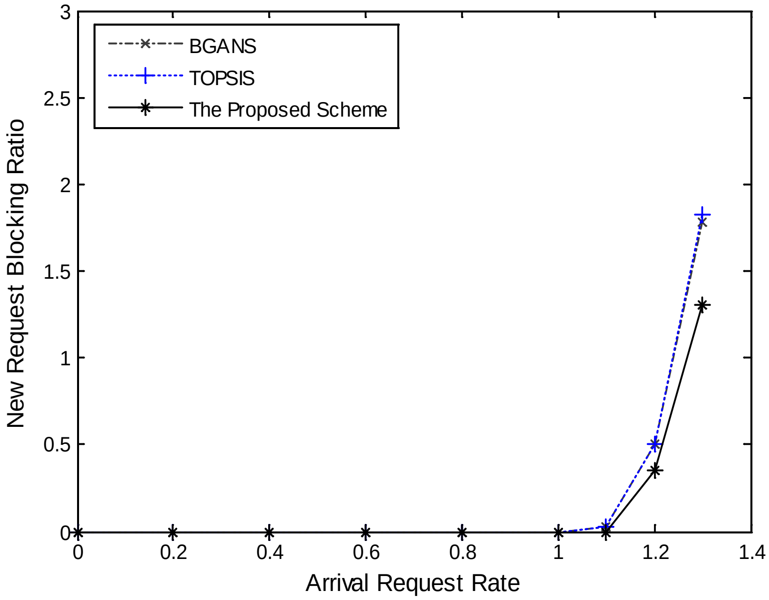


Figure 3.5: New Request Blocking Ratio

The above figure 3.5 shows the new request blocking ratio/probability versus the arrival request rate for mobile nodes connectivity. The proposed scheme shows an increase of the new request blocking probability when the arrival rate is about *1.1*, and this improvement is based on the availability of a shared bargaining resource to be allocated. The nodes solicited for data communication are not the same which reduces the probability of new blocking request. The TOPSIS and the BGANS new request blocking probability tend to the same result with different arrival request rate.

3.7 CONCLUSION

In this chapter, a bargaining-game algorithm has been proposed for the resource allocation of mobile nodes in wireless mobile ad hoc networks. The algorithm is based on the Rubinstein-Ståhl bargaining game model with the objective of maximizing the resources to be allocated to a mobile device in need. The bargaining game algorithm takes into consideration multiple factors such as the general connection duration among mobile devices, the mobility pattern, and the payload to transfer. Based on the experimental results from the OMNET++ simulation framework, we found that the scheme proposed may perform better than the TOPSIS and BGANS schemes in terms of the handoff occurrence and request dropping probability per connection.

For future work, we plan to investigate this model further with a continuous-time which is a more realistic model. We will explore the possibility of combining the bargaining game with another game theoretic model to refine the payoffs of players.

CHAPTER 4

GAME THEORETIC ANALYSIS FOR RESOURCE ALLOCATION IN DYNAMIC MULTI-HOPS NETWORKS WITH ARBITRATION

One of the major design issues in dynamic networks is the availability of resources when in need. Because of the volatility of wireless connections in mobile ad-hoc networks (MANETs), resource seems scarce when mobile devices need to forward information on a dynamic network. A connection through a mobile node may not be available because of the greediness of a selfish node. In this chapter, we address the issue of dynamic packet forwarding by a set of wireless autonomous ad hoc network nodes. Wireless nodes acting in a selfish manner try to use the resource of other nodes without being participative. We model the dynamic packet forwarding problem as a negotiation model game with an arbitrator. In our model, a group of mobile nodes (players) negotiate with a mobile arbitrator to obtain an agreeable resource allocation based on a simple majority rule to forward packets. The mobile arbitrator submits offers to each mobile device in the group, whereas mobile nodes decide to agree or disagree on the offer. The ultimate decision is made by simple majority. We investigate and solve the negotiation by finding the optimal Nash Equilibrium (NE) strategies of the game. We consider a Dirichlet distribution offers on a finite volatile and a sporadic time limitation set of mobile devices for the negotiation game. The solution obtained from negotiation ensures that a mobile device always finds a peer or arbitrator to help forwarding packets in order to keep the network flowing. Mathematical proofs and MATLAB simulations support our model.

4.1 INTRODUCTION

In recent years, there has been tremendous active research in deploying and supporting terminal mobility in dynamic networks. One of the design issues is the resource allocation and availability in ephemeral networks such as MANETs [49]. A MANET is a group of autonomous mobile devices deployed without fixed infrastructures. In such a network with a sporadic connectivity, the device mobility can be exploited for data dissemination, and low link reliability is allowed for delay-tolerant applications. Although nodes may be static or mobile, they rely on other nodes for data transfer. Furthermore, an autonomous behavior and resource limitations such as in energy power may cause a node to be selfish. Cooperation or participation to keep the network flowing is crucial among nodes in the community or group [1]. Unless there is an incentive for greedy nodes to participate in another node's data transfer, it may not be in the node's best interest to deplete its own energy power. However, refusal to be part of packet forwarding will severely hinder network reliability and degrade the node's own performance. Thus, it is essential to implement a mechanism that will motivate data transfer among nodes.

From the existing literature, researchers have proposed ways to stimulate a node's participation to strengthen network vitality. Many have discussed reward programs and incentive mechanisms to ensure that a selfish behavior is not inhibiting [82]. However, the need for an optimal solution is apparent in a volatile network which is a characteristic of MANETs. The novel mechanism proposed in this chapter enforces a game-theoretic model of communication among nodes. The model introduces a bargaining game with arbitration between mobile source nodes (players) and the intermediary mobile node (the arbitrator). The arbitrator en route to the nearest access point (AP) invokes the negotiation game with players whenever requests to forward packets are made. The arbitrator submits a share of its resource availability to each player, and the players decide to agree or disagree on their offers. The shared value is a random number generated from Dirichlet's distribution, which provides equitable outcomes for players. We investigate the NE strategies and how optimal solutions are derived to allocate the shared resource to players. The ultimate decision is based on a simple majority of players agreeing on their offers [31]. If a simple majority is reached, mobile devices may transfer data. Otherwise, new offers may be submitted again, and the cost of not reaching the majority vote is discounted from the overall resource by a factor δ *($\delta < 1$)*. Discounting successive payoffs represent the perseverance of the players waiting for a better offer. If simple majority is not ascertained by the final cycle, and at least one player is out of transmission range to end the game.

The mobility and wider transmission range of the arbitrator make it ideal for data transmission. Its mobility covers broader locations, while its wide transmission range reduces the number of hops between a source node and its destination. As a result, the arbitrator's routing table is also up-to-date with the latest routes to destinations. Furthermore, introducing the bargaining game with arbitration ensures there is an incentive for nodes to cooperate in packet forwarding and expedite network reliability.

Some early research works exist in this area, and we summarize them here. In [50], Buttyan and Hubaux introduced virtual currency as an incentive for nodes to cooperate with each other. Intermediate nodes, for example, charge the source a '*nuglet*' to transfer packet. Through the estimated route, the source allocates a set amount of ‘*nuglets’* for a packet to be delivered at destination. When an intermediate node routes packet to the next node, it decrements the *‘nuglet’* count by one. This approach does not consider the possibility of nodes charging more than a unit of currency, as well as packets dropping when there are no more tokens available for payment.

Liou *et al.* [24] proposed a bargaining game based on a network selection access scheme for call requests in heterogeneous networks. The bargaining game considers some parameters, including a candidate’s preferred method of network access, such as wireless metropolitan area networks, 3G/CDMA networks, and wireless local area networks, and the mobility pattern of the mobile device. This approach requires the network infrastructure to be static. The base stations are static while only the mobile devices are moving.

Marti *et al*. [22] studied techniques for improving the throughput in MANET in the presence of nodes that agree to forward packets but fail to deliver them. The authors categorize nodes as *watchdog* nodes that identify misbehaving nodes and *pathrater* nodes, which help routing protocols to avoid these nodes. The *watchdog* feature has the ability to detect misbehaving nodes in a static neighborhood. However, it might not be able to detect a compromised node in the presence of ambiguous collusion and false behavior.

Niyato *et al.* [45] introduced an evolutionary game theoretic approach in resolving the issue of network access selection in heterogeneous networks. The handoff to another network is dynamically handled by the users. The mobility-based method presented in [6] can be categorized as mobile-sink and mobile-relay methods, depending on the type of the mobile entity. Mobile entities can gather data from the nodes by using their short radio transmission range, which is an efficient way of communication with respect to energy.

Riordan and Grigoras [52] proposed a data mule service for mobile ad-hoc networks. The work is based on a service-driven MANET. The client is a requester of a service, and the provider of the service may no longer be on the same network due to mobility. The mule is highly mobile, and it joins a large network to have the best chance of delivering results to the requester. This approach involves the storage of multiple network memberships and requires the mule to be the data transporter itself, which is good for delay tolerant applications.

In this chapter, we are interested in resource allocation and optimization in heterogeneous MANETs with devices in full mobility. This is obtained through the proposition of bargaining games with an arbitrator applying the Dirichlet distribution.

The remainder of this chapter is organized as follows. Section 4.2 presents the system models and motivations. In Section 4.3, we propose the game theoretic analysis. Section 4.4 presents the negotiation with *n* players. Section 4.5 presents the simulation results while conclusions and future works are drawn in Section 4.6.

4.2 System Models and Motivations

In this section, we first present our system models under the problem description, our motivations towards this work and the network model.

4.2.1. Problem Description

We consider a scenario in MANET with *N* nodes indexed from *1* to *N* deployed in an area. Nodes are fixed or mounted on a vehicle moving through various routes. Each node can be a mobile router or a mobile broadcast access point. Each node also has the ability to store, process and relay packets to other nodes if there is a need to do so. Due to the limited resource of a node, relaying packets is not always in the node's best interest, but it's in the best interest of the overall health of the network. Since we have a system without a fixed infrastructure, communication between two distant nodes or an access point becomes a challenge. Nodes can be geographically isolated from other nodes, and in order to remain in communication with others, a negotiation with intermediary nodes is necessary to have their packets relayed. The packet-forwarding dilemma of selfish nodes is an issue. Incentives and rewards are motivations for greedy nodes to use their energy to relay data of other nodes.

4.2.2 Motivations

Mobile devices in MANETs are selfish due to the limited resources available to them. Due to the greediness of these nodes, it might be difficult for distant nodes to communicate. In order for a source node to communicate with a distant destination node, the source needs to run the routing algorithm and find the shortest path (multi-hop network). It must then negotiate incentives and rewards with nodes along the path to forward packets. Providing arbitrators as data carriers (mules) [52] and mobile devices with wider transmission is beneficial in a multi-hop network because they can reduce the number of hops as a result of their extended radio ranges. An arbitrator's mobility can also provide the latest location that a node previously encountered in its pathway through a routing table. Therefore, when an arbitrator offers to be the data carrier for a source node, there is a better chance of having fewer hops to reach the destination.

The arbitrator's role in the MANET introduces some implementation constraints which needs to be considered. First, multiple nodes can solicit the same arbitrator at the same time. To avoid collision packets due to the hidden node problem on the arbitrator's channel [53], the mobile nodes do not have to transmit at the same time. The hidden terminal problem occurs when a node is in transmission range of a wireless access point (AP), but not from the transmission range of other nodes communicating with the determined AP. This leads to difficulties in media access control. To solve the problem, the arbitrator implements a round robin algorithm [6] [53] coupled with the handshaking procedure of the carrier sense multiple access with collision avoidance (CSMA/CA).

Apart from accommodating selfish nodes in the MANET, the arbitrator may also have to deal with malicious nodes. These malicious nodes may collude with each other to drain an arbitrator's resource. Malicious nodes can extend the duration of the bargaining, which is achieved by generating multiple bargain requests [54]. Meanwhile, normal nodes wait to strike a bargain deal with the arbitrator before going out of radio range. Therefore, the main objective of the malicious nodes is to waste energy resources of the arbitrator and cause delays. The proposed solution to such collusion is for the arbitrator to limit the number of bargaining requests and time spent with each node.

4.2.3 Network Model

The MANET consists of wireless local area networks (WLANs) based on IEEE 802.11 standards and multiple access point (APs). Transmission devices mounted on vehicles (light poles, bicycles, taxi cabs, cars, police cruisers, fire trucks, helicopters, etc.) are considered mobile units. APs are deployed all over the WLAN as data repositories for all collected data.

The movement of mobile devices is seen as random on a 3-dimensional plane. The mobile node moves randomly and freely without restrictions, but the mobility coverage area of two different types of vehicles may be different. For example, a city police cruiser may cover city limits while a sheriff’s cruiser may cover both city and county limits. The waypoints are random vectors uniformly distributed in the service area. A mobile node keeps its neighbors informed by broadcasting any change that occurs, such as changes in speed, direction, location, etc. During each time interval, the speeds are independently and identically distributed (IID). When a mobile device arrives at a waypoint, it can stop or change its parameters. We also present the method and constraint used to recognize the arbitrator among the neighbors for the negotiation game. Nodes in need of data forwarding services broadcast their request to all of their neighbors. The eventual arbitrator broadcasts its availability to collect data from neighboring nodes. The arbitrator in the vicinity replies to the group request only if it has the energy power and resource available to deliver data to the destination.

4.3 Proposed Game Theoretic Analysis

In this section, we provide an analysis of strategic interactions with the arbitrator and the general equilibrium property of the negotiation game that uses simple majority rule with finite horizon of negotiations. A node may be a radar unit, a wireless application, or sensor involved in any monitoring activity or data supplying activity. We may have multiple nodes to monitor the same environment or event. Given the limited mobility and selfishness of nodes, a single node cannot sense and deliver data on its own [49]. Rather, a node with high mobility is used as a mule (the arbitrator) for data transfer. An arbitrator in an area collects data to be transferred to the AP and also governs the resource to be allocated to each node. The shared resource is randomly assigned. Nodes receive their offers and decide to either accept or reject them. A simple majority vote carries out the ultimate decision. It is necessary to calculate the number p of negotiators yielding to their offers, such that $p \geq int(n/2)+1$, where n is the number of negotiators, and *int* represents the integer division function. If the condition holds true, the majority of offers is accepted. Otherwise, it is rejected, the players proceed to the next round, and the resource is discounted by $\delta<1$.

4.3.1 Negotiation Model

The players are the nodes. The set of players is $N = \{1,2,\ldots, n\}$. An arbitrator is introduced as an independent participant that owns the data-carrier unit to be shared among players. The arbitrator submits offers to players and computes the decision. Players provide location coordinates, speed, and direction of their movement. Let's assume that the arbitrator represents a random generator. Consider k, a given time interval that negotiations run on. At each shot, the arbitrator makes random offers. Also consider *K* the number of interval cycles before the game is over due to node(s) being out of range. If negotiations result in no decision between players, the game ends.

Based on the current location each player yields, the arbitrator estimates the residual travel time before the group is dismantled. In order not to lose the negotiation session completely, the arbitrator offers an equal allocation on the last time interval. Each player can estimate its residual travel time with the arbitrator. The arbitrator applies the random generator described in the following subsection.

4.3.2 Dirichlet Distribution

The Dirichlet distribution by definition, captures a sequence of observations of the *n* possible outcomes with *n* positive real parameters x_i, $i=1,\ldots,n$, each corresponding to one of the possible outcomes. The probability density function (*pmf*) of the Dirichlet distribution (Dir) for variable vector $x_i = (x_1, x_2,\ldots, x_n)$ with parameter vector $(k_1, \ldots, k_n)$ is given as

$$Dir(x;k) = \frac{1}{B(k)} \prod_{i=1}^{n} x_i^{k_i - 1}, x_i \geq 0, \sum_{i=1}^{n} x_i = 1, k_i \geq 1. \tag{4.1}$$

The constant, *B(k),* in the formula

$$B(k) = B(k_1,\ldots,k_n) = \frac{\prod_{i=1}^{n} \Gamma(k_i)}{\Gamma(k_1 + \ldots + k_n)}, \tag{4.2}$$

depends on a set of parameters $(k_1, \ldots, k_n)$. They serve for adjusting the weights of the distribution and if *k* is not a constant vector, the density is not symmetric [31]. The operation Γ represents the Gamma function.

4.3.3 Negotiation Game with Three Players

For simplicity, we start by presenting a three player negotiation game with an arbitrator. The *n* players' case study will be the subject of section V. In this section, we assume that at least two players agree on their offers, the game ends. We also assume that the arbitrator is the data-carrier. The arbitrator possesses a data storage unit available for packet forwarding. For example, a 500 Megabytes of memory space available will be shared among players if they agree on the offers. A share is presented as a fraction of a unit.

Let us examine the case of three players, and consider that the negotiations cover the horizon of *K* shots. Thereafter, the game ends by count down if after *K* shots, there is no agreement and any one player is out of transmission range. Let us suppose that *k* shots remain. The arbitrator makes offers to players in a form vector (x_1^k, x_2^k, x_3^k). During each cycle, offers represent random variables distributed according to the Dirichlet law. The joint density function has the form,

$$f(x_1, x_2, x_3) = \frac{\Gamma(k_1 + k_2 + k_3)}{\Gamma(k_1)\Gamma(k_2)\Gamma(k_3)} x_1^{k_1-1} x_2^{k_2-1} x_3^{k_3-1} \tag{4.3}$$

where $x_1+x_2+x_3 = 1$ and $k_1=k_2=k_3 = 1$, so that all players have the same weight.

For any given offer vector (x_1, x_2, x_3), each of the three players has two alternatives:

(i) accepts the current offer or

(ii) rejects the current offer with the hope of a better offer at the next period.

The delay caused by the non-agreement during each shot is discounted by δ (where $\delta \leq 1$). The lost in energy for each player in terms of communication while rejecting an offer should be worth the wait. At the last shot $k = 0$ with all previous negotiations failed, all three players always receive the ultimate offers. The ultimate offer is the vector (⅓, ⅓, ⅓) in terms of storage allocation. Since the arbitrator follows majority rule, we must analyze the scenario of two out of three players' agreements to offers from the arbitrator.

4.3.4 Optimal Strategies for Majority Rule

An offer from the arbitrator is accepted if at least two of the three players consent. The horizon of negotiations is finite with *K* shots before players are out of radio transmission. Therefore, counting down to shot *k*, random offers from vector (x_1^k, x_2^k, x_3^k) are generated using the Dirichlet distribution. Let U_k denote the value of the negotiation game when *k* shots remain until the end. Let's consider (x_1, x_2, x_3) the offers for player *1*, player *2* and player *3*, respectively. Let's introduce the vector $o(x_i)$, $i = 1, 2, 3$, where *o* defines the probability that player *i* accepts the current offer x_i. Set $\bar{o}(x) = 1 - o(x)$. Let's look for an equilibrium among identical strategies.

Theorem 4.1: The optimal strategies of the players in the negotiation at period *k* possess the form

$$o_i(x_i) = \mathrm{I}_{\{x_i \geq \delta U_{k-1}\}}, i = 1,2,3.$$

The utility value of this negotiation game for player P_1 meets the formula:

$$U_k = \frac{1}{3} - 2\delta^2 U_{k-1}^2 + 6\delta^3 U_{k-1}^3 \tag{4.4}$$

Proof: The player P_1 utility payoff at period *k* is given by the formula:

$$U_k = \sup_{\mu_1} 2 \int_0^1 dx_1 \int_0^{1-x_1} dx_2 \{(Ax + B\delta U_{k-1}\}, k = 1,2, \ldots \tag{4.5}$$

From (4.5), we have $A = \mu_1\mu_2\mu_3 + \bar{\mu}_1\mu_2\mu_3 + \mu_1\bar{\mu}_2\mu_3 + \bar{\mu}_3\mu_2\mu_1$

And $B = \bar{\mu}_1\bar{\mu}_2\bar{\mu}_3 + \mu_1\bar{\mu}_2\bar{\mu}_3 + \bar{\mu}_1\mu_2\bar{\mu}_3 + \bar{\mu}_1\bar{\mu}_2\mu_3$

Where $U_0 = b; \mu_1 = \mu_1(x_1); \mu_2 = \mu_2(x_2); \mu_3 = \mu_3(1\text{-}x_1\text{-}x_2);$

$$U_k = \sup_{\mu_1} 2 \int_0^1 \mu_1(x_1)dx_1 G_k(x_1) + 2\int_0^1 dx_1 \int_0^{1-x_1} W_k(x_1)dx_2 \qquad (4.6)$$

Where $G_k(x_1) = \int_0^{1-x_1}\{(x_1 - \delta U_{k-1})(\mu_1 + \mu_2 - \mu_2\mu_3)\}dx_2$

And $W_k = (x_1 - \delta U_{k-1})\mu_2\mu_3 + U_{k-1}$

The optimal strategy for P_1 is $\mu_1(x_1) = I_{\{G_k(x_1)\geq 0\}}$

Due to problem's symmetry, the optimal strategy for P_2 and P_3 is idem $\mu_2 = \mu_3$. With $G_k(0) \leq 0$ and $G_k(1) \geq 0$ there exist a such that $G_k(a) = 0$. For and equilibrium among threshold strategies, $G_k(x_1)$ has a different shape on the intervals:

$$\begin{aligned} G_k(x_1) = (x_1 - \delta U_{k-1})(2\, aI\,\{x_1 \leq 1\text{-}2a\,\} + \\ 2(1\text{-}a\text{-}x_1)I\{1\text{-}2a < x_1 \leq 1\text{-}a\} + \\ 0I\{1\text{-}a < x_1 < 1\}) \end{aligned} \qquad (4.7)$$

With $G_k(a) = 0$ *and* $a = \delta U_{k-1}$, we can express

$$\begin{aligned} G_k(x_1) = (x_1 - \delta U_{k-1})(2\,\delta U_{k-1}\, I\,\{x_1 \leq 1\text{-}2a\,\} \\ + 2(1\text{-}\,\delta U_{k-1}\,\text{-}x_1)I\{1\text{-}2\,\delta U_{k-1} < x_1 \leq 1\text{-}\,\delta U_{k-1}\,\} \\ + 0I\{1\text{-}\,\delta U_{k-1} < x_1 < 1\}) \end{aligned} \qquad (4.8)$$

If P_2 and P_3 choose the threshold strategies $\mu_2 = I_{\{x_2 \geq \delta U_{k-1}\}}$ and $\mu_3 = I_{\{x_3 \geq \delta U_{k-1}\}}$ then the best response for P_1 must also be $\mu_1 = I_{\{x_1 \geq \delta U_{k-1}\}}$ and by substitution

$$U_k = 2\int_0^1 \mu_1(x_1)G_k(x_1)dx_1 + 2\int_0^1\int_0^{1-x_1}\{(x_1 - \delta U_{k-1})\mu_2\mu_3 + \delta U_{k-1}\}dx_1dx_2 \qquad (4.9)$$

$$= 4\delta U_{k-1} \int_{U_{k-1}}^{1-2\delta U_{k-1}} (x_1 - \delta U_{k-1}) dx_1 + 4 \int_{1-2\delta U_{k-1}}^{1-\delta U_{k-1}} (x_1 - \delta U_{k-1})(1 - \delta U_{k-1} - x_1) dx_1 + 2 \int_{0}^{1-2\delta U_{k-1}} (x_1 - \delta U_{k-1})(1 - 2\delta U_{k-1} - x_1) dx_1 + \delta U_{k-1}$$

The recurrent formula brings to the result and proof that:

$U_k = \delta U_{k-1} + \frac{1}{3}(1 - 3\delta U_{k-1})(1 - 6\delta^2 U_{k-1}^2)$ ends of the proof ■

In the case of no discounting, $\delta = 1$, and the horizon of negotiations is infinite, we have $lim_{k\to\infty}\ U_k = ⅓$. Players should always take the offers when the arbitrator suggests.

4.3.5 Equilibrium Analysis

The strategy profile in period t is represented as $\{(x_i^t, x_{-i}^t), g_{-i}^t\}$ where (x_i^t, x_{-i}^t) is the splitting rule as offered by the arbitrator and g_{-i}^t is the function with arguments as players except P_i "accept", then we have a majority which is ruled and each player gets its share [13]. Otherwise, all players get nothing or "reject". In the last period *T-1*, the strategy profile $\{(x_i^{T-1}, x_{-i}^{T-1}), g_{-i}^{T-1}\}$ is a NE if $g_j^{T-1}(|x_j^{T-1}|)$ = "accept" for $j \neq i$ and there is no value $|x_j^{T-1}| > |z_j^{T-1}|$ such that $g_j^{T-1}(|z_j^{T-1}|)$ = "accept" for $j \neq i$ that leads to the existence of a value $|x_j^{T-1}| < |z_j^{T-1}|$.

Per NE, there is no incentive for P_i to unilaterally increase its demand because any increase request would cause a rejection by another $P_j \in P_{-i}$ which will cause the game not to reach the simple majority. As part of the number of players forming the simple majority rule, no players would want to reject a share offered by the arbitrator, since any rejection of a share by the players will cause the game not to reach its simple majority quorum.

Finite Horizon Bargaining game: The finite horizon bargaining is the applicable game for the MANET with arbitration for the reason that all players are dynamics, the mobility of the players makes the bargaining finite because players will run out of transmission range and furthermore cause possibly the end of the game. The finite horizon bargaining is easily solved by backward induction.

Let's consider n players, $i = 1, 2, 3, \ldots$ the set of offers $X = [\, x_1, x_2, x_3]$, let $u_i(x)$ the utility player i derives at period t. We assume $u_i(.)$ is continuous, we normalize to 0 the payoff to players when there is no agreement. Let X_0 denote the set of offers from the arbitrator that are individually rational for all players. $X_0 = \{x \epsilon X, u_i(x) > 0 \text{ for all } i\}$, X_0 is non-empty and the payoff is assumed to be discounted by a common factor δ as $\delta^{t-1}u_i(x)$. The restriction is made to the stationary equilibrium where each player adopts the same acceptance rule in each period. Given any stationary acceptance rule σ_{-i} tracked by other players, the largest expected payoff $\bar{v}_i(\sigma_{-i})$ that player i may derive given σ_{-i}. An optimal acceptance rule for player i is thus to accept the proposal x if and only if $u_i(x) \geq \delta\bar{v}_i(\sigma_{-i})$ which is stationary. Denotes $A = \{x \epsilon X,\ \exists N_0 \subset \{1,2,3\}$, $|N_0| = n_0$, $u_i(x) \geq \delta v_i \ \forall i \epsilon N0\}$, and the equilibrium satisfies $v_i = P\, E[u_i(x) \mid x \epsilon A] + (1 - P)\delta v_i$ where $P = Pr(x \epsilon A)$

Proposition 4.1: Whatever is the majority requirement (n_0), a stationary equilibrium exists. [13]

Proof: Define the function $v \rightarrow \varphi(v)$, where $\varphi_i(v)$ corresponds to the right hand side (*RHS)* of v_i and let $\bar{u} = max_{i,x}\, u_i(x)$. The function φ is continuous from $[0, \bar{u}]^n$ to itself, thus, it has a fixed point.

4.3.6 Communication Overhead Analysis

The analysis of communication overhead in MANETs is an issue because it affects the energy consumption of an already limited battery lifetime of the mobile node. The communication overhead is related to different parameters such as the network size, node's mobility, node radio range, and network density [54]. The nodes requesting the arbitrator's service are considered a spontaneous cluster with the arbitrator as the cluster head (CH) for the bargaining process. The CH knows the identities of the nodes in need of service based on their primary request message. The reply message from the CH is to inform about the availability of an arbitrator. Nodes are in 1-hop distance from the CH [54] [51]. The negotiation between mobile nodes and the arbitrator follows an efficient cluster-based exchange of messages and data. The spontaneous cluster is dismantled once the bargaining is completed or one of the mobile nodes is out transmission range.

4.4 NEGOTIATION WITH N PLAYERS

In this section, we show how to deal with the game engaging *n* players. The arbitrator evaluates the majority $m = int(n/2)+1$, such that the majority is reached if at least *m* players accept their offers during negotiations. The arbitrator randomly generates offers in the form of vector ($x_1^k, x_2^k, \ldots, x_n^k$) at shot *k*. The joint density function of the Dirichlet distribution is described by:

$$
\begin{aligned}
&f(x_1,\ldots,x_n) = (n-1)!, \\
&\textstyle\sum_i x_i = 1, x_i > 0
\end{aligned}
\qquad (4.10)
$$

Let U_k indicates the value of the game at shot *k* and *K* denote the number of negotiation cycles before the game ends. In a negotiation game with majority rule, the arbitrator needs to have the consent of the majority players (*m* players) in order to transfer the data collected to the AP. With *n* players on the line, the arbitrator aims for a complete consent from players. The arbitrator then counts the number of players that agree on their offers. The game ends when the counting is greater or equal to *m*. For the vector (x_1^k, x_2^k,…, x_n^k) generated at shot *k*, the optimality equation is defined by:

$$
U_k^n = (n-1)! \int_{\delta U_{k-1}^n}^{1} G_k^n(x_1)dx_1 + \delta U_{k-1}^n \qquad (4.11)
$$

According to [4], the function $G_k^n(x)$ is in the form

$$
\begin{aligned}
G_k^n(x_1) &= (x_1 - \delta U_{k-1}^n) \int_{\delta U_{k-1}^n}^{1-x_1} \cdots \int_{\delta U_{k-1}^n}^{1-x_1-\ldots-x_{n-2}} dx_2 \ldots dx_{n-1} \\
&= \begin{cases} \dfrac{(x_1 - \delta U_{k-1}^n)(1 - x_1 - (n-1)\delta U_{k-1}^n)^{n-2}}{(n-2)!}, x_1 \le 1 - (n-1)\delta U_{k-1}^n \\ 0, x_1 > 1 - (n-1)\delta U_{k-1}^n \end{cases}
\end{aligned}
\qquad (4.12)
$$

By substitution into (4.10), (4.11) and also apply certain simplifications we have:

$$
U_k^n = \delta U_{k-1}^n + \frac{(1 - n\delta U_{k-1}^n)^n}{n} \qquad (4.13)
$$

Theorem 4.2: Consider the resource sharing problem with *n* players and the agreement by the players of their shared resources. The optimal strategies of players at shot *k* are determined by: [4]

$$
o_i(x_i) = \mathrm{I}_{\{x_i \ge \delta U_{k-1}\}}, i = 1, \ldots, n.
$$

The utility value of this negotiation game for a player meets the recurrent formula defined as follows:

$$U_k^n = \delta U_{k-1}^n + \frac{(1-n\delta U_{k-1}^n)^n}{n} \tag{4.14}$$

Proof: Consider the resource sharing problem with n players, the offer's acceptance requires complete consent: $p = n$

The joint density function to the Dirichlet distribution is as follows: $f(x_1,x_2,\ldots,x_n)=(n-1)!$,

Denote U^n_k the utility value of players of the game at shot k,

$\mu^0 = 1-\mu$ and $\mu^1 = \mu$, also the annotation μ^σ where $\sigma = \{0, 1\}$

$$U_k^n = (n-1)!\sup_{\mu_1}\left\{\int_0^1 \int_0^{1-x_1} \ldots \int_0^{1-x_1-\cdots-x_{n-2}} \vartheta\right\}$$

Where ϑ represents

$$\vartheta = \sum_{(\sigma_1\sigma_2\ldots\sigma_n)} \left\{\mu_1^{\sigma_1}\mu_2^{\sigma_2}\ldots\mu_n^{\sigma_n}.\begin{bmatrix} x_1, if \sum_{i=1}^n \sigma_i \geq p \\ \delta U_{k-1}^n, if \ \sum_{i=1}^n \sigma_i < p\end{bmatrix}\right\} \atop dx_1 dx_2 \ldots dx_{n-1}$$

$$U_k^n = (n-1)!\sup_{\mu_1}\{\int_0^1 \int_0^{1-x_1} \ldots \int_0^{1-x_1-\cdots-x_{n-2}} \mu_1 \ .$$

$$. \sum_{(\sigma_2\sigma_3\ldots\sigma_n)} \{\mu_2^{\sigma_2}\ldots\mu_n^{\sigma_n}.F_{1,k}\}dx_1\ldots dx_{n-1}$$

$$+\int_0^1 \int_0^{1-x_1} \ldots \int_0^{1-x_1-\cdots-x_{n-2}} (1-\mu_1). \sum_{\sigma_2\ldots\sigma_n} \{\sigma_2^{\mu_2}\ldots\sigma_n^{\mu_n}.F_{2,k}\}dx_1\ldots dx_{n-1}\}$$

The optimal strategy is defined by:

$$U_k^n = (n-1)! \int_{\delta U_{k-1}^n}^{1} G_k^n(x_1) dx_1 + \delta U_{k-1}^n \tag{4.15}$$

$$\begin{aligned} & G_k^n(x_1) \\ & = C_{n-1}^{p-1}(x_1 \\ & - \delta U_{k-1}^n) \int\limits_0^{1-x_1} \dots \int\limits_0^{1-x_1-\cdots-x_{n-2}} I\{\bigcap\nolimits_{i=2}^{p} \{x_1 \geq a\} \bigcap\nolimits_{i=p+1}^{n} \{x_i \\ & < a\}\} dx_2 \dots dx_{n-1} \end{aligned} \tag{4.16}$$

Where the function $G^n{}_{k-1}\,(x_1)$ is defined as:

$$G_k^n(x_1) = (x_1 - \delta U_{k-1}^n) \int_{\delta U_{k-1}^n}^{1-x_1} \dots \int_{\delta U_{k-1}^n}^{1-x_1-\cdots-x_{n-2}} dx_2 \dots dx_{n-1} \tag{4.17}$$

$$= \begin{cases} \dfrac{(x_1 - \delta U_{k-1}^n)(1 - x_1 - (n-1)\delta U_{k-1}^n)^{n-2}}{(n-2)!}, x_1 \leq 1 - (n-1)\delta U_{k-1}^n \\ 0, x_1 > 1 - (n-1)\delta U_{k-1}^n \end{cases} \tag{4.18}$$

By replacing the expression into (4.18), we have:

$$U_k^n = \delta U_{k-1}^n + \frac{(1 - n\delta U_{k-1}^n)^n}{n}$$

This concludes the proof. ■

```
Require: # players, $N \geq 3$; Time period before out of range, T; storage, Q; time transferring a packet, t; Cost factor, $\delta$;
Initialization: ;
c ← minvalue of player payload
While $T > 0$ do
```

```
    Arbitrator makes offers to players
    For each Player receiving offer do
      If accept (Player$_i$) then increment count End If
      If count reach Majority Then Data-Transfer
      Else  No Data-Transfer
            $Q \leftarrow Q(1 - \delta)$ ;
      End If
    Decrement T;
    End While
  End
```

Table 4.2: Algorithm for arbitration

The complete consent of the players is the target of the arbitrator when offers are made. Players have the same weight when the time comes to transfer data. The randomly generated offers made by the arbitrator are the size of the resources to transfer to destination. In case, players participating in the game have the same weights, the distribution guarantees the same opportunities for all players. However, if a player has a higher weight, its parameter will be increase during the Dirichlet distribution. Moreover, the final solution of utility depends on the length of the negotiations horizon. The algorithm in table 1 shows how resources are allocated among the players.

4.5 SIMULATION RESULTS

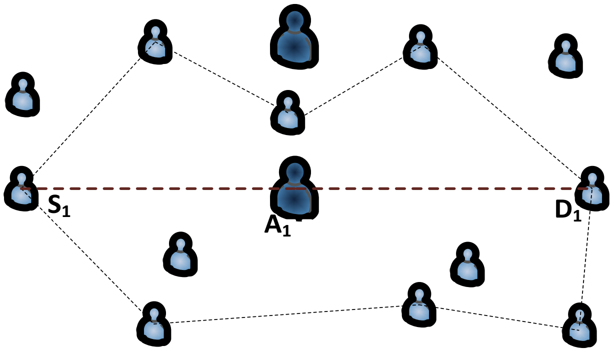


Figure 4.1: Snapshot of MANET, source S_1, destination D_1 and arbitrator A_1 with different routes to destination

In this section, we provide MATLAB simulations for better insight into analysis of the negotiations with or without arbitrators. The arbitrators use Dirichlet's distribution to make offers to players. This research work has proposed a high-level, game theoretic modeling for decisions of data transfer in MANET based on a simple majority mechanism. In the simulation, we quantitatively compare our proposed mechanism with the Service Negotiation model for Selfish nodes in the MANETs (SNSM) [53].

Parameter	***Parameter values***
Simulation Time	*500 sec*
rotocol	AODV
Number of Nodes	*20, 30, 40*
Arbitrator Nodes	*5, 10*
Transmission Range	*20m, 35m*
Node Initial Position	Randomly distributed
Mobility Model	Random Waypoint
Simulation Area	*100m x 100m*
Channel Type	Wireless Channel

Node Speed interval	*0.2 m/sec – 15m/sec*
Traffic Type	Constant Bite Rate
Time Step	*0.1 sec*

Table 4.2: Simulation Environment

The SNSM is also compared with the mechanisms of TIT-FOR-TAT (TFT) and Time-Dependent of Bourware tactics (TBD) [45] [53]. The SNSM designs a negotiation model for service bidding of selfish nodes in MANET. The use of virtual currency enables selfish nodes to participate in the network lifetime achievement.

The simulation setup parameters are provided in Table 4.2. We considered a MANET with *20* to *40* mobile nodes, including arbitrators randomly distributed initially in an area of *100m* x *100m*. Each node is free to move with a speed range of *0.2-15m/s*, and also a *20m* radio range. Arbitrators have a *35m* radio range. The heterogeneity of the mobile nodes in the network creates an asymmetric communication between a normal node and an arbitrator. Regular nodes can only communicate with an arbitrator if they agree on the offers from the arbitrator. Meanwhile, an arbitrator can directly communicate with any regular node provided that, a deal is made to find the shortest route to destination.

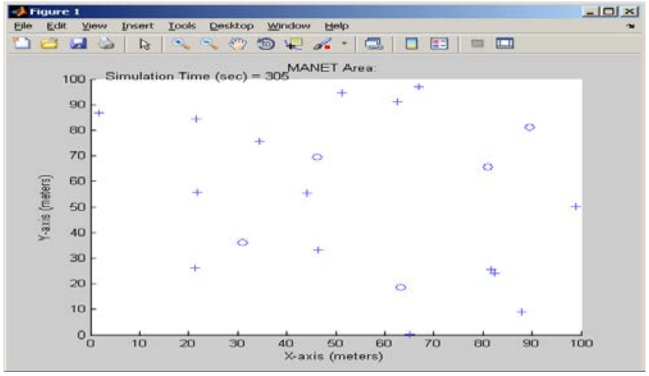


Figure 4.2. MATLAB Simulation Screen of 20 Mobile Nodes (15 normal Nodes and 5 Arbitrators)

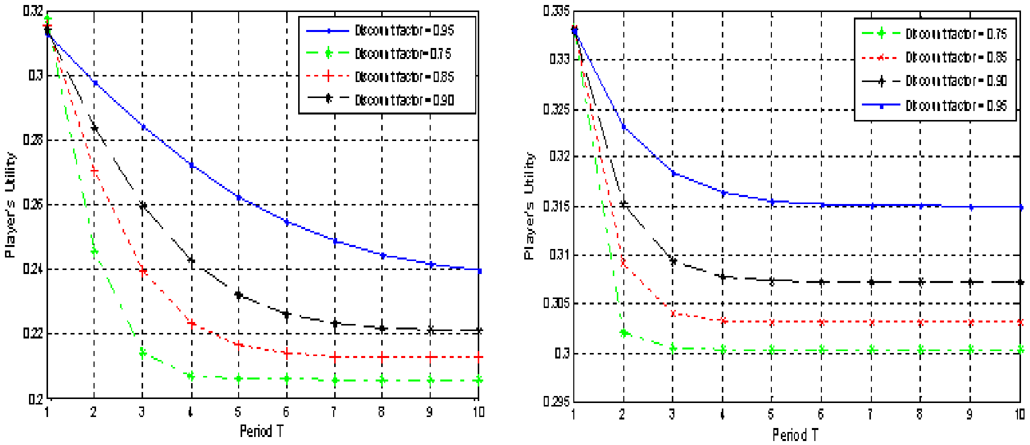


Figure 4.3: (a) Complete Consent (b) Simple Majority

Figure *4.3* represents the advantage of using arbitrators for data transfer in a network with selfish nodes. We have a *75%* connectivity failure due to mobility and selfish nodes ignoring communication requests. When injecting the network with 5 arbitrators, we have almost a *15%* decrease in connectivity failure. By increasing the number of arbitrators to *10* in a *20* node network, the connectivity failure ratio drops by *35%*. It's noticeable in the network that the arbitrators with wider radio ranges reduce the number of hops to the destination.

The offers made by the arbitrator result in acceptance or rejection by the players. Data transfer only happens if a majority of players consent. The average utility is defined as such in [53]. In our proposed scheme, the mean is half the offers made to player *i* and its minimum acceptable payload. The arbitrator's resources available to players are empirically shared between the subset of players for the duration of the negotiation.

Normalizing the shareable resource to "*1*" unit gives *1/n*, the shared value allotted to each of the *n* players. Most successful negotiation sequences occur when the minimum required load per player is lower than *1/n.*

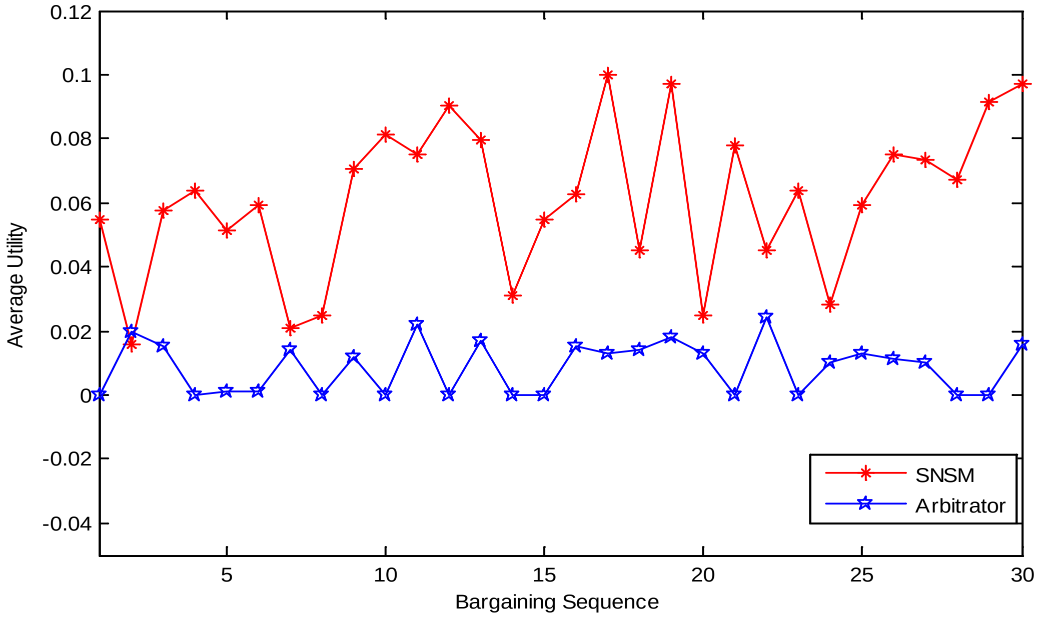


Figure 4.4: Average Utility Obtained during Negotiation Sequence for both SNSM and Arbitration

Figure *4.4* shows the average degree of utility for the SNSM with a maximum value of *0.1*. Unsuccessful rounds of bargaining are represented by the value *1*. The proposed solution with the arbitrators making offers to mobile nodes has a very low average utility. Mobile nodes also have low minimum payloads. The average utility between the offer and the minimum acceptable payload by a mobile node is almost equal to zero. The proposed solution has a better performance compared to the SNSM.

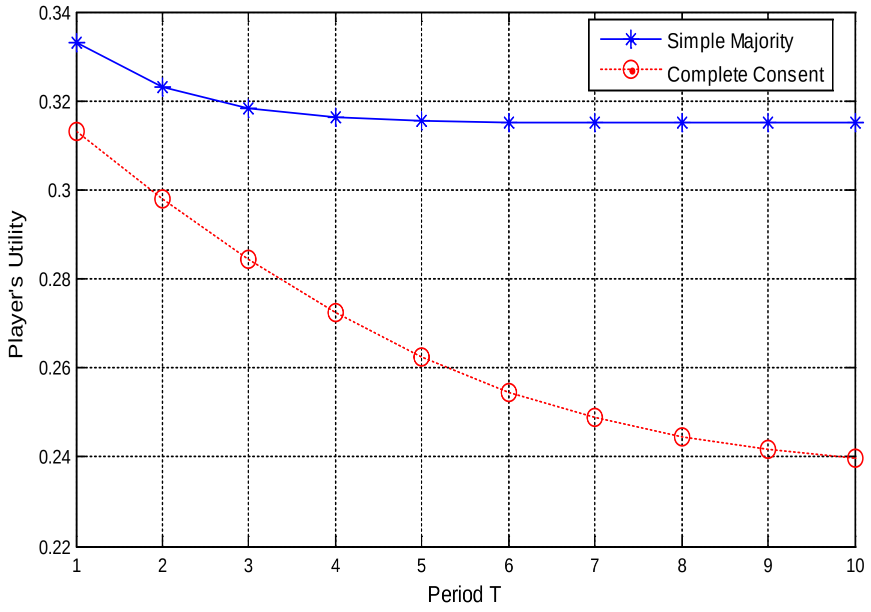


Figure 4.5: Negotiation Game with Three Players (c)

The negotiation game implemented through simulation shows in figure *4 5 (a)* that player's payoff when using the complete consent for different value of the discount factor $\delta = \{.95, .90, .85, 75\}$ decreases. Around the period $T = 6$, it tends to stabilize and remain constant. For the simple majority in figure *4.5 (b)*, the player's payoff decreases and stabilizes by the period $T = 3$. Of course, the majority player's payoff is higher than the complete consent because, only the simple majority of players' needs to agree and for the game to successfully end compared to an agreement of all the players.

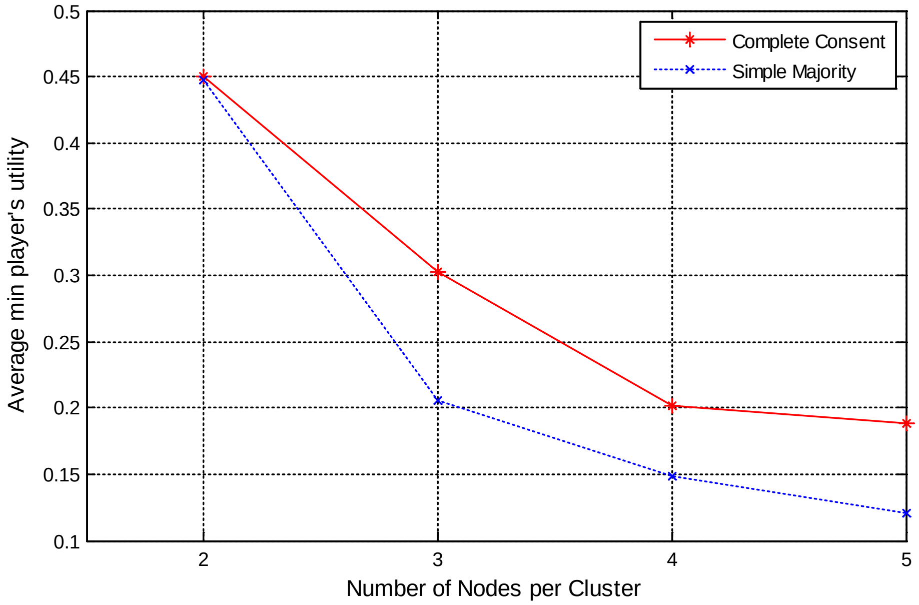


Figure 4.6: Average minimum Payoff a player received during negotiation

The figure 4.*5 (c)* shows the advantage of a simple majority in terms of player's payoff compared to complete consent. The network is also beneficial with the fact there is an agreement for the arbitrator to carry the task of data transfer over. A better player's payoff for the complete consent will be to reach an agreement by the third period *(T = 3)*. The figure *4.6* shows an estimate of the average minimum player's utility based on the number of nodes composing the spontaneous cluster. A cluster of two nodes will have almost the same minimum payoff for each node.

4.6 Conclusion and Future Work

This chapter models the problem of dynamic resource allocation in a multi-hop MANET of *N* heterogeneous nodes (including arbitrators) as a perfect information bargaining game where arbitrators make offers using Dirichlet's distribution. The proposed algorithm based on simple majority works to the advantage of the overall network through involvement of arbitrators in data transfer. The arbitrator's offers of 1/n to all requests enable the players to accept based on there being no frustrations with other nodes receiving preferential treatment. We have performed through simulation, which clearly showed that, if the arbitrators are rational, they can dynamically adapt their decisions to achieve the best benefit and optimize the network performance. The case of malicious arbitrators or malicious nodes and malicious arbitrators colluding will be the subject of future investigation.

CHAPTER 5

GAME THEORETIC MODELING OF SECURITY AND TRUST RELATIONSHIP IN CYBERSPACE

Today, online network services have evolved as the highest-emergent medium, enabling various online activities to be lucrative. However, these lucrative activities also bring new forms of privacy threats to the community. In a reliable e-business service, users should be able to trust the providers of the service to protect their customers' privacy. The service providers should not risk the personal and private information about their customers in cyberspace. There is an economic gain for a business provider when users trust the service provider. Despite those benefits, cyber security concern is the main reason some large organization may go bankrupted. Unfortunately, attackers may attempt to breach a provider's database and expose customers' private information. Therefore, in this paper, we propose a game theoretic framework for security and trust relationship in cyberspace for users, service providers and attackers. Mathematical proofs and evaluations support our model. Service providers may use the model to see how important and dissuasive against attackers is when investing in cybersecurity.

5.1 INTRODUCTION

In an ever-growing telecommunication industry, E-business gradually becomes of an importance to the social economy. While Online Social Network (OSN) has quickly grown into a wide network, for convenience, users see these OSNs not just as a platform to establish contacts, but also as a source of business, advertisement and entertainment. Although OSN users receive a variety of advantages and benefits from these services, the

OSN providers are seeking financial gain. The applications developed for these OSNs generate enormous interest in how people use cyberspace like Internets, Facebook, Instagram, and Twitter. This win-win solution also comes with new threats and privacy concerns to the community [58]. Considering the exponential increase of requests in cyberspace on a daily basis, this is a critical challenge for users and providers. For instance, malicious websites and fake URL addresses that look like the real deal. The attack is led to make the user believe he is on the right website and trick him to provide personal information. This deception can come through web-forms in an email received from an acquaintance containing a link to click; but in fact the link is embedded with a malware to collect private information from the user and his computer interactions [39].

5.1.1 Motivation

OSN providers should strive to protect their users' privacy and information. User privacy and private information in the wrong hands will definitely hurt the monetary benefits of the provider. Risk and trust are two behavioral factors that sway decision making in an uncertain environment like cyberspace. While OSN providers face cyber attack on a daily basis, it is their responsibility to educate the users about all potential breaches of security and the methods to mitigate the risk [40].

Mass media are on the front line of creating awareness information that leads people to develop a bias and trust cyberspace differently. Whenever there is a security breach the media may induce emotional outbursts about risks and their potential consequences; for example, the identity theft of Target Store credit card users and the massive hack of Home Depot customers' information. [58]. We proposed in this chapter a game theoretic approach to establishing a relationship between trust, defined as a kind of risk assessment and various factors that could affect the assessments (risk). The media can tilt the balance of information in most trust systems that considers risk as a psychological cost. Moreover, breach of security on a providers' infrastructure by attackers will have less impact if users are informed by the providers than a television broadcast or newspaper. Therefore, distrusting a providers' capability to secure users' privacy and private information will hamper any plausible positive results. It is consistent with intuition: a user who hears a security breach of private information on the news foresees a lack of investment in security infrastructure and intent to cover up compared to providers reaching out to users and inform them of the security breach and a promise to upgrade security infrastructure.

5.1.2 Contribution

This chapter centers around the proposed concept to mitigate cyber attack behavior with security implementation. The preponderance of successful attack launch by an attacker or a group of attackers may be because of the vulnerability of the security infrastructure due to a lack of adequate investment. System administrators defend the system 's infrastructure against intelligent misbehaving users (attackers), while users tempt not to trust an online service in case of a compromised of their data privacy. The specific contributions in this work are summarized below:

- We propose a mechanism design to mitigate cyber attack behavior in security implementation using a game-theoretic approach.
- We formulate an original three-player game to model conflicting and rational confrontation between players.

- We analyze the different solutions obtained from the Nash equilibrium (NE)
- We interpret the different outcomes on how they may benefits system administrator or decision-maker.

The provider's objective is to secure the users private data against an attacker whose objective is to breach the system and expose users' private information. The user's main concern is to safely use his private information in cyberspace.

Some research work exist in this area which we summarize here. In [39], Kim *et al*. examined the relationship between trust and risk as determinants of trusting behavior in e-commerce. The risk of cyberspace manners can be classified as high, low and inexistent. Cyberspace behaviors include activities such as online purchase of an article or providing private information to an e-vendor.

Kamhoua *et al*. [61] proposed a game theoretic model to help the online social network users determine the optimal policy in terms of data sharing using a zero-sum Markov game model. While the authors make the assumption that the probability transition function, the reward and the discount factor are common knowledge among players. There is a possibility that some of the information is made private or not available to the opponent. Huber *et al*. [35], presented the Friends-in-the-middle Attacks by exploiting social networking sites for spam. The impact of spam is simulated on the online social site Facebook. Raya *et al.* [36] proposed and analyzed a game theoretic model of the trust-privacy tradeoff using incentives that allow building trust and at the same time keeping the privacy loss at a minimum. The game model shows that individual players do not contribute to trust establishment unless they received an appropriate incentive. As an example, the process of revoking of access rights for misbehaving nodes is not done unless there are incentives for voting players.

Seigneur *et al.* [37] introduced an approach to achieve the tradeoff between trust and privacy in online transactions. The privacy is preserved with the use of pseudonyms for different transactions. Thus, the linkability of the transactions is prevented and a level of reputation is assigned to each of the pseudonyms. In order to increase the level of trust of an entity, a combination of several reputation levels is required and the number of pseudonyms to link depends on the reputation trust level. Lilien *et al.* [38] discuss the difference between privacy preservation and trust establishment for online transactions. Assumptions are made about users having a set of private attributes that they want to conceal and a set of corresponding credentials that are helpful in establishing trust for these users. The tradeoff problem is formulated as the choice of the minimum number of credentials to be revealed for satisfying trust requirements, such that the users' privacy loss is minimized.

Douss *et al.* [60] discussed a game-base trust establishment for mobile ad hoc networks (MANET). The authors introduce an evaluation model for trust value. Then, a computational evaluation of the methods is applied and finally, a framework is proposed for trust establishment. Han *et al.* [78] proposed a method of infiltration exploitable through cloud and not the traditional computing process: the side channels. It gives a rise to new risks as hardware to create a virtual machine (VM) is shared between users, which attackers can exploit. By starting and having the VM in the same server as a user data, an attacker can siphon private information such as web traffic and encryption keys. Given the danger of cross-side channel attacks, some user may require while using the cloud service to be physically isolated from the resource of the cloud service provider. Zhang *et al.* [79] proposed HomeAlone which is a defensive tool that helps a user determining if its VM resource allocation has an exclusive use of the physical machine. The tool can detect the activity of an attacker's co-resident VM by analyzing a portion of the L2 memory cache set aside by his VMs.

Basar *et al*. [80] explained the devastating cost of failure to properly secure a network from an attack. The authors showed how an attacker can infiltrate a network at one node, and from the compromised node, the attacker can breach easily and access other nodes of the network infrastructure. Wang *et al.* [81] analyzed the nodes' decision in a cluster environment. The cluster environment is composed of *n* clusters of *m* nodes, which is *n* x *m* individual nodes. The attacker to launch an attack chooses the number of clusters to attack, while the defender chooses how many nodes can participate in the decision in each cluster. A zero-sum game is formulated during which the defender maximizes the expected number of clusters that decide correctly and in the same time the attacker minimizes the say number. A general framework is proposed to find the Nash equilibrium. However, the assumption made is that the structure of the cluster is fixed, which give a better optimization strategy to the defender by just changing the cluster structure.

In short, the previous researches on privacy are mostly focused on the current interests of the different players, and previous works on defense against an attacker or an intruder are mostly concentrated in the interests of both players. But most of the game players would like to take the long-term strategy in face of interest for all three players in the game. In the existing literature, when using game theory frameworks, there is no three-player game. We have a two-player game: the defender against the attacker or the provider strategizing on how to improve trust with the users. None of the game approaches involve the defender, the user and the attacker at the same time. In this chapter, even though, the media viewpoints create awareness that influences users to be more bias in trust of various OSNs differently. We are interested in the relationship established between trust and risk in cyberspace using game theoretic modeling.

The remainder of this chapter is organized as follows. The section 5.2 presents the system and the threat models. In Section 5.3, we propose the game theoretic model. Section 5.4 presents the numerical results. Finally, the conclusion and future works are drawn in Section 5.5.

5.2 System and Threat Models

5.2.1 Objectives

With the development and popularization of online network service (ONS), the safety of ONS's users' privacy becomes a crucial and critical issue. The service provided gains in popularity because it facilitates the living conditions of the people. Any proven amelioration of living conditions will always attract more and more customers or users. To better serve its customer, a service provider has to deploy and make the service available anywhere and at anytime it is needed. As any lucrative business, the service provider in order to remain in business has to secure and protect its own confidential data and for the incentive of doing the business, secure and protect customers confidential and data privacy. Whenever there are financial and private information flowing around, there will always be misbehaving actors trying to take advantage of the situation.

5.2.2 System Model

The figure 5.1 illustrates our system model: An online service provider with lots of customers that use the services through their electronic devices with connections to the Internet. The users are known as regular customers with their electronic apparel (i.e. Computer, laptop, tablet, smartphone, etc.) using cyberspace (i.e. Web-apps, mobile-apps, phone-apps) to buy goods or services. Technically, the user may run different number and version of applications provided by the business service without any negative impact on this illustrated model. The applications, even though use on different devices to access the online services require an operating system to function and the operating system is managed by a service provider. In practice, a user in order to acquire goods or services online has to provide personal information, but not limited to: full name, address, DOB, social security #, credit card #, PIN#, bank account#, etc... These information in the wrong hands may cause lots of damages to the owner of the information. The damages can range from financial ruins, bankruptcy, loss of identity, debts, and more.

The attacker or group of attackers represented on figure 1 illustration as “Attacker” is an intelligent user with unorthodox behavior. The attacker's main intention is to launch an attack or even coordinated attacks to gain access to critical or confidential information of the service provider and users’ private information. Instead of the attacker launching attack against “easy” target like a user because of the minimal security an user can afford, the attacker prefers to launch attack against the service provider. In case of a successful attack, the payoff will be colossal. Therefore, there are three major players defined in our system model, the users, the providers, and the attackers. The users are known as regular customers with their electronic apparel using cyberspace (i.e. online applications) to buy goods or services. The providers are businesses developed on the cyberspace that provide goods and services that are financially profitable. The attackers are entities with malicious intent. Their agenda is to attack providers' infrastructures and collect users' privacy, private information and companies' secrets. The attackers possess the electronic gears to launch an attack on the provider's infrastructure. A direct attack on one user is not that beneficial for the attacker. Therefore, an attack on the data repository of a provider may lead to a gain in multiple users' private information.

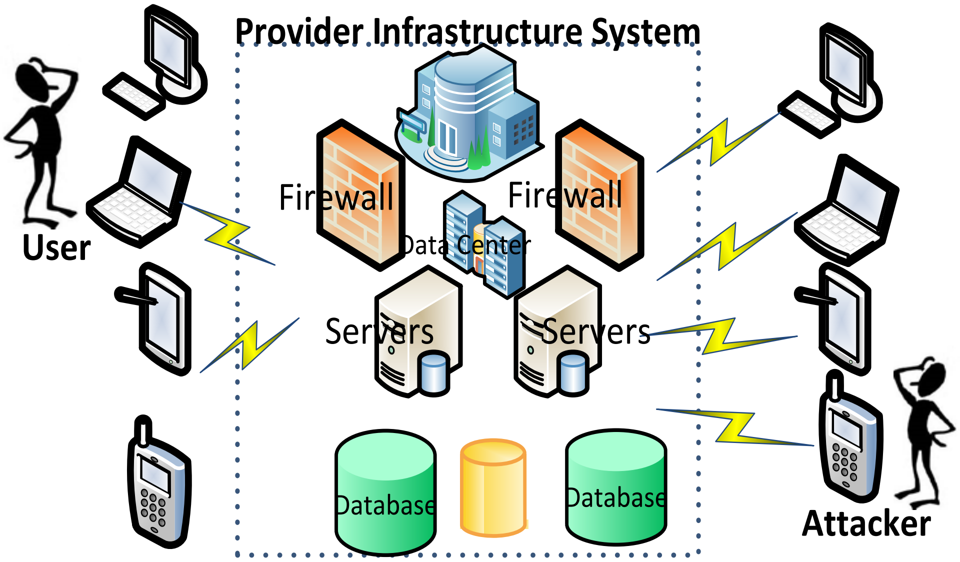


Figure 5.1: Overview of Component Interactions between User/Attacker/Provider

We assume a user needs his personal and private data available in order to conduct an e-business. We also assume that there are risks involved when information is used online. Users are aware of the potential risks; therefore the user needs to have a level of trust and confidence before providing personal information. The user takes all necessary precaution to keep his private information hidden from the public. The service providers need to invest in security for two major reasons:

1. To protect their infrastructure against daily attack perpetrates by attackers.
2. To secure transaction information made by the users.

For example, any interactions with the user that involve exchange of users' private data over the internet should be secured using secure sockets layer (SSL). The implementation of credential verification will make sure that the user using the information is the user owning the information. We assume the attacker's main objective is to breach the providers' infrastructure security system and gets the users' and company's private information. Going after a user's private data directly may not be beneficial to an attacker. Moreover, the user's data like credit card information can be cancelled and rendered useless to the attacker. The attacker monitors the providers' system for security vulnerabilities. For example, an operating system may have bugs exploitable to gain administrator credentials to the system, or strong passwords were not implemented and are easily guessed or tricked.

The goal is to make it difficult for attackers to breach the system and gain access to useful business and users' private information. Providers' data that can be breached are divided in two groups: futile and vital. Providers' strategies to be safe include investing in system upgrades, vulnerability correctness, architectural scalability of data, and network security. If a security breach occurs, this would limit the breach to futile data as much as possible, while making the system available and user friendly. Users have the tendency to either trust or are suspicious of online-sites because of the available information at risk.

In our model, we do not address the leakage of business and users' private information by mechanisms other than the attacker breaching the provider's security system. For example, a business may sell users' information to another company for financial profit. Although this constitutes a user privacy breach, it is outside the scope of our research work.

5.2.3 Trust-Risk Game Model

In spite of the risks reported about threats in cyberspace, for example, the spread of malicious worms on computing systems, cybercrime such as identity theft that may lead to financial ruin, money laundering by the drug cartel on the internet [39] [40], people still show a high level of dependency on cyberspace. Given that private information is traded for the user's trust, privacy preserving entities (cyber system providers) have to participate at a satisfactory level of trust without gratuitously revealing too much private information. Users have the tendency to trust or distrust a cyber-site because of the risk perception on sharing their private information. Hence, a user perception of low trust for a cyber-site may be associated with his perception of a high risk and its consequences on his privacy and private data. Similarly, the perception of high trust can be associated with the perception of low risk which implies negligible consequences for privacy and private data shared. Therefore, trust and risk are reverse mechanism concepts which mostly conceptually reflect how a user makes a choice to use cyberspace for business, social or private transactions. It becomes paramount to find and implement a mechanism of fairness protection between the user's private data and the provider's ability to secure. It is even questionable whether both entities would be efficient in data protection.

The use of game theory is called to solve the above related issues. We have the *Attacker-Defender game (ADG)* between the attacker and the provider and the *User-Provider game (UPG)* between the user and the provider. *ADG* captures the competitive interactions between the attacker who is trying to circumvent the provider's system and gain access to users' private data and the provider who needs to invest in securing its customers/users' private data. *UPG* models the combination of factors that helps the user assigning a level of risk (high or low) on an e-business or OSN if their privacy and private information is shared. Moreover, if data breaches occur, how efficient is the corrective approach to mitigate the damages.

We combine both games *ADG*: non-cooperative game between *2* players; the provider and the attacker, *UPG*: cooperative game between two players; the user and the provider into one game theoretic with three players: user, provider, and attacker.

5.3 Game-Theoretic Model

This section considers a game with three players: An attacker, a provider and a user. Our assumption is that the three players are rational. Therefore, they understand the system in place and can perform the necessary calculation to only take the actions that improve their expected payoff. The attacker has two defined strategies: launch an attack (*A*) on the provider’s infrastructure or *Not* launch an *attack* (*NA*). Only one of the two strategies can be used at a time by an attacker. The attacker strategy to launch an attack on the provider’s infrastructure may consist of a multi-stage process involving steps such as a brute force attack, scanning for known vulnerabilities, SQL injection, buffer overflow, exploit attack, bypass firewall rules with spoof attack, Trojan horse or backdoor attack. The provider of the system has two choices in terms of strategies, to either *Invest* in security (*IS*) or Not to Invest (*NIS*). The provider’s strategy to invest may consist of a multi-stage process and actions such as system-wide monitoring, software updates, patching of vulnerabilities, installing intrusion detection system (*ids*), clustering and duplicating data servers, and/or IP-hopping and firewalling. Therefore, the financial component tends to influence the provider to not invest in security. The user has also two strategies applicable: *trust* the provider’s cyber-site (*T*) with their personal information henceforth, uses it to make a transaction or *distrust* (*D*) the provider’s system and does not use it.

A 3-tuple represents a strategy profile for this game which indicates the action taken by each player. For example, the strategy profile *(T, IS, A)* shows that the user trusts the provider’s system to make a transaction, the provider invests in security for his infrastructure, and the attacker launches an attack to breach the provider’s system.

Let us examine the utility structure of the game. Given the profile of action, the payoff/utility is the player satisfaction. We normalize the payoffs to the players following the strategy profile. Following are the parameters used in the game:

- The parameter α represents the probability of an attacker getting detected or caught on the provider’s system, given that he has invested in security.

- The parameter *b* represents the benefit of the attacker from attacking and not getting detected or caught by the provider.

- The parameter *λ* represents the loss to the provider if an attacker launches an attack on the provider's system and the attacker is not detected or caught.

- The parameter *p* represents the loss to the attacker from getting detected while launching an attack on the provider's system.

- The parameter *σ* represents the probability that critical data in the provider's system are compromised given a successful attack. We consider that any successful attack on the provider's system will give up critical data, which means $\sigma > 0$. Moreover, not all successful attacks can compromise the provider's critical data ($\sigma < 1$). Therefore, we have $0 < \sigma < 1$.

The correctness of our game model depends on the correct estimation of the loss *λ* and the probability *α*. The guidance issued [6] by the United States Securities Exchange commission (SEC) requiring companies to disclose all cyber incidents with detail description of costs and relevant information such as insurance coverage. Therefore, the data provided from previous cyber incidents can be used to estimate the different probabilities values and cost to be used with our defined game model. There is a sense of assurance when a provider invests in security which has its reward.

- The parameter *R* represents the reward that can be calculated as a function of revenue generated by the users' transactions because the users see the provider's system a low risk in terms of divulging their private information.

- The parameter *e* represents the total expenses. Investing in security by the provider requires a total expense.
- The parameter *G* represents the gain defined as what the user gains by using the cyberspace for any transactions. For example, user shops online from the comfort of your home or office compared to spending time, driving to the store, spending money on gas, etc.
- The parameter *d* represents the cost of a user that worried about his private information being compromised or when the user is informed that there was a security breach on one of its service providers and the steps taken to monitor and mitigate the situation.

Table 5.1 shows the game model in normal form. Table 5.1 is a combination of two tables. The left-table shows the game model when the user trust *(T)* the provider's cyber system. The right-table shows the game model when the user distrusts *(D)* the provider's cyber system. The payoffs of the three players are represented in each block in three lines. The first line in the block is the user payoff. The second line is the provider payoff, and the third line represents the attacker payoff.

		*User trust (**T**)*		*User distrust (**D**)*	
		Attacker		*Attacker*	
		A	***NA***	***A***	***NA***
Provider	***IS***	$\{G - \lambda + \alpha\lambda;$ $R - e - \lambda\,(1 - \alpha);$ $b - p\alpha\}$	$\{G;$ $R - e;$ $0\}$	$\{G - \lambda + \alpha\lambda - d;$ $R - e - \lambda\,(1 - \alpha);$ $b - p\alpha\}$	$\{G - d;$ $R - e;$ $0\}$
	NIS	$\{G - \lambda + \alpha\lambda;$ $R - \lambda;$ $b\}$	$\{G;$ $R;$ $0\}$	$\{G - \lambda + \alpha\lambda - d;$ $R - \lambda;$ $b\}$	$\{G - d;$ $R;$ $0\}$

(a) User plays action (T) *(b) User plays action (D)*

Table 5.1: Stage Game in Normal Form

The payoffs are calculated as follows: If the player chooses the strategy profile *(T, IS, A)*, which means, the user trusts *(*play action *T)* the provider's system and uses it for cyber transactions, while the provider invests in security (play action *IS*) and the attacker launches an attack (play action *A*) targeting users' private information (*cf.* Left-table, 4th line, 3rd column).

The provider gets a reward *R* for investing in security and also incurs a cost *e* for the security expenses. Amid the attacker launches an attack with a probability α (because the provider has invested), it will incur a loss $\lambda(1 - \alpha)$ if successful. This will result in an expected loss of $\lambda(1 - \alpha)$ for the provider. The attacker payoff is the benefit *b* of launching without getting caught or detected less the probability α of getting detected if the provider invests in security:

$$U_{att}(T, IS, A) = b - p\alpha$$

The user payoff

$$U_{user}(T, IS, A) = G - \lambda + \alpha\lambda$$

is the difference between the gain of the user's trust in using the system and the expected loss from the system if compromised. The user's partial loss $\lambda(1 - \alpha)$ is the result of the attacker breaches into the provider's system and gains critical information which are users' private data. The player's payoffs in the other strategies profile are calculated the same way.

5.3.1 Game and Equilibrium Analysis

This section analyzes the game, derives all possible Nash equilibria from the game in Table 1, and understands its impact on the players. Per definition of Nash equilibrium profile: no player can increase his payoff by a unilateral deviation. Moreover, players are rational; each of them is playing his best strategic response to other two players' best strategies. Thus, the Nash equilibrium can help predict the behavior of the player wanting to maximize their payoff in the game.

$$R - e - \lambda(1 - \alpha) > R - \lambda$$

$$\rightarrow e < \lambda\, \alpha \tag{5.1}$$

It means that investing in security is the best option for the provider in order to lower the risk of users' private information being breached. Moreover, the attacker can only target the provider's system knowing that the provider has invested in security when we have:

$$b - p\alpha > 0 \tag{5.2}$$

The penalty is huge for the attacker to get detected while launching an attack on the provider’s system. The reward of launching an attack should be worth the risk of getting caught.

As a matter of fact, any game in strategic form has a Nash equilibrium *(NE)*. Let find the conditions applicable to the parameters for all possible pure Nash equilibria.

Theorem 5.1: If $\alpha < \alpha_0 = e/\lambda$, then the game in Table 1 admits a pure strategy *NE* profile *(T, NIS, A)*.

Proof: An examination of the eight different pure strategies in Table 1 shows that the only possible pure NE is when the provider does not invest in security, the user trusts the cyber system and the attacker launches an attack on the provider’s infrastructure. For the other strategy profiles, there is at least one player able to increase its payoff by a unilateral deviation.

When the attacker targets the system and the provider does not invest in security, we have:

$$U_{att}(T, IS, A)\text{-}U_{att}(T, NIS, A)$$

$$\rightarrow \quad R - e - \lambda(1 - \alpha) = R - \lambda \qquad (5.3)$$

$$\rightarrow \lambda\alpha - e = f(\alpha).$$

The function $f(\alpha).$ is a linear function with slope $\lambda\alpha$ and its lower bound value is the cost e. Thus, $f(\alpha)$ is increasing.

The initial value $f(\alpha_0) = \lambda\alpha_0 - e = 0.$

Case 1: if $e > \lambda\ \alpha$,

then $U_{att}(T, NIS, A)–U_{att}(T, NIS, NA) > 0$.

This condition is not the choice to fulfill to the best for the provider's system by not securing its infrastructure. The provider prefers not to invest than to invest. The attacker prefers to attack with a positive payoff the provider's system than not to attack. The strategy profile *(T, NIS, A)* is a pure Nash equilibrium because the players of the game cannot increase their payoff by a unilateral deviation.

Case 2: if $e/\lambda < \alpha < b/p$,

then we have the difference in the payoff $U_{att}(T, IS, A) - U_{att}(T, IS, NA) > 0$.

Thus, the attacker prefers to launch an attack on the provider's system than not to attack.

The payoff $U_{prov}(T, IS, A) – U_{prov}(T, NIS, A) > 0$.

Thus, the provider prefers to invest than not to invest into the security of his system. The strategy profile *(T, IS, A)* is a pure Nash equilibrium of the game because neither the provider nor the attacker can increase their payoff by a unilateral deviation.

Case 3: if $e < \lambda\alpha$ and $\alpha > b/p$

There are no pure strategy profiles for a Nash equilibrium in the game. The strategy profile *(T, IS, A)* is not a *NE* because the attacker can increase his payoff by simply changing his strategy from *A* to *NA*. The strategy profile *(T, NIS, A)* is not a *NE* because the provider can increase his payoff by simply changing his strategy from *NIS* to *IS*. With this back and forth reasoning, it conveys to us that we do not have a pure strategy NE.

However, a mixed strategy Nash equilibrium is highly plausible, and it's defined and set as follows: denote the variables $0 \leq x, y, z \leq 1$.

Let $\theta = xT + (1 - x)D$ be the probability mixed strategy *NE* of the user. From the basic game theory principles, the user optimal strategy is to randomly choose between strategies *T* and *D* such that the provider's system is at the lowest chance of security breaches.

We must have for the user: $U_{user}(T) = U_{user}(D)$

Let $\mu = yIS + (1 - y)NIS$ be the probability mixed strategy NE of the provider. From basic principles of game theory, the attacker optimal strategy is to randomly choose *y* such that the provider is indifferent when deciding between strategies *IS* and *NIS*.

We must have for the provider: $U_{prov}(IS) = U_{prov}(NIS)$

$$xz(R-e-\lambda+\lambda\alpha)+x(1-z)(R–e)+(1-x)z(R-e-\lambda+\lambda\alpha)+(1-x)(1-z)(R–e)=$$

$$xz(R-\lambda)+x(1-z)R+(1-x)z(R-\lambda)+(1-x)(1-z)R$$

$$\Longrightarrow z = z_0 = e/(\lambda\alpha) \qquad (5.4)$$

We know that $0 \leq z \leq 1$ and thus,

$$U_{prov}(IS) < U_{prov}(NIS)$$

$$\Longrightarrow 0 \leq z < z_0 \leq 1 \qquad (5.5)$$

And also

$$U_{prov}(IS) > U_{prov}(NIS)$$

$$\Longrightarrow 0 \leq z_0 < z \leq 1 \qquad (5.6)$$

Similarly, consider $\sigma = zA + (1\text{-}z)NA$ to be the probability mixed strategy of the attacker. The attacker randomizes between *IS* and *NIS* in such a way that the attacker is indifferent when choosing strategies *IS* and *NIS*. This is translated by:

$$U_{att}(A) = U_{att}(NA)$$

$$\Longrightarrow xy(b\text{-}p\alpha)+x(1\text{-}y)b+(1\text{-}x)y(b\text{-}p\alpha)+(1\text{-}x)(1\text{-}y)b=0$$

$$\Longrightarrow b\text{-}yp\alpha=0$$

$$\Longrightarrow y = y_0=b/p\alpha \qquad (5.7)$$

We know that $0 \le y \le 1$ and thus,

$$U_{att}(A) < U_{att}(NA)$$

$$\Longrightarrow 0 \le y < y_0 \le 1 \qquad (5.8)$$

and

$$U_{att}(A) > U_{att}(NA)$$

$$\Longrightarrow 0 \le y_0 < y \le 1 \qquad (5.9)$$

Given the condition in (3) and (5) are verified and the probabilities *y and z* hold. Therefore, the strategy profile $\{T, y_0IS + (1\text{-}y_0)NIS, z_0A + (1\text{-}z_0)NA\}$ is a mixed strategy Nash equilibrium. However, if the conditions are not met, then we can verify that there is no possible mixed strategy.

In summary, it is important to the provider to invest in security. The cost or expense *e* should be worth the equivalent value of loss. In other word, the effort from the provider in term of securing the users private information is very important in measured to the impact of losing customers because the trust level is low which means the provider's business is high risk and untrustworthy. The provider invests commensurably to the worth of its business may have dual impacts: 1) Users are confident to use the system for business transactions because of the investment in security and low risk of having their private information rendered public. 2) The higher the security, the better is the dissuasion to attacker to breach the system because of the penalty up to prison incarceration if they are detected and caught.

5.4 NUMERICAL RESULTS

Our game equilibria had provided a detailed exposition of the game model and its properties. In this section, we derive from the game analysis our numerical results. The MATLAB simulations support the game-theoretic techniques analyzed in this chapter. The values we have used in this MATLAB simulation is just to illustrate and provide concrete examples. The variables used in the calculation of mixed and pure strategy equilibrium were $R, e, p, \lambda, b,$ and α. We will assign values to some variables and they will remain fixed during the entire simulations while others variables increase or decrease.

For the first scenario, we will set the value of all needed parameters to $R = 1, e = 0.2, \lambda = 0.6, b = 0.5, p = 0.68$ and α is variable. We chose these values as an illustration of a non-intuitive suggestion of our game model. Figure 5 2 shows that the provider's payoff is constant when $\alpha < \alpha_0 = 0.33$ which is case *1* of the pure strategy Nash equilibrium. When the payoff of the provider is constant while the probability α is increasing, the rational player will be better looking to increase its payoff. However, the case *2* defines as another pure strategy Nash equilibrium with $\alpha < 0.73$. At $\alpha \geq 0.73$, there is a change of strategy from pure to mixed strategy Nash equilibrium. There is an attenuation on the provider's payoff, which means the frequency of the attack causes the provider to slowly increase its payoff.

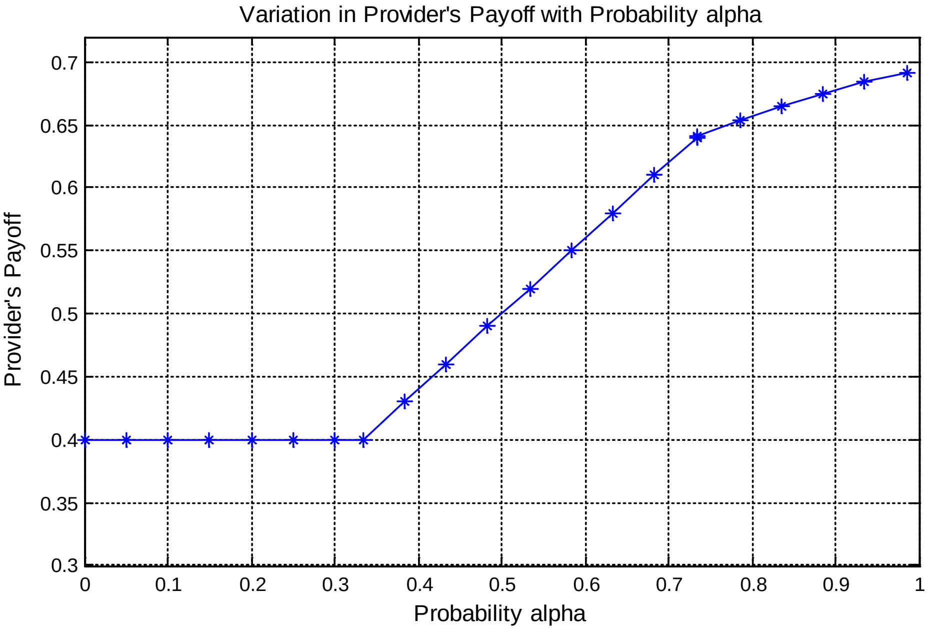


Figure 5.2: Variation in Provider's Payoff with Probability Alpha

By setting $\alpha = 0.51$ and $R = 0.95$, Figure 5.3 shows the strategy change for the pure Nash equilibrium to the mixed strategy Nash equilibrium. The loss to the provider λ is the variable in this case. We also can see the three cases of strategic change, the first one when $\lambda < \lambda_0 = e/\alpha = 0.39$, the second pure strategy is the case where $(0.39 \leq \lambda \leq 0.84)$ and the major shift occurs at the $\lambda{=}0.84$ when the provider's payoff reaches 0.34.

Moreover, the shift is to the mixed strategy Nash equilibrium. The decrease in value is for the provider's payoff its way of showing that it's not rewarded by the game when the loss increases.

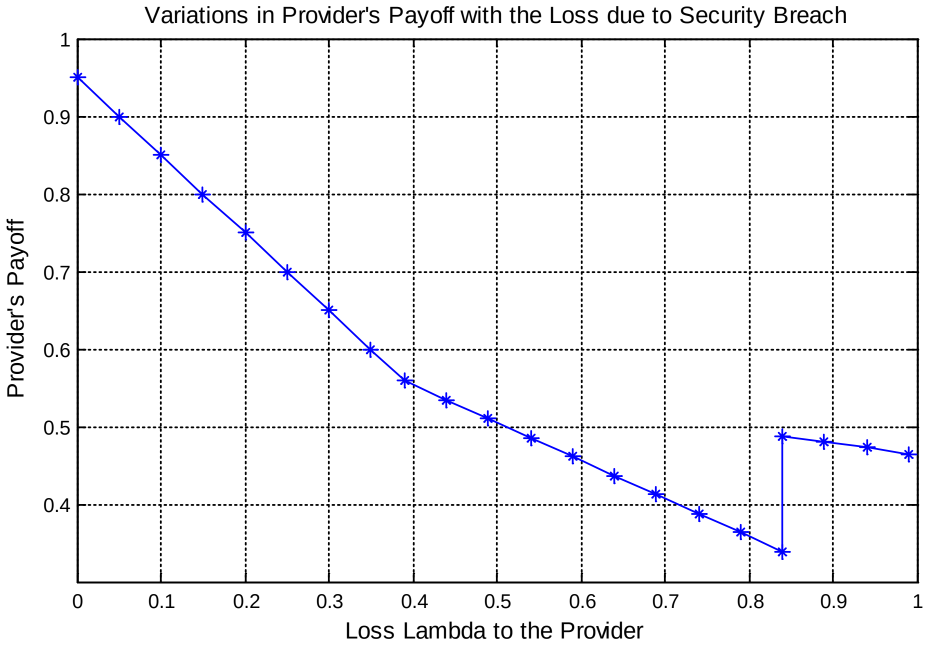


Figure 5.3: Variations in Provider's Payoff with the Loss due to Security Breach

The expense *e* translates as the cost to improve the security of the provider's infrastructure against an attack. From the values selected, we have the provider's payoff constant until it reaches $e = e_0 = 0.3$ in expense and it follows with a decrease in payoff for provider because the investment in security is paying off. There is a drop in payoff for the provider when he invests $e > 0.73$; the provider's payoff is negative. If the provider can invest in security up to $e \geq 0.7$ the loss due to attack will be minimal with less impact to the users' privacy or manageable loss of private information. The mixed strategy NE indicates that the attacker may willing to target the provider's system with a high risk of getting caught and low risk of getting breach.

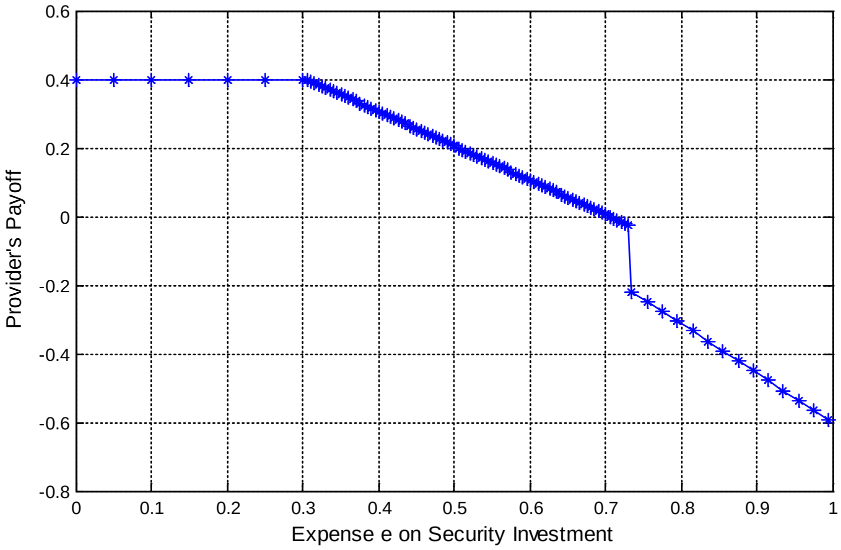


Figure 5.4: Variations in Provider's payoff

The game clearly admits multiple Nash equilibrium strategies and the expense *e* will provide guidance to players' choice.

Figure 5.5 shows that the attacker's payoff drastically dropped when there is any investment made by the service provider to improve the security of its infrastructure. If the parameter α that represents the probability of an attacker getting detected or caught on the provider's system is over *0.5* (*alpha* ≥ *0.5*) the expected probability of the attacker of not getting detected or caught is under *0.1*. In case the attacker relies on its probability gain from figure 5.5, it will be to the best interest of the service provider to invest in the security component by increasing the expense *e*, which will also increase the probability α and it will be good to have $\alpha \geq 0.5$.

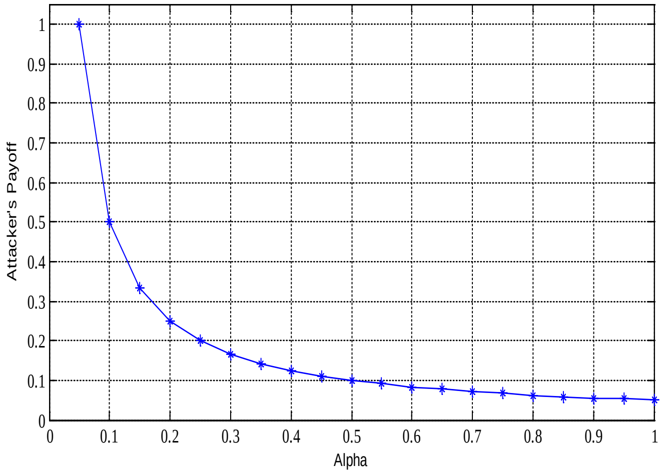


Figure 5.5: Variations in Attacker’s payoff

5.5 Conclusion and Future Work

In this chapter, we optimize the trust between the users and the provider by the use of the game theoretic approach. The three player game in this case provides a quantitative approach to perform a cost analysis of the security investment. The provider does not have the luxury to not invest in security. Any online service network where customers provide their private information should show concern with protecting consumers’ data.

This research takes into account the action of all the players. The game has multiple possible Nash equilibria that can be converted into pure strategy or mixed strategy under specific conditions. Our research finds that an increase in the frequency of attack and the provider able to mitigate the loss might cause the attacker to be detected and caught. Thus, the limited benefit generated by the attack may force the attacker to not attack because of the risk and penalties.

For future work, we plan to investigate and apply a game to come up with an optimal function for mapping the gain when the provider invests in security and the loss when the attacker succeeds in targeting the provider’s infrastructure and the users’ private data are compromised, this will clearly refine the payoff of each player.

CHAPTER 6

A GAME THEORETIC APPROACH ON RESOURCE ALLOCATION WITH COLLUDING NODES IN MANETS

Prevalent concerns with dynamic networks typically involve security. Especially with resource constraints in dynamic networks such as mobile ad-hoc networks (MANETs), security needs to be of particular consideration. In this chapter, we first analyze the solution concept involved in optimizing resource allocation and data packet forwarding. In a MANET, the availability of having data packets forwarded may be insubstantial due to the presence of selfish nodes. Nodes may not want to participate in the network to preserve their own resources. We propose a packet-forwarding problem with a negotiation game, where an arbitrator acts as a cluster head and initiates a bargaining game. Thereafter, we consider the possibility of having some group of nodes exhibit malicious behavior and collude to subvert the MANET. We investigate the problem by finding the optimal Nash Equilibrium (NE) strategies of the negotiation game. Then, we simulate the effect of the coalition of malicious nodes in a mobile environment. Simulation results support our model.

6.1 INTRODUCTION

There has been significant growth in research involving terminal mobility in dynamic networks. One category of such networks is a MANET. In a MANET, autonomous mobile devices are deployed across the area of a network. The device mobility, the absence of infrastructure, and wireless communication render the topology unstable.

Because of these characteristics, as well as resource limitations in energy such as battery life, mobile devices may face issues with connectivity and link reliability. This limited nature of resources in a MANET encourages some nodes to behave selfishly by attempting to preserve their own resources. As a result, the only way for data packets to move throughout the network is if these mobile devices rely on one another to transfer data. The reliability of the network depends on this level of cooperation. In order for data packets to be delivered from one node to another, nodes must have an incentive to be participative [49].

Existing literature provides methods on incentive mechanisms as ways to alleviate the effect of having selfish nodes in a MANET. We consider the novel implementation of an arbitrator in a MANET to initiate a bargaining game with players. The arbitrator will offer shares of its data storage as a way to optimize resource allocation in the network. These shares are fractions of the arbitrator's data storage and are randomly distributed to players. Players involved in the game will be allowed to accept or reject these offers from the arbitrator. A vote by simple majority will decide if data transfer will complete a negotiation session [31]. By the time a player is out of transmission range if the majority of players have not agreed on their resource allocation, the negotiation game ends. This implementation into the model will help maximize network reliability and increase the throughput in the MANETs. Researchers have also considered the presence of malicious behavior in dynamic networks [10] [22]. The lack of robust security measures can be considered a result of a MANET's limitation. Although many types of attacks exist, many of them focus on deteriorating the resources and services of the network. We consider a particular kind of malicious behavior in the model proposed in this chapter. In this model, a group of mobile devices can collude among itself to exploit the functionality of the arbitrator. Constant exposure to collusion will eventually degrade network reliability. This chapter investigates the bargaining game and how the proposed solution can be used to analyze the behavior of colluding nodes. There are researches in the field of mobile ad-hoc networks and some security concerns are perceivable. To improve the network reliability, Buttyan and Hubaux [50] proposed virtual currency as a way to stimulate participation in data packet forwarding. The authors proposed, each node earns certain amounts of *"nuglets"* that is used to transfer data. When a node requests to have data packets forwarded, the *"nuglet"* count decrements by one, and when a node forwards a data packet, the *"nuglet"* count increments by one. However, The solution concept, does not consider the scenario of not having enough currency to proceed with forwarding requests.

In [24], Liou *et al.* considered a bargaining game as a way of handling the access network selection. Possible access networks include wireless metropolitan access networks (WMANs), third generation/code division multiple access (3G/CDMA), and wireless local area networks (WLANs). The authors introduced a bargaining game between the participating device and the access network, such that the resource allocation of the network is negotiated between the two players after a call request is made. Although the game attempts to optimize resource allocations of the network, it requires that nodes are constituents of a network where devices may be mobile but the base station must remain static. Marti *et al*. [22] introduced a technique to improve throughput in ad hoc networks. The proposed technique is built on top of the Dynamic Source Routing (DSR) protocol. To alleviate routing misbehavior in particular, the technique involves categorizing nodes as either *watchdog* nodes or *pathrater* nodes. The *watchdog* node seeks to identify misbehaving nodes, while the *pathrater* node uses its information of misbehaving nodes to decide a better, more reliable route to take to proceed with data transfer. However, Implementing the technique, can lead to collision problems, false reports in behaviors, and collusion.

In [45], Niyato *et al.* addressed the problematic and dynamic issues of network access selection in heterogeneous networks by studying the application of evolutionary game theory. Users in the network compete for shares of bandwidth availability, where the following competition is modeled as an evolutionary game solvable by finding its evolutionary equilibrium. Two featured algorithms for network selection are scrutinized. The influence of the users competing for shares is noted in this study.

The mobility functionalities described in [41] are categorized as a mobile sink or mobile relay, which define methods either in collecting data or passing them on to the next mobile entity. These mobile nodes use their short radio transmission ranges to accumulate data efficiently. Furthermore, using parameters of a service-driven MANET as a foundation, Riordan and Grigoras [52] proposed the implementation of a data mule service appropriate for network needs. This data mule is typically highly mobile and is deployed in the area where it can be used to transmit data packets between the requester and the client. Boudec and Buchegger [64] proposed an extension of the routing protocol as the method for detecting and isolating misbehaving nodes. The proposed work essentially builds on the idea that nodes will learn from behavior by participating in “neighborhood watch” and sharing experiences concerning malicious behavior. After receiving warning information on some particular malicious nodes, a path manager will reconfigure which safe paths to take for data exchange. The method calls for improvements in the data link layer and employs the Dynamic Source Routing protocol.

In [41], Rossi *et al*. presented an intrusion detection system where collusion is considered in improving path reliability. In the intrusion detection system, the *pathrater* algorithm categorizes nodes into several different classes. Essentially, full participation in the network depends on the rating associated with class membership. Simulated results show that the system has improved tolerance for collusion among malicious nodes. However, The system, does not support statistical analysis based on optimal threshold values.

The remainder of this chapter is organized as follows. System models and motivations are surveyed in the Section 6.2, game-theoretic analysis is provided in Section 6.3, simulation environment and results are presented in Section 6.4, and conclusion and future works are articulated in Section 6.5.

6.2 MODELS AND MOTIVATIONS

This section introduces the system model under Problem Description and Network Model. Motivations behind this study are briefly provided in the final part.

6.2.1 Problem Description

Let the MANET have any number of nodes, *N*, from *1* to *N*, positioned throughout an area, such that the nodes can be rigidly placed or mounted onto some mobile object. By means of a MANET, nodes share characteristics of both a router and a broadcast access point. Meaning, a node can store and collect data packets, as well as connect to some other routing device [5]. As nodes of a MANET are usually limited in resources such as battery life and computational power, it is not favorable for nodes to forward data under requests other than their own. However, it is required for nodes to forward data packets in order to benefit the overall network. Establishing connections among nodes is therefore an expected challenge by the mobile and infrastructureless nature of a MANET [1]. To mitigate the adverse effects of having selfish nodes in the network, our proposed model requires an arbitrator to serve as a cluster head and negotiate shares of its own data-storing resource to allocate to those in need of data packet forwarding. This functionality of the arbitrator gives nodes incentive to participate in the network. The main concern with the current model is that it assumes that nodes will act independently when bargaining with the arbitrator. As a result, the possibility of malicious nodes colluding to deteriorate network reliability is considered here, which comes from the postulation that a group of nodes can coordinate together to bargain with the arbitrator.

6.2.2 Network Model

The MANET is considered as an area of locally deployed wireless devices (access points) based on IEEE 802.11 standards [24] [6]. The key features of the current model remain consistent in this model. Mobile objects are deployed throughout the area where they can represent cruisers, fire trucks, planes, etc. The access points distributed across the local area network will serve as data repositories for the accumulated data. Furthermore, the mobility of the nodes in a MANET is arbitrary, with the location of each node contained in three-dimensional space. Each node covers a dynamically sized area of the network over some random and freely determined speed and direction.

Variable-sized areas of coverage represent realistic expectations in a MANET. For example, suppose that devices are mounted on a helicopter and a police cruiser. Although both vehicles are free to move any which way, the helicopter may cover a broader area in comparison to the cruiser.

The waypoint model supports the mobility of these nodes. Waypoints are random vectors uniformly distributed across the specified area. The nodes move accordingly over time until they reach their waypoint. When a node reaches its waypoint, it may pause and reconfigure its waypoint parameters. Furthermore, we consider interactions between regular nodes and any one arbitrator. A regular node will normally request its need for data packets to be forwarded across the network, and the request will then be broadcasted to the node's neighbors for help. With enough requests from a group of regular nodes, an arbitrator will offer its service and resources, provided it has enough resources of its own to sustain its service [66] [62] [65].

6.2.3 Motivations

Current research on the topic of MANETs may only consider the event of rational and selfish nodes existing in the network. In which case, the resource allocation problem is directly addressed. This is easily supported since nodes in a MANET are characteristically constrained and limited by battery life, computational power, etc. However, it is for these same reasons that MANETs are also not secure. For example, limited computational power can limit a mobile device by making cryptographic procedures impossible or simply impractical if by having these security features drains the battery of the device as well [49].

We first consider the case when a regular node requests packets to be transferred. The node runs the routing algorithm to find the shortest path required to transfer data, then follows typical procedures of incentive or reward programs in order for other nodes to cooperate with the request. Setting arbitrators as data mules [52] and having them with a wider transmission range allow such nodes to be beneficiaries of the arbitrator's services. The arbitrator's data-carrying capability and broader range should reduce the number of hops required to pass data packets from a source to a destination. As requests to have data packets transferred accumulate, the arbitrator will have to consider more allocations of its resources. It will implement the round robin algorithm and the handshaking procedure of the carrier sense multiple access with collision avoidance (CSMA/CA) to relieve communication density and to address the hidden node problem. We also consider the opportunity a node has to collude and bring malicious intent to the network. Malicious nodes will try to use all the resources, of the participating nodes in a network such as battery life, that its reliability is eventually compromised. As mentioned before, many security threats exist in a MANET due to the very nature of its design as a network. Such threats include, but are not limited to blackhole attacks, denial-of-service attacks, routing loop attacks, and Sybil attacks [28].

In this framework, malicious nodes may cooperate to compromise the functionality of the arbitrator. Since the model requires that the arbitrator initiate a bargaining game with players making requests to have packets forwarded to the destination, and the success of the game depends on the majority vote of all players, a particular group of players may collude to upset the vote. Subverting the voting mechanism across all games in the MANET causes the deterioration of network reliability. In addition to this, prolonging any given bargaining game by evasion of a successful vote wastes the power and battery life of the arbitrator, thus exhausting its purpose.

6.3 GAME THEORETIC ANALYSIS

The following summarizes the method for optimizing resource allocations between an arbitrator and a regular node [49].

6.3.1 Negotiation Model

Let there be a set of nodes in the network such that $N = \{1,2,\ldots,n\}$ represents the set of players eligible for negotiation. Note that the arbitrator is independent of this defined set of players. The unique feature of the arbitrator lies in its data storage capability and its wider transmission range. The arbitrator's data storage capability also characterizes it as a data mule [52]. When nodes make requests to have data packets forwarded, the arbitrator will receive the requests and initiate a bargaining session. The length of time of the bargaining session will depend on the positions of the nodes involved and how long it will take for the first player to move out of range of the arbitrator. As soon as any player leaves the arbitrator's transmission range, negotiation will cease to continue.

After requests are made, the full length of time before the first player exits the arbitrator's transmission range is calculated, and the number of cycles, or shots, of negotiations are estimated. In each cycle, the arbitrator will offer shares of its resources to each player, so that the size of each share are randomly determined. This arbitrary manner of allocation eliminates the possibility of any kind of bias or partiality in forwarding data.

After the arbitrator offers resource shares in the first shot, each player in the game will have the opportunity to accept or reject the offer. If the simple majority, defined as being more than half of players in the current shot accepts their offered shares of resources, data transfer will occur. Otherwise, if the majority rejects the offer, the session will proceed to the next shot or cycle. At the very last shot, equal shares of the resource will be offered, and if the majority decides to reject the offers at the final shot, data transfer will not occur during the session.

6.3.2 Random Distribution and Optimal Strategies

The random assignment of share sizes is represented by the Dirichlet distribution, which is essentially the set of probability distributions specified by some vector *k*. The sum of all outcomes of the distribution is equal to *1*, such that the sum is proportional to the entire size of the arbitrator's data storage.

The distribution takes observations of *n* possible outcomes with positive real parameters x_i, *i=1,…,n,* and the probability density function (*pmf*) of the Dirichlet distribution (Dir) for variable vector $x_i = (x_1, x_2, \ldots, x_n)$ with the parameter vector $(k_1, \ldots, k_n)$ is given as

$$Dir(x;k) = \frac{1}{B(k)} \prod_{i=1}^{n} x_i^{k_i - 1}, x_i \geq 0, \sum_{i=1}^{n} x_i = 1, k_i \geq 1. \tag{6.1}$$

such that *B(k)* in the formula

$$B(k) = B(k_1, \ldots, k_n) = \frac{\prod_{i=1}^{n} \Gamma(k_i)}{\Gamma(k_1 + \ldots + k_n)}, \tag{6.2}$$

is dependent on parameters *($k_1, \ldots, k_n$)*, where they serve for modifying the weights of the distribution. The density is asymmetric if *k* is not a constant vector. The operation *Γ* represents the Gamma function.

Consider the negotiation game between the simple case of three players, and in a given negotiation cycle, random offers from vector *(x_1^k, x_2^k, x_3^k)* are generated using the Dirichlet distribution. Suppose U_k denotes the value of the negotiation game with *k* shots remaining and $o(x_i)$, $i = 1, 2, 3$, represent the probability that player *i* accepts the offer x_i. Finally, let $\bar{o}(x) = 1 - o(x)$. We analyze the following.

Theorem 1: The optimal strategies of players at shot *k* possess the form

$$o_i(x_i) = \mathrm{I}_{\{x_i \geq \delta U_{k-1}\}}, i = 1,2,3. \tag{6.3}$$

The utility value of the game for player *i* satisfies the formula

$$U_k = \frac{1}{3} - 2\delta^2 U_{k-1}^2 + 6\delta^3 U_{k-1}^3 \tag{6.4}$$

Proof: The proof of this theorem derives the proof theorem 5.2 in chapter 5

When *δ = 1*, which represents the case of no discounting, and the horizon of negotiations is infinite, we come to the conclusion that $\lim_{k\to\infty} U_k = ⅓$, and players should accept the resource shares that the arbitrator offers.

6.3.3 Threat Model

Malicious nodes colluding to subvert the network are typically characterized by any instance of intentionally wasting the resources and reliability of the network. In this model with arbitration, colluding nodes are considered as those that request significantly larger shares of resource allocation. By consistently requesting significantly larger shares, the colluding nodes are seeking to exploit the arbitrator's data carrying capability. As a result, and as previously mentioned, since data transfers are administered by simple majority votes, colluding nodes may also manipulate any given negotiation session by consistently rejecting their offers over the specified number of cycles.

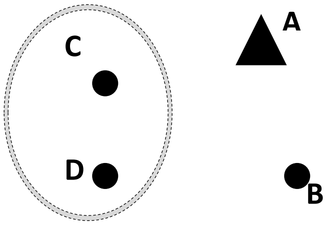


Figure 6.1: A simplification of colluding nodes interacting with both an arbitrator and a regular node in a bargaining session

In Figure 1, let *A* represent the arbitrator holding a bargaining session with nodes *B*, *C*, and *D*. Node *B* is a regular node that is selfish and behaves rationally. Nodes *C* and *D* are colluding to deteriorate the services of the network. Let node *B* bear a minimum payload of *¼* the storage of the arbitrator, *A*, and let nodes *B* and *C* bear minimum payloads of *½* each. If for example the calculated number of cycles in a bargaining session is *3*, then for each cycle, the majority vote to accept offers will never pass throughout the session, even at the final shot when equal allocations are offered.

6.3.4 System Modifications and Nash Equilibria

The negotiation model investigated in this chapter will maintain its key components, such as requests to forward data, responses to such requests, randomly generated offers, and majority-vote decisions. However, in this proposed investigation, instead of having equal allocations offered at the final shot of the negotiation session, we will consider offering equal allocations at the initial shot of the session.

We consider this conjecture as we acknowledge the simulation results in [49], which shows that successful negotiation sessions typically follow from having minimum payloads per player below *1/n*, where *n* is the set of all players involved in a given session. Also note that any involved strategy profile in which an arbitrator randomly generates offers is a Nash equilibrium. Resource allocations are optimized and rational players are anticipated to accept the offer.

6.4 SIMULATION ENVIRONMENT

6.4.1 Design Description

Although a MANET realistically exists in the third dimension, the proposed system model will be analyzed in two-dimension. Furthermore, the total area of coverage is simulated in a *100m x 100m* region and there are sub-areas defined for arbitrators. A selected arbitrator has an assigned sub-area of coverage. A single arbitrator is randomly situated in a sub-area and continues its movement within the perimeter of the sub-area throughout simulation time. The arbitrator also serves as the cluster head of mobile nodes contained in the same sub-area, when the node requests arbitrator's service.

The model also includes a predetermined amount of nodes colluding to subvert the network, with the minimum number of colluding nodes being *2*. Colluding nodes are placed at one hop distance away from each other. Regular nodes are then distributed randomly to all sub-areas. For purposes of illustration and analyzing the effects of collusion, the exemplary design will have 4 arbitrators, 3 colluding members, and 7 regular nodes deployed across the area. Arbitrators will primarily have a transmission range of *71m*, while regular nodes will primarily have the transmission range of *40m*.

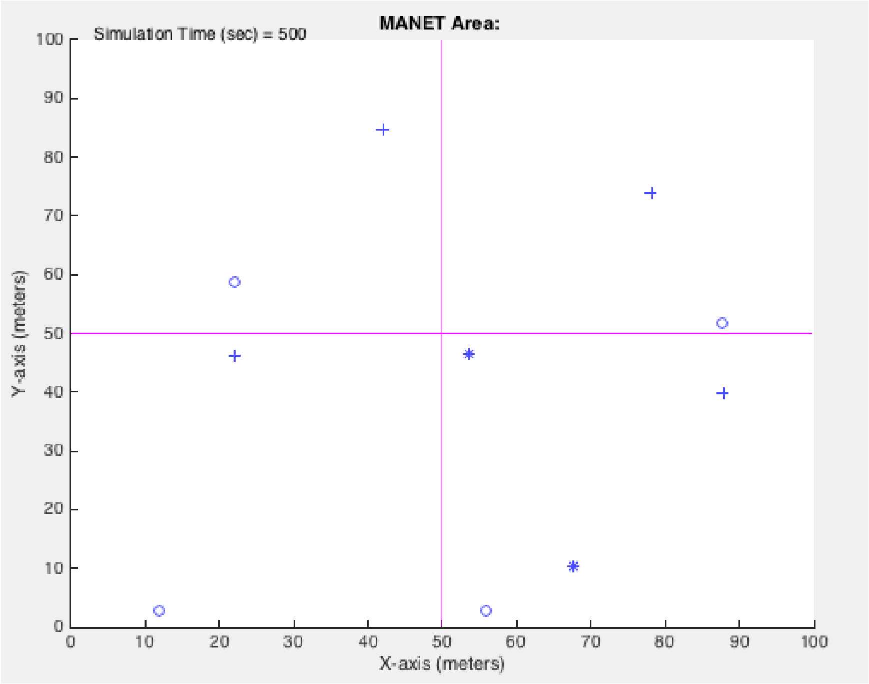


Figure 6.2: A screenshot of 10 mobile nodes, comprised of two colluding nodes and one arbitrator and one regular node in each subarea

Figure 6.2 illustrates a simplest scenario of the network model. Note that the Random Waypoint model dictates the mobility of each node [66]. The endpoint of any single node's path is uniformly distributed across the area, and the node travels on the path by some random velocity. Reaching an endpoint, the node may pause before continuing on to another waypoint. Table 6.1 summarizes the critical features of the simulated model.

Parameter	***Parameter Values***
Simulation Time	*500 sec*
Routing Protocol	*AODV*
Total Number of Nodes	*15, 20, 30*
Number of Arbitrators	*4*
Initial Node Position	*Randomly Distributed*
Mobility Model	*Random Waypoint*
Simulation Area	*100m x 100m*
Channel Type	*Wireless*
Node Speed Interval	*0.2m/s – 2.6m/s*
Traffic Type	*Constant Bitrate*
Time Step	*0.1 sec*

Table 6.1: Simulation Details

The resource sharing functionality of the arbitrator is randomly assigned via a random generator distribution. An arbitrator will carry a unit of data storage that can be allocated to each node requesting to have a data-packet forwarded. A node, for example, may request at least *1/3* of the storage, and this share is also the node's minimum payload. In this model design, the arbitrator's data storage is determined to contain *10,000* units (i.e. *10,000* bytes), and any negotiated share will be a portion of that total value.

When nodes request to have their data forwarded, the arbitrator initiates a bargaining session. Note that requests from various source nodes to forward data packets will be made to the same destination node. In order for a node situated in one subarea to forward data packets to another node situated in a different subarea, it is expected that requests will be made through two arbitrators. With this in mind, the assumption is made that if an arbitrator requests to have data packets forwarded to another arbitrator, the first arbitrator will not participate in the bargaining session prescribed by the second arbitrator.

6.4.2 Simulation Results

In order to analyze the effect of the bargaining game on collusion, a selection of values must from table 6.1 are assigned to the parameters.

We first investigate various ranges of minimum payloads. Figure *6.3* and Figure *6.4* provide the percentages of successful negotiation sessions over simulation time. Following Figure *6.3*, regular, non-colluding nodes are randomly set to have minimum payloads between *1667-3334* bytes, while colluding nodes will have minimum payloads between *4000-5000* bytes. These values are fractions of the total assigned storage space of *10000* bytes. Since colluding nodes are requesting significantly larger shares of storage, we expect nearly all voting procedures to upset occurring bargaining games. Figure 6.3 exhibits relatively consistent percentages of successful votes over simulation time. By the end of the *500s*, negotiation games are about 76% successful without collusion, while negotiation games are 37.1% successful with collusion.

Figure 6.4 illustrates a similar conclusion with the exception of colluding nodes having payloads within *3500-4000* bytes. In the first *100s* of negotiations, we exhibit sporadic instances of successful votes, as well as network performance reaching its peak with collusion in the network, showing that negotiation games may still be notably successful even with the presence of colluding nodes.

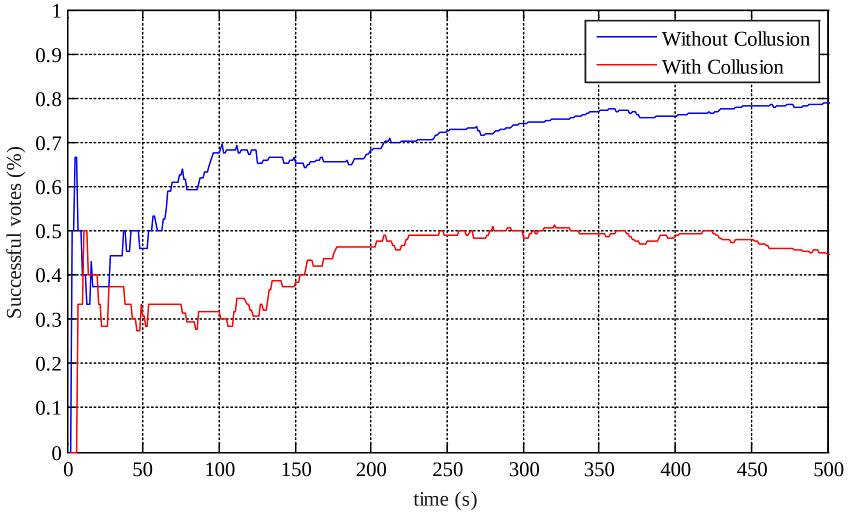


Figure 6.3: Percentage of successful negotiation sessions with minimum payload between 1667-3334 bytes

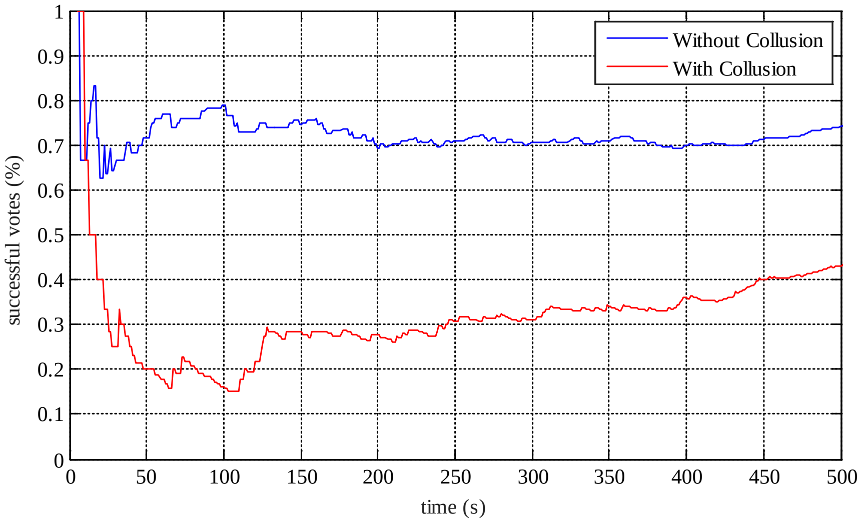


Figure 6.4: Percentage of successful negotiation sessions with minimum payload between 3500-4000 bytes

We then investigate the impact of having various ranges of velocities the nodes will have to adopt and how they relate to percentages of successful votes. Test cases of speed are the following: 0*.2-1.0 m/s*, *2.0-3.2 m/s*, *5.0-6.2 m/s*, *8.1-10.2 m/s*, *12.1-13.2 m/s*, and *14.1-15.2 m/s*. Although values are sporadic and inconsistent depending on the range of speeds, negotiation games are generally more successful when either regular nodes and colluding nodes have relatively lower mobility (low speed). Evaluating the plots in figure 5, we notice that when the minimum payloads of colluding nodes are within *4000-5000* units, the percentage of successful games more consistently deteriorates as speed ranges increase. This confirms the expectation that network reliability is compromised with higher minimum payloads and increased of speeds. Aside from this observation, we also note that different speeds have drastically affected the performance and outcomes of negotiation sessions. Moreover, nodes may want to reach a bargaining success, but the high mobility of each node may cause the communication to break because the transmission is out of range.

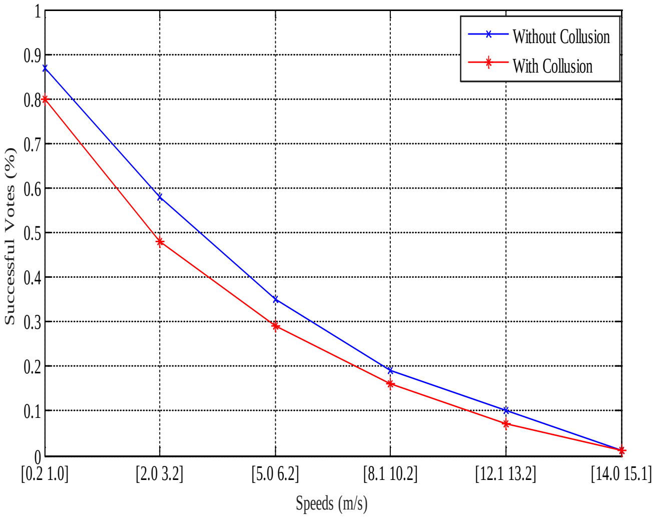


Figure 6.5: Successful negotiation over speed variations

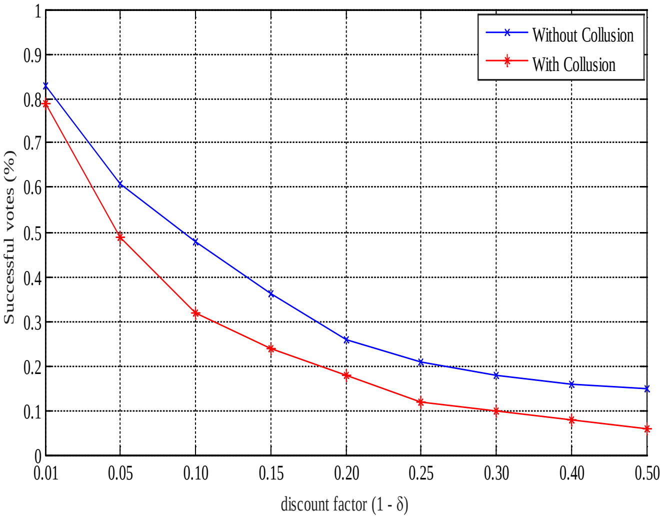


Figure 6.6. Successful negotiation over discount factors

In Figure 6.6, the relationship between successful negotiation sessions and various discount factors is investigated. Test cases of the respective delta values are the following: *0.01*, *0.05*, *0.10*, *0.15*, *0.20*, *0.25*, *0.30*, *0.40*, and *0.50*. Discount factors affect the size of resource allocations made in a successful negotiation session. Because big discounts take away a fraction of the resources over a horizon of negotiation cycles, network reliability and success rate of negotiations should deteriorate. Figure 6.6 also illustrates the case when colluding nodes have minimum payloads within *3500-4000* units. The study shows that further discounting on top of collusion present in the network significantly worsens network performance. Results also show that when delta is set at 0.05, the lowest delta value applied and tested, the network still performs uncharacteristically and relatively well even with collusion. The network performance is better when the network contains colluding nodes than when the network does not contain colluding nodes. For that matter, the network can tolerate having colluded nodes, but it is obvious that successful negotiation decreases rapidly.

6.5 Conclusion and Future Work

This chapter models the problem of colluding mobile nodes in a heterogeneous mobile ad-hoc network of N nodes using bargaining game theoretic concept as an incentive to share resources on-the-fly and where the nodes negotiate with an arbitrator on the sharing rule of consent. We investigate the perfect equilibrium strategies of this bargaining game, by observing how each player maximized his throughput against the colluded nodes. Simulated results show that the bargaining game and its effect of optimizing resource allocations can be utilized to reveal the presence of malicious nodes colluding to subvert the network. Since such colluding nodes will tend to request larger shares of the arbitrator's resource and data carrying capability, they will consequently reject offers involved in playing optimal Nash equilibrium strategies. Simulated results also show that the loss of network reliability is a direct result of the malicious behavior of colluding nodes. Furthermore, through simulation, we investigate the impact of discount factor (δ) on mobility, fairness and patient during a bargaining session, and we can argue that $\delta \to 1$ is a negligible value in our problem. Broadcasting the identity of colluding nodes by the arbitrator and their constant rejection of any offers may expose their presence in the network and dismantle the collusion. Therefore, improving security and the quality of the network.

6.6 ACKNOWLEDGMENTS

We would like to acknowledge the National Science Foundation (NSF) and the Department of Defense (DoD) for their support.

CHAPTER 7

CYBER SECURITY RESOURCE ALLOCATION: A MARKOV DECISION PROCESS APPROACH

An effective defense-in-depth in cyber security applies multiple layers of defense throughout a system. The goal is to defend a system against cyber-attack using several independent methods. Therefore, a cyber-attack that is able to penetrate one layer of defense may be unsuccessful in other layers. Common layers of cyber defense include: attack avoidance, prevention, detection, survivability and recovery. It follows that in security-conscious organizations, the cyber security investment portfolio is divided into different layers of defense. For instance, a two-way division is agility and recovery. Cyber agility pursues attack avoidance techniques such that cyber-attacks are rendered as ineffective; whereas, cyber recovery seeks to fight-through successful attacks. We show that even when the primary focus is on the agility of a system, recovery should be an essential point during implementation because the frequency of attacks will degrade the system and a quick and fast recovery is necessary. However, there is not yet an optimal mechanism to allocate limited cyber security resources into the different layers. We propose an approach using the Markov Decision Process (MDP) framework for resource allocation between the two end layers: agility and recovery.

7.1 INTRODUCTION

The goal of cyber agility is to reduce attacks by making it harder for a determined adversary to succeed. This is achieved by preventing adversaries from planning their attacks over time by relying on the static nature of the networks, and launching their attacks at the times and places of their choosing. Cyber agility employs proactive and adaptive defense techniques that include randomization, diversity and obfuscation, to increase the levels of complexity and uncertainty in a system and disrupt adversary attack planning and execution.

However, if a system administrator fully invests his cyber security resources to develop the most robust and agile systems against cyber-attack, there is no guarantee that the system will be able to avoid all attacks. In fact, it is not always possible for a system administrator to anticipate all component failures or intelligent attacks perpetrated against its modules. Attempts to predict and protect against every conceivable failure and attack become cumbersome and costly. Additionally, novel, well-orchestrated, malicious attacks can cause damages that are far beyond the abilities of most system developers to anticipate.

Regardless of how well a system is designed and secured or how well they can circumvent vulnerabilities and attacks, it will eventually show some unseen vulnerabilities, which are exploitable by attackers. Therefore, a mission-critical system implemented and placed in cyberspace should have the resources to recover from a degraded state and still carry out at least the mission essential functions (MEFs).

Cyber resilience comprises the ability to withstand, minimize, survive, and recover from the negative effects of adversity, whether man-made or natural, under all circumstances of use. Resilient systems must not only provide the continuation of Mission Essential Functions in the face of disruption by a sophisticated adversary or a non-malicious fault, but also fight through successful attacks to regain or even exceed their initial operational capability. Cyber resilience invests in recovery solutions that increase the probability of assuring MEFs during and after a successful cyber-attack.

Resource allocation in a network system between avoidance and recovery is most pressing for mission-critical systems. One of the challenges faced by any system administrator is to provide equal and adequate systems security preparedness for both threat avoidance and recovery from threats. This work proposes a mechanism to optimally allocate limited cyber security resources into different layers of cyber defense. The main contribution of this research work is to find the optimal allocations of cyber security resources during the development and deployment of mission critical system using the Markov Decision Process (MDP).

In the literature, there are some studies related to optimal resource allocations. The use of the MDP to address network security challenges has increased. The reason is that the MDP modeling supports a broad understanding of attacks and interactions in cyberspace.

Arshad *et al.* [83] presented a semi-Markov decision based fair buffer allocation policy for sensor nodes and vehicular network. The proposed model gives nodes a fair chance to transmit its data. There is a tradeoff between energy efficiency and fairness at the relay node. Also, there is an increase in the number of nodes competing for buffer also results in an increased fair buffer allocation, but the authors did not mention or discuss the proportion of resources needed.

Game theory is proposed in [73] as a modeling tool and computing for the probabilities of the expected behavior of the attackers in a quantitative stochastic model of security.

The stochastic model presented by the author analyzes a security breach as a series of intentional state changes. Assumptions are made for the possible rewards of a player in the game, allowing the calculation of the Mean Time to First Security Breach (MTFSB) for the system. The benefit of using the game theoretic approach is twofold: first, provide a more accurate model of the attackers' behavior, which can be used to assign more realistic transition probabilities in the models, and second, help the defender of the system to find optimal defense strategies and facilitate the calculation of the expected loss associated with different strategies.

In [25], the problem of sharing a resource with a time-varying capacityis presented. The objective of minimizing the mean-delay was investigated. The resource allocation is formulated as a MDP. Even though, the problem is not solvable analytically in its generality, an approximation of the solution is obtained. The authors in [63] proposed an On-line Social Network (OSN) service, an approach for helping OSN users determine their optimum levels of information sharing based on the Markov decision process while taking into consideration the payoffs (potential Reward or Cost). In [63], a decision algorithm was proposed for vertical handoff in heterogeneous wireless networks. The algorithm is based on an MDP formulation with objectives to maximize the expected reward of a connection. A stationary deterministic policy is obtained when the connection termination time is geometrically distributed.

The authors in [69] addressed some issues to initiate path optimization for a two-phase handoff protocol. The use of link cost function is to reflect the network resources utilized by a connection. The optimal policy performance has been compared with four heuristics.

The proposed model captured the tradeoff between network resources used and the handoff processing and signaling load incurred in the network. There is a drawback in the formulation when it comes to traffic distribution between voice and multimedia applications.

Ayesta *et al*. [68] investigated the problem of sharing resources of a single server with time-varying capacity. The main objective of the investigation is to minimize the mean delay. Nevertheless, the problem does not have an analytical solution. The motivation in this case is to seek an approximate solution. Two examples are provided for illustration: the extension of multi-armed bandits to develop a heuristic solution of index type and the Gittins index rule known to be optimal under the assumption of constant capacity.

Chunlei *et al*. in [75] proposed a network of threat evolution model based on network threat evolutionary behaviors, network threat propagations and also investigated the influence of network threats over network survivability. By abstracting network survivability as a dynamic game process among attacker, defender and normal users, the proposed network survivability analysis is experimented in a typical network environment.

7.1.1 Background

Computer network systems are always targets of cyber attackers. Network systems deployed online should be capable of sustaining the adversity of cyber-attacks coupled with component deterioration by integrating agility and recovery component.

Agility: In cybersecurity, agility is a system that has the property to remain operational and deliver desired and acceptable results by auto-circumventing or bypassing some vulnerability or issue that surged. For example, the implementation by the system administrator of an IP-Hopping, (a moving target defense system), will use available network data and hopping algorithms to allow a constant IP addresses to randomly change on both source and destination IP addresses [84]. The use of "hopping" IP addresses will severely diminish an attacker's ability to breach a target within a network because of the increased uncertainty of identifying the IP address of a port. Each time the attacker scans the network, he gets a different IP address. Therefore, it is difficult to locate an access point [70].

Recovery: The recovery component of a system is the ability for a system that has suffered from an attack to regain its initial operating capability as soon as possible [62]. The implementation of recovery components and procedures in a system facilitates the switch back to a running state in a timely manner [72]. Survivability is the aptitude for a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents. As example, the database system of a financial institution may suffer unrecoverable loss from cyber-attacks. With the implementation of a disaster recovery mechanism, there is less data lost and quick turnaround. The database (data and logs) can be fragmented and installed on multiple hard drives with backups equipped in each hard drive. The backup is done in two steps; there can be a daily full backup and an hourly differential-backup. On a system’s breach from attack, one of the production node’s servers and database are down. When the server node is brought back on, the data recovery procedure is fast by doing a data rebuild from the backups. The database system is prepared for restoration, so that it may be ready to move on the production environment. Resource allocation is one of the important challenges in cyber security, especially when the systems have some Service Level Agreements (SLAs). In the cyber world, the main functionalities of the system need to be active and running. However, mission-critical systems are usually constrained during design and implementation to have agility properties integrated. Specifically, the administrator mostly allocates the investment on the agility design and implementation. Therefore, it may not be to the system lifetime's best interest to have investment focus only on agility. However, refusal to allocate the investment's portion on recovery will severely hinder the mission-critical system's lifetime and impair the system's own performance. Hence, it is necessary to highly consider investment on recovery for any system deployed in the cyber world and where different interactions from different players change the states of the system.

The rest of the chapter is organized as follows. The next section describes the model formulation. In section 7.2, we describe the problem. We formulate the problem as a Markov chain in section 7.3. The Markov decision process is analyzed in section 7.4. Numerical results are in section 7.5, and the conclusion of the chapter sums up the main contributions, as well as future work.

7.2 MODEL FORMULATION

We consider that a system can be in one of the two states: state *1*, when it's up and running and state *0*, which is off, degraded or non-functional. Actions based on malicious or normal behavior can cause the system to switch from state *1* to state *0* with a certain probability. The system in state *1* integrates defense layers, such as agility, avoidance and prevention to stay in state *1*. A successful attack or a component failure can change the state of the system from state *1* to state *0*. The system in state *0* needs a good recovery mechanism to come back to state *1*, otherwise it stays and remains in state *0*.

The two-state system is represented as a Markov chain, as illustrated in Figure *7.1*.

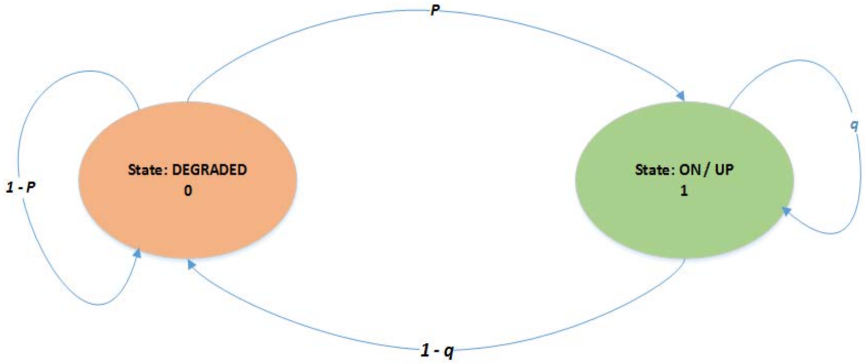


Figure 7.1: Two-state Markov chain

Figure 7.1 shows a state diagram with transition probabilities, as defined:

P_{00} = *1 – p*: is the probability that the system stays in state *0*.

P_{01} = *p*: is the probability that the system switches from state 0 to state *1*.

P_{11} = *q*: the probability that the system remains in state *1*.

P_{10} = *1* - *q*: the probability that the system switches from state *1* to state *0*

We have a state transition matrix defined as follows:

$$P = \begin{bmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{bmatrix} = \begin{bmatrix} 1 - p & p \\ 1 - q & q \end{bmatrix} \qquad (7.1)$$

We can observe that an increased investment in cyber agility will increase the probability *q,* whereas an increased investment in cyber recovery will increase the probability *p*.

7.2.1 Operational Scenario with a Two-state Markov Chain

We have a state transition matrix defined in equation (7.1) [63]. In order to explain our approach, we assume that an attacker tries to compromise the system by changing it to a degraded state (state *0*) [83]. Meanwhile, the defense team (system administrator) has two objectives:

1. Make a successful attack difficult to reach its objective (increase q) and the system to remain in state *1* i.e., cyber agility.

2. Provide a solution to recover from potential failure (state *0*) and quickly switch the system to state *1* which is the functional state, i.e., cyber recovery.

We consider that a defender, who allocates security resources between agility and recovery, maximizes the long-term fraction of time during which the system is in state *1*. Using the transition probability q *(*respectively p*)*, the steady-state probabilities indicate the long-term fraction of time during which the system is in state *1* (respectively, switches from state *0* to state *1)*. Given that the system is in state *1* at time *0*, there is a need to know the probability that the system remains UP (state 1) at the time when n is very large.

The eigenvalues of matrix P are $\lambda_1 = 1$ and $\lambda_2 = q - p$. Since p and q are probability values, $|\lambda_2| \leq 1$. P can be expressed in a diagonal form.

$$P = S^{-1}DS$$

$$= \begin{bmatrix} 1 & \frac{-p}{1+p-q} \\ 1 & \frac{q}{1+p-q} \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \begin{bmatrix} \frac{1-q}{1+p-q} & \frac{p}{1+p-q} \\ -1 & 1 \end{bmatrix} \qquad (7.2)$$

where D is a diagonal matrix, S is the matrix of eigenvectors and S^{-1} is its inverted.

The value s_i, the i^{th} row S, is the left eigenvector of matrix of transition P corresponding to λ_i meaning $S_i P = \lambda_i S_i$ a verified *2*-step transition matrix is

$$P^n = \begin{bmatrix} P_{00}(n) & P_{01}(n) \\ P_{10}(n) & P_{11}(n) \end{bmatrix} = S^{-1} D^n S$$

$$= \begin{bmatrix} 1 & \frac{-p}{1+p-q} \\ 1 & \frac{q}{1+p-q} \end{bmatrix} \begin{bmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{bmatrix} \begin{bmatrix} \frac{1-q}{1+p-q} & \frac{p}{1+p-q} \\ -1 & 1 \end{bmatrix} \qquad (7.3)$$

While extracting the common factor, we have

$$P^n = \frac{\lambda_1^n}{1+p-q} \begin{bmatrix} 1-q & p \\ 1-q & p \end{bmatrix} + \frac{\lambda_2^n}{1+p-q} \begin{bmatrix} p & -p \\ -1+q & 1-q \end{bmatrix} \qquad (7.4)$$

with $\lambda_1 = 1; \lambda_2 = q - p.$

Let us examine the state probability vector *p(n)* as *n* becomes very large.

The vector $\pi = [\,\pi_0 \;\; \pi_1]' = \lim_{n\to\infty} p(n)$

The initial state is state *1*, the state probability at time *n*

$$\lim_{n\to\infty} \pi_1 = \frac{p}{1+p-q} + \lambda_2^n \frac{-p_0 p + p_1(1-q)}{1+p-q} = \frac{p}{1+p-q} \qquad (7.5)$$

With $\lambda_2 = q - p < 1.$

This chain converges to the stationary distribution regardless of where it begins. The vector $\pi = [\pi_0 \; \pi_1]$ is called the equilibrium distribution of the chain.

7.2.2 Tradeoff: Agility vs Recovery

We assume that $P_{10} > 0$ or $0<q<1$. The system administrator cannot guarantee at *100%* that the system will not change from state *1* to state *0*. The limiting state probability is a function with two variables p and q. Since both variables are probabilities, we need to understand the behavior of both variables along their axes. The partial derivative of π_1 (7.6) according to p-axis shows an increase with p:

$$\frac{\partial\pi_1}{\partial p} = \frac{1(1+p-q)-p(1)}{(1+p-q)^2} = \frac{1-q}{(1+p-q)^2} > 0 \tag{7.6}$$

The partial derivative of π_1 according to variable q shows the increase on the q-axis. We need to find out which of the two variable p or q will make π_1 increase faster.

$$\frac{\partial\pi_1}{\partial q} = \frac{-p(-1)}{(1+p-q)^2} = \frac{p}{(1+p-q)^2} > 0 \tag{7.7}$$

And

$$\frac{\partial\pi_1}{\partial p} - \frac{\partial\pi_1}{\partial q} = \frac{1-q-p}{(1+p-q)^2} \tag{7.8}$$

The differential of equations (7.7) and both probabilities p, q produces equation (7.8) which shows that the variable that increase faster depend on the sign of *1 - q - p*. If the goal of the system administrator is to maximize the long-term fraction of time during which the system is UP (in state *1*), then security investments need to be made in order to increase the variable p or q that makes $\pi_1$increase faster. Equation (*7.8)* shows that:

$$\begin{cases} If\ q < 1-p \implies \\ Investment\ in\ Recovery\ to\ increase\ probability\ p \\ If\ q \geq 1-p \implies \\ Investmet\ in\ Agility\ to\ increase\ probability\ q \end{cases} \tag{7.9}$$

7.2.3 Security Functions

Let us consider that $q = 0$ (respectively $p = 0$) if no investment is made in agility (respectively in recovery). We also consider that $q < 1$ (respectively $p < 1$) in case a huge investment is made in agility (respectively in recovery). We consider two *security functions*: the *agility function* and the *recovery function*. The *agility function* (respectively *recovery function*) take as input the amount of dollar x invested in agility (respectively recovery) and return as output the probability q (p respectively). We make two reasonable assumptions: 1) every dollar spent on agility (respectively recovery) increases probability q (respectively p) and 2) As the total amount spent on agility (respectively recovery) increases, the marginal rate of increase in probability q (respectively p) decreases [83] [84]. With these considerations, the probabilities q and p can be represented by: $q = 1 - e^{-\beta x}$ and $p = 1 - \ e^{-\alpha x}$. The parameters α and β represent scaling factors for the function p and q, respectively.

7.2.4 Resource Allocation Scheme and Illustration

Equation (7.9) shows that the optimum investment in agility or recovery is governed by the relative value of q and $(1 – p)$. Figure 7.2 shows the probability q and $(1 - p)$ as a function of investment. For this illustration, we have chosen $\beta = 0.75$ and three different values for α, $\alpha = 0.5, 0.75, 1.5$. the probability q is an increasing function of the investment. The probability p also increases with the investment. However, the function $(1 - p)$ decreases with the investment. Each function $(1 - p)$ crosses the function q in a single point of coordinate (x^*, q^*). We can see from Figure 7.2 and Equation (7.9) that:

1) If $x < x^* \rightarrow q < 1 - p$, then all investment must be in recovery

2) If $x \geq x^* \rightarrow q \geq 1 - p$, then x^* must be invested in agility and the remainder of $(x - x^*)$ invested in recovery.

For instance, with $\alpha = 0.5$ and $\beta = 0.75$, the graph of the probability q and $(1 - p)$ intersects at $x^* = 1.12$, which means, in a mission-critical system, if the available investment is less than *1.12,* it will be best to invest in recovery. In cases where resources to be allocated are greater than *1.12* then the difference is to be allocated to agility. When $\alpha = 1.5$ and $\beta = 0.75$, then $x^* = 0.66$. In fact, x^* decreases with α while it increases with β.

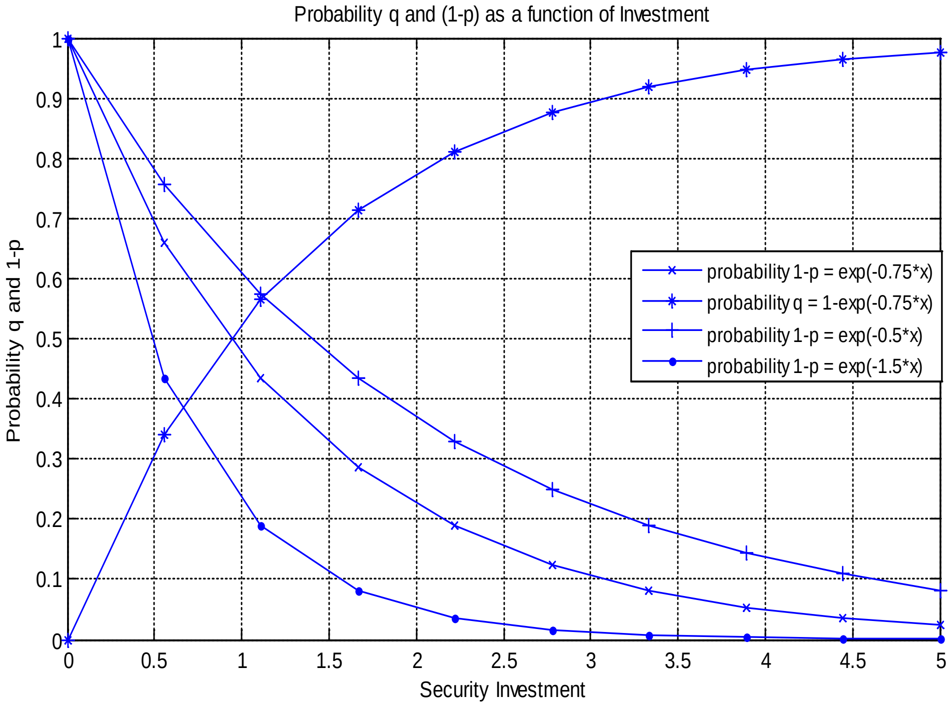


Figure 7.2: Probability *q* and (*1-p*) as a function of Investment.

7.3 THE MDP MODEL FOR RESOURCE ALLOCATION

Resource allocation is important in cyber security, especially when the need of SLAs will help assist any system to remain functional in cyberspace. The previous sections did allow us to use the security investment functions in the presence of a two-state Markov chain to modify the values of probabilities p and q. Moreover, with a transition probability attaches to every state transition, there is an intervention or interaction to trigger the change of states. The system administrator main objective is to keep the system in active state which means there is a reward when the system is up and a cost attached due to attack when the system is down.

According to the above, we are in the presence of a two-state system. The system changes state because of an attack perpetrated, the attack may be man-made or natural. A critical system implemented to run with most of the agility's component in a cyber environment should explore the possibility of making a decision when the system in a degraded state is given. Decision-making is only related to the system's current state; it is irrelevant to the previous actions and state. The MDP model can be described as follows:

7.3.1 State Space

The state space S is a finite set of states, $S = \{S_0, S_1\}$ as in Figure 7.1. |S| denotes the total number of states in the system.

7.3.2 Action Space

A finite and non-empty set of available actions $A(S_i) = \{a_k\}_{k=1,\ldots,|A(Si)|}$ associated to each state $s_i \in S$. Actions associated to a state either move the system to a different state or remain on the same state (loop). For example, $A_0 = \{a_{00}, a_{01}\}$ are the actions available in state S_0; action a_{00} makes the system remains on state S_0, and action a_{01} takes the system from state S_0 to state S_1.

7.3.3 Transition Probability

Given the time t, an action $a \epsilon A(s)$ selected in state S can transfer the system into a new state S' following a transition probability $P_a(s, s')$. The transition matrix probability is defined as in equation (7.1).

7.3.4 Reward

Given the decision-making epoch t, the selection of an action $a \epsilon A(s)$ in state S can generate a real-valued one-step reward function. $R_a(s, s')$ is the immediate reward incurred by the system as it is in state s, the action a is chosen and s' is the next time state.

7.3.5 Discount Factor

The discount factor $\delta \in [0, 1]$ describes the value of the future payoff as compared to the current payoff. Through the MDP-based approach, the main goal of a decision maker is to find an optimal policy, π*(s). The optimal policy prescribes the best possible action at any time t that the decision maker is in state s. The optimal policy π*(s) maximizes the δ-discounted average reward:

$$(1-\delta)\sum_{t=0}^{\infty}\delta^{t}R_{a_t}(S_t, S_{t+1}) \tag{7.10}$$

7.3.6 Optimal Algorithm

In this section, we introduce the optimality equations and implementation through the value iteration method to find the solutions. The solutions of the equation correspond to the optimal value functions, which also provide the basis for determining optimal policies. Under the policy π, the state-value function is used to evaluate the set of possible policies which, if executed will solve the problem presented in this chapter. The state-value function $V_R^{\pi}$of a state s is the expected return in reward point when starting in s and policy π is applied. The bellman equation is:

$$V_R^{\pi}(s) = \sum_{a \in A(s)} \pi(s,a) \sum_{s' \in S} P_a(s,s')[R_a(s,s') + \delta V_R^{\pi}(s')] \tag{7.11}$$

The optimal value function is defined as follows:

$$V^*(s) = \max_{\pi} V_R^{\pi}(s), \forall s \in S \tag{7.12}$$

The value iteration method [31] is used to find the optimum policy. The value iteration algorithm is presented in Table 7.2. The algorithm converges to the optimal state-value function V*, thus, to the optimal deterministic policy. The optimal action for each state is derived from the iteration algorithm. The transition matrix and the reward value determine the action. The value iteration algorithm is as defined in table 7.2.

```
   $V_0(s) = 0$
       **For each** state s
  **For each** action a
     Compute $Q_k(s,a) = R(s,a) + \sum_j \delta P_{(s,a)} V(s')$
  **Until** $\forall s, |V_{i+1}(s) - V_i(s)| < \varepsilon$
  **Compute** and **store** $\pi^*(s) = \arg\max_a Q_k(s,a)$
  **Compute** and **store** $V_i(s) = Q(s, \pi^*(s))$
  **Return** $< \pi^*(s), V(s) >$
```

Table 7.2: Value Iteration Algorithm

7.4 SIMULATION RESULTS

7.4.1 Model Illustration

In real life situations, probability *q* derives from the amount of resource allocated in terms of manpower and investments [76] to keep a mission-critical system in state S_1. The probability *p* is derived from the resources allocated to the system after a breach occurred from attack to switch the system back to state S_1. In a broad sense, if probability $p = 0$, meaning there is no resource allocated for recovery in case of an attack, then the long term confrontation between attacker and defender will end with the system in state S_0 and no way to switch to state S_1. With the probability $p > 0$, there is a recovery module or process implemented. The proportion of resources allocated to system's recovery depends on how long the system will remain offline and how costly is the loss due to the system being offline and not operational.

The measurement parameters such as, the mean time to recovery (MTTR), the mean time to failure (MTTF) are known for: calculating the average time that a system will take to recover from failure (MTTR) and the MTTF is the length of time expected for the system to remain operational before any failure occurred [67]. These metrics and more sustain the necessity to have the correct amount of resources allocated to recovery.

An illustrative example is to assign one unit of reward per time period for any action taken on the system, $R_{01} = +1; R_{11} = +1; R_{00} = -1; R_{10}= -1$. Here, reward R_{01} gains one unit which means, the system recovers from a failure attack. R_{11} gains one unit for the system to remain active after an attack was launched. R_{00} costs one unit for the system to remain off after an attempt to recover, and also it will cost one unit in R_{10} for the system to fail. Let's consider a unit is gained when the system remains in S_1 after an attack is perpetrated or switches from S_0 to S_1 after a recovery action. A unit is lost when an attack succeeded or a recovery action failed. Each time a mission-critical system is down, the next action or optimal action may be to bring the system back up in a running state in case the costs are lower than the loss to leave the system in a degraded state. When the system is in state S_1, there are implemented resources to circumvent and avoid failure or switch to state *0* or down.

7.4.2 Interpretation

This section provides a more detailed analysis of our MDP model illustration. The MATLAB simulations are to support the analyzed techniques presented. Notice that this work has proposed a high level MDP modeling of decision of resources allocation for a system in cyberspace. In fact, the result of any specific experiment will depend on the value attributed to the eight parameters *p*, *q*, R_{00}, R_{01}, R_{11}, R_{10}, δ and ε, where ε represents the error margin and it's a smaller positive number.

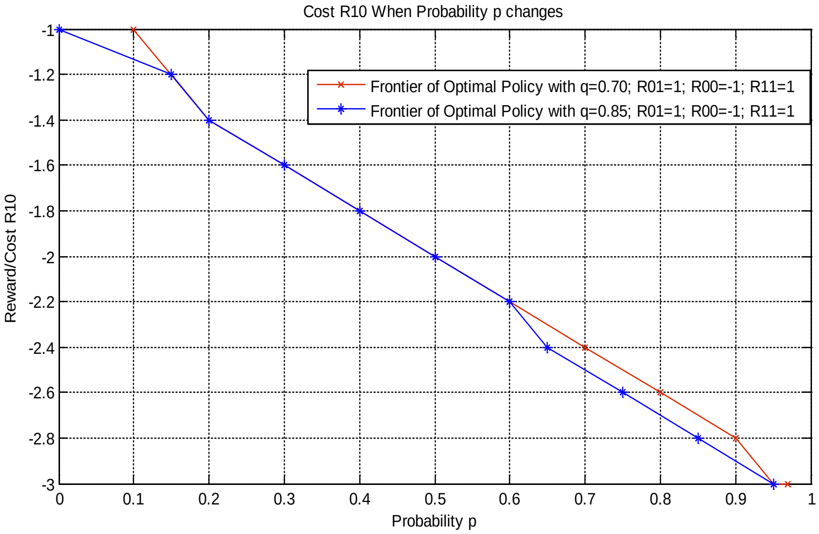


Figure 7.3: Resources variation between *p* and R_{10}

The specific values we have used in MATLAB simulations are just to illustrate a few specific scenarios. Generally, performance results will depend on the specific implementation that will also depend on particularities of the network. We examine the change in system reliability and effective behavior over time based on our dynamic analysis of a two-state MDP system [85].

Figure 7.3 shows changes in reward/cost when the system switches from state S_0 to S_1 with probability *p*. Probability q = {*0.70* for red frontier, *0.85* for blue frontier} is fixed, the cost of having the system "ON" increases with the probability of *p*. We can see that by investing in the recovery module, the probability *1-p* will be lower and the system will not remain in the fail or degraded state for too long. With the investment already made in agility to keep the system “ON”, loss R_{10} will be reduced to a minimum. Hence, the optimal action will be to recover the system each time it fails or switches into state S_0. The MTTR decreases when resources are allocated to recovery process.

The graph also reveals that, an increase of investment on agility when is already $q = 0.7$ does not seems efficient. Therefore, a 15% increase in investment on agility for $q = 0.85$ does not reduce the loss in to the system to fail.

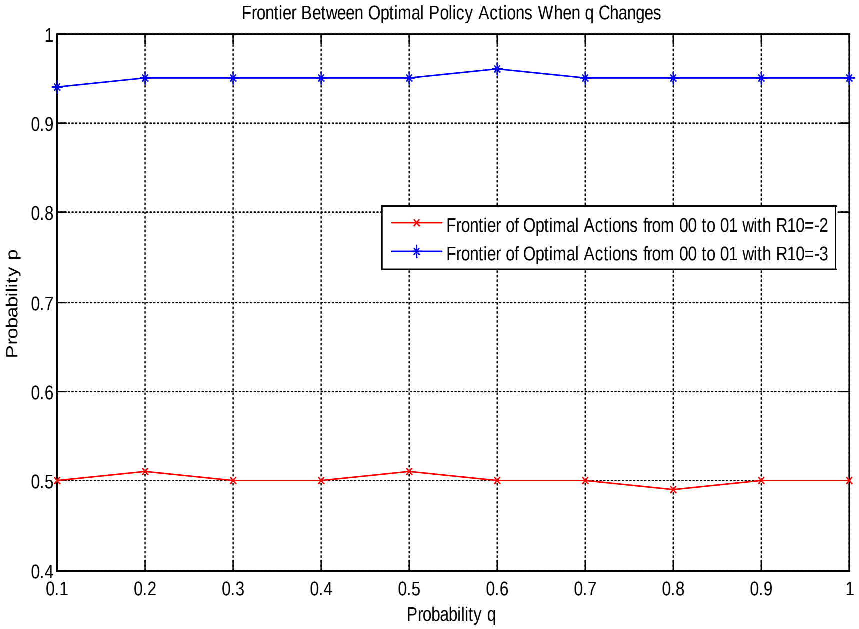


Figure 7.4: Behavior of Probabilities p and q

In case $q=0.85$, the optimal policy dictates for the system to be above the frontier and have to exit state S_0 with recovery. If the intention is to lower the cost R_{10}, it might be efficient when there is a failure in state S_0 to remain off by positioning itself below the frontier.

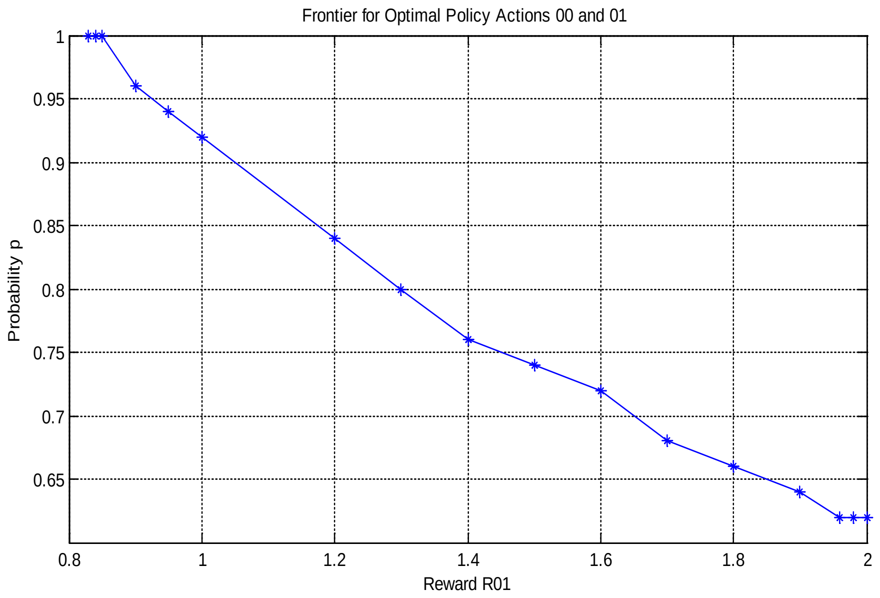


Figure 7.5: Frontier of Optimal Actions Between p and R_{01}

Figure 7.4 shows the variations between probabilities *p* and *q* when the remaining parameters are unchanged. The frontier of the change between optimal actions *00* and *01* in state S_0 is almost at the same point $p=0.5$ (respectively $p=0.95$) and $R_{10}=-2$ (respectively $R_{10}=-3$) with the remaining reward/cost set at $R_{00}=-1$, $R_{01}=+1$, $R_{11}=+1$.

For R_{10} = -2, the red line is the frontier. Below the red line ($p < 0.5$), the optimum policy is to invest in agility because of the small probability of recovery. Above the red line, ($p > 0.5$), there is a big probability of recovery changing the optimum policy which become to invest in recovery. Surprisingly, changing the probability *q* has little effect on the optimum policy as demonstrated by the almost horizontal line. However, changing R_{10} has a big impact. The frontier changes from $p = 0.5$ to $p = 0.95$ when the value of R_{10} changes from -*2* to -*3*.

Figure 7.5 captures the frontier variations between the probability *p* and the reward R_{01}. Below the frontier, both the probability to recover p and the reward to recover R_{01} are low and thus the optimum policy is to invest in agility. Above the frontier, both the probability to recover p and the reward to recover R_{01} are high and thus the optimum policy is to invest in recovery.

Figure 7.6 shows the reward R_{11} and the cost R_{10} of our system in state S_1. The minimal cost $R_{10}=-2.74$ is obtained with probability *q* set to *0.9*. The cost of failure R_{10} is too high below the frontier and thus the optimal policy is to invest in agility to avoid any costly failure. Above the frontier the optimal policy is to invest in recovery. We can see that the optimal policy is very sensitive to the variation of R_{11}.

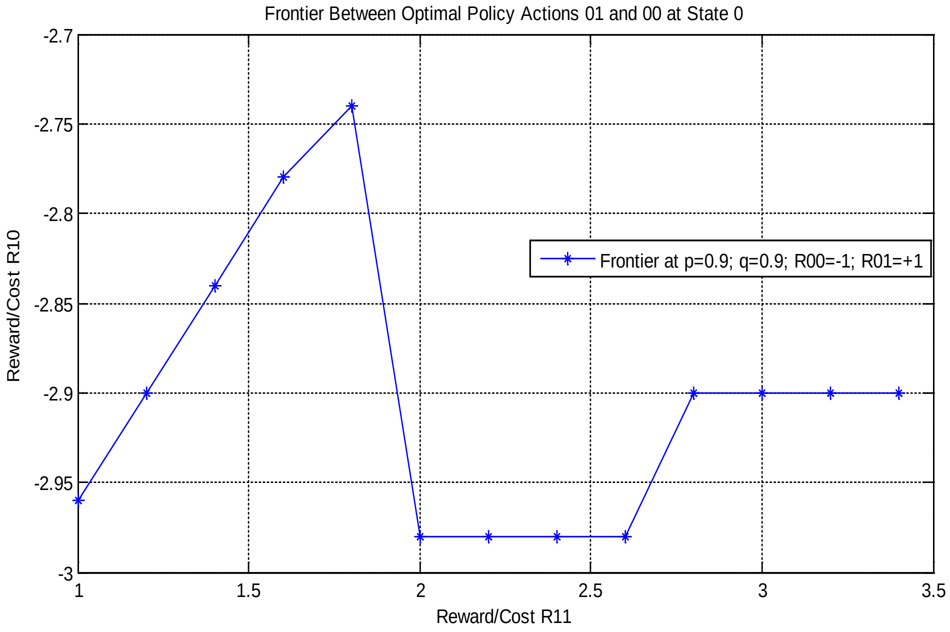


Figure 7.6: Frontier Actions Between Reward R_{10} and R_{11}

7.5 CONCLUSION AND FUTURE WORK

We investigate in this chapter, the issue of resource allocation in cybersecurity in terms of proportion sharing between agility and recovery, while approaching it by using the Markov decision process. First, the chapter explores the resource allocation proportion between agility and recovery using the Markov chain and presents the findings through limiting states probability, such that requirements from security investment should be available for the recovery component and then agility component. Second, the chapter extends the results from a Markov chain to a Markov decision process. The optimal allocation solutions should consider the gains from investing in the recovery component. The switch from a degraded state *0* to active state *1* after a period of time for any system means that the system has a recovery model implemented. Using simulations and the metrics MTTR and MTTF, this work also shows a repartition of resources that affects a mission-critical system's performance in cybersecurity.

In the future, we will consider the case of breaking down agility and recovery into multiple states with non-symmetrical interactions between states. We will also investigate the use of game theoretic models for resource optimization.

CHAPTER 8

CONCLUSION

In this dissertation, we have explored the problem of incentivizing cooperation in mobile ad hoc networks (MANETs). In a MANET as we have mentioned, there is no infrastructure to support information exchange like dedicated routers or access points. Rather, nodes have to play the crucial role of relays to help transfer data-packets across the network. With this responsibility, autonomous nodes with selfish behavior may arise to preserve nodes' energy. Cooperation among entities of such networks is important and indispensable to keep them operational in the face of selfish behavior. Adding to the fact that the autonomous node is also moving, the mobility of a device can deter or make it difficult for a selfish node to participate in overall network objectives.

This chapter reflects the contributions, discusses the limitations and proposes the future direction of our research.

8.1 DISCUSSIONS

8.1.1 Data Delivery in Mobile Environment with Incentives

We designed an incentive dynamic data delivery for a mobile environment, where mobile a node can move randomly and still participate in data-packet forwarding. We defined the bargaining model, which took into consideration the mobility factor and parameters like speed, direction and available resources of a node. Based on the routing protocol for node discovery in the mobile network, we presented the mechanism for selecting the most appropriate candidate as an intermediary node. Also, the splitting rule is followed by each negotiator during the bargaining sequence. We defined the proper evaluation metrics to evaluate the nodes participating in the overall performance of the MANET compared to other methods. The effectiveness was presented with OMNET++ as our simulation environment, where node mobility is captured as close as possible to reality. The simulation results are presented.

Limitations in the design and implementation are the overhead messages and extra power consumption for a longer bargaining time. Because of the message exchange during negotiation and the density of the network, when two nodes are in bargaining mode, their speed should be limited. A stopping procedure for the bargaining process has to be implemented in order to shorten the energy depletion.

8.1.2 Arbitration in Mobile Environment to Allocate Resources

In a mobile heterogenous environment where nodes are not homogenous, we designed an arbitration solution for heterogeneous MANETs in the presence of selfish nodes. We integrated into our solution an incentive mechanism to stimulate and enforce non-participative nodes to be part of the overall network objectives. We have simulated the arbitration solution and shown the effectiveness of applying arbitrators in a completely mobile environment to ease and secure the data transfer. By deploying arbitrators with better radio transmission range, number of hops are reduced, which also reduced the amount of energy consumption for a packet to travel from source to destination. By reducing the number of hops for a packet to travel from a source node to its destination node, it also increases the security of the network because we have less packets traveling on airwaves.

So far, we have only considered selfish nodes acting alone. The detection of malicious nodes or a coalition of malicious nodes during negotiation will improve the performance of the arbitrators in the network. Another improvement is to relax the responsibility of the arbitrator in detecting misbehaving nodes and have all nodes neighbors look after each other.

8.1.3 Network Security Game: Modeling Security and Trust Relationship in MANETs

We applied the *User-Defender-Attacker* game theoretic model to design the interactions between users, defenders, and attackers of the system in cyberspace. We formulated the characteristics of each interactive entity, including selfishness and non-cooperativeness. We also evaluated the level of security of the network and the trustworthiness of the network against attacks. The equilibrium strategies of the three-player game are derived. The simulation results are presented.

Users trust in terms of loss when the attacker breaches the system and compromises users' private data. The exact quantification of the user's loss has not been analyzed. For example, when a provider system is breached because of less investment in security and the users are informed through mass media, the trust between the provider and the users should be reevaluated and the provider penalized.

8.2 FUTURE DIRECTIONS

The first part of this research mainly involves enforcing and stimulating cooperation to forward packets in a completely mobile environment. Regardless of the above-mentioned improvements, there are other potential directions to enhance the current work, and develop a more comprehensive security and cooperation in MANETs using the game theory frameworks. A comprehensive model for an autonomous network can then be developed. Clearly, cross layer optimization techniques will improve the security and the cooperation using the framework of the game

8.2.1 Stochastic Pricing and Resource Allocation Games

The dynamic programming techniques used in Chapters 3 and 4 addressed the problem for a single decision maker acting in a mobile environment. In the asymmetric bargaining model introduced in Chapter 4, players' bargaining powers depend on their bids, which can be determined using the admission price for an optimal pricing policy or an auction. Like the authors in resource allocation [25], we have assumed that network users do not anticipate their effect on the resource allocated. However, when the users recognize that they are not merely accepting the offers, the problem becomes a game in which the setting of willingness-to-pay, demand and bids becomes strategic for the network users. Users make self-serving decisions and economists are well aware that these selfish behaviors can lead to inefficiency. Johari *et al.* [7] showed that the price of anarchy in networks with elastic supply amounts to up to 25% in efficiency loss. The measurement is obtained by computing the ratio of the NE utility function to the socially optimal utility function and showing that it is ¾ at worst [7]. Stochastic games are natural extensions of Markov decision processes to include multiple decision makers.

There are some similarities between the node degree of distribution on the real and simulated MANET, while links are much more unstable and asymmetric in real life than in a simulated MANETs environment. To alleviate this discrepancy, the link status can be modeled in a MANET using a state Markov chain model. However, the lack of available data generated from real MANET experiments could not statistically confirm these claims. Moreover, with some analytical works, we think that this future work can produce promising models to better simulate link status in MANETs.

8.2.2 Non-cooperative Implementation of the Cooperative Bargaining Solutions in Self-organizing and Self-healing Networks

In Chapter 4, we have derived a class of bargaining solutions using the bargaining concepts from cooperative game theory. The payoffs, indicated by the amount of resources allocated to the players, are sustained by a binding agreement guaranteed by each node in the network and the arbitrator. However, the enforcement of such payoffs falls outside of the domain of cooperative game theory. In MANETs, the decision-making process has to be decentralized, as in a non-cooperative game. A MANET is a collection of nodes that forms a network without fixed-infrastructure. As opposed to networks which use routers to support network functions, such as packet routing and forwarding, these functions are provided by the nodes (or hosts) themselves. Such a network can operate in a standalone fashion or may be connected to the Internet. The interconnections among nodes often change continually and arbitrarily. These networks were initially designed for military operations and play an increasingly important role in many environments, such as ad hoc networking for collaborative and distributed disaster recovery, search-and-rescue and crowd control. More recently, they have been envisaged as able to provide Internet connectivity for nodes that are not in transmission range of a wireless access point. The IEEE 802.11 wireless protocol incorporates an ad hoc networking system when no access points are present.

In wireless mobile networks (WMNs), all routers are capable of organizing and auto-reconfiguring themselves wirelessly, which means that no cabling is needed to connect them. These nodes form a rich radio mesh connectivity among themselves that is difficult to provide in wired networks. The principle is similar to the wired Internet; data will hop from one node to another until it reaches its given destination. While wireless node connectivity significantly reduces the upfront deployment and subsequent maintenance costs, the rich mesh connectivity helps to deliver high levels of reliability and robustness. Mesh networks are self-healing and extremely reliable because each node is connected to several others and if one drops out, due to hardware failure or man-made attacks, its neighbors simply find another route. Because of these attractive features, WMN is being considered for a wide variety of applications, such as backhaul connectivity for cellular radio access networks, combat systems and citywide surveillance systems. It can effectively extend a network by sharing access to a higher cost network infrastructure.

Due to the complexity of the mobility and traffic models as well as the infrastructureless, dynamic topology of these networks, non-cooperative game theory is the primary tool for studying players, which are independent decision makers whose actions potentially result in efficiency loss. A vast number of works on the application of non-cooperative game theory in MANETs are surveyed in [42]. Another approach is to study the implementation of the Pareto-optimal bargaining solutions in a non-cooperative manner.

8.2.3 Route Calculation Based on Routing protocol and Coalition Information

The way the non-cooperation model is currently integrated with the routing protocol (AODV) in chapter 3 helps fight selfish behavior through the bargaining agreement: Do not drop packets sent from or destined to members after agreement. However, this can be more effective if AODV proactively uses the nodes that are inclined to accept offers available to build its routing table. For example, AODV could be modified to give priority in choosing multi point relays (MPRs) to alliance companions such that resulting routes involve more nodes with less bargaining power, hence achieving more reliable routes. This could greatly enhance the packet delivery ratio of the network under the integrated system. We highly believe that this could be a promising future of the current work.

8.3 SUMMARY

In this dissertation, we have explored the problem of stimulating cooperation in mobile ad hoc networks (MANETs) by investigating nodes cooperation in improving the network throughput using the bargaining game theoretic model. We investigated the data forwarding task between nodes in a highly dynamic network using an arbitrator for resource allocation. Also, the investigation led us to consider the possibility of having colluded nodes in our mobile ad-hoc network interfering with the arbitrator negotiation process. In order to prevent complacent offers to players, the arbitrator uses a random generator to assign offer without memory of previous offers. Finally, we investigated the interactions between users, providers and attackers in cyberspace using a three-player game theoretic approach to strengthen the security by providing to decision-makers the optimized investment in defending users' privacy and private data against security breaches.

REFERENCES

[1] R. Myerson "Game Theory: Analysis of Conflict" Harvard University Press, 1997

[2] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol," in Proceedings of the 3rd ACM International Symposium on Mobile Ad hoc Networking & Computing (MobiHoc) pp. 226-236, New York, NY, USA, 2002.

[3] M. Refaei, L. DaSilva, M. Eltoweissy, and T. Nadeem, "Adaptation of reputation management systems to dynamic network conditions in ad hoc networks," IEEE Transactions on Computers, vol. 59, pp. 707-719, May 2010.

[4] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, pp. 107-121, Deventer, The Netherlands, 2002.

[5] L. Zhou and Z. Haas, "Securing ad hoc networks", IEEE Network, vol. 13, no. 6, pp. 24 -30, 1999.

[6] Z. Han, D. Niyato, W. Saad, T. Basar, A. Hjorungnes "Game Theory: in Wireless and Communication Networks: Theory, Models and Applications" Cambridge University Press, 2012.

[7] R. Johari and J. N. Tsitsiklis. Efficiency loss in a network resource allocation game. Math Oper. Res., 29(3):407–435, 2004.

[8] C. Kamhoua, N. Pissinou" Mitigating Selfish Misbehavior in Autonomous Wireless Multi-hop Networks Using Stochastic Game Theory" in proceedings of the 35th IEEE Conference on Local Computer Networks (LCN 2010) Denver, Colorado, USA. October 2010.

[9] C. Courcoubetis, F.P. Kelly, and R. Weber. "Measurment-based usage charges in communication networks". Technical Reports, Statistical Laboratory, University of Cambridge, 1997.

[10] L. Buttyan, J-P. Hubaux "Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks" Technical Report DSC/2001/001, Swiss Federal Institute of Technology-Lausanne, Department of communication systems, January 2001.

[11] M. Jakobsson, J-P. Hubaux, L. Buttyan, “A micro-payment scheme encouraging collaboration in multi-hop cellular networks” in Financial Cryptography, pp. 15-33, Springer, 2003.

[12] A. Josang R. Ismail “The Beta Reputation System” In Proceedings of the 15th Bled Electronic Commerce Conference, June 2002.

[13] M. Felegyhazi, J-P. Hubeaux, L Buttyan “Nash Equilibria of Packet Forwarding Strategies in Wireless Ad Hoc Networks” IEEE Transaction on Mobile Computing, vol.5, No.5, May 2006.

[14] S. Zhong, J. Chen, Y. Yang “Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks” IEEE INFOCOM 2003.

[15] S. Ganeriwal and M.B. Srivastava, ”Reputation-based Framework for High Integrity Sensor Networks” presented at ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN’04),Washington, D.C.,USA, October 2004.

[16] S. Brahma, M. Chatterjee, “A bargaining game for channel in dynamic spectrum access networks”, Proceedings of IEEE Globecom, Miami, FL, Dec. 2010.

[17] W. Yu, K. J. R. Liu, “Secure Cooperation in Autonomous Mobile Ad-Hoc Networks Under Noise and Imperfect Monitoring: A Game-Theoretic Approach” IEEE Transactions on Information Forensics and Security, Vol. 3, No. 2, June 2008.

[18] L. Yan, “Cooperative Packet Relaying in Wireless Multi-hop Networks” International Conference on Advanced Information Networking and applications Workshops, IEEE Computer Society. 2009.

[19] L. Yan, S. Hailes, “Designing Incentive Packet Relaying Strategies for Wireless Ad Hoc Networks with Game Theory” in IFIP International Federation for Information Processing; Wireless Sensor and Actor Networks II; Ali Miri; (Boston: Springer) , Vol. 264, pp. 137-148, 2008.

[20] S. Zhong, J. Chen, Y. Yang “Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks” IEEE INFOCOM 2003.

[21] V. Srinivasan, P. Nuggehalli, C.F. Chiasserini, R. R. Rao. “Cooperation in Wireless Ad Hoc Networks”, IEEE Infocom, San Francisco, CA, USA, 2003.

[22] S. Marti, T. Guili, K. Lai, M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks”, 6th ACM Conf. on Mobile Computing and Networking, Boston, MA, pp 255-265, August 2000.

[23] N. Othman, S. Weber,”Towards tag-based cooperation for mobile ad hoc networks” in Reliable Distributed Systems Workshops, 30th IEEE Symposium on, pp. 20-25, 2011.

[24] Y. Liou, R. Gau, C. Chang, “A bargaining game based access network selection scheme for HetNet”, Proceedings of IEEE International Conf. on Communications, pp: 4888-4893, Sydney, Australia, June 2014.

[25] E. Stevens-Navarro, Y. Lin, V. Wong, “An MDP-based vertical handoff decision algorithm for heterogeneous wireless networks”, IEEE Transactions on Vehicular Technology, Vol. 57, No. 2, March 2008.

[26] F. Bari, V. Leung, “Automated network selection in a heterogeneous wireless network environment”, IEEE Network. Vol. 21, no. 1, pp. 34-40, Jan. 2007.

[27] X. Xie, H. Chen, H. Wu, “Bargain-based stimulation mechanism for selfish mobile nodes in participatory sensing network”, IEEE Conf. on Communications Society, SAHCN, Rome, Italia, pp: 1-9, June 2009.

[28] S. Basagni, A. Carosi, C. Petroli, C. Phillips, “Coordinated and controlled mobility of multiple sinks for maximizing the lifetime of wireless sensor networks”, Journal of Wireless Network, Vol. 17, No 3, pp 759-778, April 2011.

[29] I. Ståhl, “Bargaining theory”, The Economic Research Institute (EFI), Stockholm School of Economics, November 1972.

[30] H. Gintis, “Game Theory Evolving: A Problem-Centered Introduction to Modeling Strategic Interaction”, 2nd Edition, Princeton Universitiy Press, 2009.

[31] V. Mazalov, “Mathematical Game Theory and Applications”, John Wiley and Sons, Ltd, 1st edition, 2014.

[32] A. Jade, S. K. Madria, M. Linderman, “ Incentive Based Routing Protocol for Mobile Peer to Peer Networks” Tenth International Conference on Mobile Data Management: Systems, Services and Middleware, 2009.

[33] J. Nash. The bargaining problem. Econometrica, 18, 1950.

[34] J. A. Hassan, M. Hassan, S. K. Das, “A Brinkmanship Game Theory Model for Competitive Wireless Networking Environment” in proceedings of the 35th IEEE Conference on Local Computer Networks (LCN 2010). Denver, Colorado, U.S.A. October 2010.

[35] M. Huber, M. Mulazzani, E. Weippl, G. Kitzler, S. Goluch, “Friends-in-the-middle attacks: Exploiting social networking sites for spam”, IEEE Internet Computing, Vol. 15, No. 3, pp. 28-34, May-June 2011.

[36] M. Raya, R. Shokri, J. Hubaux, “On the tradeoff between trust and privacy in wireless ad hoc networks”, ACM, Proceedings. 3rd ACM conference on Wireless network security, Hoboken, NJ, pp: 75-80, March 2010.

[37] J M. Seigneur, C. Jensen, “Trading privacy for trust”, In Proceedings. Of iTrust’04 LNCS, Vol. 2995, pp. 249-253, 2004.

[38] L. Lilien, B. Bhargava, “Trading privacy for trust in online interactions”, Idea Group, 2008.

[39] K. Kim, B. Prabhakar, S. Park, “Trust, perceived risk and trusting behavior in internet banking”, Asia Pacific Journal of Information Systems, Vol. 9, No. 3, September 2009.

[40] C. Ntuen, J. Chenou, E. Idoye, “Modeling the relationship between trust and risk in cyberspace”, Proceedings Of the Industrial and Systems Engineering Research Conference, Krishnamurthy and Chan, Eds, 2014.

[41] A. Rossi, S. Pierre. “Collusion-resistant reputation-based intrusion detection system for MANETs”, International Journal of Computer Science and Network Security, Vol. 9 No. 11, November 2009.

[42] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, W. Qishi “A Survey of Game Theory as Applied to Network Security” 43rd Hawaii International Conference on System Sciences (HICSS). Honolulu, HI, USA. March 2010.

[43] A. Rasheed, R. Mahapatra, “The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks”, IEEE Transactions on Parallel & Distributed Systems, vol.23, no. 5, pp. 958-965, May 2012.

[44] S. Munir, B. Ren, W. Jiao, B. Wang, “Mobile Wireless Sensor Network: Architecture and Enabling Technologies for Ubiquitous Computing”, 21st Int’l Conference on Advanced Information Networking and Applications Workshops, pp: 113-120, Niagara Falls, Ont., May 2007.

[45] D. Niyato, E. Hossain, “Dynamics of Network Selection in Heterogeneous Wireless Networks: An Evolutionary Game Approach”, IEEE Trans. Vehicular. Technology.,Vol. 58, pp,2008-2017, May 2009.

[46] A. Varga, R. Hornig, “An overview of the OMNeT++ simulation environment,” in Proceedings of the 1st international conf. on Simulation Tools and Techniques for Communications, Networks and Systems (SIMUTools 2008), March 2008, pp. 60:1–60:10.

[47] Y. Wang, S. Chen, H. Goudarzi, M. Pedram, “Resources Allocation and Consolidation in a Multi-Core Server Cluster Using a Markov Decision Process Model”, IEEE 14th International Symbosium on Quality Electronic Design, pp 635-642, Santa-Clara, CA, March 2013.

[48] H. Zeng, H. Deng, K. Meng, S. Luo, X. Yu, A. Mody, M. Sherman, J. Mueller, Z. Wang, “From Spectrum agility to Network Agility: Proactive and adaptive

Reconfiguration For Reliable Communication in tactical Networks", IEEE Military Communications Conference, pp 1663-1668, San Diego, CA, November 2013.

[49] L. Yamen Njilla, N. Pissinou, "Dynamics of Data Delivery in Mobile Ad-hoc Networks: A Bargaining Game Approach", IEEE Computational Intelligence and Security in Defense Applications (CISDA), Verona, NY, USA, May 2015.

[50] L. Buttyan, J-P Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks", ACM/Kluwer Mobile Networks and Applications, 8(5), October 2003.

[51] M. Riordan, D. Grigoras, "Data Mule Service for Mobile Ad-Hoc Networks", IEEE 11th International Symposium on Parallel and Distributed Computing, Munich, Germany, pp. 227-234, June 2012.

[52] Y. Yang, S. Guo, X. Qiu, L. Meng, "A Service Negotiation Model for Selfish Nodes in the Mobile Ad hoc Networks", IEEE International Conference on Communication, pp. 1-5, Kyoto, Japan, June 2011.

[53] C. Maghmoumi, H. Abouaissa, J. Gaber, P. Lorenz, "Analysis of communication overhead for a clustering-based security protocol in ad hoc networks", Int'l Journal on advances in telecommunications, Vol. 3, No 1 & 2, 2010 .

[54] O. Compte, P. Jehiel "Bargaining and Majority Rules: A Collective Search Perspective", Journal of Political Economy, Vol. 118, No. 2, pp. 189-221, April 2010.

[55] P. Faratin, C. Sierra, N. Jennings, "Negotiation Decision Functions for Autonomous Agents", International Journal of Robotics and Autonomous System, pp. 159-182, 24(3-4), 1997.

[56] J.-P. Hubaux, T. Gross, J. Le Boudec, M. Vertterli, "Toward Self-Organized Mobile ad-Hoc Networks: The Terminodes Project", IEEE Communication Magazine, Vol. 39, pp:118-124, 2000.

[57] J. Xie, A. Das, S. Nandi, A. Gupta, "Improving the Reliability of IEEE 802.11 Broadcast Scheme for Multicasting in Mobile Ad-Hoc Networks", IEEE Proc. Communication, Vol. 153, No.2, April 2006.

[58] W. He, C. Xia, H. Wang, C. Zang, Y. Ji, "A game theoretical attack-defense Model oriented to network security risk assessment" Proceedings of IEEE International Conference on CSSE, Vol. 3, pp. 498-504, Wuhan, China, Dec. 2008.

[59] United States Securities and Exchanges Commission, "CF disclosure guidance: Topic No. 2 - Cybersecurity", http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[60] A. Douss, R. Abassi, S. Fatmi, “A Trust Management Based Security Mechanism Against Collusion attacks in a MANET Environment”, 9th International Conf. on Availability, Reliability and Security, pp. 325-332, Fribourg, Switzerland, September 2014.

[61] C. Kamhoua, L. Kwiat, K. Kwiat, J. Park, M. Zhao, M. Rodriguez, “Game Theory Modeling of Security and Interdependency in a Public Cloud”, IEEE 7th Int’l Conference on Cloud Computing, pp: 514-521, Anchorage, AK, USA, June 2014.

[62] S. Buchegger, J. Le Boudec, “Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks”, 10th EUROMICRO Workshop Proceedings on Parallel, Distributed and Network-based Processing, pp. 403-410, Canary Islands, 2002.

[63] J.-H. Cho, A. Swami, I.-R. Chen, “A Survey on Trust Management for Mobile Ad Hoc Networks”, IEEE Communications Society, pp. 562-583, October 2010.

[64] M. Boutin, “Random Waypoint mobility model.” http://www.mathworks.com/matlabcentral/fileexchange/30939-random-waypoint-mobility-model, Apr. 2011 [June 2015].

[65] D. Leversage, E. Byres, “Comparing Electronic Battlefields: Using Mean time-to-Compromise as a Comparative Security Metric”, Proceedings of the 4th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, Russia, September 2007.

[66] J. Park, S. Kim, C. Kamhoua, K. Kwiat, “Optimal State Management of Data Sharing in Online Social Network OSN) Services” in the 11th Intl. Conference on Trust, 2012.

[67] U. Ayesta, M. Erausquin, P. Jacko, “Resource-Sharing in a Single Server with Time-Varying Capacity”, Invited paper, IEEE 49th Annual Allerton Conference, September 2011.

[68] V. Wong, M. Lewis, V. Leung, “Stochastic Control of Path Optimization for Inter-Switch Handoffs in Wireless ATM Networks”, IEEE/ACM Transactions on Networking, Vol. 9, No. 3, June 2001.

[69] A. Jabbar, “A Framework to Quantify Network Resilience and Survivability”, PhD Thesis, The University of Kansas, Lawrence, KS, May 2010.

[70] J. Sterbenz, D. Hutchison, E. Cetinkaya, A. Jabbar, J. Rohrer, M. Scholler, P. Smith, “Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks: Special Issue on Resilient and Survivable Networks, Vol. 54, No. 8, pp: 1245–1265, June 2010.

[71] C. Kamhoua, K. Kwiat, J. Park, “Surviving in Cyberspace: A Game Theoretic Approach”, Academy Publisher, Journal of Communications, Vol 7, No. 6, June 2012.

[72] A. Bianco, L. Giraudo, D. Hay, “Optimal Resource Allocation for Disaster Recovery”, IEEE Global Telecommunications Conference, pp 1-5, 2010.

[73] K. Salhammar, S. Knapskog, “Using Game Theory in Stochastic Models for Quantifying Security”, Journal of Stochastic Models for Combined Security and Dependability Evaluation, NUST, 2007.

[74] S. Liu, P. Zhang, H. Sun, “Research on Defense in-depth Model of Information Network Confrontation”, IEEE 4th International Conference on Computational and Information Sciences, pp 267-270, 2012.

[75] W. Chunlei, M. Qing, D. Yiqi, “Network Survivability Analysis Based on Stochastic Game Model”, IEEE 4th International Conference on Multimedia Information Networking and Security, pp 99-104, 2012.

[76] R. Rue, S.L. Pfleeger “Making the Best Use of Cybersecurity Economic Models” IEEE Security & Privacy,Volume: 7 , Issue: 4 , 2009.

[77] S. Neuhaus, B. Plattner, “Software Security Economics: Theory, in Practice” Workshop on the Economics of Information Security (WEIS) 2012.

[78] Y. Han, T. Alpcan, J. Chan, C. Leckie, “Security Games for Virtual Machine Allocation in Cloud Computing”, in proceeding of the 4th International conference on Decision and Game Theory for Security, Vol. 8252, pp: 99-118, Springer Verlag, New York, USA, 2013.

[79] Y. Zhang, A. Juels, A. Oprea, M. Reiter, “HomeAlone: Co-Residency Detection in the Cloud via Side-Channel Analysis”, in the proceedings of IEEE Symposium on security and Privacy,pp: 313-328, Berkeley, California, USA, May 2011.

[80] T. Basar, T. Alpcan, “Network Security: A Decision and game theoretic approach”, Cambridge University Press, 2010.

[81] L. Wang, Z. Li, S. Ren, K. Kwiat, “Optimal Voting Strategy against Rational Attackers”, The 6th International Conference on Risks and Security of Internet and Systems CRiSIS, pp: 1-8, Timisoara, Romania, September 2011.

[82] C. Kamhoua, N. Pissinou, S. Makki, “Game Theoretic Analysis of Cooperation in Autonomous multi-hop Networks: The Consequences of unequal Traffic Load”, Proceedings of the IEEE Globecom 2010, Miami, FL, USA, Dec. 2010.

[83] S. A. Arshad, M. A. Murtaza, M. Tahir, “Fair Buffer Allocation Scheme for Integrated Wireless Sensor and Vehicular Networks using Markov Decision Processes”, Proceedings of Intl. Conf. on , 2012.

[84] H. Wang, C. Jin, K. Shin, “Defense Against Spoofed IP Traffic Using Hop-Count Filtering”, IEEE/ACM Transactions on Networking, Vol. 15 No. 1, pp 40-53, February 2007.

[85] M. Puterman, “Markov Decision Processes: Discrete Stochastic Dynamic Programming”, 1st Edition, John Wiley - Interscience, 2005.

VITA

LAURENT LAVOISIER YAMEN NJILLA

2015	Doctoral Candidate, Electrical and Computer Engineering Florida International University Miami, Florida
2005	M.Sc., Computer Engineering and Networking University of Central Florida Orlando, Florida
1999	M.Sc., Computer Science The University of Yaounde I/ Faculty of Science Yaounde, Cameroon
1997	B.Sc., Computer Science The University of Yaounde I/ Faculty of Science Yaounde, Cameroon
2014 - 2015	McKnight Dissertation Fellowship Award
2005	National Society Black Engineers (NSBE) Fellows Award
2009 – 2015	Senior Systems Analyst The City of Miami Beach, Information Technology Department Miami Beach, Florida
2014-2014	Summer Intern Air Force Research Laboratory, Cyber Security Division Rome, New York
2005 – 2008	IT Systems Analyst Kimberly-Clark Corporation, Business to Business Division Roswell, Georgia

PUBLICATIONS AND PRESENTATIONS

1. Laurent Yamen Njilla, “Game Theoretic Modeling of Security in Mobile Heterogeneous Wireless Sensor Networks ”, McKnight Doctoral Research and Writing Conference, Tampa, FL, February 2014.
2. Laurent Yamen Njilla, Niki Pissinou, “Dynamics of Data Delivery in Mobile Ad-hoc Networks: A Bargaining Game Approach”, IEEE Computational Intelligence and Security in Defense Applications (CISDA), Verona, NY, USA, May 2015.
3. Laurent Yamen Njilla, Niki Pissinou, Kia Makki, “Game Theoretic Modeling of Security and Trust Relationship in Cyberspace”, Submitted to the International Journal of Communication Systems (IJCS), Edition 2015.
4. Laurent Yamen Njilla, Niki Pissinou, Kia Makki, “ Game Theoretic Analysis for Resource Allocation in Dynamic Multi-hop Networks with Arbitration”, Submitted to the IEEE Conference on Computer Communications, (INFOCOM 2016), 10-15 April 2016, San Francisco, CA, USA.
5. Laurent Yamen Njilla, Patricia Echual, Niki Pissinou, Kia Makki, “A Game Theoretic Approach on Resource Allocation With Colluding Nodes in MANETs”, Submitted to the IEEE International Systems Conference (SysCon 2016), 18-21 April 2016, Orlando, FL, USA.
6. Laurent Yamen Njilla, Charles Kamhoua, Kevin Kwiat, Patrick Hurley, Niki Pissinou, “Cyber Security Resource Allocation: A Markov Decision Process” In Preparation for IEEE Transaction on Communication.
7. Laurent Yamen Njilla, Charles Kamhoua, Kevin Kwiat, Patrick Hurley, Niki Pissinou, “Cyber Security Resource Allocation: A Markov Chain Analysis” In Preparation for IEEE Workshop paper Submission.