Secure Routing in Intelligent Device-to-Device Communications

Dissertation submitted in

fulfillment of the requirement for the award of the

Degree of Doctor (Dr .rer.nat.) of the Georg-August-Universität Göttingen

within the doctoral program Mathematics and Computer Science

of the Georg-August University School of Science (GAUSS)

submitted by

Msc. Hadeer Elsemary

SEPTEMBER 2016

Thesis Committee

- Prof. Dr. Dieter Hogrefe, Telematic Group, Computer Science.
- Prof. Dr. Xiaoming Fu, Computer network Group, Computer Science.

Members of the Examination Board Reviewer:

- Reviewer: Prof. Dr. Dieter Hogrefe, Telematic Group, Computer Science.
- Second Reviewer: Prof. Dr. Xiaoming Fu, Computer network Group, Computer Science.

Further members of the Examination Board:

- Prof. Dr. Winfred Kurth, Computer Graphics and Ecological Informatics Group, Computer Science.
- Prof. Dr. Florentin Woergoetter, Computational Neurosciences, Computer Science.
- Prof. Dr. Carsten Damm, Theoretische Informatik und Algorithmische Methoden, Computer Science.
- Prof. Dr. Jens Grabowski, Software Engineering for Distributed Systems, Computer Science.

Date of the Oral Examination: 16. September 2016

Declaration

I at this moment declare that this thesis entitled "Secure Routing in Intelligent Device-to-Device Communications" is the consequence of my research except as cited in the references. I do not concurrently submit this thesis in the candidature of any other degree. I confirm that:

- This work was done wholly or mainly while in the candidature for a research degree at this University.
- Where I did not submit previously any part of this thesis for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. Except for such quotations, this thesis is entirely my work, and I have acknowledged all primary sources of help.
- Where I have done all the work in this thesis by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signature :

Student : Hadeer Elsemary

Date : 16.09.2016

Supervisor : Prof. Dr. Dieter Hogrefe

Co-Supervisor: Prof. Dr. Xiaoming Fu

For my beloved mother and father

Acknowledgment

I thought about everyone to whom I might want to express my appreciation for their support in making this thesis possible. So, first, I ought to express my most profound gratitude and inconceivable gratefulness to my first supervisor and the committee chair, Prof. Dr. Dieter Hogrefe, who in somehow has contributed in making this study conceivable. He has been a steady source of support and ideas during the previous three years. I gained hugely from his vision, polished methodology, working morals and longing for incredibleness.

I should express my thankfulness also to the committee member, Prof. Dr. Xiaoming Fu, for his knowledge, help in the investigation of the data and for providing valuable feedback whenever requested. His experience and vision have played such a central role during my Ph.D. studies.

My best thanks go to Dr. Emmanuel Panaousis, senior lecturer of cyber security and privacy school of computing, engineering and mathematics, University of Brighton, for his assistance and help in providing me the necessary technical suggestions during my research period. I would also like to thank him for opening up the collaboration opportunities. In particular, good thanks go to Dr. Xu Chen for his assistance and help.

In this very particular moment, I would like to express my deepest thanks to my father for his love encouragements and support during the last three years.

Furthermore, my sincere appreciation to the sponsor Deutscher Akademischer Austausch Dienst (DAAD) with the financial assistance. Special thanks also go to the coordinators at the DAAD for their efforts and help for granting me that rare opportunity. I should express my thankfulness to my friends and colleagues for their continuous love and encouragement.

Hadeer Elsemary, Goettingen

Abstract

Device-to-Device (D2D) communications have received exceptional attention nowadays due to the overabundance number of applications and services. Therefore, D2D is expected to be a vital technical component in Internet of Things and to play a significant role with the next generation 5G. On the other hand, due to the growth demand of D2D, it becomes an ideal target for attackers. Moreover, the rapid rise in mobile capabilities opens the door to the cyber criminals that explore new avenues for malware attacks. In spite of the fact that the literature proposed security schemes for malware attacks. However, the research field is still immature and unexplored in depth due to the fast evolution of malware. Accordingly, malware attacks formalize security risk that threatens the mobile network. A noteworthy concern is that the malware attacks are going on at a rate far surpassing the development of safety techniques.

The fundamental goal of our thesis is to propose a novel secure, energy-aware stochastic routing protocol based on a game-theoretic approach for security improvement against malware attacks in Device-to-Device network. The proposed protocol considers for the security requirement, as well as the energy system constraints. As a first step toward thwarting the success of the malware attacks, we try to hinder the malware infection by detecting the malware before it infects the targeted devices.

Moreover, the proposed routing protocol considers the attacker's behavior and the computation of decision makers' strategies.

The effectiveness of the proposed routing protocol has been evaluated using network simulator. Through extensive simulations, we have validated the effectiveness of proposed protocol by comparing its performance with the traditional routing protocols and with another strategic customized protocol. Results are presented to illustrate the efficiency of the proposed routing protocol regarding the detection rate and overall expected payoff compared with traditional routing protocols and another strategic customized protocol in case of three different attacks distribution.

Contents

List of Figures

List of Tables

List of Appendices

List of Abbreviations

ACO	ant colony optimization
AODV	Ad-hoc On-demand Distance Vector
BS	Base Station
D2D	Device-to-Device
DSR	Dynamic Source Routing
FQL	Fuzzy Q-learning
IDS	Intrusion Detection System
IoT	Internet of Things
LP	Linear Programming
LTE	Long Term Evolution
MANETs	Mobile Ad-hoc Networks
MDC	Mobile Device Cloud
MEC	Mobile-Edge Computing
NE	Nash Equilibrium
P2P	Peer-to-Peer

PNE	Pure Nash Equilibrium
RREP	Route Reply
RREQ	Route Request
SSR	Secure Stochastic Routing
UDP	User Datagram Packet
Wi-Fi	Wireless Fidelity

Chapter 1

Introduction

This chapter presents the thesis direction, mentions the motivation behind choosing the research problem, including the research question, objectives, contributions and structure of this argument.

Section 1.1 describes the motivations and the challenges behind this research. Section 1.2 explores the problem statement in particular, including the research question while Section 1.3 discusses the research aims and objectives. Section 1.4 identifies the significant contributions of the researcher and her supervisors to this research and the related publications conducted under the work in this thesis. Finally, Section 1.5 briefly summarizes the structure of the thesis.

1.1 Research Motivation

Device-to-Device (D2D) communication has been broadly recognized as a promising component of the next generation 5G cellular networks [15]. Notwithstanding, D2D communications have received significant consideration both in industry and academia due to the growing number of applications and services that can leverage proximity oriented communication, including local services, content sharing, gaming, group multicast, context-aware applications [33].

On the other hand, due to the intense demand and the benefits of D2D communication in various and significant areas, new severe security threats are expected on Device-to-Device network. Accordingly, this prevents practically a successful deployment of D2D communications. Researchers focus much more on the connectivity on D2D. However, the security issue needs more consideration for practical applications. Like this, the problem of D2D security is still less addressed in both academic and industrial fields [13].

Furthermore, the growth in computation, sensor and communication capabilities of mobile devices make us move towards advanced mobile security threats. The mobile malware attack is one of the security threat that formalizes a serious security risk that threatens to retard the large-scale reproduction of wireless applications [38].

Malware threats rocketed on mobile devices and can bypass the security mechanisms of the devices using advanced techniques [71]. Furthermore, the gap between security systems and real world security is only growing bigger [9]. Although the security schemes proposed to isolate the infected devices and prevent malicious attacks, e.g., DoS, the isolating and the tracking of the infected devices are still challenging [48].

Motivated by all previous trends, lightweight, efficient countermeasures, and designs to hinder the mobile malware infection are highly required. To solve these security problems in a D2D network, a novel secure and energy-aware routing protocol based on game theory is proposed in this thesis. This proposed routing protocol studies the interaction between the network and the attacker for security enhancement and to hinder the malware attack.

1.2 Problem Statement

Due to the explosive growth in demand for Device-to-Device Communication in large areas, it has become an attractive target for attacks. Accordingly, new severe security threats are expected on Device-to-Device network such as inference attack and DDoS [16], [78].

In fact, the growth in computation, sensor, and communication capabilities of mobile devices makes us move towards advanced mobile security threats. Also, cyber security is moving from infrastructure to advanced mobile infrastructure-less threat [49].

Recently, the attackers have been focusing their efforts on mobile platforms. There has been a sharp rise in the number of reported new mobile OS vulnerabilities [3] from 115 in 2009 to 163 in 2010 (42% more vulnerabilities).

In 2015, there were 1.966.324 registered notifications of attempted malware infections that aimed to steal money via on-line access to bank accounts. The annual statistics for 2015 are based on data received between November 2014 and October 2015 [5]. Therefore, mobile malware attacks represent a serious security risk that threatens to retard the large-scale reproduction of wireless applications [38].

Furthermore, the malware attacks rocketed on mobile devices can bypass the security mechanisms of the devices using advanced techniques

[71] as well as the tracking and isolating of infected devices remains very challenging [48]. However, the existing security schemes for malware attacks are not efficient [48].

A noteworthy concern is that the malware attacks are happening at a rate far surpassing the evolution of security techniques. The gap between security systems and real world security is just becoming bigger [9]. However, the problem of Device-to-Device security is still less addressed in both academic and industrial fields [16].

As a result, the mobile malware threats are soon to be considered a hot topic. To accomplish secure, intelligent Device-to-Device Communication in the future, research issues need to be addressed [16].

As a first step toward thwarting the success of the malware attacks, we seek to mitigate the mobile infection. Motivated by all previous trends, lightweight [16] countermeasures hinder the mobile malware infection are highly required [48].

1.2.1 Research Question

How to hinder a malware attack during the infection phase in multi-hop Device-to-Device network using a lightweight energy-aware solution?

The traditional routing protocols like (DSR) [36] and (AODV) [62] establish the network connectivity from the source node to target node using the single shortest path for message delivery. These protocols utilize the single path and are typically prone to failure or malicious attacks and with the emphasis on cloud computing and distributed computing, the network is further exposed to security attacks.

Accordingly, these deterministic approaches are not flexible for the variable dynamic network conditions [16]. In addition, the operational constraints of the devices and the security requirements are not considered necessary for the D2D network.

Question: Is it possible to design an intelligent and secure routing protocol that can distribute the data traffic in such an intelligent way to achieve security, considering the resource constraints through optimal routes regarding malware detection efficiency and energy awareness?

In this thesis, a secure and energy-aware stochastic routing protocol has been designed based on a game-theoretic approach for D2D network. The proposed routing protocol computes several routes between the source-target node pairs, then formulates the routing probabilities, which optimize the security regarding malware detection efficiency as well as consider the energy constraints of the devices for the route availability, network lifetime, and long-term connectivity.

Accordingly, routes that are created have probabilities within a set of constraints. Then, the secure and energy-aware route is selected stochastically from these routes to forward the messages.

1.3 Research Objectives

The principle goal of this research is to present a novel secure and energy-aware routing protocol based on the game theoretical model for security enhancement in Device-to-Device network considering both the security requirements and the system energy constraints.

Another goal is to evaluate the performance of the proposed protocol using a packet level network simulator compared to other traditional protocols. All the more succinctly, our goals are summarized as follows.

- To propose a novel end-to-end probabilistic energy-aware routing protocol based on game theory for D2D communications for security improvement by mitigating mobile malware infection. Malware detection is considered by investigating the mobile malware detection techniques residing on devices to detect the malware before it infects the device.

- To compute several routes between the source-target node pair, then investigate the selection of the optimal end-to-end path. The optimal routes are identified regarding malware detection efficiency and considering network lifetime by balancing the energy load among all a set of computed routes.

- To evaluate and validate the effectiveness of the proposed routing protocol by comparing the simulation results of the proposed protocol with other non-strategic traditional protocols and another strategic customized protocol in case of three different attack cases.

1.4 Thesis Contributions

Based on the research objectives mentioned in the previous section, the researcher and her supervisors have proposed a novel end-to-end secure stochastic routing protocol based on a game-theoretic model for D2D communications that improves the security and considers the system energy constraints. The following are the thesis contributions.

- A new end-to-end secure routing protocol based on a game-theoretic model for D2D communications has been proposed that takes security defense routing decisions strategically.

  The proposed routing protocol computes several routes between the source-target node pair, then formulates the probabilities which optimize the security regarding malware detection efficiency and energy awareness.

  Accordingly, paths that are created have probabilities within a set of constraints. Then, the secure and energy-aware route is selected stochastically from these routes to forward the messages.

- The proposed routing protocol considers the energy constraints of the devices to guarantee the path availability, and this improves the network survivability by maintaining the network connectivity.

- The proposed routing protocol studies the interaction between the attacker and the defender as a zero-sum repeated game taking into account the attacker's behavior. It has investigated a dynamic scheme regarding calculating malware detection rate and new malware behaviors.

- The performance and effectiveness of the proposed routing protocol have been evaluated through simulations using network simulator Omnet++.

  Through extensive simulations, the performance of the proposed routing protocol has been validated. The simulation results have been illustrated, demonstrating its effectiveness and how it outperforms the traditional routing protocols and other strategic customized protocol regarding overall expected payoff and detection rate in case of three different attacks distribution.

1.4.1 Published Papers

The papers that have been published in this research [28], [27]:

- "Malware-defense Secure Routing in Intelligent Device-to-Device Communications".

- "Mitigating Malware Attacks via Secure Routing in Intelligent Device-to-Device Communications".

1.5 Thesis Organization

The rest of the thesis is organized as follows.

- Chapter 2 describes the background of the research problem that is presented in this thesis. This chapter presents an overall survey of D2D communication security research by providing a detailed explanation of the D2D security requirements, vulnerabilities of the mobile devices, malware attacks, and evaluation of the existed security schemes.

  For the research question and objectives considered in this thesis, chapter 2 provides an adequate background to understand the research problem and the idea. This chapter reviews the detailed state-of-the-art regarding game theoretic approach in relevant research fields that combines four areas: security, routing, D2D network, and intrusion detection.

- Chapter 3 presents the proposed game theoretic protocol for security in Device-to-Device network. It describes the examined system model, attack model, and game model.

  The proposed secure routing protocol based on game theoretic approach is discussed by setting the system model and its components, including the attacker model and presenting the utility functions for both the defender and attacker.

- Chapter 4 describes and discusses the simulations of the results of the proposed routing protocol. It discusses the evaluation, interpretation of the results against the background of the relevant literature in 3 different attack cases.

  The performance of the proposed secure routing protocol is evaluated regarding the overall expected payoff and the detection rate. Also, a critical assessment is carried out to compare the results for three routing protocols (SCP, DSR, AODV) in the case of three different attack cases with the proposed secure routing protocol.

  The performance of the optimal defense strategy for the proposed protocol regarding the detection rate of the malicious messages has been evaluated. The effectiveness of the proposed routing protocol is compared with other non-strategic protocols DSR and AODV as well as with another strategic customized protocol.

- Finally, Chapter 5 concludes this thesis explaining the results and findings and highlights the main contributions of the thesis on the research objectives. It defines the limitations of the research and the main avenues for future research orientation in the field of security for Device-to-Device communications. Finally, some suggestions for future work are given.

Chapter 2

Background and Literature Review

This chapter provides the adequate background to understand the research problem presented in this thesis and reviews the detailed state-of-the-art regarding game theoretic approach in relevant research fields.

In Section 2.1, the fundamentals of the characteristics of Device-to-Device Communication and the Device-to-Device applications are introduced. It also mentions the security requirements needed in Device-to-Device Communications and emphasizes the security issues and the challenges with Device-to-Device Communications.

Section 2.2 gives an overview of the game theory approach and its importance. It also investigates the game theoretic applications for security and intrusion detection in the network.

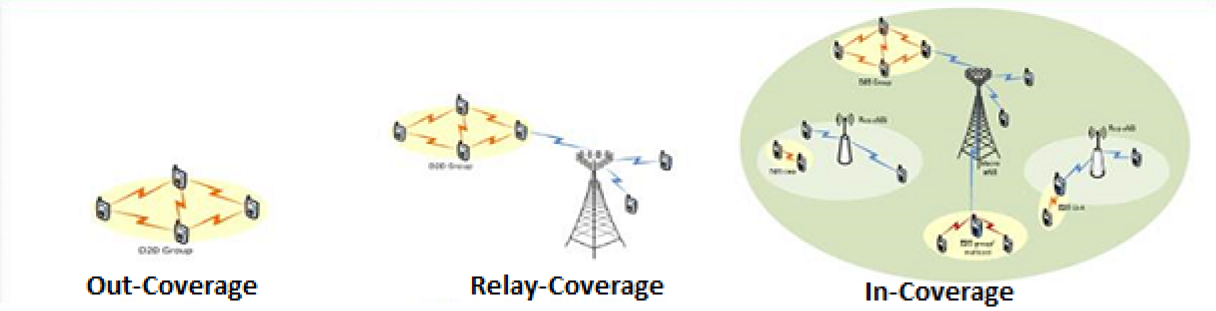


Figure 2.1: D2D communication application scenarios [2]

2.1 Device-to-Device Networks

2.1.1 Device-to-Device Characteristics

Due to the recent rapid growth in demand for the mobile communication network, new technologies are proposed to improve throughput, communication delay and computational offloading [32]. Device-to-Device (D2D) Communication has been widely recognized as a promising and innovative feature of the next generation 5G cellular networks [15].

Due to D2D Communication manifold advantages, the traditional approach has gained much interest nowadays. D2D Communication provides high bit-rate, low communication delay and computational offloading as well as high throughput in the cell area [33].

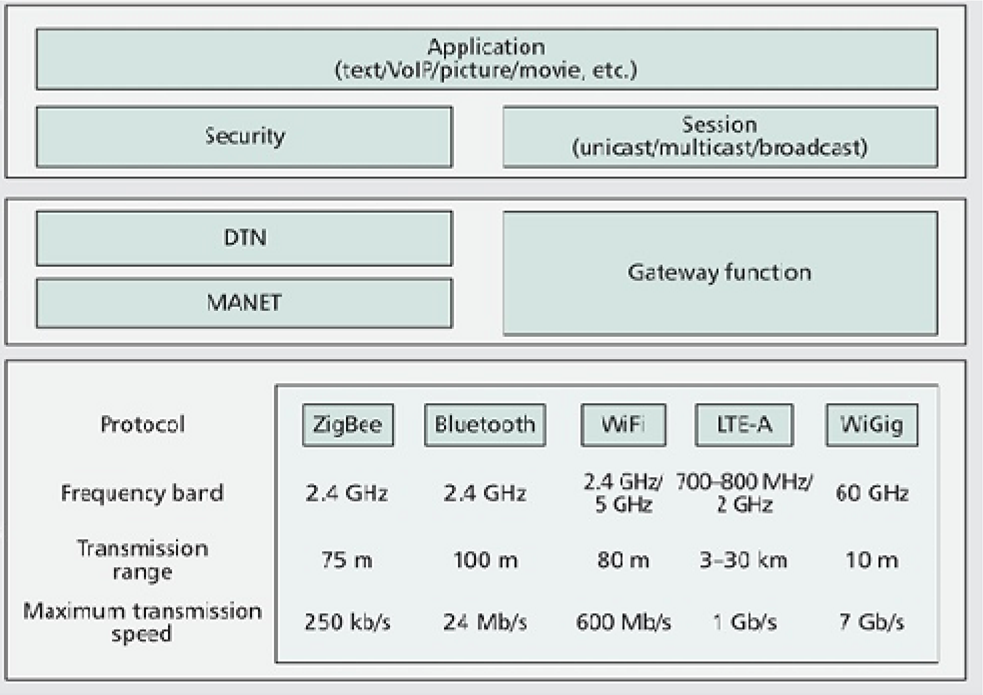
D2D Communication is proposed as a mean of gathering the proximity, hop gains and reuse [33]. Furthermore, it enables direct communication between two mobile devices on a cellular network without passing through a base station or core network. The communication can occur on the mobile spectrum (e.g., Long Term Evolution (LTE)) or unlicensed spectrum (e.g., IEEE 802.11) [15], such that the D2D short range provides higher data rate and better energy efficiency than cellular technologies.

D2D is categorized into three exemplary types according to infrastructure and involved network entities [73] as shown in figure 2.1.

- In-Coverage: where D2D Communications between devices are controlled by the Base Station (BS).
- Relay-Coverage: where user devices exist at the cellular edge. D2D Communication extends the coverage of the BS through relaying the device information through the other covered devices.
- Out-Coverage: where the D2D Communication takes place in case of absence of the network coverage such that D2D Communication looks like MANET.

Also, the inherent characteristics of a regular D2D Communication are unlike the other networks which include network entities to carry out some network functions. Accordingly, there are certain features of a standard D2D Communication include the following [16].

- Heterogeneity of devices: Devices are different in functionality and applications.
- Device cooperation: Any device can communicate anytime in a cooperative manner with any other device.
- Device constraints: Devices have resource constraints like battery life, memory, and processing power.
- Self-organization and self-configuration: Devices in D2D networks have self-organizing capabilities and devices can determine the configuration parameters autonomously.
- Unpredictable mobility: D2D networks consist of highly mobile and stationary devices. Mobile devices can be rapidly repositioned and


Application
(text/VoIP/picture/movie, etc.)
Security
Session
(unicast/multicast/broadcast)
DTN
MANET
Gateway function

Protocol	ZigBee	Bluetooth	WiFi	LTE-A	WiGig
Frequency bard	2.4 GHz	2.4 GHz	2.4 GHz/ 5 GHz	700-800 MHz/ 2 GHz	60 GHz
Transmission range	75 m	100 m	80 m	3-30 km	10 m
Maximum transmission speed	250 kb/s	24 Mb/s	600 Mb/s	1 Gb/s	7 Gb/s

Figure 2.2: Factors for multihop D2D communications [55]

may get disconnected from the network, which causes unpredictable changes in the network topology.

- Multi-hop communication: Devices have low power transmitters and receivers. Accordingly, each device can act as a router and cooperate to share, collect, and relay information over multiple hops.

D2D communication between devices can be directly or typically be multiple hops in nature as in (IoT), the device will communicate with each other independently without any centralized control. In multi-hop D2D network, the devices cooperate to share, collect, and relay information in a multi-hop manner. Figure 2.2 summarizes the major critical factors required for the multi-hop D2D communication systems [55].

Due to the recent market demand for new services such as context-aware and proximity services, the industry is exploiting new use cases and new business models. These use cases are based on D2D communication as shown in figure 2.3 [15], e.g., local services, content sharing, gaming, group

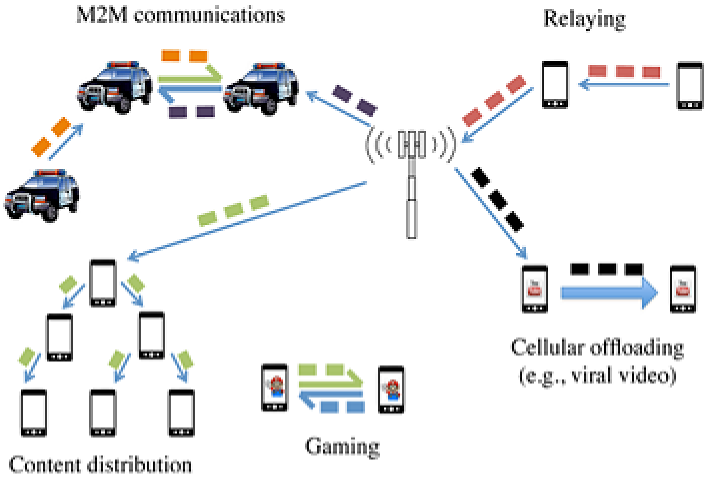


Figure 2.3: Use-cases of D2D communications [15]

multicast, and context-aware applications. Therefore, D2D is expected to be a vital technical component in Internet of Things (IoT) [16] and will play a significant role with the next generation 5G.

2.1.2 Device-to-Device Applications

D2D communications have received significant recent attention both in industry and academia due to the growing number of applications and services that can leverage proximity oriented communication, including pervasive healthcare monitoring, social networking, public safety and rescue and location-based services [15]. Furthermore, D2D communication supports new models based on the proximity of the devices, e.g., social networking applications and facilitates new types of Peer-to-Peer (P2P) services [15].

The importance of multi-hop D2D communication is realized in the disaster scenarios and public safety communication where the communication infrastructure is physically damaged, and the communication is enabled among devices independent of the network operator [55]. However, relay by mobile terminals (smartphones, laptops, tablet PCs) could deliver messages through multi-hop D2D communication. Furthermore, the de-

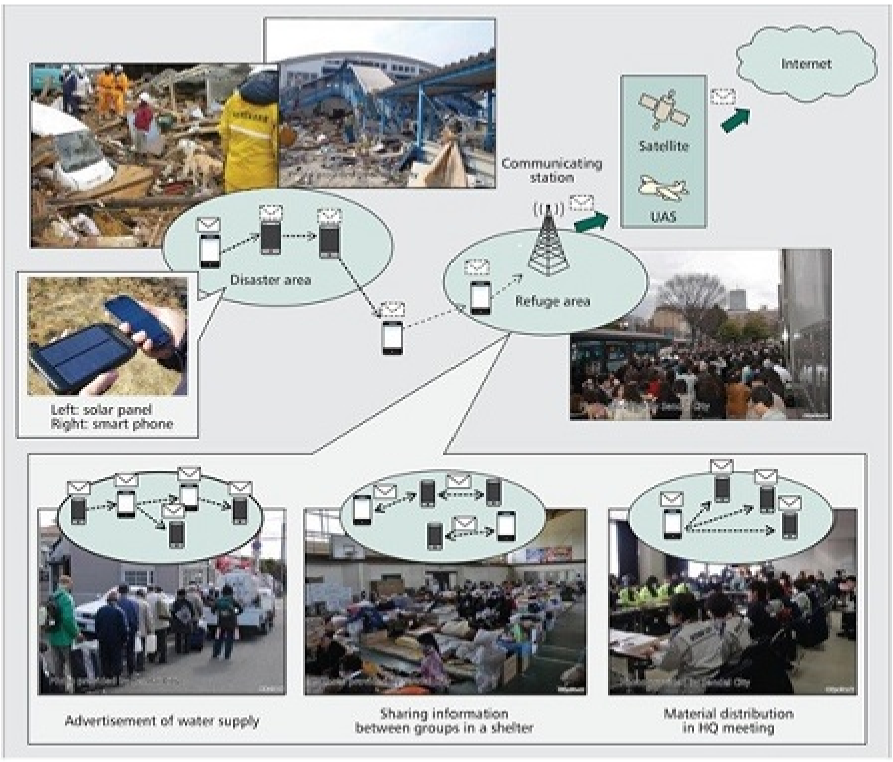

Internet
Satellite
UAS
Communicating station
Disaster area
Refuge area
Left: solar panel
Right: smart phone
Advertisement of water supply
Sharing information between groups in a shelter
Material distribution in HQ meeting

Figure 2.4: D2D application in Disaster Relief [55]

centralized infrastructure-less multi-hop communication plays an essential role in the disaster salvage and emergency cases [55]. Relay by mobile terminals can be the unique option for emergency situations and in designing systems for disaster recovery, where there is no communication infrastructure [55] as shown in figure 2.4.

Additionally, it can be applied for commercial purposes (e.g., advertisement, coupons, and flyer distribution) by delivering advertisements to subscribers when they are in the surrounding area instead of the traditional methods such as emails [55]. Another important application is the sharing of information (i.e., exchange of private message, document) among groups in places outside the cellular coverage (e.g., mountains, island, military domain). Additionally, D2D Communication facilitates the sharing of information among groups of people where the mobile communication is highly congested [55].

2.1.3 Classifications of Routing protocols for Intelligent D2D Communications

D2D communication between devices can be directly or typically be multiple hops in nature as in (IoT), the devices will communicate with each other independently without any centralized control. In the multi-hop D2D network, the devices cooperate to share, collect, and relay information in a multi-hop manner, thus performing routing functions.

Traditional routing protocols, e.g., DSR and AODV determine the shortest path taken from messages traversing between a source node and target node. However, these deterministic approaches are not flexible for the unpredictable dynamic network conditions. In addition, the operational constraints of the devices [16] and the security requirements are not considered necessary for D2D network. Accordingly, the communication between devices should be achieved through efficient routing algorithms, which support energy efficiency and scalability.

As a result, intelligent algorithms are needed for the routing processes to accomplish an end-to-end communication between devices. The classifications of the intelligent routing algorithms on D2D characteristics are as follows [16].

- Stochastic/Probabilistic Algorithms: These algorithms have individual optimization objectives, and formulate routing probabilities that optimize the criteria of interest. These routing algorithms are suited for the dynamic network conditions and the unpredictable mobility of the devices and take into consideration the operational constraints than the deterministic approaches. Also, the traditional deterministic routing protocols are single-path routing protocols that leave the route at the risk of interception as it is predictable and easy to be eavesdropped and determined by the attacker.

Examples of these algorithms are proposed for optimization objectives in the wireless multi-hop network [65], [43], and another set of proposed protocols based on game theory approach to security problems [18], [19], [17], [67].

- Bio-inspired Algorithms: These algorithms address the challenges in large-scale networks by considering the heterogeneity of devices, decentralized and self-organized systems, and the resource constraints. Examples of these algorithms include swarm intelligence-based algorithms proposed for preventing a DoS attack such as the ant colony optimization (ACO) [37] and the human immune system [61].

- Hierarchical Algorithms: These algorithms are classified to tree-based and cluster-based algorithms [44]. Some features in these algorithms limit their general use for D2D communications [16].

- Context-aware Algorithms: These algorithms use the gathered context and information about the status of the devices within the network and select the best routes based on the collected information.

In this thesis, we have chosen the Stochastic/Probabilistic algorithm in the design of our intelligent proposed routing protocol of multi-hop D2D communication. Since the traditional routing protocol is a single-path routing, which relays the packets over a single path from the source device to target device, this is considered a single point of failure. Once the route is compromised, all the connections will be interrupted. Accordingly, this routing protocol cannot solve the challenges that are raised from inherent characteristics of D2D communications [16]. Furthermore, these single-path protocols leave the routes at the risk of the eavesdropping and interception because these routes will be predictable and easy to be determined by the attacker.

The stochastic routing algorithms have optimization objectives and are better suited for D2D communication rather than the other deterministic traditional approaches [16]. These algorithms explore the existence of multiple paths between the source and target node pair and select the path stochastically from those paths to forward the packets to minimize the predictability of the decision by the attacker.

Therefore, this algorithm can support the security requirements, consider the unpredictable mobility and the constraints of devices, as well as improve the network survivability by maintaining the network connectivity.

2.1.4 Security Requirements in D2D Communications

The authors of [73] have identified the critical security requirements in D2D communication recently and have evaluated the existed security schemes. The security requirements for the D2D communication system should achieve Confidentiality and Integrity, Authentication, Privacy, Non-Repudiation, Revocable, Availability, and Dependability.

On the other hand, they have investigated the existing security schemes that have been developed for D2D communications since 2000, which are classified to four primary design purposes about security as follows: Authentication and Key Management, Secure Routing, Access Control, and Physical Layer Security.

2.1.5 Security Challenges in Device-to-Device Communications

Due to sufficient demand and benefits of D2D communication in different areas, new severe security threats are expected on D2D networks. Furthermore, the direct connections between devices via short-range technologies (i.e., Wi-Fi, Bluetooth) are more vulnerable to security threats [49]. Therefore, D2D communication has become an attractive target for attackers due to its explosive growth in demand of D2D in vast areas.

Despite the importance of the security requirements needed in D2D communication [73], the security requirements for multi-hop D2D communication depend on the type of the application. While some applications may require less security, other applications may require more security (i.e., private message exchange, distributing important documents). As a result, the security concerns in the multi-hop D2D communication should be addressed to support all the possible applications [55]. However, the academia and industry have not yet investigated these security issues of the D2D communication seriously [13].

In fact, the impressive growth in computation, sensor and communication capabilities of mobile devices opens the door to the cyber criminals that explore new avenues for mobile malware attacks and makes us move towards advanced mobile security threats [49]. Additionally, mobile devices are prone to new severe threats [8] as they are capable of initiating advanced security attacks without passing through a powerful centralized entity. It is worth mentioning that cyber security is moving from infrastructure to advanced mobile infrastructure-less threat [49].

As a result, mobile devices are considered an attractive launching pad for mobile malware attacks [8]. Recently, the attackers have been focusing their efforts on mobile platforms. There has been a sharp rise in

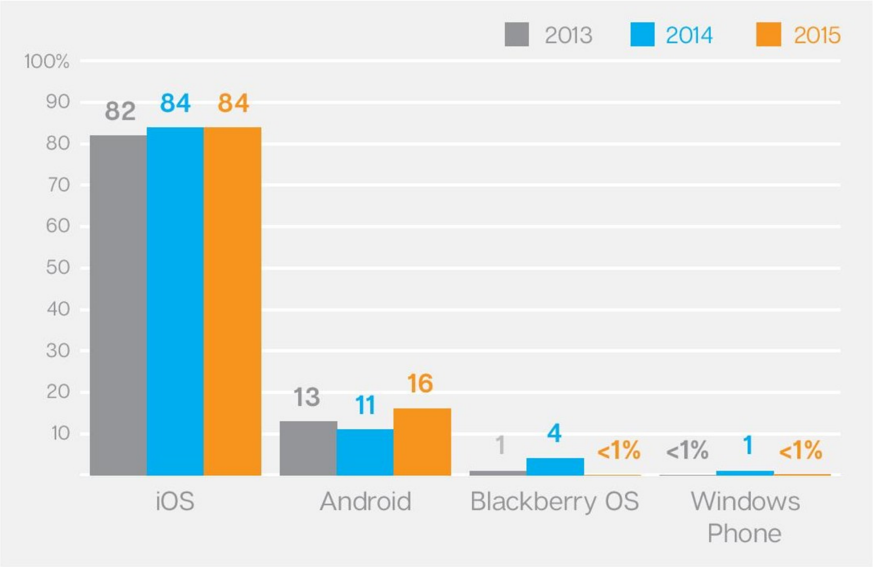


Figure 2.5: Mobile vulnerabilities by Operating System [4]

the number of reported new mobile OS vulnerabilities [3] from 115 in 2009 to 163 in 2010 (42% more vulnerabilities). In the same trend, researchers give increasing attention to the security issues. Recently, iOS vulnerabilities have recorded for the greatest number 71 of mobile vulnerabilities as shown in figure 2.5, with research often fueled by the interest to jailbreak devices or gain unauthorized access to install malware [4].

In 2015, there were 1.966.324 registered notifications of attempted malware infections that aimed to steal money via on-line access to bank accounts. The annual statistics for 2015 are based on data received between November 2014 and October 2015 [5] as shown in figure 2.6 and figure 2.7. These graphs demonstrate the number of malicious applications doubled in 6 months to reach 700.000 malware for Android in June 2015 [10].

Therefore, mobile malware attacks are becoming a significant threat to the mobile wireless network. Mobile malware attacks formalize a serious security risk that threatens to retard the large-scale reproduction of wireless applications [38]. Additionally, mobile malware can disseminate offensive content or provide unauthorized access to the personal and finan-

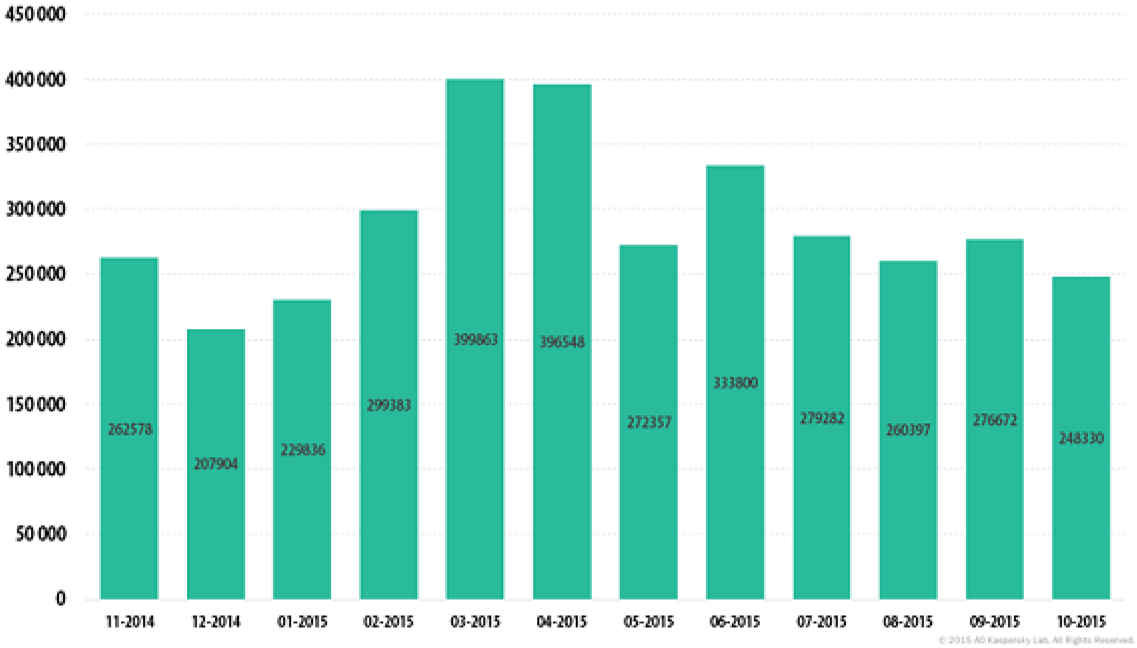


Figure 2.6: Number of users attacked by financial malware, 2014-2015 [5]

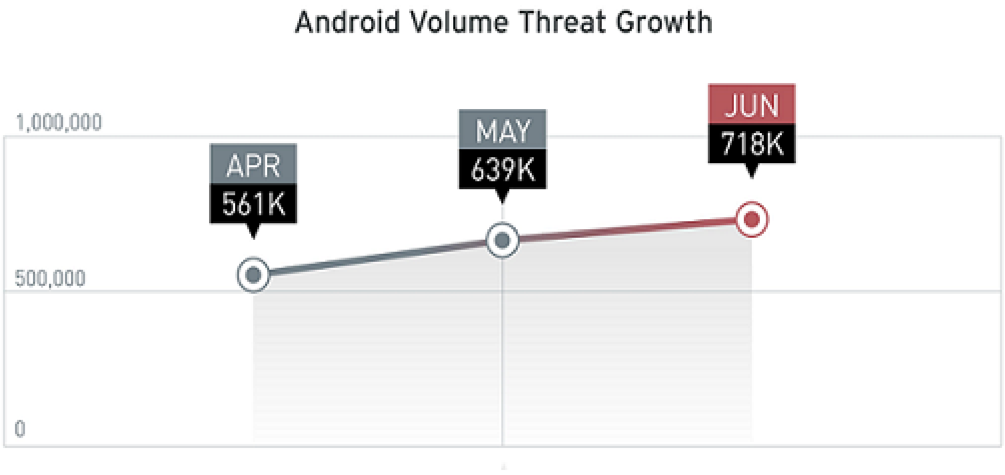


Figure 2.7: Malware Threat Growth [10]

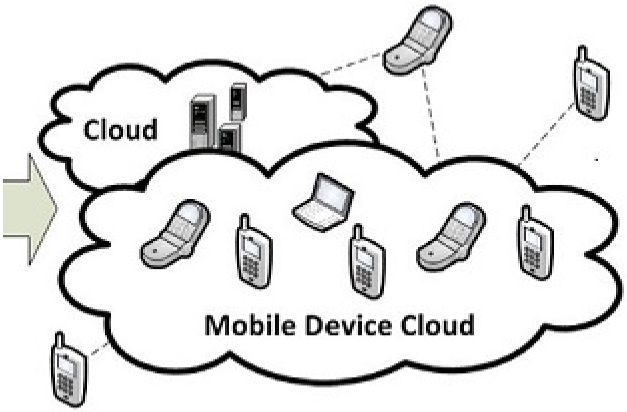


Figure 2.8: Mobile Device Cloud [63]

cial information (e.g., mobile banking, private data, and SMS). Furthermore, these attacks sometimes attempt to disrupt the normal functions of the devices [38], alter the network traffic, or even kill the device or launch epidemic attacks. However, this research field is still immature and unexplored in depth [16], [55].

As a result, the mobile malware threats are to be considered a hot topic in the next future. Researchers have recognized the security threat of these attacks in a mobile wireless network. Accordingly, they have been studying the maximum damage of malware attacks taking the dynamic behavior of the malware and the evolution of future malware into consideration [38], [39].

Researchers focus much more on the connectivity. However, the security issue has to receive more attention for practical applications [55]. Researchers have been studying the malware spread and propagation within the wireless network and cellular networks. However, no studies are conducted so far on disconnected distributed mobile networks such as Mobile Device Cloud (MDC) [48], [49], [63] as shown in figure 2.8. Sophisticated malicious attacks such as targeted attack and epidemic attack are introduced in MDC, where the infected devices are coordinated together forming a mobile distributed botnet. Once MDC is infected, the attacker launches malicious attacks from the infected nodes. Malware attacks leverage the advantages of the D2D communications in MDC via short range wireless technology in masking the malicious infection and increase the propagation rate [49].

On the other hand, the mobility of the devices can increase the malware infection and propagation rate. Also, applying the prevention techniques that hinder the malware infection expensive in regards to energy and time. Accordingly, the tracking and the isolation of the malware attacks are very challenging [48]. Therefore, to accomplish secure and intelligent D2D Communication in the future, research issues need to be addressed [16].

Motivated by all previous trends, lightweight, efficient countermeasures, and designs to hinder the malware infection are highly required. As a result, the mitigation of the malware infection is considered a first step toward thwarting the success of the malware attacks.

2.2 Applications of Game Theory to Network Security

To enhance and improve the security and the performance of the complicated wireless systems which cannot be modeled using the traditional methods, a game theoretic approach is introduced. This section provides an overview of the game theory approach and summarizes some basics and definitions of the game model along with related work of applications of game theory to enhance security and the intrusion detection in the mobile network.

2.2.1 Game Theory

At first, the game theoretic approach has been used mainly in economics for the modeling competition among organizations and companies. Then, it was utilized in other areas including security, politics, and biology. The game theoretic approach has been recognized recently to enhance and study the network security and privacy in both wired and wireless networks [34], [41].

Researchers contributed to the game theory development and wrote books about it [47], [30], such as John Nash [51] who made fundamental contributions, best known of which is Nash Equilibrium. Since 1940s, researchers have developed different concepts in game theory, such as a cooperative game, non-cooperative game, and repeated games.

The game theory proved to be a powerful mathematical and analytical tool for the study of the security problem in the network. Furthermore, the game theory addresses the different forms of the network security challenges and mobile applications, where the players with opposite aims and goals compete with each other [45].

2.2.2 Game Theoretic Formulation

Game theory focuses on the relationship between the decision-makers in the game model, then predicts their optimal decisions. A game model consists of three main components: a set of players, a set of strategies or actions, and utility or payoff function.

A *player* is a decision maker who acts in a way that outcomes in mutual or conflicting consequences. Game theory provides the best decision techniques that are assuming that the players are rational and they decide strategically about their actions taking into account the behavior of the others.

Strategies aim at solving and relieving the problems and providing the possible solutions. Strategies are categorized as the following.

- *Pure strategy*: A player chooses to take one action with probability one.
- *Mixed strategy*: A player chooses randomly between the available possible actions. This strategy is defined as a probability distribution over all the available pure strategy.
- *Dominant strategy:* A strategy that in any case is the best action chosen by the other players.

Strategic Game definition:

- set of players N={1,.....n}
- each player has a set of possible strategies.
- each player chooses one strategy $s_i \epsilon S_i$
- $s = (s_1, ...s_n)$ is the vector of strategies for all players called also strategy profile or state. let $S = S_1 X......X S_n$
- Utility or payoff for each player: assigns cost or utility to outcomes. For player i, the cost function or the utility function is:

  $C_i : S \rightarrow \Re$ or $u_i : S \rightarrow \Re$
- *Pure Nash Equilibrium* (PNE)*:* A Strategy vector is a PNE if it is

S_i	set of all available strategies to player i
s_i	action of player i
s_{-i}	actions of all players not player i
u_i	payoff to player i
$u_i(s)$	payoff of player i when s is played
$u_i(s_i, s_{-i})$	expected payoff to player i when other players play s_i

Table 2.1: Strategic game notation

stable such that for every $i \epsilon N$ and $s_i \epsilon S_i$:

$u_i(s) = u_i(s_i, s_{-i}) \geq u_i(s^{`}{}_i, s_{-i})$

- *Mixed Nash Equilibrium:* It is a mixed strategy profile $x = (x_1, ..., x_n)$, such that a player could choose a profile based on mixed strategy.

Theorem **(Nash's Theorem [51])**

John Nash, as part of his Ph.D. thesis, has proved in 1950 that:

Every game that has a finite strategic form, with finite numbers of players and a finite number of pure strategies for each player, has at least one Nash Equilibrium (NE) involving pure or mixed strategies.

- *Zero-sum Games* is a mathematical representation of a problem in which each player's gain (or loss) of utility is exactly balanced by the losses (or gains) of the utility of the other players. Such that, when the total benefits of the players are added up, and the total losses are subtracted, they will sum to zero [26].

$\sum_{i \epsilon N} u_i(x)$ = 0, for each $x \epsilon N$.

Two players zero sum games:

$u_2(x)$ = - $u_1(x)$, for each $x \epsilon X$

Minimax Theorem (John von Neumann) [53]

The optimal strategy to employ is one that maximizes your minimum gain (or minimizes your maximum possible loss).

The theorems state that for every finite two-person zero-sum game there exists a strategy for each player, such that if both players employ the strategy, they will arrive at the same expected payoff. This means that one player will lose the maximum of the minimum that he expected to lose, and the other player will win the minimum of maximum he could have possibly won.

So, in a Maximin strategy you try to maximize your expected payoff while assuming that given whatever strategy you use, your opponent will use a strategy that minimizes your expected payoff. In brief, you are trying to maximize the minimum of your expected payoff.

This thesis assumes that a two-player zero-sum game is a pair of strategies that a rational pair of decision makers' might choose to maximize their payoffs. Each decision maker is rational and knows his actions, form expectations about any other decision makers' actions, has preferences, and chooses his action according to an optimization process.

2.2.3 Game Theoretic Approach for Network Security

Due to the continuity of the evolution of networks and mobile applications, the security requirements have revolutionary modified. Theoretical models play a vital role in network security and provide the tool for modeling situations where security-related decision makers have to do specific actions [45].

In such models that target the network security problems, the decision makers play the role of either the attacker or the defender with different aims. An attacker attempts to infringe the security or cause damage to the network, while the defender tries to evaluate and take enough measures to improve and enhance the system security design [45]. Accordingly, game theory has become one of the best analytical tools used for strategic decision making and the design of the efficient security protocols in the networks.

Since the mobile networks play a vital role in the modern society, we are facing the evolution of new severe types of security problems and mobile attacks. Accordingly, the network agents (i.e., users, mobile devices, software) required being involved in fulfilling the security requirements.

Game theoretic security-related decisions help to allocate limited resources and estimate the expected risks and loss. Security games are considered as a special class of games that study the interaction between malicious attackers and defenders [45].

Security games solutions are applied as a fundamental for formal decision making and algorithm development as well as for predicting attacker behavior and actions. According to the type of available information to the players, the action spaces and the payoff, security games can be classified from simple game to more complicated stochastic and incomplete information game.

Furthermore, they are applied to the security problems ranging from intrusion detection to privacy in MANET, vehicular, and mobile networks [45], [60].

2.2.4 Related Work

This section reviews the state-of-the-art regarding game theoretical approaches at the intersection between 4 fields: security, routing, intrusion detection, and Device-to-Device network. This set of work proposed to enhance and optimize the intrusion detection.

This section gives a detailed literature review of the examined works and concludes by comparing this state-of-the-art in a table.

- In [59], Paramasivan *et al.* proposed an approach that obtains a threshold value that used to design and develop a secure routing protocol to detect and find the malicious activities.

  They applied a dynamic Bayesian signaling game model to study the interactions between regular and malicious nodes. The normal nodes monitored and evaluated their neighbors by using reputation system, then to update their beliefs using Bayes rule.

  This game achieved the Perfect Bayesian Equilibrium, analyzed different strategies and discussed the importance of focusing on minimizing the malicious node's payoff and on increasing the normal node's payoff when they follow the Nash Equilibrium.

- In [25], Debjit *et al.* proposed a game theoretic scheme for efficiently detecting the malicious nodes that dropped the packets in MANET. This scheme is based on a modified AODV protocol such that the packets transmitted through end-to-end least cost path in terms of amount of idle time only from the source to the destination node.

  There is a predefined threshold limit, and once any misbehaving node reached this limit, it will be isolated from the network. This scheme proved the smallest idle time and greater availability.

- Bohacek *et al.* [18] introduced a stochastic routing based on game theory that mitigates the effects of interception, eavesdropping, and improves fault tolerance.

  They considered zero-sum games between the attacker and the defender by formulating the problem as an optimization problem with timely cost. They presented two techniques to compute multi-path routing tables and select among these paths randomly to forward the packets.

- Bohacek *et al.* [17] introduced Secure Stochastic Routing Protocol (SSR) to enhance security by making the eavesdropping and interception maximally difficult. This protocol explores multiple paths, and the packets are forwarded over multiple paths according to a certain probability.

  Accordingly, SSR minimizes the effects of eavesdropping, interception, and traffic monitoring attacks and increases the throughput of the network.

- In [14], Raja Wassem *et al.* proposed a trust-aware wireless routing protocol for detection and isolation of malicious nodes in the network.

This protocol aims at establishing the optimal route with trusted nodes and forwarding the packets efficiently from the source node to the destination node. This protocol shows high delivery ratio and efficient in routing overhead in the presence of malicious nodes.

- In [57], Emmanuel *et al.* proposed secure routing based on game theory. The proposed protocol determines the lowest risk path to forward the message considering the cost for message forwarding and inspection and quality of service. They modeled the game as a zero-sum complete information game between network and attacker. They derived the defender's strategy for the network to study the security damage when the attack is succeeded based on complete information. However, the authors did not consider any dynamic scheme to derive the defense strategies. They did not consider either the fast malware evolution or the changes of the detection capabilities of the devices. The work done in this thesis has been inspired by [57], we extend the model by considering another security parameter and energy constraints in our game model.

- Ribeiro *et al.* [66] proposed distributed stochastic routing protocol to find the rate-optimal routes in the wireless multi-hop network. The proposed protocol matches the random nature of the mobile wireless network.

  They considered three rate optimal criteria, which are practical for distributed scheme, which includes maximization of the minimum rate, a weighted sum of the rates, the product of rates, and the source's rate.

- In [77], [75], [76], Yu *et al.* proposed the secure routing and packet forwarding game is submitted, and they used game theory to study the interaction between the good nodes and malicious nodes under noise and imperfect monitoring.

They derived the optimal defense strategies with extensive evaluation of the effectiveness of these strategies. The work above considered only the insider attackers.

- In [72], Swetha. N *et al*. proposed a dynamic mean field game theoretic method for optimal detector algorithm for detecting polymorphic malware.

  Furthermore, they introduced polymorphic signature scheme to address the problem of sharing the false evidence from malicious nodes by studying the interaction among the malicious nodes and legitimate nodes. This method proved high detection rate and more efficiency.

- Mohi *et al*. [46] proposed a secure routing protocol that prevents passive denial of service attacks and enforces node cooperation. This scheme based on a Bayesian game that studies the interactions between monitoring devices and nodes of the network.

  Local Intrusion Detection System (IDS) monitors the nodes in each stage of the game using the updated beliefs about the nodes then inform the central IDS about the malicious nodes.

  Then the central IDS will notify the whole network and local IDS will isolate the malicious nodes from the routing functions. The number of dropped packets due to selfish nodes is decreased, while the throughput of the network is high.

- A. Agah *et al*. [11] proposed a mechanism for the prevention of DoS attacks. The proposed game theoretic routing protocol aims at detecting the non-cooperative nodes that dropped the packets.

They formulated the routing problem as a non-cooperative nonzero-sum two-player game between an attacker and a network. The nodes with a bad reputation will be labeled as malicious and placed on the ignore list; then this list will be broadcasted to the whole network to isolate these nodes from the network.

- M. Khouzani *et al.* [39] developed a zero-sum dynamic game model between the wireless network and the malware to investigate the dynamic behavior of the malware over the time and derive the optimal defense strategy to the network.

  They presented a robust defense two phased strategy through dynamic choices of patching and reception rates. They proved that these defense strategies could be implemented on the resource constrained wireless devices.

  The performance evaluations demonstrated that the overall damage is significantly better than the fixed patching and reception rate.

- Shamshirband *et al.* [68] proposed a combination between game theoretic approach and Fuzzy Q-learning (FQL) algorithm to prevent the DoS attack. The Fuzzy Q-learning algorithm provides learning parameters to IDS to recognize the future attacks. Once the attack is identified, the IDS will be notified of the infected node.

  The integration between the FQL and the game theory enhances the energy efficiency and leads to performance that exceeds any other defense approach.

- M. H. R. Khouzani *et al.* [40] proposed dynamic zero-sum game method to model the strategy of malware's confrontation and the defense strategy of the wireless network.

They have investigated how the network can dynamically change its countermeasures parameters to reach a defense strategy (i.e., a rate of patching) against the spread of malware. They have demonstrated that there are saddle-point strategies lead to a robust defense strategy.

- In [12], Agah *et al.* proposed a secure routing protocol aims at preventing the passive denial of service attack by detecting and isolating the malicious nodes in wireless networks.

  They modeled the problem as a repeated game between an intrusion detection system (IDS) and nodes to identify the malicious nodes that accept the forwarding of the packets then fail to do it.

  The proposed protocol enforces the cooperation among the nodes and punishment for non-cooperative behavior. Based on the reputation of the nodes, the IDS will identify the malicious nodes with a negative reputation and isolate them from participating in the routing functions.

  Accordingly, the best-chosen path is the path that consists of less number of the malicious nodes. To decrease the false alarms of the IDS, IDS will miss-detect more malicious nodes.

- In [74], Wang *et al.* analyzed the interactions between malicious nodes and regular nodes using game theory. They proposed a Bayesian game with imperfect monitoring to detect the malicious node and the game achieved the perfect Bayesian Nash Equilibrium in the mixed strategy.

Furthermore, after detection, a second game is played, so the regular node observes the behavior of the malicious node and evaluates the helpfulness of the malicious node and decides to either keep or isolate it. The game achieves the Bayesian Nash Equilibrium under the mixed strategy.

- M.Felegyhaz *et al.* [31] presented a game theoretic model to investigate the nodes cooperation using incentive mechanisms in the ad-hoc wireless network. They proposed a repeated game scheme to study the Nash Equilibrium of packet forwarding strategies with punishment strategy.

  They proved theorems with a very high probability of the Nash Equilibrium for both cooperative and non-cooperative strategies to detect the selfish nodes.

- Cho *et al.* [20] proposed mathematical models based on Stochastic Petri nets to analyze and discover the optimal rate for IDS tasks to optimize the mean time to failure of the system.

  They also discussed how to improve the reliability of a mission-oriented group communication system in MANET, given operational conditions, system failure definitions, and attacker behavior information. They also discussed how to cope with insider attacks to prolong the system lifetime.

- Shen *et al.* [69] proposed a game theoretic model to prevent the propagation of the malware in a wireless network. This model represented the malware propagation model in seven states.

  They formulated a malware-defense differential game between the network and the malware, such that the network can choose its optimal defense strategies dynamically to minimize the overall the damage cost, whereas the malware changes its strategies over the time to maximize the damage cost.

The performance evaluation demonstrated that this approach could help the network achieve the optimal defense strategies when the malware varies its strategies dynamically over the time.

- Khouzani *et al*. [38] formulated a mathematical framework to study the maximum overall damage of the malware in the mobile wireless network when the malware dynamically changes its parameters. Then they explained how to design the suitable countermeasures given the damage function of the malware.

  Finally, the numerical analysis demonstrated that the damage could be reduced when the nodes installed the patches at a maximum possible rate and chose the minimum reception gains.

- Calinescu *et al*. [19] proposed a stochastic game theoretic model considering the routing problem between k source and destination pairs. They formulated a zero-sum game between the attacker and the designer.

  The authors proved that the randomized defense strategies could minimize the effects of the attacks on the links chosen by the attacker who aims at increasing congestion on these links.

- Sarkar *et al*. [67] proposed an energy-efficient stochastic multipath routing protocol based on game theory for Mobile Ad-hoc Networks (MANETs). The proposed protocol computes multiple paths between source and destination node. Then an energy-efficient path is stochastically selected from those paths to forward the packet.

Also, this protocol provides secure data flow through random paths from the source node to the destination node in the network. The random data traffic paths minimize the jamming, interception, and hijacking data packets because the attacker needs to overhear all available paths from the source to the destination node. The performance evaluation demonstrated that the proposed protocol achieved significant performance.

We conduct a comparison with the related work based on the game theory described and mentioned in the details above. Then we conclude by identifying the contributions of this thesis.

As shown in table 2.2, a set of game theoretic routing protocols aims at optimizing the routing decision to enhance and improve the intrusion detection. They target the detection of insider attackers and isolate the misbehaving and malicious nodes.

Table 2.2: Comparison with related work

Related work	Features	Thesis' contributions
[59]	Secure routing protocol based on a dynamic Bayesian game aims to evaluate and detect the malicious nodes.	End-to-end routing protocol considers the energy constraints of the devices and targets the external attacker
[25]	Game theoretic end-to-end routing protocol seeks to identify the selfish and misbehaving nodes then isolate them.	The energy-aware and secure routing protocol targets the external attacker, not the insider selfish and misbehaving nodes.
[30]	Shortest path protocol is used by applying a repeated game model to detect malicious internal nodes.	End-to-end routing protocol targets the external attacker, not the insider selfish and the misbehaving nodes.
[75],[77], [76]	Game theoretic secure routing aims at forwarding the packets to detect and isolate the malicious nodes.	End-to-end protocol investigates the selection of the optimal routes among all the available routes and this protocol considers the energy constraints of devices and targets the external attacker.
[12], [11]	Secure routing protocol for prevention passive DoS attack as a repeated game aims to isolate malicious nodes and the optimal path with less number of malicious nodes	The energy-aware and secure route with highest detection capabilities is selected and this protocol considers the energy constraints of devices and targets the external attacker.
[46]	Secure routing protocol for prevention passive DoS attack based on a multistage Bayesian game model aims to evaluate the nodes then to isolate the malicious nodes.	End-to-end routing protocol investigates the selection of the optimal routes among all available routes and considers the energy constraints of devices and targets the external attacker.

All the previous works address the problem of isolating and detecting infected nodes, however, the tracking and isolating of the infected devices is challenging and still an open research question. We propose a novel energy-aware end-to-end secure routing protocol that aims at improving the security and hindering the malware attacks than traditional routing protocols, e.g., DSR, AODV during the infection phase.

Also, table 2.3 conducts another comparison between the proposed stochastic routing protocols and thesis' contributions, demonstrating that the related work addresses only the problems of interception, jamming, eavesdropping and hijacking. Another set of related work based on game theory that focuses on optimizing the intrusion detection such as [20], [60], [56], [42], and [74]. All the previous works aim at coping with malicious nodes and detecting the misbehaving nodes. While the proposed work [68] and [72] aims at improving the detection rate of the IDS against malware attacks. On the other hand, the work that is done in this thesis aims at hindering the malware attacks against the external attackers.

Table 2.3: Comparison with stochastic protocols

Related work	Features	Thesis' contributions
[67]	Energy-efficient stochastic multipath protocol based on game theory aims to minimize the jamming and interception	Energy-aware end-to-end stochastic routing protocol hinders the malware attacks (i.e., external attacker)
[19]	Stochastic routing protocol based on a zero-sum game between the attacker and the defender minimizes the effects of the attacks on the links chosen by the attacker who aims at increasing congestion on these links.	Stochastic routing protocol based on a repeated zero-sum game between attacker and the defender hinders the malware attacks (i.e., external attacker) and considers the energy constraints of the devices
[17]	Secure Stochastic routing protocol minimizes the effects of eavesdropping, interception and traffic monitoring attacks	Stochastic end-to-end routing protocol based on a repeated zero-sum game between the attacker and the defender hinders the malware attacks (i.e., external attacker) and considers the energy constraints of the devices
[18]	Stochastic routing based on game theory that mitigates the effects of interception, eavesdropping, and improves fault tolerance, considers zero-sum games between the attacker and the defender by formulating the problem as an optimization problem with timely cost.	Stochastic routing protocol based on a repeated zero-sum game between the attacker and the defender hinders the malware attacks by formulating the problem as an optimization problem with malware detection efficiency and route energy awareness.

2.3 Summary

In this chapter, firstly, the overview and fundamental concepts of the D2D communication, including the characteristics and applications are presented. Secondly, we have discussed the security requirements and challenges and issues that arise in the D2D communication and the proposed approach solving the security problems in the D2D networks. Finally, we have briefly described the applications of game theoretic approach for the network security. In the next chapter, we will present the proposed game theoretic routing protocol for security in D2D network in details.

Chapter 3

Proposed Secure Routing in D2D network

This chapter introduces the proposed secure routing protocol for D2D communications. This protocol called Repeated Malware-defense Secure Routing (RMSR).

Section 3.1 describes the system model and its different components. It also describes the attack model in details.

Section 3.2 presents the game model called Energy-aware Defense Routing Game (EDRG) that formulates the interactions between the attacker and the defender then discuss its components. We formulate in this section the theorem and solution of the game EDRG and describe how to solve the game EDRG.

Finally, Section 3.3 describes in details the proposed routing protocol based on a game theoretic approach called Repeated Malware-defense Secure Routing (RMSR) and presents in details its different stages.

3.1 System Description

Due to the real world, mobile cloud-based services face excessive networking latency and longer response time; D2D communications have been used for such operations that have brought the need for a large amount of messages transactions between the remote data centers and the edge network. Mobile-Edge Computing (MEC) [7] offers low latency, high-bandwidth, and real-time localized services and applications as in paradigms [48], [49], [64], and [78]. Such that the D2D communication takes place among the cooperative, mobile devices via the short range wireless technologies (e.g., Wi-Fi, ZigBee, Bluetooth).

To motivate our system model, we consider a paradigm in [78] demonstrating multi-hop D2D communication. The mobile device communicates with one another in a D2D multi-hop manner by using the short-range wireless connections (i.e., Wi-Fi) to provide low latency and fast services so that the communication between devices takes place at the application layer.

Also, there is a gateway that acts as a hub between the mobile devices in the D2D network and the other world such as a remote data center. Also, this gateway is exploited to offer several higher-level and low latency real-time local services to the mobile devices such as local storage and real-time local data processing.

The gateway provides the management of queries for the mobile users (e.g., file, information, service) in the D2D network. Accordingly, the gateway is considered as a trusted device that is responsible for addressing and handling the localized queries of the mobile users [64].

3.1.1 Attack Model

As shown in figure 3.1, a malicious device called the attacker compromised the gateway or replaced it by a fake one [70], [79]. According to this, the attacker has authorized access (i.e., root access) and can be inside the legitimate gateway interacting with the other devices as a trusted device. The attacker can inject or monitor any traffic once he takes control of gateway.

First, he starts to identify and gather publicly the available information from the traffic about his target such as the IP address of the target and his area of interests through a series of failed and successful attempts over time to get deeper into the target's network, and then select which target devices to infiltrate.

We assume that the attacker aims at infecting a particular device within the D2D network, depicted as "Target" in figure 3.1. Then, in this way, the attacker can inject any message attached with malware or use a zero-day exploit to attack the targeted victim residing in the network to infect it and compromise its accessibility (i.e., DoS). During the infection phase, the attacker aims at infecting as much devices as possible to launch the DoS attack from all the infected devices to increase the damage on the network.

Furthermore, we assume that all the devices have different intrusion detection capabilities and different energy levels. Therefore, all the available routes from the source to target device have different detection capabilities to detect malware. Accordingly, from the attacker's preference, some routes minimize the chances of detection of malware before it reaches the targeted device.

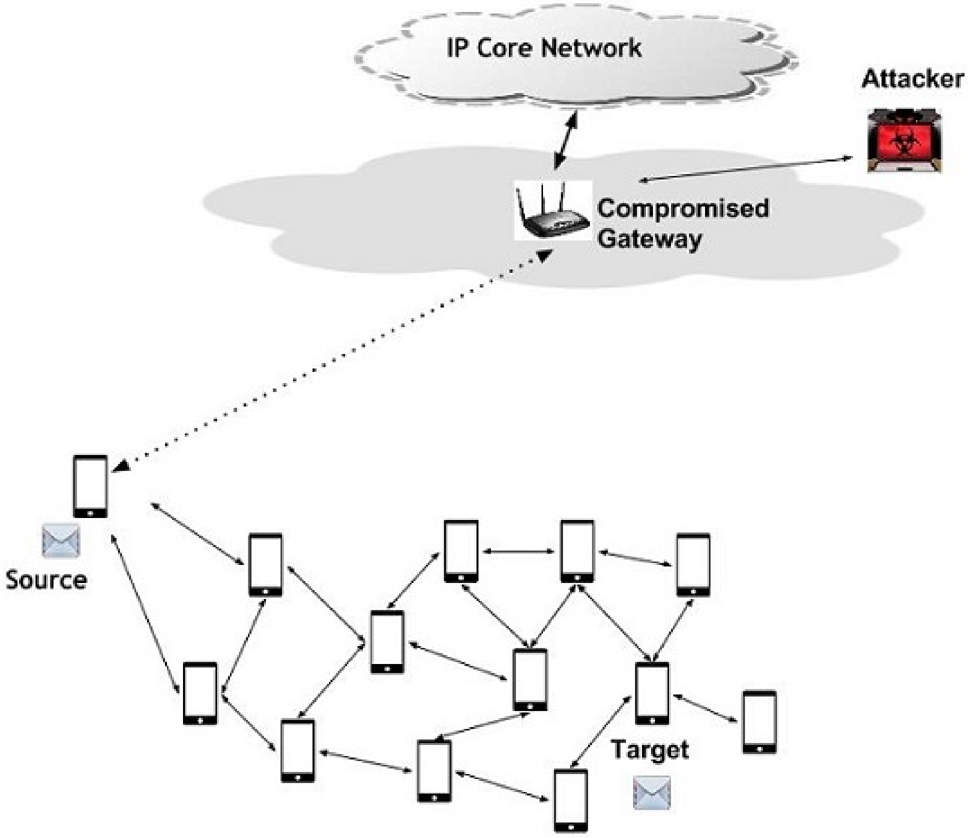


Figure 3.1: Adversarial Model

3.1.2 Problem Formulation

Let's assume a multi-hop D2D network of $\mathcal{N}$ trusted mobile devices denoted by $[\mathcal{N}]$. We assume that there are no malicious devices in the network. We denote the source device by S and the targeted device T and refer to any request or query for file or service or data as message indicated by Q.

When the device S receives Q and need to deliver Q to the device T, then S must find a route to the targeted device T to forward Q such that intermediate devices are needed to relay Q towards T . For each T, there is a set of all routes $[R]$ from the device S to the T device. The S selects $r_j \in [R]$ to deliver Q, where $[N_j]$ is the set of devices along the route r_j.

We consider that software-based malware detection systems with detection capabilities to be deployed on each device. Every device is running an anti-malware software, and it can also carry out the real-time network traffic monitoring. We denote by $[\mathcal{M}_\omega]$ the set of $\mathcal{M}_\omega$ as a different malware available to the attacker to infect mobile devices that run the mobile operating system ω.

For each $\omega \in [\Omega]$, we assume $\mathcal{C}_\omega$ anti-malware software (i.e., Resources) expressed by the finite set $[\mathcal{C}_\omega]$. Anti-malware detection software is residing on each mobile device n_i and each anti-malware software has its detection rate to detect successfully certain malware type.

The routing is a cooperative process, where the messages are relayed among devices. Any device along the route detects the intrusion with substantial evidence of anomalies; it is responsible for responding quickly to the intrusion and taking the appropriate action for future attacks [80].

We denote by $B(c_k^i, \mathcal{M}_m)$ (i.e., the True Positive [29]), the capability of the device n_i that runs the anti-malware software c_k to successfully detect the malware $\mathcal{M}_m$.

Accordingly, the disability of the device n_i to detect the malware $\mathcal{M}_m$ (i.e., False Negative [29]) is, $D(c_k^i, \mathcal{M}_m)$ = 1 - $B(c_k^i, \mathcal{M}_m)$.

As a result, for the fixed route r_j, the disability of r_j to detect malware $\mathcal{M}_m$ (i.e., the False Negative [29]) is given by:

$$D(r_j, \mathcal{M}_m) := \prod_{n_i \in N_j} D(c_k^i, \mathcal{M}_m) \tag{3.1}$$

Therefore, the route detection capability of r_j to successfully detect malware $\mathcal{M}_m$ before it reaches the targeted device T (i.e., True Positive [29]) is given by:

$$\psi(r_j, \mathcal{M}_m) := 1 - D(r_j, \mathcal{M}_m) \tag{3.2}$$

Also, the multi-hop D2D Communication and malware detection process will necessitate cooperation between devices. Some devices may not collaborate to relay other device's traffic because of their limited available energy.

Therefore, our protocol guarantees the route availability during the routing process and considers the energy level of the devices in the routing decision. It selects the path, where all the intermediate devices along the chosen route have enough energy levels to participate in the routing process.

Formally the energy-level of device n_i, $n_i \in [\mathcal{N}]$ is given by:

$$E(n_i) = \frac{E_r}{E_{max}}$$

Such that E_r is the remaining energy and E_{max} is the maximum energy available for the device.

Therefore, the route energy level on r_j is derived by multiplying the energy level of all the devices along the path r_j as follows:

$$E(r_j) := \prod_{n_i \in N_j} E(n_i) \tag{3.3}$$

3.2 Energy-aware Defense Routing Game (EDRG)

In the previous section, we have described the system and its different components. In this section, we apply the game theoretical framework to investigate the interactions between the defender and the adversary.

We consider a non-cooperative two-players zero-sum game played by the D2D network (i.e., defender) and the opponent (i.e., the attacker) to derive the optimal strategic routing decisions for the defender. The defender aims at selecting the optimal route to deliver Q to T, while the attacker aims at infecting the targeted device T and then launching a DoS attack. This game is repeated every time for t_{max}.

We assume that the defender has the probability distribution of different existing malware types for each mobile platform. Furthermore, the mobile devices learn more about the attacker actions from the Intrusion Detection System (IDS) residing on mobile devices during the subsequently repeated game.

3.2.1 Strategies and Payoffs

- **Strategy set**: The strategy set of a player refers to all possible moves the player can take.

  We consider that the defender's pure strategies are a finite action set of all possible routes $r_j \in [R]$ from the S device to T device. The attacker's pure strategy is a finite action set of different malware types $\mathcal{M}_m \in [M_\omega]$ from which the attacker selects to send to T aiming its infection.

  In the game EDRG, a pure strategy profile is a pair of defender and attacker actions, (r_j, M_m).

- **Payoff**: The defender's preferences or criteria of optimality are specified by its payoff function or utility function.

  For a given pure strategy profile (r_j, M_m), we define the U_Θ as the payoff of the defender; that depends on the route detection capability of each malware type and the route energy-level. We define U_Ψ as the payoff of the attacker, where the attacker's payoff is opposite to defender's payoff (i.e., zero sum game).

We consider the defender is the row player in the payoff matrix and the attacker is the column player as shown in table 3.1.

For a given pure strategy profile (r_j, $\mathcal{M}_m$), $r_j \in [R]$, $\mathcal{M}_m \in [M_\omega]$, the payoff of the defender is given by:

$$U_\Theta(r_j, \mathcal{M}_m) = [\psi(r_j, \mathcal{M}_m)\mathcal{V} + E(r_j)] \tag{3.4}$$

Table 3.1: Payoff matrix example

	M_1	M_2	M_3	M_4
r_1	3,-3	1,-1	1,-1	2,-2
r_2	2,-2	0,0	1,-1	0,0
r_3	1,-1	1,-1	3,-3	2,-2
r_4	0,0	2,-2	1,-1	1,-1

where the first term represents the route detection capability, the $\mathcal{V}$ is the defender's security gain value (monetary), where $\mathcal{V} > 0$ and the second term represents the overall route energy level.

The defender's payoff is the expected gain of detecting the malware before infecting the targeted device depends on the route detection capability summed up the route energy level.

In two-player zero-sum games with a finite number of actions for both players, there is at least a Nash Equilibrium (i.e., optimal routing strategy) in mixed strategy [50]. When there are some of the player's strategies obviously are optimal and more beneficial than the others, so it is better to assign higher probabilities to these strategies.

Accordingly, how to create mixed strategies such that each player can play one of his pure strategies with a certain probability?

To derive the optimal defense routing strategies, we consider the mixed strategy of both decision makers. The defender's mixed strategy X = $[x_1, x_2, \ldots, x_\xi]$ is the probability distribution over different routes in $[R]$ (i.e., pure strategies) from the S device to T device. Where x_j is the probability that the defender will choose its j-th route to deliver Q .

The attacker's mixed strategies Y = $[y_1, y_2, \ldots, y_\eta]$ is the probability distribution over different malware (i.e., pure strategies) against targeted devices. Where y_l is the probability that the attacker will choose its l-th malware to infect device.

The game consists of mixed strategy profile (X, Y), therefore the payoff of the defender is denoted by:

$$\mathcal{U}_\Theta \equiv U_\Theta(X,Y) = \sum_{j=1}^{\xi}\sum_{l=1}^{\eta} x_j y_l U_\Theta(r_j, \mathcal{M}_m) \tag{3.5}$$

where

$\sum_{j=1}^{\xi} x_j$=1

$\sum_{l=1}^{\eta} y_l$=1

For zero-sum games, the defender's strategy guarantees his payoff of value (V) regardless of attacker's strategy, and similarly, the attacker can guarantee himself a payoff of value (-V). The maximin means that the defender maximizes the minimum payoff possible for the attacker. Because the game is zero-sum, he also maximizes his minimum gain [52]. This means that the defender's gain is considered the attacker's loss.

For a zero-sum game, $\mathcal{U}_\Psi$ = - $\mathcal{U}_\Theta$, this means that the defender's gain is considered the attacker's loss.

Theorem 1:

There is an optimal solution to the game where

$\max_X \min_Y U_\Theta(X,Y)$ = $\min_Y \max_X U_\Theta(X,Y)$

3.2.2 Solution of EDRG

The minimax theorem states that the minimax solution in zero-sum games matches the NE. This means that the NE represents the optimal defense routing strategies against the attacker. On the other words, regardless of the attacker strategy, the optimal defense strategies of the defender guarantee the maximum performance [52].

For mixed strategy profile (X^*, Y^*) is the mixed Nash Equilibrium if:

- $U_\Theta(X^*, Y^*) \geq U_\Theta(X, Y^*)$; in case the attacker chooses Y^*

On the other hand, the maximin solution is the maximin strategy for the defender if:

- $\max\limits_{X} U_\Theta(X^*, Y) \geq \max\limits_{X} U_\Theta(X, Y)$

Linear Programming (LP)

Linear Programming (LP) can take a problem where the idea is to optimize a specific value given certain constraints for that value. There is a mathematical approach that is a branch of Linear programming called the simplex method.

Therefore, a game payoff matrix can be converted to an LP problem and applied to the simplex algorithm to derive the Nash Equilibrium (i.e., mixed strategies) for the game [35].

Fact A Linear Programming can be solved in Polynomial Time.

Example 3.2.2 describes the output of the simplex method after explaining the game (i.e., mixed strategies of the defender and the attacker).

Example 3.2.2

X = [0.6, 0, 0.4, 0]

This vector refers to the mixed strategy of the defender, which represents the probability distribution over the available routes. The defender will forward 60% of the data traffic over r_1 and 40% of the data traffic over r_3.

3.3 Repeated Malware-defense Secure Routing Protocol

In the previous section, we have described the game model and formulated the zero-sum game between network and attacker. We have also introduced the game solution and how to compute the optimal strategies.

In this section, we present the proposed routing protocol, which is called Repeated Malware-defense Secure Routing Protocol (RMSR).

RMSR has characteristics of reactive protocols and was mainly inspired by the functionalities of reactive protocols, which means that Route Discovery stage is used for route finding – on Demand as well as the source route is included in the packet header.

It consists of three main stages: Route Discovery stage, Route Selection stage, and Message Forwarding stage and we describe each stage in details as the following.

Table 3.2: RREQ of RMSR protocol

Hop Count
RREQ ID
Destination IP Address
Destination Sequence Number
Originator IP Address
Originator Sequence Number

3.3.1 Route Discovery stage

In this section, we describe in details the first stage of the proposed RMSR protocol, which is *the Route Discovery stage*, which consists of two parts.

First, the S needs to find the route to the targeted device T. S first broadcasts the Route Request (RREQ) [36] as shown in 3.2 towards the targeted device T.

Each intermediate device decides if to accept and forward the RREQ or not depending on its energy level. If it is less than a threshold value, the intermediate device will either drop the RREQ message or the message is forwarded towards the targeted device T.

As a result, this will guarantee that all intermediate devices have enough energy levels along the route to forward the message and participate in the routing process.

When T receives RREQ, it prepares the Route Reply message (RREP) as shown in table 3.3 and puts the reverse route then sends back to the S. Figure 3.2 shows the flow chart part (I) from this stage briefly.

When T sends back the RREP on the opposite route, each intermediate device receiving the RREP updates the route detection rate field by multiplying its detection capabilities using equation 3.2 and updates the

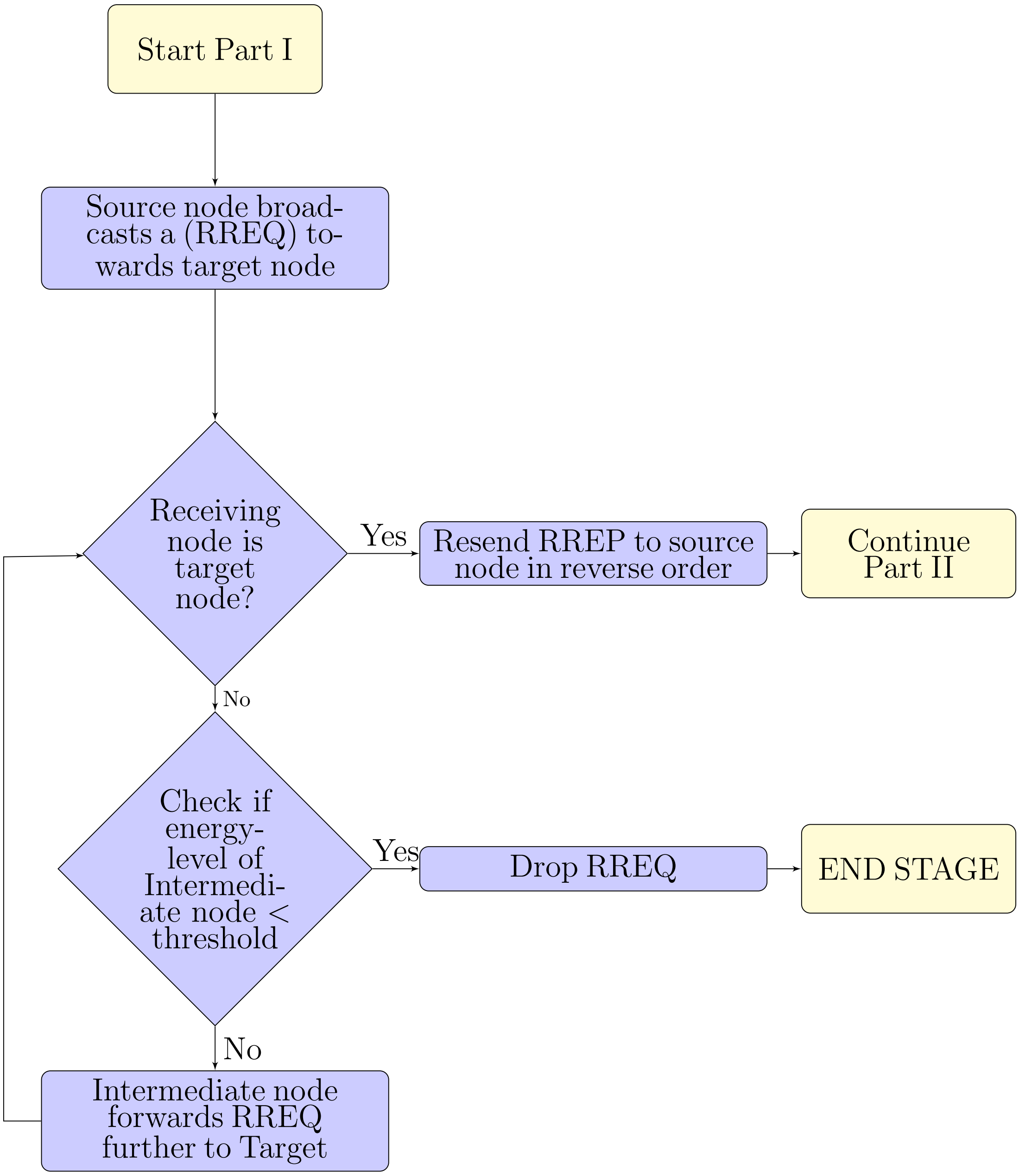

Start Part I
Source node broadcasts a (RREQ) towards target node
Receiving node is target node?
Yes
Resend RREP to source node in reverse order
Continue Part II
No
Check if energy-level of Intermediate node < threshold
Yes
Drop RREQ
END STAGE
No
Intermediate node forwards RREQ further to Target

Figure 3.2: Route Discovery stage Part (I)

Table 3.3: RREP of RMSR protocol

Hop Count
Destination IP Address
Destination Sequence Number
Originator IP Address
Life time
Route Detection rate
Route Energy-level

route energy level field by multiplying its energy level using equation 3.3.

When the Route Reply reaches S, S stores it in the routing table. S collects several routes to the device T. Then S will use the gathered information in its routing table in the next stage. Figure 3.3 shows the flowchart part (II) from this stage briefly.

3.3.2 Route Selection stage

After S receives several routes from the *Route Discovery* stage, then stores the gathered information in its routing table for deriving the optimal routing strategy. The *Route Selection* stage begins by using the collected information to obtain the optimal routing strategies as discussed in section 3.2.

After calculating the mixed strategy, S saves the routes for cache time t_{max}, then selects the optimal route stochastically according to the derived optimal routing strategy to forward the message Q. When the device S selects the route stochastically, the next *Message Forwarding* stage begins.

S must cache these routes for t_{max}, and after t_{max}, new optimal routing strategy must be derived. This means that EDRG is needed to be re-

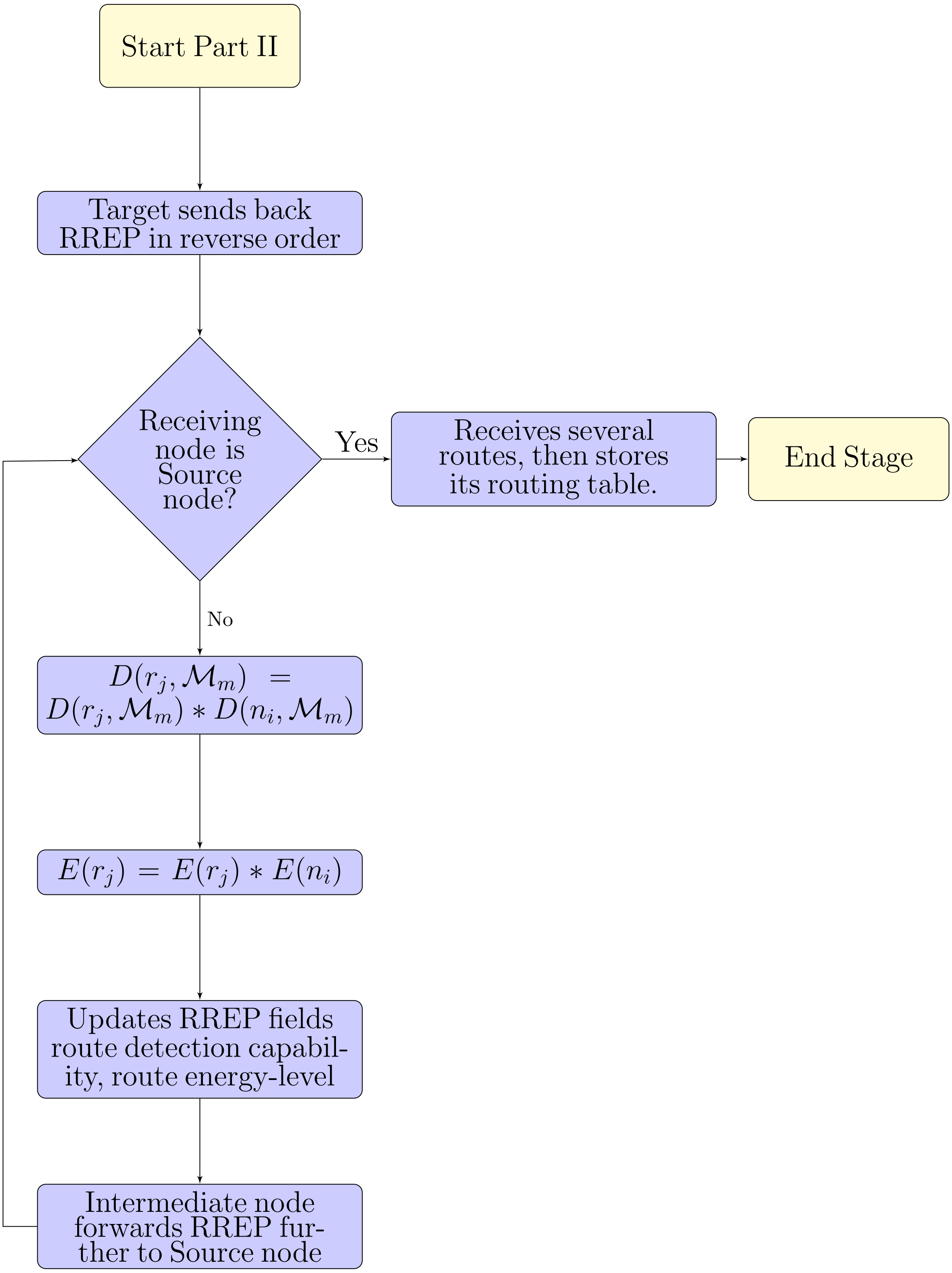

Start Part II
Target sends back RREP in reverse order
Receiving node is Source node?
Yes
Receives several routes, then stores its routing table.
End Stage
No
$D(r_j, \mathcal{M}_m) = D(r_j, \mathcal{M}_m) * D(n_i, \mathcal{M}_m)$
$E(r_j) = E(r_j) * E(n_i)$
Updates RREP fields route detection capability, route energy-level
Intermediate node forwards RREP further to Source node

Figure 3.3: Route Discovery stage Part (II)

peated every t_{max} because the mobile devices learn more about the attacker actions and behaviors from the Intrusion Detection System and the game history.

During t_{max}, if there are no more valid routes in the cache due to energy depletion of devices, the *Route Discovery* procedure must be initiated, and EDRG will be repeated to derive the correct routes.

3.3.3 Message Forwarding stage

Once the device S selected the route, the *Message Forwarding* stage started as the following:

Each intermediate device along the chosen route received the message Q participated in detecting the occurrence of these malicious messages with strong evidence of anomalies; it will respond quickly to the intrusion and take the appropriate action for future attacks.

Accordingly, if it finds a malicious message, it will drop it. Otherwise, it will forward it towards the device T. The following figure 3.4 summarizes all the stages:

Algorithm 1 Repeated Malware-defense Secure Routing

```
procedure RMSR($Sourcenode(S), Targetnode(T)$, Query $Q$)
ROUTE DISCOVERY Stage (Part I)
S broadcasts a Route Request message(RREQ);

    if $n_i$ node receives RREQ then
        if $n_i$ is not $T$ then
            $n_i$ should broadcast RREQ to their neighbors;
        else
            $T$ sends back the Route Reply (RREP) containing the full reverse
            source route
ROUTE DISCOVERY Stage (Part II)
    if $n_i$ device receives RREP then                ▷ Intermediate Nodes
        if $n_i$ is not $S$ then
            $D(r_j, \mathcal{M}_m) \leftarrow D(r_j, \mathcal{M}_m) * D(c_k^i, \mathcal{M}_m)$;
            $E(r_j) \leftarrow E(r_j) * E(n_i)$;
            Then appended two new fields in the RREP
            (route detection capability, route energy-level).
        if $n_i$ is $S$ then
            $\psi(r_j, \mathcal{M}_m) \leftarrow 1 - D(r_j, \mathcal{M}_m)$;
            After the $S$ receives several routes, stores its routing table.
ROUTE SELECTION Stage:
    First ← $S$ uses its routing table to compute the payoff matrix then derive
the optimal defense plan using LP
    Second ← $S$ selects the route $R$ probabilistically according to optimal
    defense plan to forward the message.
MESSAGE FORWARDING Stage:
    Each node belongs to route $R$ inspect $Q$;
    if $n_i$ found malicious message then

        $n_i$ will drop message ;
    else
        $n_i$ relays the message to $T$ ;
```

Figure 3.4: RMSR protocol stages

3.4 Summary

In this chapter, firstly, the system model of the network with mobile devices and the attack model were described. Secondly, we have formulated the problem between the network and the attacker as a zero-sum non-cooperative game by presenting the payoff functions for both decision makers then proving theoretically the optimality of game solution.

Finally, we have described the proposed game theoretical routing protocol in details in each stage and summarized the overall routing protocol in an algorithm.

In the next chapter, we present the simulation results of the proposed game theoretic routing protocol. We demonstrate the effectiveness of the proposed game theoretic routing protocol regarding malware detection efficiency and energy awareness in D2D network. The performance of the proposed protocol is also shown practically against different attackers' behavior in the next chapter.

Chapter 4

Simulation Results and Discussion.

In this chapter, we validate the theoretical analysis conducted in Chapter 3 and evaluate the effectiveness of the proposed game theoretic routing protocol in Device-to-Device network through extensive simulations. The simulations are performed using the Omnet++ network simulator and the INET framework.

Then, we evaluate the performance of the optimal routing strategies of the defender against three different attacks distribution: Uniform Attack, Optimal Attack, and Weighted Attack.

We compare the proposed routing protocol practically regarding the detection rate and the overall expected payoff of the defender with the traditional routing protocols (e.g., AODV, DSR) and strategic customized protocol SCP.

4.1 Network setup

We have performed the simulations using the Omnet++ network simulator and the INET framework. We have considered that a D2D network consists of 20 mobile devices, each is equipped with anti-malware software to detect malicious messages.

In these simulations, the mobile devices are randomly deployed inside a rectangular area of 800 x 800 m. Such that each mobile device has fixed transmission power with a maximum transmission range 200 meters and the mobile devices send (UDP) traffic.

The total simulation time varies from (10, 20, 40, 60 mins) to prove the accuracy of the results. Table 4.1 summarizes the simulation fixed parameters.

Table 4.1: Simulation parameter values

Parameter	Value
Number of nodes	20
Mobility model	Linear Mobility
Mobility Speed	10mps
Mobility Update Interval	0.1s
Packet generation rate	2 packets/s
Packet size	512 bytes

4.2 Anti-malware software and Malware

We assume anti-malware software as shown in table 4.2 with their detection rates, such that each mobile device is equipped with anti-malware software.

We consider one attacker in our simulations who aims at infecting a targeted device residing in D2D network. The attacker has a finite set

Table 4.2: Anti-malware software

Antimalware software	Detection rate
iTL [21]	99.9%
iDMA [22]	100%
Touchstroke[23]	87.5%
Profiler [24]	99.8

of different malware types $\mathcal{M}_m \in [M_\omega]$ from which the attacker selects to send to targeted device T aiming at its infection. We assume the attacker chooses one of these malware types: keylogger, Spam, Rootkit iSAM, Spyware, iKee-B, Premium-Rate [21], [22], [23], and [24].

4.3 Attack Distribution Cases

We consider in the simulations three different attacks distribution to evaluate the effectiveness of the proposed routing protocol.

We simulate three different attack distribution, each attack case defines the attacker preferences.

- *Uniform* attack distribution: the attacker gives no preferences to any malware type, this means that all malware types are chosen with equal probability. This approach assumes that the attacker has no knowledge about the capability of the intrusion detection in the network to decide which malware type will be difficult to detect.

- *Optimal* attack distribution: the attacker gives preferences to certain malware types to maximize his payoff. He chooses the malware type according to his mixed strategy (i.e., Nash Equilibrium) assigned by the minimax solution.

- *Weighted* attack distribution: the attacker gives preferences to certain malware types to maximize his payoff (i.e., proportional to his payoff). He chooses the malware type according to the following [58].

  STEP ONE: For each column in payoff matrix, the average payoff value of the column is computed.

  STEP TWO: Add the total average payoff value of the all the columns to derive the total sum.

  STEP THREE: For each column (i.e., Malware type), the probability distribution for each malware type is calculated by dividing its average payoff value derived from step one by the total sum obtained from step two.

4.4 Performance Analysis

In this section, we first perform a practical study to validate and prove our theoretical analysis of optimality. We conduct simulations to test the effectiveness of the optimal routing strategies and how they perform against different attacks distribution created by *Uniform, Optimal,* and *Weighted* approaches.

We compare practically first the performance of the optimal routing strategies of proposed routing protocol, which are given by the Nash Equilibrium after solving the security game with the other two deterministic non-strategic protocols (i.e., DSR and AODV) against three different attacks distribution.

Then, we compare the performance of the optimal routing strategies of the proposed routing protocol with another strategic customized routing protocol against various attacks distribution.

Through simulations, the theoretical results are illustrated, demonstrating how each routing protocol performs regarding overall *expected payoff* and *detection rate.*

- Overall Expected value of payoff: it involves maximizing the expected value of objective or payoff function regarding malware detection efficiency and route energy awareness. This term refers to what the defender will get or gain based on a certain decision taken by the defender and the attacker, (i.e., expected value in reaching optimal decisions regarding malware detection efficiency and route energy awareness) as shown in the example 4.4.

Example 4.4

Given the payoff matrix of Rock-Paper-Scissors zero-sum game as shown in table 4.3. The vectors of mixed strategies of the game as given by:

X=[1/2 , 1/2, 0]

Y=[1/3, 2/3, 0]

therefore, the overall *expected payoff* is computed as follows:

$U_D(X,Y)$=(1/2 * 1/3 * 0) + (1/2 * 2/3 * -1) + (1/2 * 0 * 1) + (1/2 * 1/3 * 1) + (1/2 * 2/3 * 0) + (1/2 * 0 * -1) + (0 * 1/3 * -1) + (0 * 2/3 * 1) + (0 * 0 * 0) = -1/6.

Table 4.3: Rock-Paper-Scissors game example

	M_1	M_2	M_3
r_1	0,0	-1,1	1,-1
r_2	1,-1	0,0	-1,1
r_3	-1,1	1,-1	0,0

4.4.1 Performance Comparisons

Firstly, we plot the overall *expected payoff* and the *detection rate* of the proposed protocol RMSR and other two traditional non-strategic protocols against three different attacks distribution: *Uniform, Optimal,* and *Weighted.*

Then, we plot the overall *expected payoff* of the defender and the *detection rate* of RMSR and another strategic customized protocol against different attacks distribution.

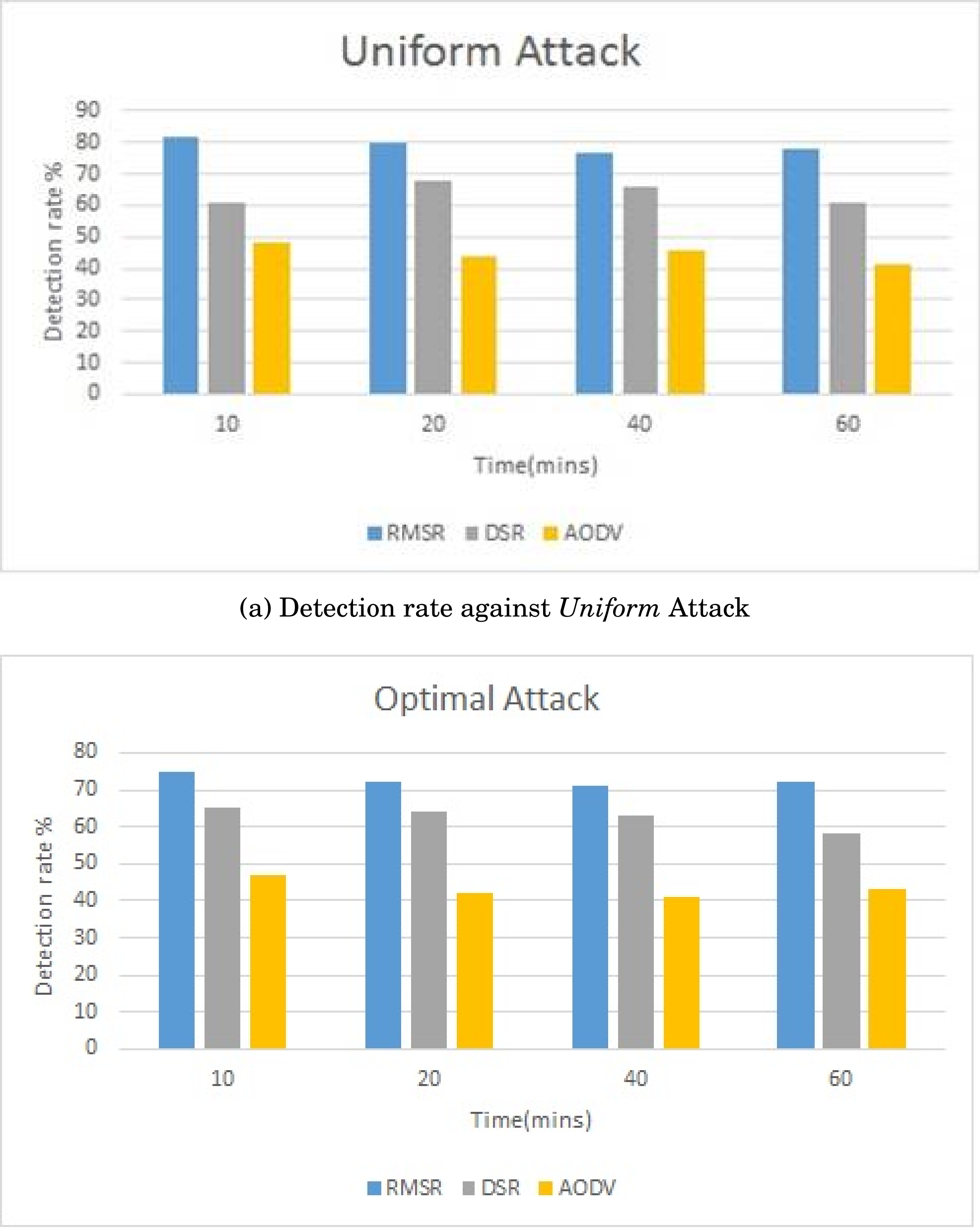
- **Non-strategic protocol**

  1. Detection Rate

     - When comparing the proposed RMSR protocol with the other two deterministic protocols as shown figure 4.1a, we can see that the proposed RMSR protocol achieves its highest detection rate 83% against the *Uniform* attack distribution.

     - While in the case of *Optimal* attack distribution as shown figure 4.1b, the proposed protocol RMSR has detection rate 15% greater than DSR and 32 % higher than AODV.

     - We can also see in figure 4.2, that the proposed RMSR protocol achieves its highest detection rate 70% against the *Weighted* attack distribution.



(a) Detection rate against *Uniform* Attack

(b) Detection rate against *Optimal* Attack

Figure 4.1: Malware detection rate for 3 routing protocols against *Uniform* and *Optimal* Attack

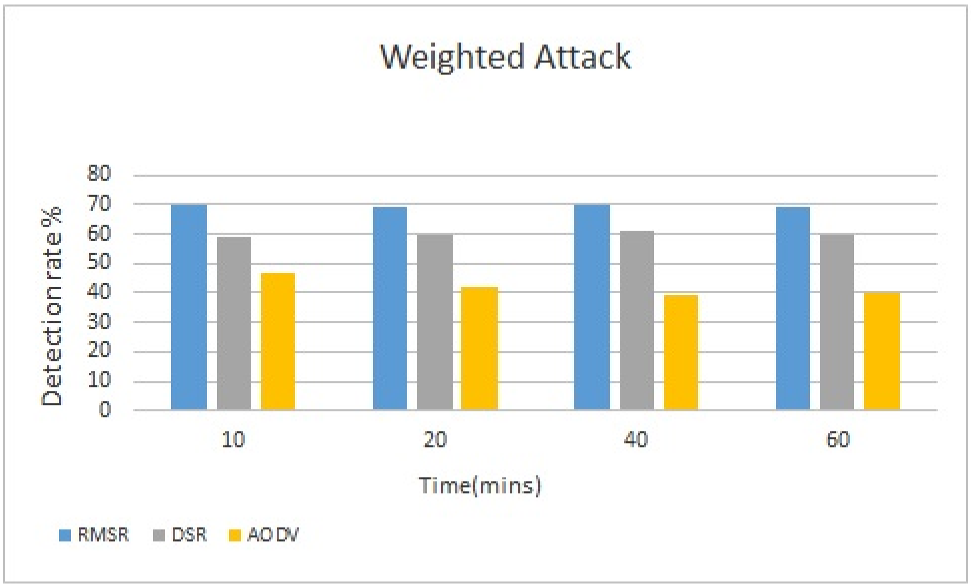


Figure 4.2: Detection rate against *Weighted* Attack

2. Overall Expected Payoff

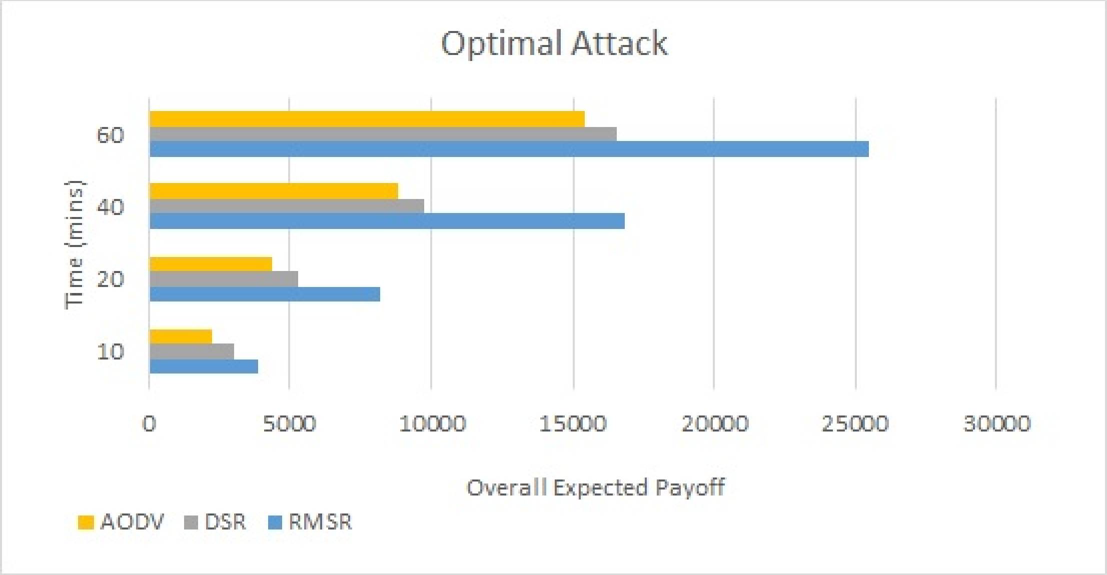
   Similarly, the proposed protocol RMSR achieves the best performance regarding overall *expected payoff* among the other two traditional routing protocols.

   – We can see in figure 4.3a the percentage improvement of the proposed protocol RMSR against the *Optimal* attack distribution by 52% and 72% compared to the DSR and AODV respectively.

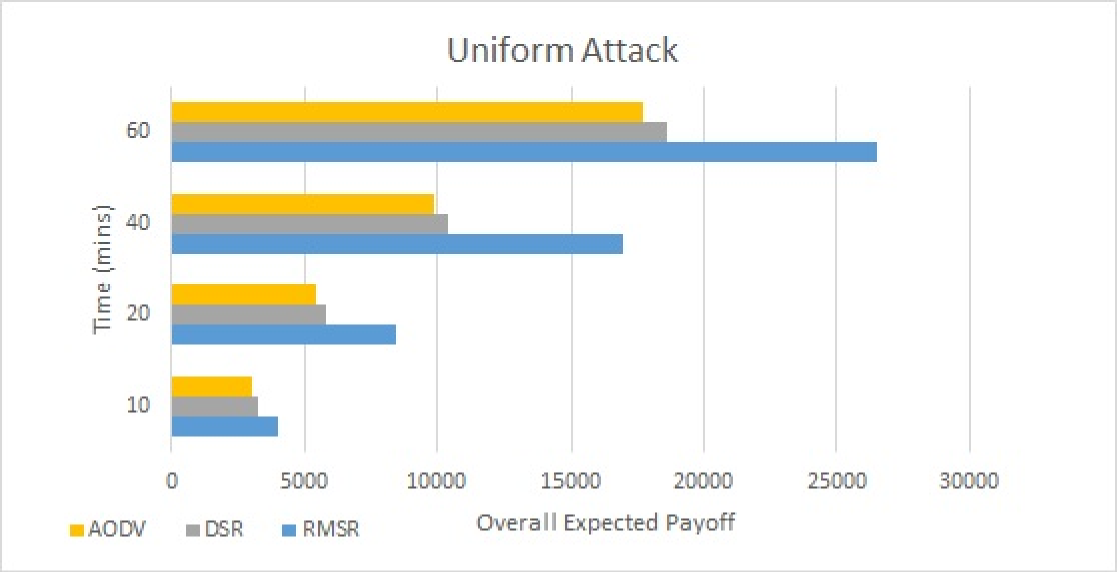
   – While in the case of the *Uniform* attack distribution as shown figure 4.3b, the percentage improvement values of the proposed protocol are 63% and 78% compared to the DSR and AODV respectively.

   – In figure 4.4, we can see the percentage improvement values of the proposed protocol are 40% and 52% compared to the DSR and AODV respectively against the *Weighted* attack distribution.

Although the proposed protocol RMSR is stochastic, however, it outperforms the other two deterministic protocols in case of all attacks distribution.



(a) Overall Expected Payoff against *Optimal* Attack



(b) Overall Expected Payoff against *Uniform* Attack

Figure 4.3: Expected Payoff of the defender for 3 routing protocols against *Uniform* and *Optimal* Attack

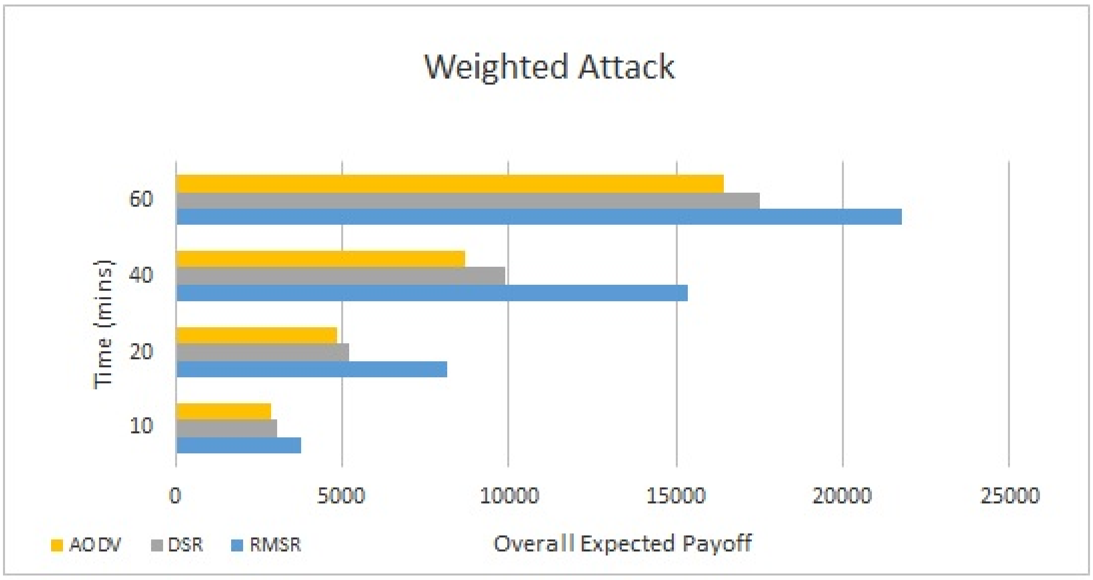


Figure 4.4: Overall Expected Payoff against *Weighted* Attack

Table 4.4: Payoff matrix for zero-sum game

	M_1	M_2	M_3
r_1	1,-1	2,-2	0,0
r_2	3,-3	1,-1	3,-3
r_3	1,-1	0,0	2,-2

- **Strategic Customized Protocol**

To evaluate and prove the optimality of our proposed protocol RMSR, we present another strategic customized routing protocol called SCP.

Given that the probability distribution of different existing malware types, we develop strategic customized routing protocol, which provides the optimal proportion routes to their average capabilities of malware detection.

This protocol is as the following algorithm [58]:

STEP ONE: The average payoff value is calculated as equation 4.1 for each route.

$$U_{\Theta}^{\sim}(r_j) := \frac{\sum_{\mathcal{M}_m \in \mathcal{M}_\omega} U_{\Theta}(r_j, \mathcal{M}_m)}{\mathcal{M}_\omega}, \forall r_j \in [R] \tag{4.1}$$

STEP TWO: Calculate the total average payoff value of all the routes.

Total = $\sum_{r_j \in [R]} U_{\Theta}^{\sim}(r_j), \forall r_j \in [R]$

STEP THREE: Then the probability of route r_j to be selected to relay the message is calculated as equation 4.2.

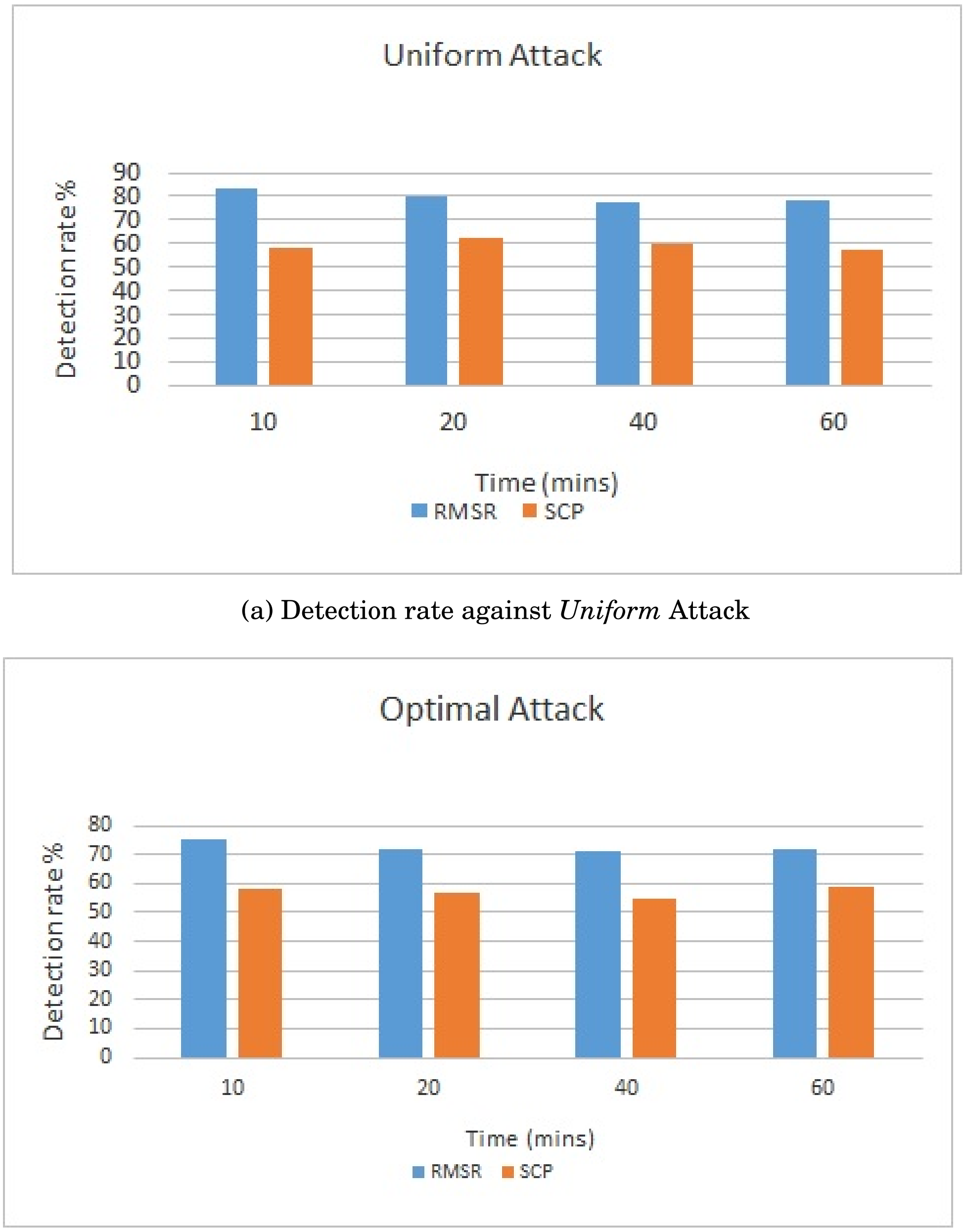
$$1 - \frac{U_{\Theta}^{\sim}(r_j)}{Total}, \forall r_j \in [R] \tag{4.2}$$

1. Detection Rate

   - When comparing the proposed RMSR protocol with the customized SCP protocol as shown figure 4.5a, the proposed protocol RMSR outperforms the SCP protocol and achieves a detection rate 25% higher than SCP against the *Uniform* attack distribution.

   - While in the case of *Optimal* attack distribution as shown in figure 4.5b, the proposed protocol RMSR achieves a detection rate 19% higher than SCP.

   - In figure 4.6, we can see that the proposed RMSR protocol achieves a detection rate 13% higher than SCP against the *Weighted* attack distribution.



(a) Detection rate against *Uniform* Attack

(b) Detection rate against *Optimal* Attack

Figure 4.5: Malware detection rate for RMSR and SCP against 2 attack cases

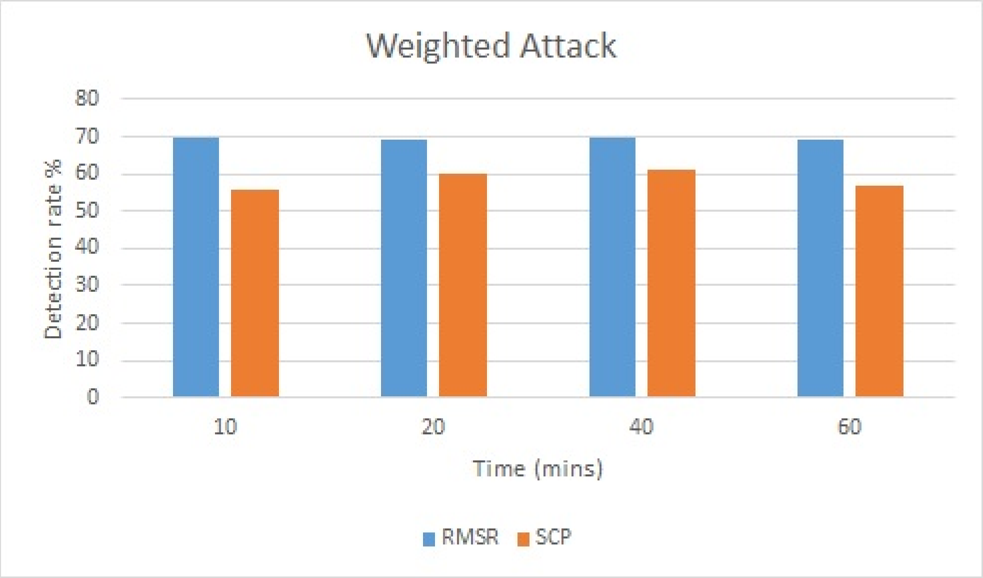


Figure 4.6: Detection rate against *Weighted* Attack

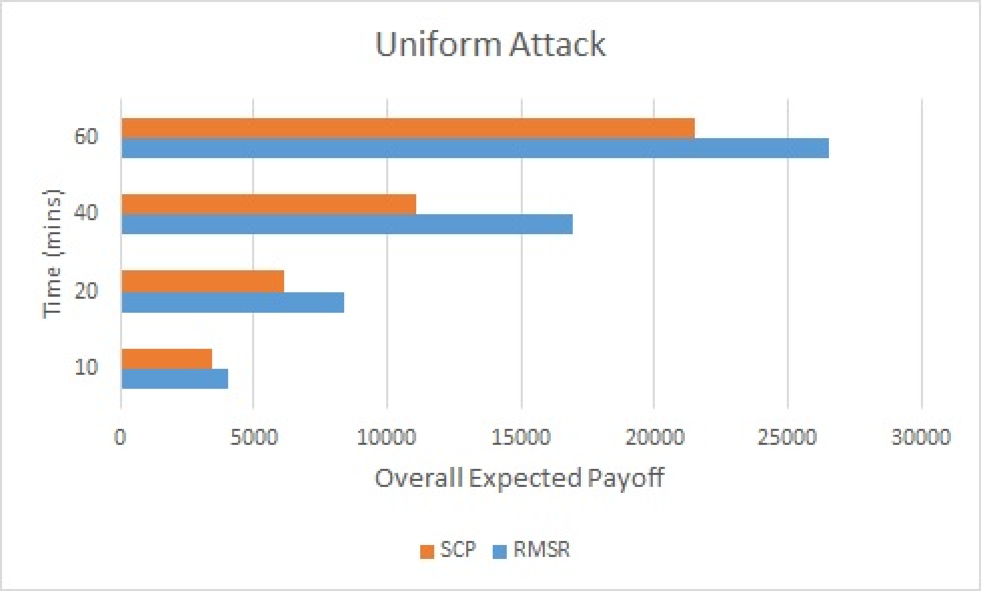
2. Overall Expected Payoff

   As shown figure 4.7, we can see that the proposed protocol RMSR performs better than SCP regarding overall *expected payoff* against two different attack cases.

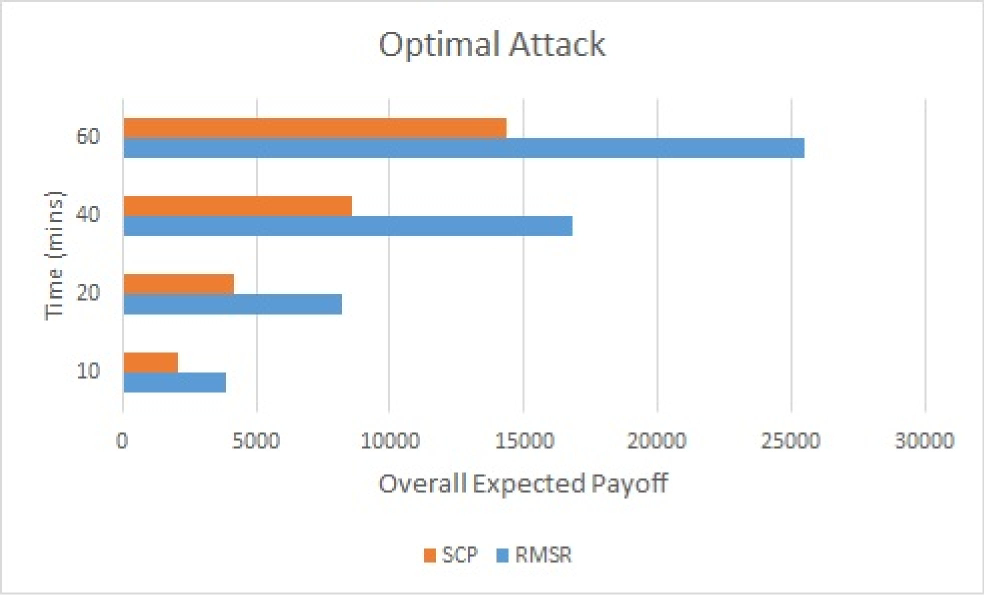
   - In figure 4.7a, we can see the percentage improvement of the proposed protocol RMSR against the *Uniform* attack distribution by 31% compared to SCP.

   - While in the case of the *Optimal* attack distribution as shown in figure 4.7b, the percentage improvement values of the proposed protocol RMSR are 89% compared to SCP.

   - Also, we can see in figure 4.8 the percentage improvement of the proposed protocol RMSR against the *weighted* attack distribution by 29% compared to SCP.



(a) Overall Expected Payoff against *Uniform* Attack



(b) Overall Expected Payoff against *Optimal* attack

Figure 4.7: Overall Expected Payoff of the defender for RMSR and SCP against *Uniform* and *Optimal* Attack

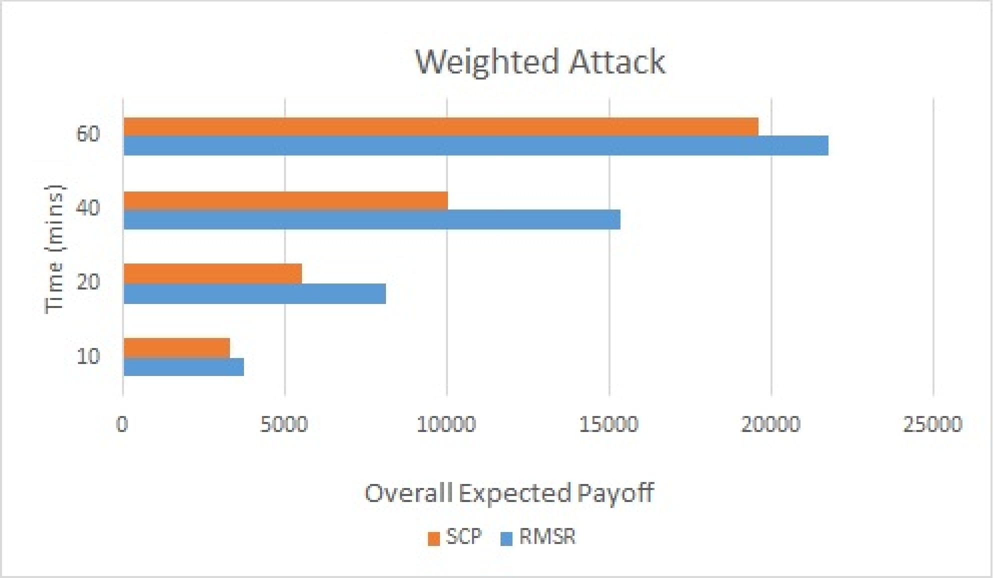


Figure 4.8: Overall Expected Payoff against *Weighted* Attack

4.5 Summary

In this chapter, we firstly introduced the network simulation environment: one external attacker is trying to attack the D2D network which consists of N devices. Where, each device is equipped with IDS to detect certain malware type. In this study, we considered a smart and a rational attacker who can choose his strategy intelligently to maximize his payoff.

Secondly, we presented different attacks distribution which is used for comparison and evaluation. Then we introduced the simulation results to validate the analytical results discussed in chapter 3.

Finally, through simulation, we evaluated the effectiveness and the performance of the proposed game theoretic protocol in D2D network and compared it with the other traditional routing protocols and strategic customized protocol against different attacks distribution.

Chapter 5

Conclusions and Future Work

In this chapter, we conclude this thesis by explaining our results and findings. Then, we demonstrate the research achievements and highlight the main contributions of the thesis on the objectives of the research.

We also emphasize the limitations and the challenges of this research. Then, we mention the main avenues for future research orientation in the field of security for Device-to-Device communications and provide several suggestions and recommendations for future work as well as speculations on future trends.

5.1 Conclusions

In this thesis, our most significant contributions fall within the area of secure routing in intelligent Device-to-Device communications. The primary objective is to propose energy-aware solutions for security in Device-to-Device communications to hinder the malware attacks during the infection phase in the presence of the external attacker.

Firstly, we investigated the main research areas of the security in Device-to-Device communications and identified the security requirements, issues, and challenges. Also, we reviewed the evolution of the malware attacks and mobile devices' capabilities.

Secondly, we reviewed in details the state-of-the-art in the fields of malware attacks, intrusion detection, and secure routing in D2D network, then concluded by a comparison with our proposed routing protocol.

Thirdly, to obtain optimal routing strategies, we formulated the security game to model the interactions between the attacker and the D2D network. The interactions presented using the payoff function and payoff matrix. Then, we proposed a novel game-theoretic energy-aware routing protocol for enhancing the security in D2D network. To the best of our knowledge, stochastic routing for mitigating the malware infection as well as considering the energy constraints has not been suggested in D2D communications.

Finally, we designed and performed the simulations to evaluate the performance and the effectiveness of the proposed game theoretic routing protocol against three different attacks distribution. We demonstrated that the game has the Nash Equilibrium leading to optimal routing strategy.

The simulation results showed that with the optimal routing strategy, the defender could pick the intelligently the optimal energy-aware routes that enhance the security and maximize the chances of the malware detection.

The simulation results indicated that the proposed protocol based on strategic plan outperforms the other non-strategic traditional protocols and another strategic customized protocol. Unlike the existing works on security games, the proposed protocol can make optimal routing decisions to deliver the traffic from source to target device in D2D network. Both the security requirements and the energy constraints were considered in the proposed routing protocol.

5.2 Future Work

One of the limitations of our contribution is the assumption that there are no malicious devices. In the case of malicious internal devices that have control on the IDS, there is no trust guarantee among the devices.

Also, one of the considerations in this thesis is that we have considered the minimum mobility of the devices. In the case of high mobility, we would like to discuss distributed stochastic routing protocol in a hop-to-hop manner instead of end-to-end manner, such that each device selects a neighbor to forward a packet according to a probability distribution.

Accordingly, in our future work, we would like to consider that each device evaluates its neighbor and will try to find the next hop to forward the message.

In future research, we would also like to design and develop a more robust game theoretic scheme to cope with the other advanced attacker's strategies such that the pure strategy of the attacker consists of is a malware type and set of devices to infect. This new game theoretic scheme should be applied to handle this case.

We would also like to consider the cops and robbers N-players game approach for routing in D2D network. In this scheme, for a given period, some devices act as n-cops are equipped with IDS that chases robber, then it will be shown how many cops are needed to catch the robber.

Also, in our future research, we plan to combine both the game theoretic approach with Fuzzy Q-learning algorithm [1] in D2D network. It will improve the detection accuracy rate of the devices over the time due to the learning capabilities of the devices as well as detect new, different attacks.

It is expected that by merging the game theory with a Fuzzy Q-learning method, the performance of the new scheme will outperform that any other defense method.

As our proposed routing protocol has assumed that the decision makers have complete information about each other's payoff matrix, which is not valid practically [54]. Accordingly, we plan to formulate security games with imperfect observations as a fictitious play game. The fictitious play game is a "belief-based" learning rule, so each decision maker forms beliefs about opponent's mixed strategy, then compute the best strategy on these beliefs [6].

References

[1] Enhancements of Fuzzy Q-learning Algorithm. http://journals.bg.agh.edu.pl/COMPUTER/2005/cs2005-05.pdf. 2005.

[2] International Workshop on Device-to-Device (D2D) Communication With and Without Infrastructure. http://d2dgc13.prosjekt.uia.no. 2013.

[3] Internet Security Threat Report. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf. 2016.

[4] Internet Security Threat Report. http://www.symantec.com/connect/downloads/internet-security-threat-report-volume-16. Accessed: 2011.

[5] Kaspersky Security Bulletin. Malware Evolution 2015. https://securelist.com/files/2015/12/KSB_2015_Statistics_FINAL_EN.pdf. Accessed: 2015.

[6] Learning in Games. http://web.stanford.edu/~jdlevin/Econ%20286/Learning.pdf. 2006.

[7] mobile-edge computing - introductory technical white paper. https://portal.etsi.org/portals/0/tbpages/mec/docs/mobile-edge_computing_-_introductory_technical_white_paper_v1%2018-09-14.pdf. 2014.

[8] Security Threat Report 2014. www.sophos.com/en-us/medialibrary/pdfs/other/sophos-security-threat-report-2014.pdf. Accessed: 2014.

[9] Security Threat Report 2015. https://www.sophos.com/threat-center/medialibrary/PDFs/other/sophos-trends-and-predictions-2015.pdf. 2015.

[10] trendlabs-security-roundup. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-2q-2015-trendlabs-security-roundup.pdf. 2015.

[11] A. Agah, K. Basu, and S. K. Das. Enforcing security for prevention of dos attack in wireless sensor networks using economical modeling. *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005*, pages 8 pp. – 535, 7-7 Nov. 2005.

[12] Afrand Agah and Sajal K. Das. Preventing dos attacks in wireless sensor networks: A repeated game theory approach. *International Journal of Network Security*, 5:145 – 153, 2007.

[13] Muhammad Alam, Du Yang, Jonathan Rodriguez, and Raed A. Abdalhameed. Secure device-to-device communication in lte-a. *IEEE Communications Society*, 52:66 – 73, 2014.

[14] Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal, and Kashif Naseer Qureshi. Malicious node detection through trust aware routing in wireless sensor networks. *Journal of Theoretical and Applied Information Technology*, 74(1), 2015.

[15] Arash Asadi, Qing Wang, and Vincenzo Mancuso. A survey on device-to-device communication in cellular networks. *IEEE Communications Surveys & Tutorials*, 16:1801 – 1819, 2014.

[16] Oladayo Bello and Sherali Zeadally. Intelligent device-to-device communication in the internet of things. *IEEE Systems Journal*, PP:1 – 11, 2014.

[17] S. Bohacek, J. P. Hespanha, K. Obraczka, Junsoo Lee, and Chansook Lim. Enhancing security via stochastic routing. *Proceedings Eleventh International Conference on Computer Communications and Networks, 2002.*, pages 58 – 62, 2002.

[18] Stephan Bohacek, Joao Hespanha, Junsoo Lee, Chansook Lim, and Katia Obraczka. Game theoretic stochastic routing for fault tolerance and security in computer networks. *IEEE Transactions on Parallel and Distributed Systems*, 18:1227 – 1240, 2007.

[19] G. Calinescu, S. Kapoor, K. Qiao, and J. Shin. Stochastic strategic routing reduces attack effects. *Global Telecommunications Conference (GLOBECOM 2011)*, pages 1 – 5, 2011.

[20] Jin-Hee Cho, Ing-Ray Chen, and Phu-Gui Feng. Effect of intrusion detection on reliability of mission-oriented mobile group systems in mobile ad hoc networks. *IEEE Transactions on Reliability*, 59:231 – 241, 2010.

[21] D. Damopoulos, G. Kambourakis, and S. Gritzalis. From keyloggers to touchloggers: Take the rough with the smooth. *Computers & Security*, 32:102 – 114, 2013.

[22] D. Damopoulos, G. Kambourakis, S. Gritzalis, and S. Park. Exposing mobile malware from the inside (or what is your mobile app really doing?). *Peer-to-Peer Networking and Applications*, pages 1 – 11, 2012.

[23] D. Damopoulos, G. Kambourakis, and G. Portokalidis. The best of both worlds: a framework for the synergistic operation of host and cloud anomaly-based ids for smartphones. *Proc. 7th European Workshop on*

System Security, 2014.

[24] D. Damopoulos, S. A. Menesidou, G. Kambourakis, M. Papadaki, N. Clarke, and S. Gritzalis. Evaluation of anomaly-based ids for mobile devices using machine learning classifiers. *Security and Communication Networks*, 5:3 – 14, 2012.

[25] Debjit Das, Koushik Majumdera, and Anurag Dasguptab. Selfish node detection and low cost data transmission in manet using game theory. In *Eleventh International Conference on Communication Networks*, volume 54, pages 92 – 101, 2015.

[26] Peter Duersch, Joerg Oechssler, and Burkhard C. Schipper. Pure strategy equilibria in symmetric two-player zero-sum games. *International Journal of Game Theory*, 41:553 – 564, 2011.

[27] Hadeer Elsemary. Mitigating malware attacks via secure routing in intelligent device-to-device communications. In-Press, 2016.

[28] Hadeer Elsemary and Dieter Hogrefe. Malware-defense secure routing in intelligent device-to-device communications. *The 1st International Conference on Advanced Intelligent System and Informatics (AISI2015), November 28-30, 2015, Beni Suef, Egypt*, 407:485 – 495, Springer 2015.

[29] Tom Fawcett. An introduction to roc analysis. *Pattern Recognition Letters 27*, 27:861–874, 2006.

[30] M. Felegyhazi and J. Hubaux. Game theory in wireless networks: A tutorial. *tech. rep., EPFL*, 2006.

[31] Mark Felegyhazi, Jean-Pierre Hubaux, and Levente Buttyan. Nash equilibria of packet forwarding strategies in wireless ad hoc networks. *IEEE Transactions on Mobile Computing*, 5:463 – 476, 2006.

[32] Daquan Feng, Lu Lu, Yi Yuan-Wu, Geoffrey Ye Li, Shaoqian Li, and Gang Feng. Device-to-device communications in cellular networks. *IEEE Communications Magazine*, 52:49 – 55, 2014.

[33] Gabor Fodor, Stefano Sorrentino, Pontus Wallentin, Qianxi Lu, and Nadia Brahmi. Device-to-device communications for national security and public safety. *IEEE Access*, 2:1510 – 1520, 2015.

[34] A. Gueye. *A Game Theoretical Approach to Communication Security, PhD Thesis, University of California at Berkeley, CA, USA*. PhD thesis, University of California at Berkeley, Berkeley, CA, USA, 2011.

[35] Dale Hogarth. *Program for Solving Two-person Zero-sum games*. PhD thesis.

[36] D. Johnson, Y. Hu, and D. Maltz. The dynamic source routing protocol (dsr) for mobile ad hoc networks for ipv4. 2007.

[37] Dimple Juneja and Neha Arora. An ant based framework for preventing ddos attack in wireless sensor networks. *International Journal of Advancements in Technology (IJoAT)*, 1, 2010.

[38] M. H. R. Khouzani, Saswati Sarkar, and Eitan Altman. Maximum damage malware attack in mobile wireless networks. *IEEE/ACM Transactions on Networking*, 20:1347 – 1360, 2012.

[39] M. H. R. Khouzani, Saswati Sarkar, and Eitan Altman. Saddle-point strategies in malware attack. *IEEE Journal on Selected Areas in Communications*, 30:31 – 43, 2012.

[40] M. H. R. Khouzani, Saswati Sarkar, and Eitan Altman o. A dynamic game solution to malware attack. *Proceedings IEEE INFOCOM, 2011*, pages 2138 – 2146, April 2011.

[41] X. Liang and Y. Xiao. Game theory for network security. *IEEE Com-*

munications Surveys and Tutorials, 15:472 – 486, 2013.

[42] Yu Liu, Cristina Comaniciu, and Hong Man. A bayesian game approach for intrusion detection in wireless ad hoc networks. *GameNets '06 Proceeding from the 2006 workshop on Game theory for communications and networks*, 2006.

[43] C. Lott and D. Teneketzis. Stochastic routing in ad-hoc networks. *IEEE Transactions on Automatic Control*, 51:52 – 70, 2006.

[44] Kassio Machado, Denis Rosario, Eduardo Cerqueira, Antonio A. F. Loureiro, Augusto Neto, and Jose Neuman de Souza. A routing protocol based on energy and link quality for internet of things applications. *Sensors 2013*, 13:1942 – 1964, 2013.

[45] Mohammad Hossein Manshaei, Quanyan Zhu, Tansu Alpcan, Tamer Basar, and Jean pierre Hubaux. Game theory meets network security and privacy. *Journal ACM Computing Surveys (CSUR)*, 45, 2013.

[46] Maryam Mohi, Ali Movaghar, and Pooya Moradian Zadeh. A bayesian game approach for preventing dos attacks in wireless sensor networks. *Communications and Mobile Computing, 2009. WRI International Conference on CMC '09.*, 3:507 – 511, 2009.

[47] O. Morgenstern and J. Von Neumann. Theory of games and economic behavior. 1944.

[48] Abderrahmen Mtibaa, Khaled A. Harras, and Hussein Alnuweiri. Malicious attacks in mobile device clouds: A data driven risk assessment. *IEEE Journal on Selected Areas in Communications*, pages 1 – 8, 2014.

[49] Abderrahmen Mtibaa, Khaled A. Harras, and Hussein Alnuweiri. From botnets to mobibots: a novel malicious communication paradigm

for mobile botnets. *IEEE Communications Magazine*, 53:61 – 67, 2015.

[50] Nash and J.F. Equilibrium points in n-person games. *Proc. of National Academy of sciences*, 36:48–49, 1950.

[51] J. Nash. Two person cooperative games. *Econometrica*, 21:128 – 140, 1953.

[52] J. Von Neumann and O. Morgenstern. *Theory of games and economic behavior*. Princeton university press, 60th anniversary commemorative edition, 2007.

[53] John Von Neumann and Oskar Morgenstern. Theory of games and economic behavior. *Princeton University Press.*, 1947.

[54] K. C. Nguyen, T. Alpcan, and T. Basar. Security games with incomplete information. *IEEE International Conference on Communications*, pages 1 – 6, 2009.

[55] Hiroki Nishiyam, Masaya Ito, and Nei Kato. Relay-by-smartphone: realizing multihop device-to-device communications. *IEEE Communications Magazine*, 52:56 – 65, 2014.

[56] Jasmina Omic, Ariel Orda, and Piet Van Mieghem. Protecting against network infections: A game theoretic perspective. *IEEE INFOCOM 2009*, pages 1485 – 1493, 2009.

[57] Emmanouil Panaousis, Tansu Alpcan, Hossein Fereidooni, and Mauro Conti. Secure message delivery games for device-to-device communications. *5th International Conference, GameSec 2014, Los Angeles, CA, USA, November 6-7*, 8840:195–215, 2014.

[58] Emmanouil Panaousis, Eirini Karapistoli, Hadeer Elsemary, Tansu Alpcan, MHR Khuzani, and Anastasios A. Economides. Game theoretic path selection to support security in device-to-device communi-

cations. Under Review at Elsevier Ad Hoc Networks, 2016.

[59] Balasubramanian Paramasivan, Maria Prakash, and Madasamy Kaliappan. Development of a secure routing protocol using game theory model in mobile ad hoc networks. *Journal of Communications and Networks*, 17(1):75 – 83, 2015.

[60] A. Patcha and J. M. Park. A game theoretic formulation for intrusion detection in mobile ad hoc networks. *International Journal of Network Security*, 2:131 – 137, 2006.

[61] Shital Patil and Sangita Chaudhari. Dos attack prevention technique in wireless sensor networks. *Elsevier, Proceedings of International Conference on Communication, Computing and Virtualization (ICCCV)*, 79:715 – 721, 2016.

[62] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc on-demand distance vector (aodv) routing. 2003.

[63] Mikko Raatikainen, Varvana Myllarniemi, Subhamoy Ghosh, Jari Paakko, Tomi Mannisto, Mikko Ylikangas, Olli Korjus, and Eero Uusitalo. Towards mobile device cloud. 2011.

[64] Amir-Mohammad Rahmani, Nanda Kumar Thanigaivelan, Tuan Nguyen Gia, Jose Granados, Behailu Negash, Pasi Liljeberg, and Hannu Tenhunen. Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems. *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, pages 826 – 834, 9-12 January 2015.

[65] A. Ribeiro, G. B. Giannakis, Z. Q. Luo, and N. D. Sidiropoulos. Modelling and optimization of stochastic routing for wireless multihop networks. *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*, pages 1748 – 1756, 6-12 May 2007.

[66] Alejandro Ribeiro, Nikolaos D. Sidiropoulos, and Georgios. B. Giannakis. Optimal distributed stochastic routing algorithms for wireless multihop networks. *IEEE Transactions on Wireless Communications*, 7:4261 – 4272, 2008.

[67] Sajal Sarkar and Raja Datta. A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks. *Elsevier Adhoc Networks*, 37:209 – 227, 2016.

[68] Shahaboddin Shamshirband, Ahmed Patel, Nor Badrul Anuar, Miss Laiha Mat Kiah, and Ajith Abraham. Cooperative game theoretic approach using fuzzy q-learning for detecting and preventing intrusions in wireless sensor networks. *Elsevier Engineering Applications of Artificial Intelligence*, 32:228 – 241, June 2014.

[69] Shigen Shen, Hongjie Li, Risheng Han, Athanasios V. Vasilakos, Yihan Wang, and Qiying Cao. Differential game-based strategies for preventing malware propagation in wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 9:1962 – 1973, 2014.

[70] Ivan Stojmenovic and Sheng Wen. The fog computing paradigm: Scenarios and security issues. *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems*, pages 1 – 8, 7-10 Sept. 2014.

[71] G. Suarez-Tangil, J. E. Tapiador, P. Peris-Lopez, and A. Ribagorda. Evolution, detection and analysis of malware for smart devices. *IEEE Communications Surveys & Tutorials*, 16, 2014.

[72] Swetha.N, Sasirekha.K, and Deepika.K. Malware detection in dtn using game theory. *International Journal of Emerging Technology in Computer Science & Electronics*, 13, 2015.

[73] Mingjun Wang and Zheng Yan. Security in d2d communications: A review. *Trustcom/BigDataSE/ISPA*, 1:1199 – 1204, 2015.

[74] Wenjing Wang, Mainak Chatterjee, and Kevin Kwiat. Coexistence with malicious nodes: A game theoretic approach. *Game Theory for Networks, 2009. International Conference on GameNets'09.*, pages 277 – 286, 2009.

[75] Wei Yu, K. J., and Ray Liu. Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 6:507 – 521, 2007.

[76] Wei Yu, K. J., and Ray 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*, 3:317 – 330, 2008.

[77] Wei Yu, Zhu Ji, and Liu K.J.R. Securing cooperative ad-hoc networks under noise and imperfect monitoring: Strategies and game theoretic analysis. *Information Forensics and Security, IEEE Transactions*, 2:240 – 253, 2007.

[78] Kuan Zhang, Kan Yang, Xiaohui Liang, Zhou Su, Xuemin Shen, and Henry H. Luo. Security and privacy for mobile healthcare networks: from a quality of protection perspective. *IEEE Wireless Communications*, 22:104 – 112, August 2015.

[79] Lizhuo Zhang, Weijia Jia, Sheng Wen, and Di Yao. A man-in-the-middle attack on 3g-wlan interworking. *International Conference on Communications and Mobile Computing 2010*, 1:121 – 125, 12-14 April 2010.

[80] Yongguang Zhang and Wenke Lee. Intrusion detection in wireless ad-hoc networks. *MobiCom '00 Proceedings of the 6th annual interna-*

tional conference on Mobile computing and networking, pages 275 – 283, 2000.

APPENDICES

Appendix A

List of Symbols

You can summarize here the symbols used in this thesis as shown in table A.1 and the EDRG game notations as shown in table A.2

Table A.1: List of symbols

Symbol	Description
$[\mathcal{N}]$	set of $\mathcal{N}$ mobile devices
S	Source device
T	Target device
Q	Data Query
$[R]$	set of available routes from S to T
r_j	j-th route
$[N_j]$	set of devices along r_j
n_i	i-th device
$E(n_i)$	Energy-level of device n_i
$E(r_j)$	Route energy-level on r_j
E_r	Remaining energy for a device
E_{max}	Maximum energy available for a device
ω	Operating system
Ω	set of mobile operating systems
$\mathcal{M}_m$	m-th malware
$[C_\omega]$	set of anti-malware controls that runs ω
$[M_\omega]$	set of malware that infects a device that runs ω
$B(c_k^i, \mathcal{M}_m)$	Capability of the device n_i that runs the anti-malware software c_k to successfully detect the malware $\mathcal{M}_m$.
$D(c_k^i, \mathcal{M}_m)$	Disability of the device n_i to detect malware $\mathcal{M}_m$
$D(r_j, \mathcal{M}_m)$	Disability of route r_j to detect $\mathcal{M}_m$
$\psi(r_j, \mathcal{M}_m)$	Capability of route r_j to successfully detect $\mathcal{M}_m$ before it reaches T

Table A.2: EDRG game notations

Symbol	Description
$U_\Theta(r_j, \mathcal{M}_m)$	Payoff of the defender with pure strategy profile
U_Ψ	Payoff of the attacker
$\mathcal{V}$	Defender's security gain value
X	Defender's mixed strategy
Y	Attacker's mixed strategy
x_j	Probability that defender will choose j-th route
y_l	Probability that defender will choose l-th malware to infect device
$U_\Theta(X, Y)$	Payoff of the defender with mixed strategy profile
X^*	Defender's Nash Equilibrium
Y^*	Attacker's Nash Equilibrium
$U_\Theta(X^*, Y^*)$	Payoff of the defender with Nash Equilibrium
$U_\Psi(X^*, Y^*)$	Payoff of the attacker with Nash Equilibrium

Appendix B

Two-Person Zero Sum Games

Definition: Two players zero sum games [26]

$u_2(x)$ = - $u_1(x)$ for each $x \in X$, valid for all x strategies.

Representation as one matrix $M \in \mathcal{R}^{mXn}$

In pure profile (i, j):

player 1 has a_{ij} utility and player 2 has utility of - a_{ij}.

How to solve the zero-sum game?

Example: Matching pennies

$$[A] = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \tag{B.1}$$

utility $u_1(x_1, x_2)$ = - $u_2(x_1, x_2)$ = $\sum_{i=1}^{m} \sum_{j=1}^{n} x_{1i}.x_{2j}.a_{ij}$.

= $x_1^T.M.x_2$

Using linear programming to solve the optimization problem in polynomial time.

Given vector $c \in \mathcal{R}^n$, matrix $M \in \mathcal{R}^{nXm}$ and vector $b \in \mathcal{R}^m$

Find $x \in \mathcal{R}^n$ that satisfies M . $x \leq b$ and maximizes c^T. x

Assume player 1 chooses x_i first then player 2 chooses the best response x_2 against x_i.

In the best response $x_2, x_{2j} > 0$ only if the expected utility of strategy j is minimal.

The utility of player 2: $\sum_{j=1}^{n} \sum_{i=1}^{m} x_{1i}.a_{ij}.x_{2j}$

= $\underset{j=1}{min}^n \sum_{i=1}^{m} x_{1i}.a_{ij}$ = $\underset{j=1}{min}^n \; V$

The utility of player 1:

$V \leq \sum_{i=1}^{m} x_{1i}.a_{ij}$ for j=$1 \ldots n$

so player 1 wants to maximize V. So player 1 chooses x_1 in order to maximize V.

Then using linear programming: Maximize V

such that

V - $\sum_{i=1}^{m} x_{1i}.a_{ij} \leq$ 0, for j=$1 \ldots n$.

$\sum_{i=1}^{m} x_{1i}$=1, for i=$1 \ldots m$.