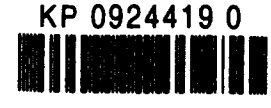
Security for Mobile Ad-hoc Networks

Emmanouil A. Panaousis

Wireless, Multimedia & Networking Research Group
Faculty of Science, Engineering & Computing
School of Computing & Information Systems
Kingston University London

This dissertation is submitted for the degree of
Doctor of Philosophy (Ph.D.)

2012



1. External Examiner: Professor Keith Martin

Director of the Information Security Group (ISG)

Royal Holloway, University of London

Egham Hill

Egham, Surrey TW20 0EX

United Kingdom

2. Internal Examiner: Dr Eckhard Pfluegel

Senior Lecturer

Kingston University London

Penrhyn Road, Kingston-Upon-Thames

London KT1 2EE

United Kingdom

Signature from Chair of PhD committee:

Faculty of Science, Engineering and Computing (SEC)

School of Computing and Information Systems (CIS)

Kingston University London

Penrhyn Road, Kingston-Upon-Thames

London KT1 2EE

ABSTRACT

Ad-hoc networks are crucial enablers of next generation communications. Such networks can be formed and reconfigured dynamically and they can be mobile, standalone or internetworked with other networks. Mobile Ad-hoc NETworks (MANETs) are established by a group of autonomous nodes that communicate with each other by establishing a multihop radio network and maintain connectivity in an infrastructureless manner. Security of the connections between devices and networks is crucial. Current MANET routing protocols inherently trust all participants being cooperative by nature and they depend on neighbouring nodes to route packets to a destination. Such a model allows malicious nodes to potentially harm MANET communications links or reveal confidential data by launching different kind of attacks. The main objective of this thesis is to investigate and propose security mechanisms for MANET communications mainly emphasising on emergency scenarios where first responders' devices communicate by establishing a decentralised wireless network. To this end, we have proposed security mechanisms for innovative routing and peer-to-peer overlay mechanisms for emergency MANETs proposed supplementarily to the findings of this thesis. Such security mechanisms guarantee confidentiality and integrity of the emergency MANET communications. We have also proposed novel ways of improving availability in MANETs in presence of intrusion detection systems by increasing the nodes' lifetime based on a novel game theoretic routing protocol for MANETs. We have thoroughly evaluated the performance of all the proposed mechanisms using a network simulator. The main objective of undertaking these evaluations was to guarantee that security introduces affordable overhead thereby respecting the Quality-of-Service of MANET communication links.

Acknowledgments

As I started to think of all the people to whom I would like to express my appreciation for their support, in making this thesis possible, the list continued to grow. First, I am fortunate and proud to have been advised by Christos Politis. He has been a constant source of support and ideas during the past four years. I learned tremendously from his vision, professionalism, working ethics and desire for excellence. Always available, always with a smile, he would help me see the bigger picture in academic, professional, and personal matters. I would also like to thank him for opening up several collaboration opportunities. It was tremendously crucial that he was instrumental in creating the right environment within the Wireless, Multimedia & Networking (WMN) research group.

I would like to thank my family and especially my grandparents for their continuous support, love and encouragement during my PhD studies but also for their guidance in difficult times. The reason I am here today is them thereby my goal was to make them proud by trying harder every "PhD" day.

My best thanks to my fiancee Virginia. Her patience and love to me has played such a central role that I don't know where to start. Her support and accurate advices during hard research moments enhanced my work ethics crucially.

I should express my thankfulness to my colleagues and friends, Grant Millar and Arvind Ramrekha for their invaluable collaboration during these three and a half years. Arvind was leading the activities within the realm of QoS routing for MANETs while Grant was responsible for designing the novel ROBUST P2P overlay architecture for MANETs. I would also like to thank Maria Martini for agreeing to be my second supervisor and for providing valuable feedback whenever requested. Additionally, I would also like to thank all my colleagues in the WMN research group for their professionalism which created an ideal environment for research.

In particular, kind thanks must be given to Eckhard Pfluegel and Professor Keith Martin (director of the ISG at Royal Holloway) who agreed to be my PhD examiners.

Furthermore, my sincere thanks to the School of Computing & Information Systems (CIS) at Kingston University London which generously supported me with a research student scholarship. I would also like to thank all the partners from academia, industry and research institutes, who I met with working for the EU FP7 ICT-SEC PEACE project. Discussions with them have greatly shaped my thinking. I will never forget the final project review and the excellent comments we received by the project reviewers and the EC officer. Most importantly, the financial support of this project is highly appreciated.

Last but not least, I would like to thank my previous teachers and colleagues whose personalities and educational methods have affected me most. The advisor of my MSc dissertation, Professor George C. Polyzos has play a key role in my research path by introducing me to the technologies of wireless and mobile communications and constantly encouraging me to publish my first scientific paper. Thus, I would really like to thank him along with my previous colleagues from MMLAB, Pantelis Frangoudis, Christoforos Ververidis and Konstantinos Katsaros.

Table of Contents

List of Figures

List of Tables

To my family and Virginia for their unconditional support.

List of Abbreviations

$\mathcal{NE}$	Nash Equilibrium
3DES	Triple Data Encryption Standard
ADVSIG	Advanced Signature System
AES	Advanced Encryption Standard
AH	Authentication Header
AODV	Ad hoc On demand Distance Vector
AODV-WADR	AODV Wormhole Attack Detection Reaction
AOMDV	Ad-hoc On-demand Multipath Distance Vector
ARAN	Authenticated Routing for Ad hoc Networks
ATT	Actual Traversal Time
ATT-WADR	Actual Traversal Time Wormhole Attack Detect and Reaction
BNE	Bayesian Nash Equilibrium
CA	Certificate Authority
CBR	Constant Bit Rate
CML	ChaMeLeon
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
D-H	Diffie-Hellman
DARPA	Defense Advanced Research Projects Agency
DARWIN	Distributed and Adaptive Reputation mechanism for WIreless ad hoc Networks
DCF	Distributed Coordination Function
DES	Data Encryption Standard
DHT	Distributed Hash Table
DNS	Domain Name System
DoS	Denial-of-Service
DSR	Dynamic Source Routing
DYMO	Dynamic MANET On-demand
EC	European Commission
eMANET	Emergency MANET
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standards
FR	First Responder
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GTMR	Game Theoretic MANET Routing
HIDS	Host-based Intrusion Detection System

HMAC	Hash-based Message Authentication Code
HUMO	HUman Mobility mOdel
ICMP	Internet Control Message Protocol
ICV	Integrity Check Value
IDEA	International Data Encryption Algorithm
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol Security
LAN	Local Area Network
LANMAR	Landmark Ad Hoc Routing Protocol
LTE	Long Term Evolution
M2M	Machine-to-Machine
MAC	Medium Access Control
MAC	Message Authentication Code
MANET	Mobile Ad hoc Network
MCM	Mission Critical Mobility
MD5	Message Digest 5
MIPS	Millions Instructions Per Second
MITM	Man-In-The-Middle
MPP	Mobile Peer-to-peer Protocol
MPR	MultiPoint Relays
MTT	Maximum Traversal Time
MTTF	Mean Time To Failure
MTU	Maximum Transmission Unit
NetTT	Network Traversal Time
NGN	Next Generation Network
NHDP	NeighborHood Discovery Protocol
NIST	National Institute of Standards and Technology
NodeTT	Node Traversal Time
ns-2	network simulator-2
NST	Network Size Threshold
OLSR	Optimized Link State Routing
OLSRv2	Optimized Link State Routing version 2
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
P2P	Peer-to-Peer
P2PSIP	Peer-to-Peer Session Initiation Protocol
PBE	Pareto Bayesian Equilibrium
PDA	Personal Digital Assistant
PEACE	IP-based Emergency Application and serviCes for nExt generation networks
PKI	Public Key Infrastructure
PSK	Pre-Shared Key
QoS	Quality-of-Service
RC5	Rivest Cipher 5
RDP	Routing Discovery Packet
RF	Radio Frequency
RFID	Radio-Frequency identification

ROBUST	Reliable Overlay Based Utilisation of Services and Topology
RREP	Route Reply
RREQ	Route Request
RSA	Rivest, Shamir and Adleman
RTT	Round Trip Time
S-D	Source-Destination
SA	Security Association
SA-OLSR	Security Aware Optimized Link State Routing
SAODV	Secure Ad hoc On-demand Distance Vector
SAR	Security-Aware ad hoc Routing
SCML	Secure ChaMeLeon
SHA	Secure Hash Algorithm
SHARP	Sharp Hybrid Adaptive Routing Protocol
SkiMPy	Simple key management for MANETs
SLSP	Secure Link-State routing Protocol
SPD	Security Policy Database
SPIT	SPam over Internet Telephony
SRP	Secure Routing Protocol
SYN	SYNchronous
TBRPF	Topology Broadcast based on Reverse-Path Forwarding
TC	Topology Control
TCP	Transmission Control Protocol
TFT	Tit-For-Tat
TTL	Time-To-Live
UDP	User Datagram Protocol
VCG	Vickrey-Clarke-Groves
VLC	VideoLAN Client
WEP	Wired Equivalent Privacy
WG	Working Group
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Networks
ZRP	Zone Routing Protocol

Chapter 1

Introduction

"It shouldn't surprise you that a system that is designed to be manufactured as cheaply as possible is designed with no security constraints whatsoever". Peter Neumann

This chapter introduces the direction of our work, the motivation that drives us into carrying out this research, and the research contributions of this thesis. In Section 1.1, we introduce fundamental issues of *Mobile Ad-hoc NETworks* (MANETs) emphasising security. Section 1.2 discusses the research objectives while Section 1.3 presents our main research contributions and mentions the main publications related to the work undertaken in this thesis. Finally, in Section 1.4 we briefly outline this thesis' main structure.

1.1 Research motivation

1.1.1 Mobile ad-hoc networks

The *Wireless Local Area Networks* (WLANs), developed back in the 1990s, are one of the most important license-exempt access network technologies nowadays. They allow data, voice and video communications over a wireless channel. A particular class of standards which has clearly dominated the market is the IEEE (Institute of Electrical and Electronics Engineers) 802.11 wireless LAN, also known as *Wireless-Fidelity* (Wi-Fi). These networks can operate in two modes; (i) *infrastructure*, which uses a wireless access point, and (ii) *ad-hoc*

mode, which allows the creation of a self-configuring network consisting of mobile routers (for example laptops, smart phones) which are interconnected by wireless links. The latter are called MANETs [1] and their scope is to enable routing functionalities into the mobile nodes. A MANET, as described by the Internet Engineering Task Force (IETF) MANET Working Group (WG), is a temporary or permanent autonomous network comprised of free roaming nodes intending to establish wireless communications in absence of network infrastructures.

The main role of MANETs is to enable wireless and mobile communication services without using the expensive service-provider network and without having a previously set up infrastructure. The network in that case is decentralised and the mobile nodes must accomplish network activities (network discovery) and must deliver the messages to each other by acting as routers. Therefore, MANET devices are able to sense the presence of other devices, establish communication links among them and communicate information.

MANETs consist of a set of self-organised communicating devices that may play the role of a data *source*, *destination* or *router*. Data can be sent directly from a source to a destination if both are within the same communication range of each other. This range is defined, each time, by the enabling technology such as Zigbee (IEEE 802.15.4), Bluetooth (IEEE 802.15.1) and Wi-Fi (IEEE 802.11).

1.1.2 MANET applications

In the following we categorise the major MANET applications:

- *Wireless mesh networks*: these networks can provide both indoor and outdoor broadband wireless connectivity in urban, suburban, and rural environments without the need for costly wired network infrastructure. Examples of such networks could be the following:
  - *Public Internet access networks*: These are wireless mesh networks that could provide broadband, for instance, in a town;

  - *Intelligent transportation systems*: Wireless mesh networks could act as information delivery systems to control transportation services;
  - *Public safety systems*: Wireless mesh networks could be the vehicle to address the requirements of law enforcement agencies and city governments by supporting military communications or emergency communications as substitute of current Public Protection Disaster Relief (PPDR) systems.

- *Opportunistic Networks*: these networks can provide intermittent Internet connectivity to rural and developing areas in low prices. Another application of opportunistic networks could be, for instance, wildlife monitoring to track wild species, examine their behaviour and understand their reaction to the ecosystem changes due to human activities.

- *Vehicular Ad-hoc Networks*: these networks use ad-hoc communications to assist driving and increasing car safety. Examples of such communications could be the propagation of data from the roadside and from other cars or the provision of information regarding obstacles on the road, emergency events and traffic information to drivers (requiring multi-hopping mainly due to line-of-sight limitations).

- *Wireless Sensor Networks*: these networks consist of wireless, battery powered sensors with computing and communication capabilities. Examples of applications of wireless sensor networks that target to communicate information between sensors or to a central entity, could be the following:

  - *Tracking applications*: wireless sensor nodes can be deployed to sense the presence of persons and objects in certain areas;
  - *Smart homes*: in today's houses wireless sensors and actuators can communicate with the environment and people, delivering next generation services as smart metering, smart lighting and so on;
  - *Environmental monitoring*: wireless sensors can be used for forest fire detection,

flood detection, to allow a fast reaction before an accident becomes uncontrollable;

- *Health monitoring*: wireless sensors can be used as part of a health monitoring system provided to a patient. Such sensors could, for instance, communicate with the patient's doctor in order to send notifications about the health status or alarms in case of an emergency health condition.

1.1.3 Emergency MANETs

The transition to *Next Generation Networks* (NGNs) is often coupled with the vision of innovative services providing personalised and customisable services over an all-IP (Internet Protocol) infrastructure. To enable a smooth transition, next generation all-IP networks need not only to support more services but also to support current vital services such as *emergency services.*

Our modern densely populated cities have created an Achilles heel for public safety services where natural or man-made disasters often result in high casualties. In these events, existing telecommunication infrastructures, such as *Global System for Mobile Communications* (GSM), may either collapse or get congested. For instance, the 2005 London bombings have exposed the inadequacy of current *Public Protection and Disaster Relief* (PPDR) communication systems for modern response operations.

Therefore, it is important to design and develop alternative means of communication infrastructure, such as mobile ad-hoc networking, to allow First Responders (FRs) to communicate in a reliable manner. In addition, as current PPDR systems are significantly expensive to operate[1], MANETs can have a significant economic impact by reducing the cost of procuring and operating PPDR communication systems. MANETs can also reduce the cost of mobile data traffic compared to existing traditional PPDR technologies and will have no operational cost by using license exempt parts of the spectrum. Additionally, cross-border European PPDR initiatives would be feasible at much lower cost since MANETs

[1] At the moment First Response (FR) organisations must pay whenever FRs communicate with each other.

can provide an appropriate interoperable communication platform.

In a nutshell, migrating PPDR systems to NGNs, such as MANETs, will significantly help FRs to enhance their response during emergency situations by:

- providing multimedia services (text, video, data) and,
- establishing an all-IP based system allowing FRs from the same or different organisations to communicate with each other. Such a system will also help citizens to look efficiently for friends and relatives in case of large scale disasters. In addition, the all-IP nature of MANETs enables interoperability with other IP-based technologies such as *Wireless Sensor Networks* (WSNs).

To meet the above challenges, the EU FP7 ICT-SECURITY PEACE project investigated the provisioning of day-to-day emergency communications in next generation all-IP networks. Part of PEACE's scope was to deploy MANETs to reduce operation cost compared to traditional PPDR systems, enable interoperability between different emergency teams such as police, fire brigade, paramedics and enable communication when traditional telecommunications infrastructures, such as 3G, have failed.

This PhD was funded by PEACE thereby some of the objectives of this thesis have been examined within the realm of emergency communications as described in this project. Consequently, this thesis was partially required to operate within the constraints set by PEACE. For instance, the selected scenarios consider emergency network communications by being simulated and evaluated using the *Mission Critical Mobility* (MCM) model [2] which has been developed within the context of PEACE. The main functionality of MCM is the simulation of the FRs' mobility during rescue missions, in presence of obstacles.

The main PEACE research contributions concerned with the provision of high Quality-of-Service (QoS) multimedia communications for emergency MANETs (eMANETs) are the following:

- A novel MANET routing mechanism which outperforms traditional MANET routing protocols in terms of QoS such as *delay* and *jitter*;

- Security for such a routing mechanism (one of the contributions of this thesis, this will be part of the research objective RO2, as introduced in section 1.2);
- A novel peer-to-peer overlay for MANETs which outperforms the traditional Distributed Hash Tables (DHTs) mechanisms in terms of *average path length, average lookup delay* and *completed lookups*;
- Security for such a novel peer-to-peer overlay architecture (part of the research objective RO3).

1.1.4 MANET characteristics

A great number of authors have investigated aspects, requirements and solutions for MANET security, such as [3]. The task of creating solutions for providing the standard security goals of *confidentiality, integrity* and *availability* is particularly challenging in MANETs, primarily due to their following characteristics:

- *Exposure through the wireless medium*: MANETs impose several challenges since the use of wireless links allows a large set of attacks to target these networks. This happens because signals are propagated from a source node over the open air to all directions and prospective attacks can be launched by anyone and from any direction. Although a mechanism can provide confidentiality and integrity of the messages sent over a MANET, it can not provide defence against traffic analysis. In addition, adversaries can launch a *Denial of Service* (DoS) attack, such as jamming, in oder to disrupt the MANET communications.
- *Weaknesses of routing protocols*: MANET nodes need to cooperate with each other to carry out routing functionalities, as in Fig. 1.1. Thus, routing can introduce a significant security hole in the presence of malicious nodes. Data tampering, DoS and impersonation attacks are some examples of malicious activities that can be easier, than WLANs, launched against MANETs due to the cooperative nature of routing protocols.

- *Lack of fixed and centralised infrastructure:* MANETs do not deploy any fixed infrastructure meaning that central nodes to direct packets do not exist. Therefore, monitoring traffic in MANETs becomes a harder problem while public key cryptography schemes are hard to employ since they require the existence of a *Certificate Authority* (CA) which must be a central trusted point. Another aspect of MANETs that increase the difficulty for monitoring the network traffic is the network segmentation which takes place when MANET nodes move in different locations of the network in a way that they make communication partitions while some of them lose connection towards some destination nodes. The same situation occurs when MANET nodes die faster by exhausting their battery levels.

- *Limited resources*: MANET devices are usually smart devices such as mobile phones, personal digital assistants, tablets or laptops. These have limited memory, battery level, processing power and cannot support very high network bandwidth. These hinder the application of computationally intensive security algorithms such as greedy asymmetric cryptographic schemes and data management.

- *Mobility and dynamic topology*: In MANETs, nodes are allowed to move peremptorily, thereby network topology can change in a non-stochastic manner causing changes to the MANET routing tables. Consequently, this can cause high complexity in terms of network management. Also, the frequent changes in the dynamic network topology makes hard to differentiate normal from malicious behaviour. In addition, due to mobility reasons nodes can be at risk of being compromised.

1.1.5 Security of MANETs

The main security requirements applied to MANETs are summarised as follows:

- *Confidentiality:* In a MANET only the sender and the intender receiver of a message should be able to reveal its contents.

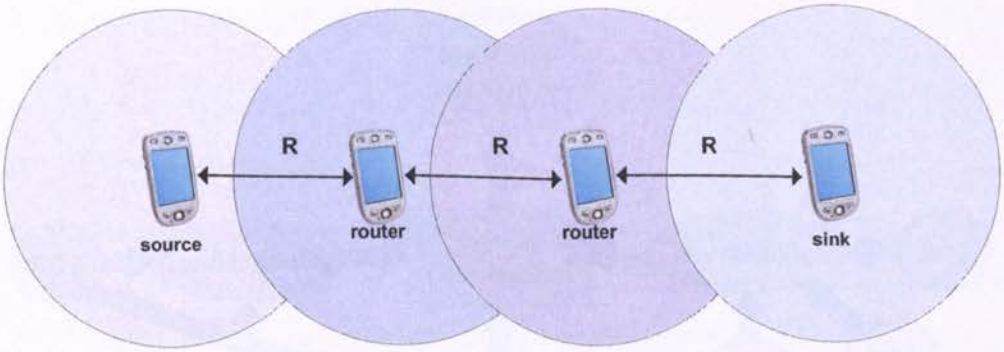


Figure 1.1: Multihop ad-hoc communication.

- *Integrity: Message integrity* ensures that messages can be modified only by authorised MANET nodes using authorised ways. Any unauthorised alteration can be detected by other MANET nodes. On the other hand, *message origin authentication* guarantees that both the sender and the receiver of a message must be able to confirm that the other communication party is who claims to be. Furthermore, when *entity authentication* is satisfied, each MANET node can verify the identity of the other communicating party while *data authentication* guarantees as to the origin of data. *Non-repudiation* ensures that the origin of a message cannot deny having sent the message.
- *Availability*: Such a requirement aims to ensure that network services are available in spite of malicious activities.

1.2 Research aims and objectives

This thesis aims to contribute to MANET security by applying symmetric cryptography to secure existing MANET protocols and architectures. Another goal is to conduct network performance evaluation using packet level network simulators. In this way, this thesis prepares the grounds for prototype implementations. The main Research Objectives (ROs) of this thesis are summarised, as follows:

RO1. To improve *availability* in emergency MANETs by mitigating wormhole attacks, based on extending the *Ad hoc On-Demand Distance Vector* (AODV) [4] routing protocol;

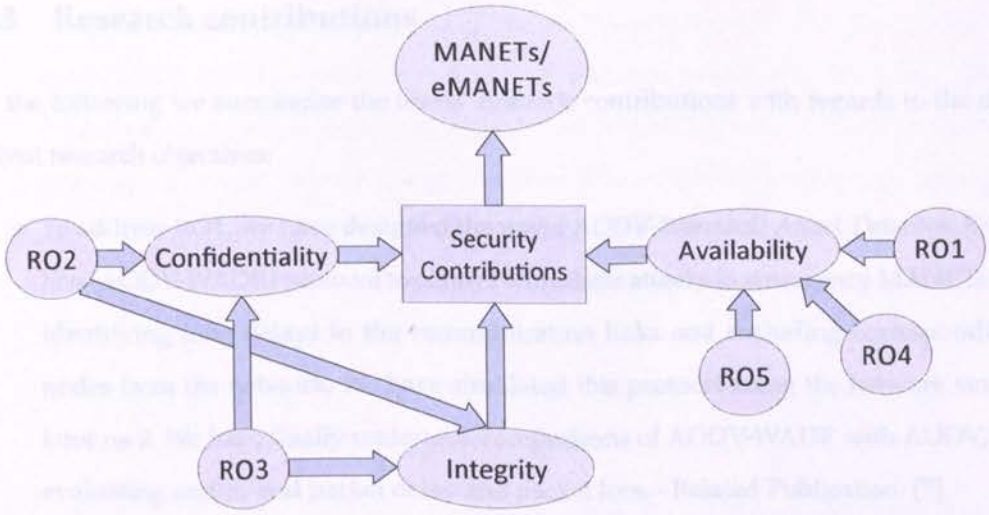


Figure 1.2: Schematic representation of the thesis' research objectives and their correlation with the main security requirements.

RO2. To establish *confidentiality* and *integrity* for emergency MANETs by providing a secure version of the *ChaMeLeon* (CML) routing protocol published in [5];

RO3. To provide security for peer-to-peer (P2P) overlays in MANETs by extending the *Reliable Overlay Based Utilisation of Services and Topology* ROBUST architecture published in [6];

RO4. To devise new game theoretic models for formulating interactions between MANET IDSs and a group of malicious nodes, with an emphasis on defending routes and nodes;

RO5. To use these models for the design of a novel game theoretic routing protocol, reducing the network-wide intrusion detection cost of protecting MANET routes.

Throughout this dissertation, we will refer to these objectives by using their acronyms RO1 – RO5.

1.3 Research contributions

In the following we summarise the thesis' research contributions with regards to the different research objectives:

- To address RO1, we have designed the novel *AODV-Wormhole Attack Detection Reaction* (AODV-WADR) protocol to control wormhole attacks in emergency MANETs by identifying long delays in the communication links and excluding corresponding nodes from the network. We have simulated this protocol using the network simulator ns-2. We have finally undertook comparisons of AODV-WADR with AODV, by evaluating end-to-end packet delay and packet loss. - Related Publication: [7].

- To achieve RO2, we have designed the *Secure ChaMeLeon* (SCML) protocol. SCML is the secure version of CML and it has been designed by using a hybrid version (AH and ESP in transport mode) of IPsec tailored for MANETs. SCML has been simulated in ns-2 in order to evaluate its performance in terms of *throughput, extra routing load* due to security and *average end-to-end packet delay* showing that the protocol can support high QoS communications in emergency cases. Within the same context, we have undertook comparison of SCML with the pure CML, CML using IPsec in AH mode and CML using IPsec in ESP by evaluating the *cumulative packet end-to-end delay, cumulative routing control load* and *cumulative throughput*. More importantly, we have undertook comparison with SAODV, in terms of *routing control load* and the *ratio of data to routing control load*. - Related Publications: [8], [9] and [10].

- Regarding RO3, we have designed the secure version of the novel peer-to-peer overlay architecture for MANETs, called ROBUST, by *securing the DHT signalling messages, using symmetric key encryption*. To evaluate the performance of this secure architecture we have used ns-2 simulations. The results illustrate the *end-to-end DHT data request delay and overhead*, and *DHT signalling packet loss* to ensure that such a secure peer-to-peer overlay architecture can support high QoS communications which is a crucial requirement of emergency MANETs. - Related Publication: [6].

- To address RO4, we have proposed two game theoretic models. The first model is a non-cooperative, non-zero sum game model that aims to minimise the energy spent for intrusion detection to defend the different MANET routes. The second model proposes an optimal defence strategy for MANETs by deriving the intrusion detection effort required to achieve an "optimal" balance between intrusion detection cost, for defending MANET nodes, and detection accuracy. Based on the second model, we have undertaken numerical analysis using MATLAB to evaluate the MANET utility by deriving its performance for different types of *networks, mobility levels, packet sizes* and *intrusion detection rates*. - Related Publications: [11] and [12].

- RO5 has been fulfilled by the proposed *Game Theoretic MANET Routing* (GTMR) protocol which increases MANET availability by reducing the network-wide intrusion detection cost for defending MANET routes, based on a non-cooperative game theoretic model. By developing GTMR in ns-2, we have conducted comparisons with AODV, OLSR and AOMDV, to evaluate the *average node lifetime, total routing overhead, average end-to-end packet delay* and *average intrusion detection energy cost per node*. This contribution addresses RO5. - Related Publications: [11] and [13].

1.4 Thesis structure

The remainder of this thesis is organised as follows. Chapter 2 presents an overview of the state of the art in relevant research fields. This chapter presents a general survey of MANET security research by providing a detailed explanation of the MANET security requirements, vulnerabilities and attacks. It also discusses how the emergency MANET setting changes the security requirements and the assumptions that have been made throughout this thesis regarding emergency MANETs. For each of the research questions considered in our work, this chapter provides adequate background to understand the problem being worked on, presents a detailed literature review of the examined topics and concludes by identifying our contributions. Chapter 3 focuses on secure routing approaches for emergency

MANETs. First, it proposes and evaluates a routing protocol which improves *availability* in emergency MANETs by mitigating wormhole attacks based on extending the well-known AODV protocol. Second, it proposes and evaluates a secure version of the CML routing protocol to establish *confidentiality* and *integrity* for emergency MANETs. In Chapter 4 we examine how to provide security for peer-to-peer (P2P) overlays in MANETs. Especially, we propose the secure version of the novel peer-to-peer overlay architecture for MANETs, called ROBUST, by securing the DHT signalling messages. We then present and discuss the performance evaluation results retrieved by developing this DHT architecture in ns-2 and comparing this protocol with the pure ROBUST by evaluating average end-to-end DHT data request delay, overhead and DHT signalling packet loss. Chapter 5 examines how to increase MANET availability in presence of intrusion detection systems, by reducing the network-wide intrusion detection cost for defending either the MANET routes or nodes. We have used game theory to model non-cooperative security games between a MANET and a group of collaborative malicious nodes called *malicious coalition* (MC). Specifically, we propose two game theoretic models as follows. Model I formulates the situation where a MANET defends routes whilst Model II examines the case where the MANET protects individual nodes. Based on Model I, we propose and evaluate the *Game Theoretic MANET Routing* (GTMR) protocol which maximises the utility of the MANET at the NE thus leading to an optimal defence strategy for the MANET. Based on Model II we derive the optimal intrusion detection effort (monitoring probability) for each MANET node in order to achieve the best balance between intrusion detection cost and detection accuracy in MANETs. Chapter 6 concludes this thesis summarising our findings and highlighting our main contributions with respect to the thesis' objectives. We also deduce the research limitations and the main avenues for future work in the field of security for mobile ad-hoc networking.

Chapter 2

Background and Literature Review

"The artist is nothing without the gift, but the gift is nothing without work", Emile Zola

This chapter provides the background required to understand the rest of the thesis. In Sections 2.1 and 2.2, we will discuss fundamental MANET issues such as routing and peer-to-peer overlays. We have then, in Section 2.3, given a detailed explanation of the MANETs' security requirements (a more detailed version of the brief coverage in the introduction), vulnerabilities and attacks against MANETs. This section also summarises the main areas of MANET security related to this thesis. In Section 2.4, we introduce the notion of emergency MANETs, innovative routing and *peer-to-peer* (P2P) protocols for such a network and the security assumptions that have been made in this thesis due to the mindset defined by the emergency MANET concept. Sections 2.5 – 2.8 discuss related to this thesis' work. Section 2.5 deals with wormhole attacks against MANETs, Section 2.6 examines secure routing mechanisms for MANETs, Section 2.7 discusses security for peer-to-peer overlays in MANETs and finally Section 2.8 investigates game theoretic applications that enhance intrusion detection in MANETs. For each of the research questions this chapter provides enough background for the reader to understand the problem being worked on, a literature review in the context of this problem and finally identifies the gaps in the existing research that this thesis intends to tackle.

2.1 Routing for MANETs

The MANET *Working Group* (WG) of the *Internet Engineering Task Force* (IETF), formed in 1997, is currently leading the standardisation activities for an appropriate *Internet Protocol* (IP) based routing protocol functionality for both static and dynamic wireless routing topologies. The establishment of the MANET WG has been a catalyst towards research in the field of MANET routing, sparkling the creation of several scientific forums and the publication of vast amount of scientific papers addressing related challenges and possible solutions. The protocols developed by the MANET WG are considered to be the most suitable routing approaches for implementation. In addition to well-known wireless networking problems, MANETs present researchers with several peculiar routing challenges as described in [14], [15], [16]. There are two main MANET routing approaches as follows:

- *Proactive MANET routing*: The proactive routing approach, also known as *table driven routing*, consists of maintaining consistent and updated route information between all possible *Source-Destination* (S-D) pairs in the routing tables. Thus, routes between S-D pairs are always available reducing the latency in route establishment. Since a large amount of routing information is periodically disseminated and stored, the downside to such an approach is the high overhead of control packets and power consumption even when no data is being transmitted. *Optimized Link State Routing* (OLSR) [17] is a very popular proactive protocol, and in fact it is used for most of the implementations currently considered by IETF.

- *Reactive MANET routing*: A reactive routing approach, also known as *on-demand routing*, establishes and maintains routes between S-D pairs when requested by the data source node. Although such an approach generates routing overhead only on-demand, it nevertheless requires added latency for route discovery before routes are established. The *Dynamic Source Routing Protocol* (DSR) [18] is a well-known reactive protocol that utilises route discovery and route maintenance on-demand to route data from a source to a destination. The *Ad hoc On-Demand Distance Vector* (AODV) routing

protocol [4] is another well-known reactive protocol. AODV uses an on-demand route discovery and maintenance algorithm for route establishment in unicast routing and it is based on a modified Bellman-Ford [19] algorithm. AODV attempts to improve DSR by maintaining routing tables at the nodes, thus data packets do not have to contain routes. Another reactive MANET routing protocol is the AOMDV (Ad-hoc On-Demand Multipath Distance Vector) [20]. The main property which distinguishes AOMDV from AODV is that it enables loop-free and mutually link-disjoint multiple paths to a destination of a communication path providing fault tolerance. AOMDV chooses an optimal path until this breaks. Alternative routes are cached and they will be called only when a link failure occurs.

- *Hybrid MANET routing*: Hybrid MANET routing protocols use both reactive and proactive routing methods. There is also another classification of such routing protocols based on their zonal and converged characteristics. In zonal routing approaches, both reactive and proactive routing functionalities are used in different demarcated network areas. In converged approaches adaptivity mechanisms are required to change protocol operation from reactive to proactive and vice versa. A novel MANET routing protocol called ChaMeLeon (CML) [21] is an adaptive hybrid routing approach that differs from previous protocols in that it does not maintain routing zones. Alternatively, CML operates in a converged approach that is optimally maintained using three phases of operation (Oscillation (O)-phase, Proactive (P)-phase and Reactive (R)-phase) while each phase has amplified features on top of the utilised flat routing mechanism that works in parallel to the traditional routing protocol.

In this thesis, routing is a fundamental starting point of our work, as we improve various aspects of AODV when accomplishing our research objectives RO1 and RO5, and CML within the security extensions for our objective RO2.

2.2 Peer-to-peer overlays for MANETs

The lack of centralisation built within MANETs should adhere developers to apply the same peer-to-peer paradigm when building applications and services. For example when node A wishes to contact node B and does not know any other information except the fact the node is referred to as node B it must utilise some distributed name lookup scheme which should return an IP address from the name. The same concept can be applied in many services making the transition from traditional client-server networks to MANETs where the services depend on a system which would normally rely on a central entity. Examples of such services include; DNS [22], P2PSIP [23], Distributed File Systems (DFS) [24] and general information sharing using rich media such as images. All of these services can be combined to create a media rich peer-to-peer (P2P) group collaboration environment.

A pure peer-to-peer network does not encompass the notion of clients or servers. Peer nodes act as both clients and servers to other network nodes. Peer-to-peer systems usually implement an abstract overlay network, above the physical network topology. Nodes in an overlay can be seen as being connected by virtual or logical links, each of which corresponds to a path, likely through several physical links, in the underlying network.

Therefore to exploit the synergy of the peer-to-peer paradigm in MANETs, one must look towards an integrated solution to applications and information sharing, such as *Distributed Hash Tables* (DHTs). The motive for using DHT in MANETs is due to an extremely quick setup time in both application and network layer in addition to the fact that no additional infrastructure is needed in either layer other than the devices themselves.

DHTs allow us to find the exact location of a party or piece of information stored within the network, using a piece of simple meta-data for example a name and domain, as proposed in *Peer-to-Peer Session Initiation Protocol* (P2PSIP) [23]. However the use of DHTs is not limited to simple name resolution and their distributed structure also allows for fast propagation and high availability of information through the network. When applied to MANETs which have no central authority, DHTs could provide the answer to distributed services such as *Domain Name System* (DNS), P2PSIP, distributed storage and information

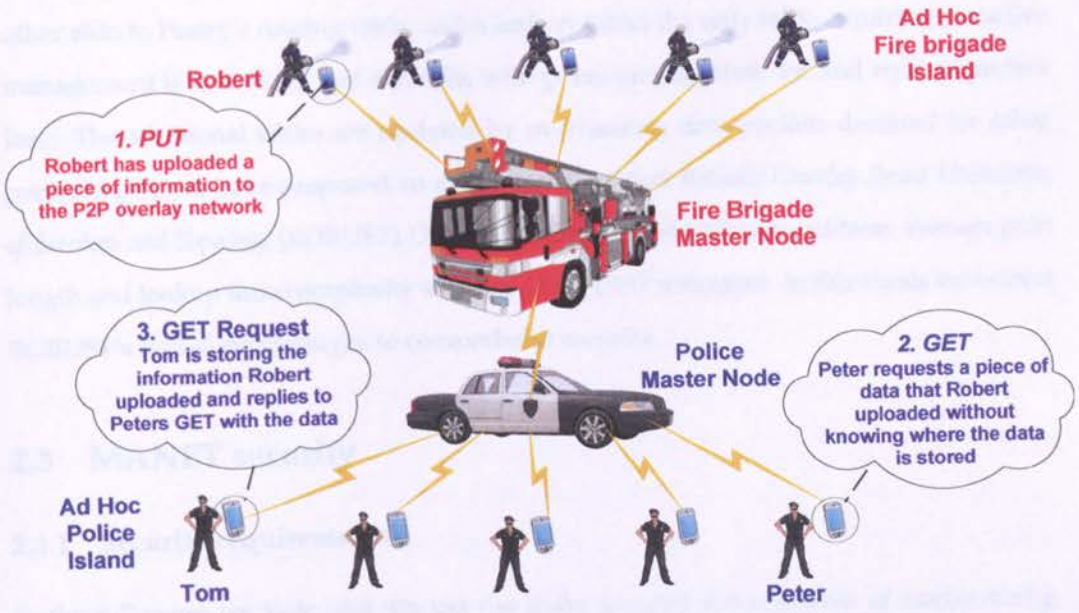


Figure 2.1: An example of how data sharing works in a DHT.

sharing, whilst aiding service lookup and discovery. Last but not least, all types of data could be stored redundantly and accessed easily and quickly by any peer.

The authors of [25] specifically examine cross-layer DHT MANET protocols. The examined architectures are Etka [26], *Mobile Peer-to-peer Protocol* (MPP) [27], a Gnutella optimisation for MANETs [28], FastTrack over AODV [29], and MADPastry [30]. Amongst these architectures, Etka and MADPastry are structured P2P overlays whilst the rest are unstructured. The Etka [26] architecture tightly integrates the structured P2P protocol based on DHTs with the routing architecture of MANETs by mapping logical DHT peer identities (IDs) to their MANET IP based counterparts causing the two separate architectures to merge into one structure. This is achieved by integrating the Pastry DHT with the *Dynamic Source Routing* (DSR) MANET multi-hop routing protocol at the network layer. MADPastry [30] is a DHT substrate which acts by combining the Pastry DHT with AODV MANET routing at the network layer. This can lower the overhead needed to maintain the DHT. While the architecture utilises three different routing tables (one akin to AODV's routing table, an-

other akin to Pastry's routing table, and a leaf-set table) the only table requiring proactive management is that of the leaf-set table, with peers pinging their *left* and *right* respective leafs. The additional tables are updated by overhearing data packets destined for other peers. In [31], we have proposed an architecture entitled *Reliable Overlay Based Utilisation of Services and Topology* (*ROBUST*) DHT for emergency MANETs to address average path length and lookup time complexity when sending DHT messages. In this thesis we extend ROBUST's signalling messages to comprehend security.

2.3 MANET security

2.3.1 Security requirements

In the following we state and discuss the main security requirements of *confidentiality*, *integrity* and *availability* within the context of MANETs.

2.3.1.1 Confidentiality

Confidentiality guarantees that message content is never revealed to MANET entities that are not authorised to interpret it. Due to MANETs' wireless links being easily susceptible to eavesdropping, confidentiality is very crucial for protecting the transmission of private information. Especially, any leakage of data or control traffic (such as routing) information could be really harmful in certain circumstances such as emergency cases, where human life is in danger. In MANETs, confidentiality becomes more challenging because intermediate nodes might need to forward a message from a source to a destination. In this case, any malicious MANET node is likely to try revealing the confidential message content as a first step towards different kind of physical or network attacks.

2.3.1.2 Integrity

Message integrity ensures that transmitted information (data or control) is not changed by any unauthorised entity. Sometimes, this alteration could be due errors caused by the

wireless nature of the links rather than by malicious actions launched against the MANET links. To identify and recover from such errors, protocols such as TCP and IP employ checksums.

However, an attacker could manipulate data by insertion, deletion, or substitution. *Message origin authentication* guarantees the identity of the other MANET node that is communicating with. *Entity authentication* is focusing on the verification of a claimant's MANET node identity through actual communication. In a MANET, if such an attribute is not in place, an attacker can masquerade as a legitimate node, hence it is likely to gain unauthorised access to MANET resources. On the other hand, *data authentication* is concerned with verifying the origin of data. In this way, data integrity is also provided by this attribute.

Non-repudiation ensures that a MANET node cannot refuse its activities (such as having sent a malicious message or having received a message) or pretend that another node has committed an action.

2.3.1.3 Availability

Availability ensures that network services are available when required by the various entities in the network. This attribute is mainly geared towards attacks such as denial-of-service that attempt to prevent authorised users from accessing important services.

2.3.2 MANET vulnerabilities

Vulnerabilities in MANETs mainly reside in their routing functionalities (implemented by MANET routing protocols) and in the use of wireless links. These key functionalities rely on trust between all the participating nodes.

2.3.2.1 Routing vulnerabilities in MANETs

In terms of MANET routing vulnerabilities we have the following:

- The delivery of a packet to a destination node is done in a hop-by-hop manner thereby cooperation from the intermediate nodes is required.

- The right delivery and transport of the packets relies on the information that other nodes (potentially untrusted) disseminate.
- A malicious node can compromise the routing protocol (this can be done in several different ways as we discussed later on) and then this node can control the incoming and outgoing traffic of a part of the MANET.
- A malicious node can inject wrong routing information creating false routing table entries thus hardening the end-to-end MANET communications.
- A malicious node could block, modify or drop any traversed control (routing) or data traffic.

2.3.2.2 Use of the wireless links

The use of wireless links can introduce vulnerabilities in MANETs as discussed in the following:

- Makes it easier for an attacker to intercept MANET traffic when it is within the transmission range of a node.
- Due to the wireless nature of the links and the limited transmission range, cooperation is essential to forward the message to a destination node.
- Makes MANETs very vulnerable to attacks varying from passive eavesdropping to active interfering.
- Due to MANET protocols comply with predefined rules for accessing the wireless channel, a malicious node can modify such protocols in order to launch a denial-of-service attack.

2.3.2.3 Other vulnerabilities

Other MANET vulnerabilities are summarised as follows:

- Due to their limited resources, MANETs might encourage adversaries to launch denial-of-attacks in order to drain the battery of legitimate nodes.
- Due to the MANETs' uncertain nature (introduced by the wireless medium and their decentralised architecture), erroneous behaviours such as packet dropping might appear as malicious activities or vice-versa.
- In MANETs, nodes are likely to be physically captured and operated by a malicious user. In that case, cryptographic keys and data can be exposed.
- Mobility can also make it difficult for nodes to realise where a node's churn (join and leave the MANET) is due to the mobile nature of the communications or as a result of malicious activities that try to exhaust bandwidth and power resources.
- In MANETs where Intrusion Detection Systems (IDSs) are operated, it is more difficult to obtain enough audit data compared to wired networks. This can be a problem for IDSs trying to distinguish anomaly behaviour by defining normal behaviour profiles.
- In MANETs the autoconfiguration mechanism introduces new vulnerabilities. Such a mechanism is crucial for the MANET communications since there is not a server or node acting as such which correctly assigns IP addresses. Hence, a protocol is required to execute the network configuration automatically and dynamically, by using all MANET nodes as if they were servers with IP addresses' management capabilities. Such functionality, is vulnerable for instance against malicious nodes that pretend to be using any of the addresses selected by a joining node thereby colluding such a join process.

2.3.3 Attacks in MANETs

Attacks against a MANET might be launched by malicious nodes that are not part of the network (outsiders). MANET nodes protect their communication through the use of cryptographic techniques which enable secure verification of a node identity by other nodes

preventing malicious outsiders from penetrating the MANET resources. Apart from the external attackers, attacks could be launched by nodes that are authorised to be part of the MANET (insiders) or they are compromised nodes (hacked devices).

MANET routing protocols are inclined to be attacked by malicious nodes. Most of the times, such protocols do not encompass any security mechanisms thereby being vulnerable to node misbehaviour. In the following we summarise the most popular attacks against MANET routing protocols:

- *Packet dropping*: This attack is launched when a MANET node advertises routes through itself to other nodes aiming to start dropping the received packets instead of relaying them to the next appropriate hop towards a destination;
- *Black hole attack*: According to this attack an adversary advertises, through the routing protocol, itself as having the shortest path to a destination. In this way, the malicious entity can intercept the packets destined for such a node. Then, the attacker can choose between the following:
  - drop the packets performing a denial-of-service attack;
  - launch a man-in-middle-attack relaying the packets to other preferred nodes.
- *Selfish nodes*: In some cases, MANET nodes might opt to abstain from the routing process in order to save their battery power. This can lead to the fragmentation of a MANET (nodes cannot see each other due to this fragmentation) especially if several nodes follow such a method;
- *Wormhole attack*: According to this attack, malicious nodes cooperate to transfer control (such as routing) and data packets out of band by using other communication channels disturbing the conventional operation of routing protocols;
- *Spoofing*: In this attack a MANET node tries to fake the identity of another node in order to receive all the packets destined for such a node as well as advertise wrong MANET routes;

- *Rushing attack*: According to this attack, a malicious node rushes some routing packets towards the destination in order to place itself between source and destination. In that case the initiator of a route request will be unable to discover any usable routes (routes that do not include the attacker). A rushing attack acts as an effective denial-of-service attack against routing protocols.

- *Routing packets modification in transit*: In these attacks nodes modify routing messages sent by other nodes in order to mislead legitimate MANET nodes by modifying critical transmitted routing information such as the sequence number on a routing packet. In this case, fresh route advertisements are not taken into account.

2.3.4 Intrusion detection in MANETs

One of the most important aspects of security is to provide defence-in-depth meaning that multiple defence layers need to prevent adversaries from harming the MANET communications. A mechanism which prevents malicious activities is called *first layer of defence*. Such a mechanism can be a secure routing protocol which provides *confidentiality* and *integrity*. Apart from these mechanisms, a *second layer of defence* [32] called intrusion detection can be used to protect a network.

An *intrusion detection system* (IDS) is responsible for monitoring the events occurring in a MANET and detecting signs of intrusions. One can distinguish between *host-based IDS* (HIDS) and *network-based IDS* (NIDS). The former is used when the actual MANET nodes perform the intrusion detection functionalities while the latter denotes third party IDS, dedicated to defending the network.

Especially in MANETs, solutions like the one proposed in the seminal paper [33], equip all nodes with HIDSs and they operate in *promiscuous* mode to continuously or periodically monitor the traffic sent or received by their neighbours towards the collection of adequate information to identify malicious activities (see Fig. 2.2).

For instance, to defend against packet dropping attacks in MANETs, intrusion detection must be accomplished by a monitoring application such as the ones proposed in [34]

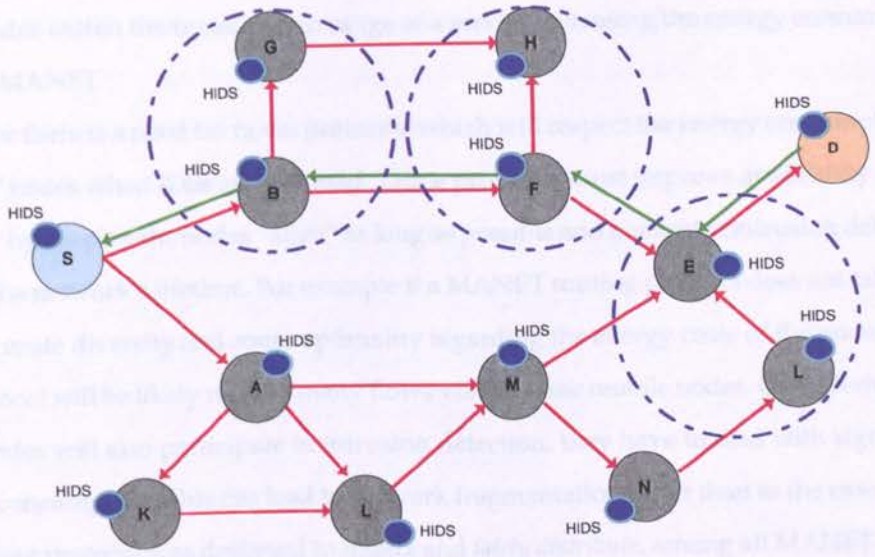


Figure 2.2: Host intrusion detection systems are running in each MANET node to protect the network against malicious activities.

and [35]. According to these solutions, when a packet is sent to a destination, it will have to be forwarded by the one of the neighbouring nodes of the originator. In order for the sender to be able to confirm this, every node must act as a detection node [36].

IDSs can be used for the detection of many different MANET attacks, and for a comprehensive survey of solutions we refer to [37] and [38].

In wired networks where battery life is not a concern, the promiscuous mode does not affect the performance of the network although it needs higher computational effort. In MANETs where lightweight devices constitute the network, any proposed protocol must respect the energy consumption, incurred due to the use of IDSs. In that way, *availability* of the network resources will be improved.

Thus, any energy-cost analysis must take into account the energy that a mobile node uses in order to identify malicious activities in the network. This overhead is part of the intrusion detection. Especially in MANETs, energy can be considered as a distributed network resource and is non-renewable because a node has a monotonically decreasing and finite energy level. It is also important to stress here that broadcast traffic is processed

by all nodes within the transmission range of a sender increasing the energy consumption across a MANET.

Hence there is a need for novel protocols which will respect the energy consumption of MANET nodes when IDSs are operated. These protocols must improve availability across MANET by keeping the nodes "alive" as long as possible and guarantee intrusion detection during the network's lifetime. For example if a MANET routing protocol does not take into account route diversity and route optimality regarding the energy costs of the nodes, then the protocol will be likely routing many flows via the same mobile nodes. Considering that these nodes will also participate in intrusion detection, they have to deal with significant battery consumption. This can lead to network fragmentation faster than in the case where the routing protocol was designed to *respect* and *fairly distribute*, among all MANET nodes, the energy costs occurred due to intrusion detection.

In this thesis, we work on an innovative research area examining how to improve availability in MANETs, in presence of host-based intrusion detection systems, by improving the network-wide intrusion detection cost and rate.

2.3.5 MANET security areas related to the thesis

The main areas of MANET security related to this thesis are summarised as follows:

- *Secure routing*: Routing in MANETs plays a crucial role for the delivery of control (routing) and data packets. Most security threats target routing protocols in MANETs due to nodes are associated and collaborate with any other node including attackers. Such malicious entities can compromise the confidentiality and integrity within a MANET.

- *Secure peer-to-peer overlays*: If malicious peers exist in a peer-to-peer overlay, they can damage the MANET communications by, for instance, providing legitimate nodes with erroneous lookup results or inoperative data;

- *Key management*: The existence of secure communication channels is especially crucial

in MANETs. These channels are required for many operations such as exchanging data or control packets in the case of functions like routing. To make this secure communication possible, it is necessary for nodes to have access to the proper keying material. This is the objective of the key management process.

- *Improving intrusion detection cost and rate*: In MANETs attempts to detect intrusions in a distributed manner could be highly expensive in terms of battery consumption. Considering the limited resources nature of MANETs, energy efficient network-wide intrusion detection is important to increase availability of the network resources and indirectly assist power management in MANETs.

2.4 Emergency MANETs

Two chapters of this thesis are concerned with security solutions for emergency MANETs. These solutions are designed to support routing and peer-to-peer overlays for such networks. We will thus further explore the particular characteristics of the corresponding research areas to prepare the ground for describing our security solutions.

2.4.1 Routing for emergency MANETs

Within the context of emergency MANET multimedia communications operating within a pre-defined disaster area, CA, the authors in [5], have designed and developed a novel hybrid and adaptive routing protocol called *ChaMeLeon* (CML). The main concept behind CML is the adaptability of the utilised routing mechanism towards changes in the physical and logical state of the network so that the overall performance of the routing algorithm is improved. The importance of such an approach resides in the fact that nodes in emergency MANETs have to provide a certain level of QoS routing to support multimedia communications and cope with limited resources.

CML does not specify any special security countermeasures against malicious entities. Attacks include for example cases where an adversary can send a change phase

packet to call the o-phase of CML and the routing behaviour to change accordingly. In this way, CML will not operate in the proper routing mode and the MANET's performance will not be optimal considering the real number of nodes in the network. Another attack is launched when malicious nodes change the "hop value" in the CML HCReq packet. In this case, legitimate nodes believe that the size of the network has changed and CML oscillates unreasonably. Thus, security effective approaches have to be integrated into CML to provide MANET nodes with the basic security requirements.

2.4.2 Peer-to-peer overlays for emergency MANETs

Authors in [31], have proposed the *ROBUST* DHT for emergency MANETs. The aim of the architecture is to decrease the average path length and lookup time when sending DHT messages thereby decreasing *stretch*, while decreasing the maximum path length from the $O(\log N)$ complexity seen in most common DHTs used today, where N is the number of MANET peers.

The concept central to ROBUST DHT is to use a clustered hierarchical topology to support emergency MANETs. This means that peers will be clustered together based on proximity in the underlying MANET. The peers will be connected via a super peer which keeps track of peers within the cluster and also carries out cluster maintenance. Cluster peers will be able to communicate with one another, however peers within each cluster will forward their queries to their dedicated super peer. If the destination lies outside of the cluster, the peer will forward the query to the super peer responsible for the destination peer, and the destination peer will then reply to the request.

2.4.3 Security for emergency MANETs

In order to provide real-time communications in emergency environments, MANETs can be a possible network infrastructure solution. These networks must be deployed and operate in a self-organised manner regardless of topology changes, environment alterations, link breaks or network disruptions. They should also provide audio and video communication

among the nodes that comprise the network, with Quality of Service (QoS) restrictions to be taken into account. Therefore, any security solution for emergency MANETs must think of the overhead that is caused due to security and it must allow high QoS communications by respecting parameters such as *end-to-end packet delay, jitter* and *packet loss*.

Based on the emergency communications mindset, in this thesis we assume that a pre-shared symmetric key has been distributed among the MANET nodes (for instance such a key could be hard-coded in the devices). This could be done by pre-installing such a key into the devices before they are provided to first responders.

Additionally, MANETs are simulated by using an obstacle-aware model called *Mission Critical Mobility* (MCM) [2] which emulates the movement of first responders during rescue missions. MCM implements the two-way ground propagation model and the Random Waypoint mobility model in presence of obstacles. The MCM model is available for download and installation at [39].

2.5 Wormhole attacks in MANETs

The wormhole attack [40] needs at least two adversaries geographically separated. Adversaries record packets or bits at one location in the MANET and tunnel them to another location through a private network shared with a colluding malicious node. The attackers aim to launch a *Man-In-The-Middle* (MITM) attack, in order to drop packets, listen to confidential information, modify transmitted routing or data packets, selectively forward packets (to avoid detection) or to disrupt the proper operation of the MANET routing protocol, by making routing unable to find consistent routes to any destination. Key material is not required to launch such attacks and the attackers all they need is two transceivers and one high quality out-of-band channel.

This attack can be launched in two ways:

- A malicious node encapsulates a packet received from one of his neighbours and forwards this to another adversary located in a different neighbourhood as we illustrate in Fig. 2.3;

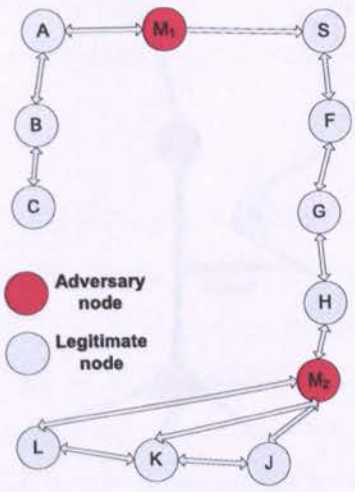


Figure 2.3: The wormhole attack against a MANET (case of encapsulated packets).

- Malicious nodes create a wormhole tunnel using an out-of-band channel as depicted in Fig. 2.4. This channel can be a wired link or a high frequency wireless link at a different frequency band. Received packets are transmitted through the tunnel from one place of the MANET to another where another adversary replays them locally [41].

These attacks constitute a serious threat against MANET routing protocols because they can force all the routes to pass through the wormhole tunnel. What happens is that a wormhole tunnel helps adversaries to advertise routes with smaller number of hops between two MANET locations that are not, in reality, in the same neighbourhood. Due to the fact that the majority of the MANET routing protocols do not encompass any intrusion detection mechanisms, legitimate MANET nodes include the malicious routes to their routing tables. In this way, adversaries succeed in poisoning the routing tables of nodes.

A representative feature of wormhole attacks consists of relatively longer packet latency than normal wireless propagation latencies on a single-hop. The load on a single route can also increase, leading to typically longer queuing delays. However, this is not a sufficient condition for the existence of a wormhole attack, because packet transmission is affected

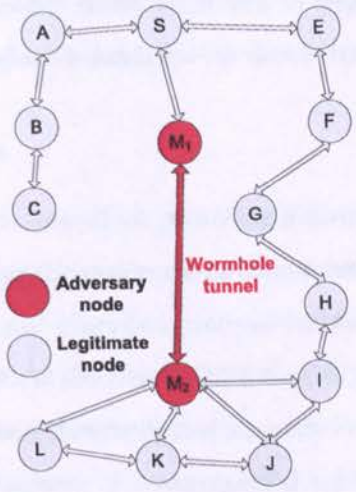


Figure 2.4: The wormhole attack against a MANET (case of out-of-band channel).

by various factors like congestion and traditional processing [42].

2.5.1 Related Work

In [43] authors take advantage of the concept of directional antennas to prevent wormhole attacks while in [41] a novel protocol named TrueLink is proposed to defend MANETs against such attacks. This mechanism is virtually independent of the routing protocol used. In addition, disjoint path based approaches have been adopted such as the statistical approach in [42] which is based on multipath routing.

The DelPHI protocol [44] focuses on the delays due to different routes to a receiver. DelPHI is closer to our model because the delays and the number of hops of disjoint paths are used to conclude if a certain path is under a wormhole attack.

In [45], authors use only connectivity information to check for forbidden substructures in the connectivity graph and as a result are able to detect the wormhole attack.

In [40], authors propose the concept of a *packet leash* as a general mechanism for detecting and preventing wormhole attacks. Furthermore, they categorise the leashes into *geographical* leashes and *temporal* ones. A geographical leash verifies that the receiver of a packet is within

a certain distance from the sender whilst according to temporal leash the packet has an upper bound on its lifetime which bounds the maximum traverse distance.

2.5.2 Thesis contribution

Our research is the first which focuses on providing defence against wormhole attacks in emergency MANETs respecting the requirements of such networks as discussed previously in this chapter. In addition, our proposed protocol entitled *Ad hoc On-Demand Distance Vector-Wormhole Attack Detect and Reaction* (AODV-WADR) [7] is similar to the mechanism proposed in [40] with the critical difference that the node that decides if a wormhole attack has finally occurred is the originator of a message and not the receiver as authors propose in [40]. In that case, the protocol ensures that identification will take place even if the final receivers of the data or routing packets are not legitimate MANET nodes.

2.6 Secure routing for MANETs

In MANETs, the network relies on the cooperation of individual nodes which provide relaying functions. In the case where the source and destination nodes cannot directly connect to each other, intermediate nodes act as packet routers for multi-hopping data from a source to a destination. Hence, MANETs can be described as fully distributed, autonomous and cooperative communication networks that can be effectively operated without the need for pre-established infrastructures.

The successful deployment of such dynamic and self-organised networks mainly depends upon using a suitable routing protocol. For instance, routing mechanisms for MANET multimedia applications may have to satisfy certain applications' *Quality-of-Service* (QoS) requirements while at the same time being subject to dynamic constraints such as varying wireless link qualities along routes, link breakage due to mobility of nodes and battery limitations of participating lightweight devices.

Secure operation of the MANET routing protocol is critical because of the absence of a fixed infrastructure. Nodes are associated and will cooperate virtually with any node in-

cluding adversaries. Adversaries can cause the disruption of the route discovery and data forwarding operations. For instance, adversaries can obstruct the propagation of legitimate queries and routing updates. Disruption of the route discovery can cause systematic problems to the flow of data. In order to prevent such attacks it is important for the receiver node to mainly verify the authenticity of the sender and the integrity of the data. The most efforts have been towards the achievement of these goals. In a nutshell, secure routing is concerned about nodes which can compromise the main security requirements of confidentiality and integrity in a MANET.

2.6.1 Related work

Within the context of secure routing, the authors in [46] propose a secure version of AODV named SAODV which stands for *Secure AODV*. This protocol uses digital signatures, asymmetric encryption keys and hash chains. The protocol provides characteristics such as integrity, non-repudiation of the routing data and authentication of the nodes within a MANET. SAODV takes advantage of the pure routing functionality of AODV while it adds security mechanisms on top of it. Nodes sign the messages that they want to send such as RREQs and RREPs in order to authenticate themselves to the destination nodes. This signature protects the non-mutable information of AODV messages, which is all the information apart from the hop count field that changes in every transmission of the message in a hop-by-hop frequency until it reaches the destination.

SAODV uses another scheme to protect the hop count information based on the concept of hash chains by using message digests mechanisms. The protocol uses asymmetric cipher and each node has to store a pair of keys and the authenticated public keys of the other nodes. However, SAODV is considered adequately strong to defend MANET communications, asymmetric cryptographic schemes are considered inappropriate in terms of energy consumption and speed for lightweight handheld devices. According to [3] asymmetric cryptography is slower than symmetric in addition to the fact that for "lightweight" [1]

[1] In terms of battery consumption.

devices is high when the former is used.

AODV-SEC [47] is an extension of *Secure AODV* (SAODV) that uses a *Public Key Infrastructure* (PKI) as a trust anchor therefore nodes can be identified using certificates. However, due to the fully distributed topology of MANETs, the assumption of PKI can introduce significant problems in terms of the deployment and operation of such a protocol.

ARAN which stands for *Authenticated Routing for Ad-hoc Networks* [48] is a secure routing protocol similar to SAODV which targets at securing on demand routing protocols. ARAN assumes that there is a trusted certificate server called T. A certificate per node is generated by T and distributed accordingly before all nodes join the MANET. The certificates are authenticated by each node by using the T's public key. When a source node S wants to find a path to a destination node D, it broadcasts a *Route Discovery Packet* (RDP) which is similar to the RREQ in AODV.

Every node which receives the message, after it checks that the certificate has not been expired, it extracts the public key of S from it, to verify the authenticity of the sender and checks its digital signature. If all the security checks are positive, the intermediate node signs the message using its private key, attaches its certificates and then rebroadcasts the RDP message to its one-hop neighbours. If D receives the message, establishes a reverse route to S through its one-hop neighbour which sent this message and sends a RREP to S. It is worth stressing here that intermediate nodes do not change the original RDP message created by S but they add only their certificate and their signature. The authors recommend that is more beneficial to send packets through the 'RDP route' even if it is not the shortest path to D since on the other shorter routes, malicious nodes can cause higher delay and damages. ARAN provides authentication and non-repudiation services by using pre-determined cryptographic certificates.

The SAR which stands for *Security-aware Ad-hoc Routing* protocol, published in [49], supports routing through trusted nodes than using the shortest path. SAR assumes a trust hierarchy in a way that nodes lower in the hierarchy are less trusted than nodes belong to the higher levels. This categorisation determines the way of the routing procedure. Al-

though the concept is quite generic and can be tailored to support many MANET routing protocols, the authors in [49] have slightly modified AODV so that nodes add a new field to the RREQ message, called *RQ_SEC_REQUIREMENT*. This indicates the security level that a node can support. If a node cannot support the requested level, it must drop the packet otherwise add a field called *RQ_SEC_GUARANTEE* and forwards it to its neighbours as in AODV. The RREP packet indicates the security level of a path using the aforementioned field. SAR assumes also cryptography through a key that is shared among all nodes at a right trust level. The authors recommend that different security properties can be incorporated in the routing protocols depending on the application needs across a MANET.

In [50] the authors propose a novel protocol, called *Secure Routing Protocol* (SRP). They have applied SRP to DSR assuming that there is a bidirectional *Security Association* (SA) between nodes that desire to exchange messages and shared secret keys which are used to protect the exchanged routing messages. Specifically, the keys are used for signing routing messages and thus ensuring their tamper-proof.

According to SRP, nodes sign only the non-mutable fields of the routing messages providing sufficient security for the routing functionalities. The source of each RREQ, attaches an SRP header to the message whilst a sequence number is initialised when the SA between the two MANET nodes is established. In addition, a *Message Authentication Code* (MAC) is generated by a hash function on the IP header, routing message, SRP extension, and source-destination pair's shared key.

Any intermediate node which receives a RREQ and it has not seen it before, attaches its address to RREQ and rebroadcasts it as in DSR. If nodes have seen the message, they drop it whilst they keep track of the RREQ that they have received by one-hop neighbours to ignore them in case of an excessive number of RREQs have been sent to them. In this way, DoS attacks are prevented. When the destination node receives one or more RREQ, checks its sequence number and the MAC field and it sends a RREP for all the RREQ with the correct sequence number[2].

[2]Because they might be more than one coming from different multiple paths.

The authors in [50] suggest that the mutable fields of the routing messages do not need to be protected since malicious nodes can disrupt the route anyway by just dropping packets routed through it, and hence protecting the path information does not introduce significant value. Furthermore, SRP does not provide maximal protection against route maintenance errors. As MANET nodes can send route error messages towards the previous hops through the source route, malicious nodes can fake error broken route messages.

An alternative solution to SRP is Ariadne [51], which provides authenticity of the information provided by the intermediate nodes on the path between a source and a destination in addition to the features that SRP offers. Ariadne is similar to SAODV allowing nodes to authenticate routing messages and verify their integrity. However, Ariadne is more complicated than SAODV due to RREQ messages in DSR being modified by each forwarding node to include their own address.

In [52] authors propose a secure version of OLSR that protects packets using identity-based cryptography and periodically or when necessary refreshes cryptographic keys using threshold cryptography. The protocol allows only non-malicious nodes to participate in the bootstrap process while it introduces improvements in routing setup and maintenance.

A strong assumption in Ariadne is that each node can estimate the end-to-end transmission time towards any other MANET node. The authentication of the messages take place by using one of the following mechanisms; pairwise secret keys between each pair of nodes, TESLA or digital signatures. The authors also assume that each MANET node has a one-way hash chain used along with TESLA and all the nodes require to know the authentication key of every other node in this key chain. Each RREQ includes an *keyed-Hashing for Message Authentication* (HMAC) which is created using the intermediate node's TESLA key for the time interval specified in the RREQ. In this way, each node is able to authenticate the messages on a route from a source to a destination. The latter performs two checks and if they are successful, it sends a RREP, that includes an HMAC, back to source. The first check ensures that the TESLA keys have not yet been disclosed for the time interval defined in the message whilst the second check must verify that the value of the hash chain field has

been derived correctly. When the source receives the RREP message, it verifies three things before accepting the route as valid; the values of the key list, the target MAC and the MAC list.

Based on the SRP and Ariadne, the authors in [53] have proposed the reverse protocol of Ariadne called *endairA*. Its main difference with Ariadne is that intermediate nodes sight the RREP instead of the RREQ. The authors have proved that their protocol is secure in a MANET with a single compromised node whilst it introduces less energy consumption than Ariadne, since the nodes need to sign only the RREP messages. On the contrary, in Ariadne each node needs to sign a RREP which is flooded in the network forcing each node to sign a message.

The paper [54], expresses using a formal language, the different types of trust relations between nodes running OLSR. The authors present a formal textual description of the trust issues for OLSR that enable an effective interpretation of attacks against OLSR in terms of trust classes and relations. In this way they claim that they can set the conditions to use trust-based reasoning towards the mitigation of particular vulnerabilities of OLSR. For a more extended work on trust management issues for MANETs, [55] is a complete survey that readers can refer to.

Furthermore, paper [56] proposes a security mechanism to be integrated into OLSR. This mechanism distributes asymmetric cryptographic keys between the nodes in the network and "global timestamps" are used to avoid replay attacks determining whether any message is "too old" or not. The strong assumption of this mechanism is that trusted nodes cannot be compromised.

In [57] authors present an overview of security attacks against *OLSR version 2* (OLSRv2), and show that OLSRv2 provides some inherent protection whilst in [58] authors discuss their implementation of an extension of the OLSR source code appearing in [59]. Their solution is based on signing each routing control packet using a digital signature to authenticate the message. Another consideration of this implementation is a timestamp mechanism to avoid replay attacks.

Last but not least, the paper [60] proposes a mechanism to enhance the security of the OLSR against external attackers based on message signing and sender authentication. The authors also deal with the case in which an adversary compromises a trusted node. The mechanism is based on recording recent routing information such as HELLO messages and using this information to prove the link state of a node at a later time by a new *Advanced Signature System* (ADVSIG) control message.

The paper [61] proposes a new secure version of OLSR called *Security Aware Optimized Link State Routing* (SA-OLSR). The protocol does not need any specialised hardware (for example *Global Positioning System* (GPS)) and complete information of the whole MANET whilst preventing many attacks. To validate SA-OLSR, authors have implemented the protocol using the network simulator ns-2 and they have examined a mis-relay attack as a case study. They show that the attack can totally disrupt the operation of OLSR whilst SA-OLSR is not affected. The quantitative indication for the aforementioned observation is that SA-OLSR has higher packet delivery ratio than OLSR in presence of adversaries.

Moreover, in [62] authors propose a secure fully distributed algorithm for OLSR based on the secret sharing idea. The algorithm is based on threshold cryptography and it has been implemented using the OPNET simulator. Simulation results show that the additional delay due to the security considerations is affordable and suitable to the OLSR routing specifications operating in a transparent way.

The paper [63] proposes a hybrid protection scheme for OLSR based on identity-based digital signatures and hash chains. Since only a part of the messages are signed the rest include an undisclosed value from the hash chain to enable lightweight authentication. In this manner adversaries can hardly insert additional and false routing messages even if these are not signed. The protocol is implemented using ns-2 tools and the simulation results highlight the average measured channel utilisation per second, for OLSR traffic for various network sizes, security overheads and signature to hash ratios.

In [64] authors present a key management protocol, called *Simple key management for MANETs* (SkiMPy) which allows MANET nodes to agree on a symmetric shared key, used

in the beginning of the network's lifetime to exchange digital certificates. The same key can be used to provide data confidentiality along with preinstalled certificates to provide node authentication with the need for a third trust party. SKiMPy has been developed as a plugin for the OLSR. The evaluation results show that SKiMPy scales linearly with the number of nodes in worst-case scenarios.

The paper [65] proposes a distributed and self-organised security scheme for OLSR. The scheme is based on threshold cryptography mechanisms to ensure the integrity of the routing messages. Authors show that the delay introduced by the scheme is acceptable and suitable to the routing requirements.

Last but not least, in [66] authors propose the *Secure Link-State routing Protocol* (SLSP) for securing link-state routing using asymmetric cryptographic tools. Each node has a public-private key pair which broadcasts periodically or on-demand to all the m-hop neighbours. The discovery of the neighbours is achieved in the SLSP through signed hello messages with MAC and IP addresses to avoid impersonation attacks.

2.6.2 Thesis' contribution

This thesis tackles the challenge of secure routing for emergency MANETs by mainly providing a security framework for the *ChaMeLeon* (CML) routing protocol. This framework utilises efficient symmetric cryptographic techniques in order to reduce time and space overhead supporting MANET multimedia communications. CML does not specify any special security countermeasures against malicious entities while all the previous MANET routing protocols, proposed in literature, have not taken into account the specific characteristics of emergency MANETs as they have been discussed earlier in this chapter. In addition, such protocols secure only one specific protocol giving less flexibility in cases where we want to utilise a hybrid MANET routing approach like CML.

2.7 Secure peer-to-peer overlays for MANETs

Adversaries within a P2P network [67] are those peers which intentionally do not follow the protocol rules. For instance, a malicious peer might provide legitimate peers with erroneous lookup results or inoperative data. In addition, as far as P2P systems inherently rely on the relationships among the participating peers, the security requirements of *confidentiality* and *integrity* arise with a need to be addressed by proper security extensions regarding signalling messages. With regards to these two different requirements the following attacks against P2P overlays could be launched in a MANET:

- *Attacks against integrity*:
  - A *peerID faking* attack is launched by a malicious peer that advertises itself as part of the DHT, persuading legitimate peers that it has cached some piece of data indicated by the fake announced *peerID*;
  - According to work in progress [68] in a *bootstrap abuse* attack, the bootstrap peers are compromised during the bootstrap process and any joining peer affiliated with them is negatively affected by any potential attacks the adversaries are planning to launch against the legitimate peers;
  - A *DHT routing* attack [67] is commenced by adversaries that have entered the DHT and do not obey the routing logic. The said malicious peers may announce false routing table information to other legitimate peers or they may route queries of data further than the destination peer in order to increase the latency within the P2P network. Attackers may additionally return incorrect lookup results hence increasing dramatically the likelihood of lookup failures;
  - In the *Sybil* attack [67] a hostile peer or coalition of peers attempt to generate multiple virtual *peerIDs* of other peers. One crucial consequence of this attack is the partial or total disruption of the replication functionality which becomes worse when popular and essential data is replicated;

- Moreover, adversaries can launch a *data alteration or corruption* [68] attack, namely they can modify or totally disrupt stored data as a first step towards the total disruption of the P2P overlay networks functionality or they may *replay*[3] the same messages during the networks lifetime, confusing the legitimate peers and damaging the proper P2P operation. Additionally, according to [69] adversaries may start an *on-off* attack where they occasionally behave correctly or maliciously in order to remain undetected whilst concurrently harming the P2P communication links.

- *Attacks against confidentiality*: According to the *snooping* attack[4], malicious peers succeed to reveal confidential information exchanged among peers. This attack is classified as a passive attack and it can be extremely dangerous when appropriate security mechanisms have not been implemented in advance to protect the privacy of the P2P communications links.

2.7.1 Related work

In the majority of the proposed DHTs for MANETs published in the bibliography little thought has been given to security considerations. Especially, in all of the papers regarding DHT MANET protocols there is no mention of security for the DHT signalling messages, especially in terms of *confidentiality* and *integrity*. The most of the DHT-based P2P protocols take for granted that the participating peers behave legitimately and abstain from implementing major security measures. The latter are expected to be employed by software implementations that defend the P2P network against potential adversaries.

A scientifically interesting issue is that the topology mismatch problem where the overlay network topology does not match that of the underlying network causing the overlay network to *stretch* out over the physical network. This issue must be considered in all DHTs designed for MANETs. In [70] the authors propose to negate the problem by

[3] Launching a *replay* attack.

[4] *Snooping*, in a security context, is unauthorised access to another person's or company's data. The practice is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission.

sending messages with very short Time To Live (TTL) when setting up the overlay. This creates an overlay with very strong proximity between the peers. The size of an optimised ring transmitted by a member of a group containing N members is $O(2N) \sim O(N)$.

The authors of [25] specifically examine cross-layer DHT MANET protocols. The examined architectures are Etka [26], Mobile Peer-to-peer Protocol (MPP) [27], a Gnutella optimisation for MANETs [28], FastTrack over AODV [29], and MADPastry [30]. Amongst these architectures, Etka and MADPastry are structured peer-to-peer overlays whilst the rest are unstructured. The Etka [26] architecture tightly integrates the structured P2P protocol based on DHTs with the routing architecture of MANETs by mapping logical DHT peer IDs to their MANET IP based counterparts causing the two separate architectures to merge into one structure. This is achieved by integrating the Pastry DHT with the DSR (Dynamic Source Routing) MANET multi-hop routing protocol at the network layer.

MADPastry [30] is a DHT substrate which acts by combining the Pastry DHT with AODV MANET routing at the network layer. This can lower the overhead needed to maintain the DHT. While the architecture utilises three different routing tables (one akin to AODV's routing table, another akin to Pastry's routing table, and a leafset table) the only table requiring proactive management is that of the leaf-set table, with peers pinging their *left* and *right* respective leafs. The additional tables are updated by overhearing data packets destined for other peers.

The analysis in [25] shows that for the above approaches, exploiting the synergy between MANETs and DHTs can yield measurable improvements and benefits. However issues are raised concerning the efficiency of using an interface between the application and routing layer, as apposed to combining both architectures at the routing level. The authors conclude that more study is needed in the area in order to clarify both systems potential and their suitability to specific scenarios.

2.7.2 Thesis' contribution

In the majority of the proposed DHTs for MANETs, published in the bibliography, little thought has been given to security considerations. According to our knowledge, in all papers that are concerned with DHT protocols for MANETs there is no mention of security for DHT signalling messages. The most of DHT-based P2P overlays take for granted that the participating peers behave legitimately and abstain from implementing major security measures. This thesis innovates by providing security for the novel peer-to-peer architecture for emergency MANETs, called ROBUST.

2.8 Applications of game theory to MANET security

Along with the proliferation of decentralised wireless networks, game theoretic models grew and help us realise and enhance the performance of advanced and complex wireless systems which cannot be optimally modelled using traditional optimisation methods. In this section we summarise fundamental issues of game theory along with related work of applications of game theory to enhance intrusion detection in MANETs.

2.8.1 Game theory

Game theory is a branch of mathematics which models situations amongst decision makers. In this thesis, we use the terminology as introduced in [71], one of the authoritative textbooks in game theory.

A *player* is a decision maker who is acting in a way that potentially results in mutual or conflicting consequences. In fact, game theory outlines what the best decision techniques are assuming that (i) the decision makers are rational and (ii) they strategically decide about their actions taking into account their knowledge or expectations of other players.

The players of the game take *decisions* on what *move* to undertake, from a range of available *actions*. This decision is motivated by their *strategy*. In fact, the strategy might change during the game (in which case one refers to a *multi-stage game*). The union of all the

players' strategies is referred to as the *strategy profile* of the game. Each player has a *payoff* (or, using the similar notion, a *utility*) function which indicates the benefits of outcomes resulting from his actions, using numerical values. A player's strategy is designed in such a way that maximises his payoff.

According to [71], *"a game is a description of strategic interaction that includes the constraints on the actions that the players can take and the players' interests, but does not specify the actions that the players do take"*.

Strategies must aim at easing problems and propose potential solutions. Well-known strategies are the following:

- *pure strategy*: a player chooses to take one action with probability 1;
- *mixed strategy*: a player chooses randomly between possible moves. This strategy is a probability distribution over all the possible pure strategy profiles;
- *dominant strategy*: is a strategy that is better regardless of the actions chosen by the other players;

Depending on the number of players we could have one-player, two-players or N-players games, where $N \geq 2$. A *solution* of a two-player game is a pair of strategies that a *rational* pair of players might choose to maximise their payoffs. Each rational player is aware of his alternatives, forms expectations about any unknowns, has clear preferences, and chooses his action deliberately following an optimisation process.

In Table 2.8.1, a game with two players is described where one player's actions are identified with the rows and the other player's with the columns. We can see that the set of actions of the row player is $\{A, B\}$ and that of the column player is $\{C, D\}$. We say that a player has a finite strategy set if this player has a number of discrete strategies available.

The two values in the box formed are the players' utility values for the different strategy tuples. The first value is the payoff of the row player and the second is the payoff of the column player, correspondingly.

Table 2.1: A convenient representation of a two-player strategic game in which each player has two actions.

	C	D
A	w_1, w_2	x_1, x_2
B	y_1, y_2	z_1, z_2

2.8.2 Game theoretic formulation

In the following we introduce fundamentals symbols used in game theoretic formulations. Let $G = (S, U)$ be a game, S_i the set of actions available to player i. Then, let $S = S_1, \ldots, S_N$, where N is the number of players in the game, be the set of all available joint actions that can be played in a game. Thus, a joint action $s \in S$ is a vector $s = s_1, \cdots, s_N$, where $s_i \in S_i$. Let $s_{-i} = (s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_N)$ denote the joint action taken by all players except player i.

Let $u_i(s)$ be the payoff to player i for the joint action s and $u_i(s_i, s_{-i})$ be the expected payoff to player i when it plays s_i and the other players play s_{-i}. This means that the utility value of a player i depends on the s_i as well as the actions chosen by the other players and describes how the player benefits from the game. In Table 2.2 we have summarised the notations that have been used in this section.

Table 2.2: Fundamental notation.

$\{1, \cdots, N\}$	players
S_i	the set of all available strategies to player i
S	the set of all available to players joint actions
s	the set of joint actions one per player (strategy profile)
s_i	action of player i
s_{-i}	actions of all players apart from i
$u_i(s)$	payoff to player i when s is played
$u_i(s_i, s_{-i})$	expected payoff to player i when other players play s_{-i}

2.8.3 Equilibrium

A reasonable prediction of the outcome of a game is an *equilibrium*, which is a strategy profile where each player chooses a best strategy in order to maximise his *utility*.

The solution that is most widely used for game theoretic problems is the Nash equilibrium ($\mathcal{NE}$) [71]. In game theory, $\mathcal{NE}$ is the solution of a non-cooperative game involving two or more players, in which no player has anything to gain by changing only his or her own strategy unilaterally. According to [72]

Definition A strategy profile $s^* \in S^*$ is a $\mathcal{NE}$ if no unilateral deviation in strategy by any single player is profitable or; $\forall\ i,\ u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*)$. ■

The following theorem is named after John Forbes Nash who proved in 1950 as part of his PhD thesis that

Theorem 2.8.1 (Nash's Theorem [73]) *Every game that has a finite strategic form, with finite numbers of players and finite number of pure strategies for each player, has at least one $\mathcal{NE}$ involving pure or mixed strategies.* ■

2.8.4 Related work

We will now review the state-of-the-art of applications of game theory to enhance intrusion detection in MANETs. This is a fairly new area of research and hence the following review of the literature covers the majority of the published work.

Authors in [74] and [75] have modelled intrusion detection in a MANET using the concepts of multistage dynamic non-cooperative games with incomplete information. They have assumed that *host-based IDSs* (HIDSs) are running in the MANET nodes to carry out intrusion detection functionalities. They define a basic signalling game which basically has two players; one receiver and one sender. The authors believe that MANET intrusion detection can be modelled as such a game and they clarify in detail the reasons for that. The players of the game are the attacker and the MANET. The former targets at sending a malicious message which, unless it is detected by any HIDS, harms the targeted legitimate

node. The authors examine the reduction in false alarms when the sensitivity of the system is decreased and they conclude that the cost due to undetected intrusion is more critical than the cost of false alarms.

In [76] authors examine security issues in wireless sensor networks which are divided in a number of clusters. In this work the wireless sensor network is responsible for defending cluster head nodes against malicious nodes which launch DoS or spoofing attacks. Authors formulate the attack-defence problem as a non-cooperative, two-player, non-zero-sum game between an attacker and a wireless sensor network. They then prove that this game achieves Nash equilibrium, thus leading to a defence strategy for the network. Finally, they propose the Utility based Dynamic Source Routing (UDSR) protocol, which takes into account the total utility of each node, which equals the difference between gain and cost. Some more papers that examine the application of game theory to model security games between MANET and malicious nodes in presence of intrusion detection systems have been summarised as follows.

The papers [77] and [78] propose an IDS mechanism for MANETs, based on a Bayesian game formulation. The attacker aims at damaging as much as possible the MANET communications with keeping himself stealthy and the MANET tries to maximise its utility represented by the tradeoff between the risk of losing a lot of energy[5] and the potential to increase its defending capabilities. The MANET have incomplete information about the type of the adversary and two game types have been examined; static and dynamic.

In [79] authors examine the challenge of decreasing the false alarms generated by cooperative IDS in MANETs. To this end, they use a cooperative game theoretic framework to analyse any detection and its significance within a MANET. To decrease the number of false alarms, MANET nodes use security classes to map different intrusions into such classes and with the corresponding security response. By assuming the threat models of cache poisoning and malicious flooding and by using previous-historic data, they accordingly modify the security classes to reach minimal number of false alarms.

[5]Due to heavy monitoring.

The authors in [80] present a game theoretic model to study the energy cost incurred due to HIDS and the necessity for keeping the HIDS sensors on during the entire's MANET lifetime. Their main contribution is the derivation of how frequent HIDS must operate to detect malicious activities depending on different network conditions.

In [81], the authors have used a cooperative game theoretic approach to show how to increase the efficiency of detecting intrusions especially in the network and application layer. They also claim that the model can easily be extended to detect attacks in any other layer and detect attackers individually. The paper [82] examines the packet forwarding approach which could form a reputation-based system for MANETs. By using evolutionary game theoretic models, the authors have shown that although nodes would like to act selfishly, the best strategy for them is to cooperate.

The paper [83] proposes a unified framework that is able to extend the IDS lifetime by using the notion of clusters and balancing the energy consumption among all cluster nodes. The authors of this work have used the *Vickrey-Clarke-Groves* (VCG) mechanism to compute node reputations and elect the most cost-efficient node while at the same time they detect and punish any mis-behaving entity[6] by refraining from giving them access to the cluster services. In addition they define a zero-sum non-cooperative game between leader-IDS and intruder with incomplete information about the intruder's identity. This game helps maximising the detection probability in the leader-IDS device by recommending an optimal sampling strategy.

In [13] we have proposed a game theoretic approach called *AODV-Game Theoretic* (AODV-GT). According to this protocol, each node chooses to route its packets through the route, which satisfies the following criteria (i) less number of malicious nodes probabilistically attack this route and (ii) less energy consumption of the participating IDSs. These criteria maximise the utility of the MANET at the $\mathcal{NE}$.

[6]Simple node or cluster leader.

2.8.5 Thesis' contributions

The work done in this thesis has been inspired by [76] and a preliminary version of it appears in [13]. In particularly, we extend the model in [13] by introducing more security parameters in our game formalism. As an application of this game model, we propose a novel MANET routing protocol which enables more energy efficient host-based intrusion detection than traditional routing approaches such as AODV, OLSR and AOMDV. We show that such a protocol extends the *availability* of network resources. Furthermore, we elaborate profound simulations using our novel network simulator developed in ns-2. We depict several different graphs to show that our protocol, although it increases the logical complexity of the system, it respects the Quality-of-Service (QoS) of delay sensitive data keeping the computational effort to an "acceptable" level.

Another contribution of this thesis is a non-cooperative game theoretic model to derive the optimal intrusion detection effort (monitoring probability) that must be spent by each MANET node in order to achieve the best balance between intrusion detection cost, for defending MANET nodes, and detection accuracy therefore proposing an optimal defence MANET strategy.

2.9 Summary

In this chapter a number of MANET issues have been discussed. We first give a background on routing and peer-to-peer overlays for MANETs. We then summarise the main MANET security issues and we define the mindset of emergency MANETs which has influenced the majority of the work elaborated in this thesis. We also give a background on the topics related to the research questions that this thesis has examined and the research gaps that this thesis has tackled.

Chapter 3

Secure Routing for Emergency MANETs

"Security's worst enemy is complexity", John von Neumann

This chapter presents two different secure routing approaches for emergency MANETs. Section 3.1 proposes a routing protocol which improves *availability* in emergency MANETs by mitigating wormhole attacks based on extending the AODV protocol. This protocol, called *Ad hoc On-Demand Distance Vector-Wormhole Attack Detect and Reaction* (AODV-WADR), controls wormhole attacks by identifying long delays in the communication links and excluding corresponding nodes from the network. Furthermore, this section presents and discusses the performance evaluation results retrieved by developing the AODV-WADR protocol in ns-2 and comparing this protocol with AODV in terms of *end-to-end packet delay* and *packet loss*.

In Section 3.2, we present a secure version of the *ChaMeLeon* (CML) routing protocol [5] to establish *confidentiality* and *integrity* for emergency MANETs. More precisely, it proposes the novel SCML protocol, a secure version of CML, which has been designed by using a hybrid version (AH and ESP in transport mode) of IPsec tailored for MANETs. In this chapter, we present and discuss the performance evaluation results retrieved by developing SCML in ns-2. We compare this protocol with the pure CML, CML using IPsec in AH mode

and CML using IPsec in ESP mode, by evaluating the cumulative packet end-to-end delay, cumulative routing control load and cumulative throughput. We have also undertook comparisons with SAODV by assessing the routing control load and the ratio of data to routing control load. All the results show that SCML introduces affordable overhead thus it can support high QoS multimedia communications.

3.1 Securing emergency MANETs against wormhole attacks

In this section, we consider the case of wormhole attacks in MANETs, as discussed in Chapter 2. We propose a secure routing protocol called *Ad hoc On-Demand Distance Vector-Wormhole Attack Detect and Reaction* (AODV-WADR) [7], to improve *availability* in emergency MANETs by mitigating wormhole attacks, based on extending the AODV protocol. The main contributions of this section are summarised as follows:

- We have designed the novel AODV-WADR protocol to control wormhole attacks in emergency MANETs by identifying long delays in the communication links and excluding corresponding nodes from the network;
- We have simulated this protocol using the network simulator ns-2;
- We have undertook comparisons with AODV, by evaluating end-to-end packet delay and packet loss. We show that AODV-WADR outperforms AODV in terms of packet loss while the delay introduced by AODV-WADR is considered negligible compared to the protocol's benefits.

3.1.1 AODV-WADR

In the following we describe our novel AODV-WADR protocol. This is integrated into AODV in order to apply low overhead defence against adversaries who have launched a wormhole attack against a MANET. Our scenarios, as defined in Chapter 2 of the thesis, focus on emergency cases where high QoS multimedia services are required to support emergency communications.

As we have mentioned, AODV is a reactive routing protocol designed for MANETs. The protocol uses an on-demand routing algorithm to discover and save routes between nodes only when deemed necessary. Thus, when adversaries succeed to create a wormhole tunnel, wrong routing information is flooded through the MANET corrupting the information in the routing tables.

In AODV-WADR, links which experience long delays are treated as suspicious and wormhole verification must be performed on them. AODV-WADR enables a node to confirm whether a neighbour has created a wormhole tunnel within the MANET or not. After the detection of the wormhole attack by a source node S, which seeks a route to destination D, the former deletes the route which includes the malicious nodes and adds them to a blacklist called *blacklist_wadr*.

3.1.1.1 Terminology

For a more convenient reading of this section, we summarise the following terminology:

- NET_TRAVERSAL_TIME (NetTT) [4]: is the maximum expected time in milliseconds waiting to receive a *Route REPly* (RREP) after sending a *Route REQuest* (RREQ);
- NODE_TRAVERSAL_TIME (NodeTT) [4]: is the maximum expected wireless propagation latency on a single-hop;
- ACTUAL_TRAVERSAL_TIME (ATT): is the actual period of time from sending a RREQ until receiving a RREP;
- ACTUAL_TRAVERSAL_TIME_WADR (ATT_WADR): is the time between the transmission and the reception of a *msg_wadr*[1] message;
- MAXIMUM_TRAVERSAL_TIME (MTT): equals $6 \times NodeTT$. This result is derived by multiplying the number of hops between S and D which equals 3 for a three hops away route, times 2 because NodeTT is the time for one-hop traversal. We

[1]This is the name of the AODV-WADR message.

explain, later on in this section, the reason for choosing only three hops routes in AODV-WADR.

- *Hop_Count*: is the hop count included in the AODV message and indicates the number of hops between a source and a destination.

3.1.1.2 Methodology

We suppose that a node *S* wants to discover a route to a destination node *D*. According to AODV, if *S* does not have a specific entry route for *D*, it broadcasts a RREQ or it sends a RREQ to the next hop along the last updated route which has been cached in its routing table for *D*.

In AODV-WADR:

- *S* simultaneously starts a timer in order to be able to calculate the ATT from the time it sends the RREQ until the reception of the RREP;
- When *S* does not receive any RREP during the next NetTT milliseconds, it acts according to AODV;
- On the other hand, if *S* receives the RREP, it checks the *Hop_Count*. If the *Hop_Count* does not equal 3, the node ignores the AODV-WADR implementation and it continues its routing operation according to AODV. If the *Hop_Count* equals 3, *S* implements AODV-WADR.

AODV-WADR enables the detection and prevention of wormhole attacks only by nodes which are three hops away from the destination node. This is true due to the following:

- Since every node keeps information about only the next hop node, according to [4], it would be more difficult for a node that is further than three hops away from the destination to suspect which node, on the route between itself and the destination, has launched a wormhole attack. For instance, if such a node suspects a wormhole attack then it has to suspect more than two nodes between itself and the destination (since

it is further than three hops away). In that case, there is a risk an innocent node to be blamed. This uncertainty makes us define that the detection process in AODV-WADR takes place by nodes which are two hops away from the other end of a wormhole tunnel.

- If *S* detects and prevents a wormhole attack, all the other nodes which have a route to *D* through *S* will avoid relaying their traffic through the wormhole tunnel;

Due to the nature of AODV which acts in a hop-by-hop manner, the three-hop wormhole tunnel detection is adequate to secure the MANET communications against wormhole adversaries since the legitimate nodes which detect the malicious parties terminate any communication with them. In this way, the AODV-WADR addresses the wormhole problem along the entire path from a source to a destination.

When ATT is higher than MTT, *S* suspects a wormhole attack due to the fact the message was transmitted slower. What happens is that adversaries use enhanced hardware to transmit the packets further away than one-hop distances but the time of transmission is not likely to be smaller than the time of an IEEE 802.11b transmission towards a single-hop unless they have used a specialised technology with usually comes with an undesired cost for them. However, the above phenomenon can be due to wireless propagation effects or delays in the *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA) algorithm. That is why AODV-WADR has to check if the abnormal delay is due to the existence of a wormhole attack or a link error.

After the suspicion, nodes have to establish pairwise cryptographic material during the second phase of the AODV-WADR. This allows the nodes to encrypt the packet in order to avoid malicious nodes to find out the content of the messages. In this way, adversaries cannot understand that a detection process is taking place in order to start to behave legitimately until the end of the detection process.

The establishment of such cryptographic keys takes place by *S* and *D* executing a *Diffie-Hellman* (D-H) key exchange to create a shared secret key. For this purpose, the pre-shared network wide key, discussed in Chapter 2 is used, as indicated by the emergency MANET

mindset. In that sense, intermediate nodes are trusted. The D-H method is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

S must inform D that they have to implement the D-H method. If S does not receive a response from D during the next NetTT milliseconds, it deletes the route to D from its routing table and it adds the next hop node to a blacklist. This blacklist is used by S in order to keep itself informed about the nodes that it should not be trusted and it excludes them from its routing tables. It is worth noting here that the nodes must periodically forward their blacklist to their one-hop neighbours to update them about the current malicious entities in the MANET.

After the successful creation of the common unique secure session key, S sends an encrypted message *msg_wadr* to D using *Advanced Encryption Standard* (AES)[2] [84] and it starts a timer in order to calculate the actual traverse time (ATT_WADR) of *msg_wadr*. If ATT_WADR is higher than MTT the node detects a wormhole attack. Afterwards, it deletes the next hop node from its routing table and adds it in the *blacklist_wadr*. In Algorithms 1, 2 and Figures 3.1, 3.2, we summarise the main functionalities of AODV-WADR.

Each node that detects the wormhole attack will never again update its routing tables with a route which is in its *blacklist_wadr*. For example, the first hop node M_1 (as it is depicted in Fig. 2.4, in the route $S, \cdots, D$) is considered as the creator of the wormhole tunnel and after the detection it is included in the *blacklist_wadr* of S. As a result, the communication between the source and the destination node will be established in the future through a different route preventing the creation of wormhole attacks by the detected adversary.

It is beneficial for the overall operation of AODV-WADR, nodes to update their blacklist every a timeout. This is important, especially in cases where "failures" in the wireless links might be wrongly translated as signs of a wormhole tunnel existence. In that case,

[2]We choose for the encryption of *msg_wadr* the AES algorithm because it is fast in both software and hardware, easy to implement and requires little memory [84]. The selection of AES is based also on the fact that the standard has been designed to be resistant to well-known attacks and also exhibits simplicity of design.

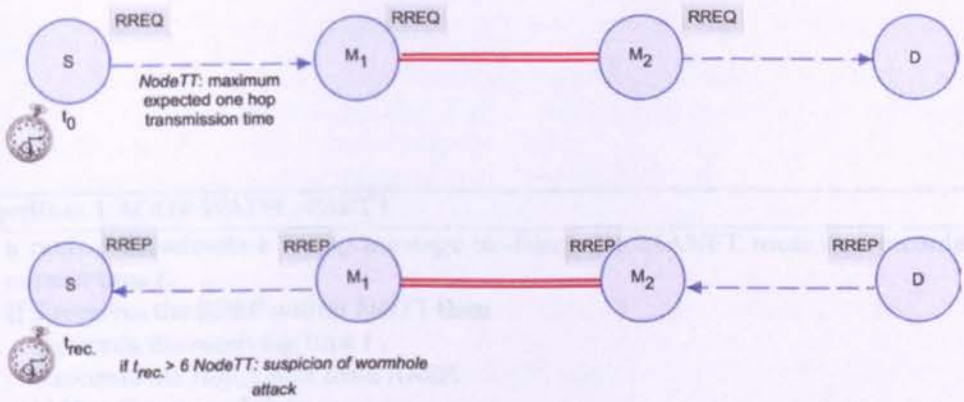


Figure 3.1: Representation of AODV-WADR algorithm 1.

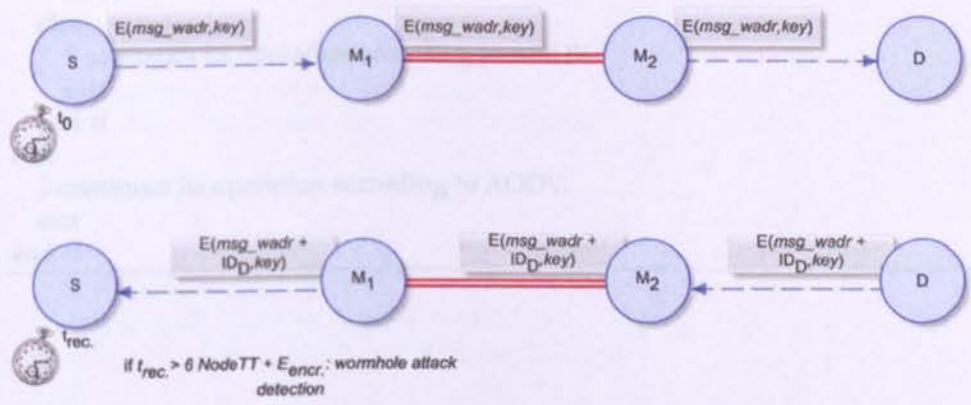


Figure 3.2: Representation of AODV-WADR algorithm 2.

Algorithm 1 AODV-WADR - PART I

1: a node S broadcasts a RREQ message to discover a MANET route and records the current time t.
2: **if** S receives the RREP within NetTT **then**
3: S records the receiving time t'.
4: S records the *Hop_Count* from RREP.
5: **if** *Hop_Count* == 3 **then**
6: S calculates the ATT as $t' - t$.
7: **if** ATT is higher than 6· NodeTT **then**
8: S suspects a wormhole tunnel in route r.
9: S runs algorithm 2.
10: exit
11: **else**
12: S considers the route between itself and D as safe against wormhole attacks and continues its operation according to AODV.
13: exit
14: **end if**
15: **else**
16: S continues its operation according to AODV.
17: exit
18: **end if**
19: **else**
20: S continues its operation according to AODV.
21: exit
22: **end if**

Algorithm 2 AODV-WADR - PART II

1: S sends a message to D in order to create a a shared secret session key (this key can be used to encrypt subsequent communications using a symmetric key cipher) using the *Diffie-Hellman Exponential Key Exchange* method.
2: **if** S receives a respond data message from D within NetTT **then**
3: S and D implement *Diffie-Hellman Exponential Key Exchange* method.
4: S sends an encrypted with the secure session key message *msg_wadr* to D using the Advanced Encryption Standard (AES) and records the current time t_{wadr}.
5: D decrypts *msg_wadr*, adds its ID number, encrypts *msg_wadr* using AES and sends it back to S.
6: **if** S does not receive *msg_wadr* within NetTT **then**
7: S considers a wormhole attack.
8: S deletes r from its routing table.
9: S adds in its *blacklist_wa* the next hop node.
10: exit
11: **else**
12: stores the receiving time t'_{wadr}.
13: S calculates ATT_WADR as $t'_{wadr} - t_{wadr}$.
14: **if** ATT_WADR is less or equal to 6· NodeTT **then**
15: S considers the route r between itself and D as safe and continues its operation according to AODV.
16: exit
17: **else**
18: S considers a wormhole attack.
19: S deletes route r from its routing table.
20: S adds in its *blacklist_wa* the next hop node.
21: exit
22: **end if**
23: **end if**
24: **else**
25: S considers a wormhole attack.
26: S deletes route r from its routing table.
27: S information its *blacklist_wa* with the next hop node.
28: exit
29: **end if**

the deletion of the next hop node according to AODV-WADR will be inappropriate. To overcome such situations, each node must check whether blacklisted parties in its list have been also blacklisted by its one-hop neighbours. In this way, if a node incorrectly deletes a suspicious node from its routing tables, it has to identify such an error and add back the blamed node in its routing table. This will happen due to the fact that other legitimate nodes will not add this node in their blacklist unless they experience a similar link failure. In that case, AODV-WADR still proposes a better route, in terms of QoS, to a destination even though a wormhole tunnel was not established.

3.1.2 Simulation results

We have used the network simulator ns-2, to evaluate the performance of AODV-WADR compared to the traditional AODV. The mobility was simulated using the *Mission Critical Mobility* (MCM) [2] model for ns-2.

We have shown a series of results to make clear that AODV-WADR is more efficient in terms of packet loss than AODV when malicious nodes have launched one or more wormhole attacks. In our simulations, we use different types of field configurations including 10, 25, 35, 50 and 65 mobile nodes which are moving randomly, pausing for a fixed time of 5 seconds and then moving randomly again in a $1000m \times 1000m$ area or $2000m \times 2000m$ area. The two different speeds which are considered are 1 m/s and 2 m/s. The simulation time is limited to 1000 seconds due to the fact that after a series of experimentations, we observed the same trends in the results for longer simulations.

Furthermore, the data rate chosen is 64 kbps and the mobile devices transmit text and voice data over *Transmission Control Protocol* (TCP) or *User Datagram Protocol* (UDP). To evaluate the performance of AODV-WADR, we compare its performance with AODV in terms of delay and packet loss. Specifically, *packet loss* is the failure of one or more transmitted packets to arrive at their destination and *delay* is caused when routing packets in MANETs take more time than expected to reach their destination. We summarise the simulation parameters in Table 3.1.

Table 3.1: The simulation parameters used in ns-2 simulator during the evaluation of AODV-WADR.

Examined approaches	AODV, AODV-WADR
Pause Time	5 sec
Number of Nodes	10, 25, 35, 50, 65
Data Rate	64 kbps
Nodes' Speed	1, 2 m/s
Simulation Time	1000 s
Mobility Model	Mission Critical Mobility
Simulation Areas	1000m x 1000m, 2000m x 2000m
Traffic Types	UDP, TCP

3.1.2.1 Packet loss

First, in Fig. 3.3 and 3.4 we depict the packet loss as a function of the number of nodes in TCP and UDP data traffic, respectively, for a $1000m \times 1000m$ area. Second, in Fig. 3.5, 3.6 we depict the corresponding results for a $2000m \times 2000m$ area. In both cases, we observe that there is a lower packet loss in AODV-WADR. Such reduction occurs due to the detection of the wormhole tunnel and the exclusion of the malicious nodes from the path between source and destination. In this way, the availability of the network resources is increased.

Packet loss is lower in AODV-WADR due to the detection of the wormhole tunnel and the exclusion of malicious nodes which have launched a Denial-of-Service attack (for example dropping packets). Consequently, this increases the availability of the network resources. Also, due to TCP sends more packets it consequently has higher packet loss than UDP otherwise the ratio of lost packets to sent packets is similar for both protocols.

From Fig. 3.5, we notice that for an $2000m \times 2000m$ area there is higher packet loss than an $1000m \times 1000m$ area because we have further links so more packets are generated including acknowledgements of TCP. These finding are the opposite in the case of UDP as Fig. 3.6 shows. The lower packet loss in the case of the $1000m \times 1000m$ area is explained due to the less interference caused in a larger network area when the number of devices

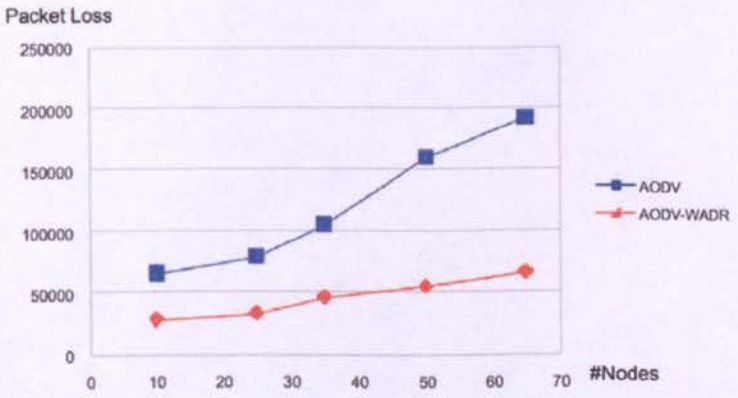


Figure 3.3: The packet loss for different number of nodes moving in a $1000m \times 1000m$ area (TCP traffic).

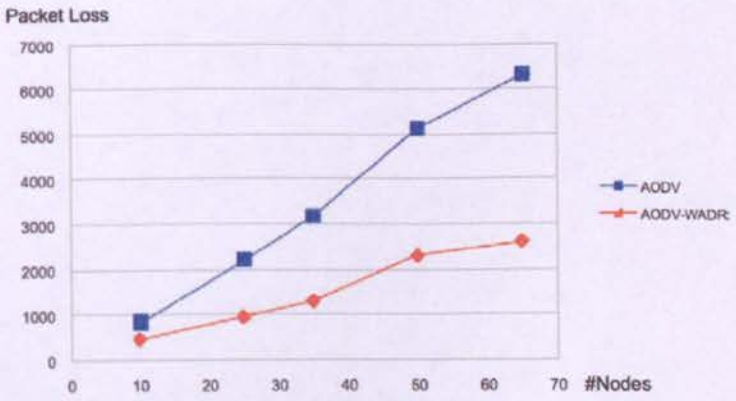


Figure 3.4: The packet loss for different number of nodes moving in a $1000m \times 1000m$ area (UDP traffic).

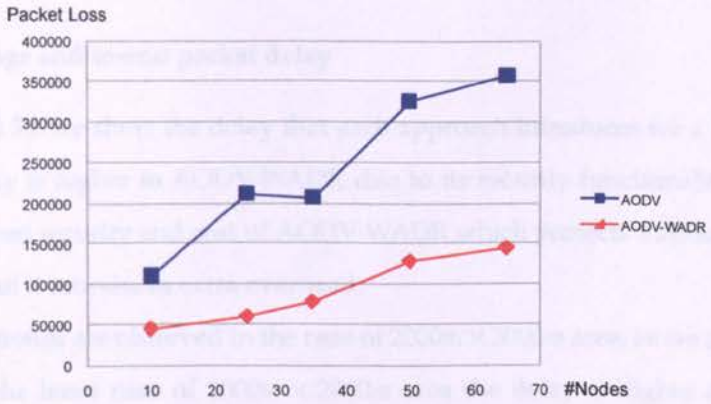


Figure 3.5: The packet loss for different number of nodes moving in a $2000m \times 2000m$ area (TCP traffic).

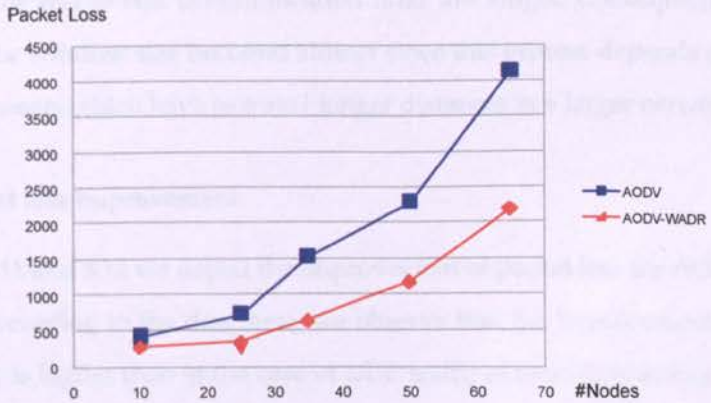


Figure 3.6: The packet loss for different number of nodes moving in a $2000m \times 2000m$ area (UDP traffic).

remains the same. Hence, the lower interference causes less congestion and less packet loss.

3.1.2.2 Average end-to-end packet delay

In Fig. 3.7 and 3.8 we show the delay that each approach introduces for a $1000m \times 1000m$ area. The delay is higher in AODV-WADR due to its security functionalities. This is the tradeoff between security and cost of AODV-WADR which protects a system from wormhole attacks but it introduces extra overhead.

The same trends are observed in the case of $2000m \times 2000m$ area, as we show in Fig. 3.9 and 3.10. In the latter case of $2000m \times 2000m$ area the delay is higher due to the fact that AODV-WADR needs more time to detect the malicious nodes for the larger area of $2000m \times 2000m$ than for the $1000m \times 1000m$ area.

The delay is higher in TCP because the protocol causes more congestion than UDP. As latency increases, in TCP, the sender may spend more time waiting on acknowledgements instead of sending packets. We notice also that the delay is higher for a larger network area because AODV-WADR needs more time to identify malicious nodes in addition to the fact that the end-to-end communication links are longer. Consequently, the process of adjusting the window size becomes slower since this process depends on the received acknowledgements which have to travel longer distances in a larger network area.

3.1.2.3 Packet loss improvement

Last, in Fig. 3.11 and 3.12 we depict the improvement of packet loss for AODV-WADR, for both areas. According to the diagrams, we observe that the improvement of packet loss for TCP traffic is higher than in the case of UDP traffic in most simulations. This happens because the protocol has to retransmit the packets if they are dropped, so if the packet loss reduces, the improvement will be more pronounced than in UDP. This is also the reason that a wormhole attack can cause cause higher damage to TCP if packets are dropped due to such an attack.

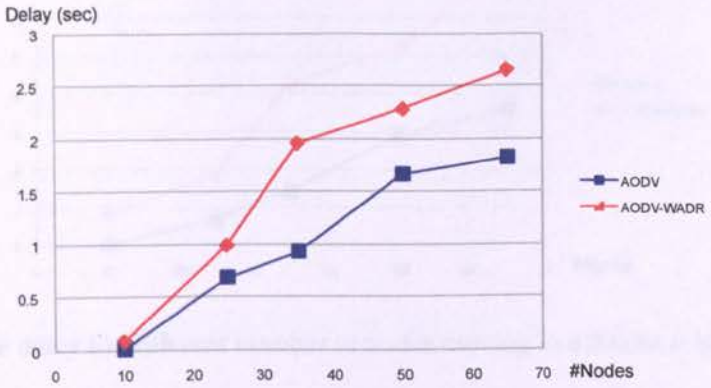


Figure 3.7: The delay for different number of nodes moving in a $1000m \times 1000m$ area (TCP traffic).

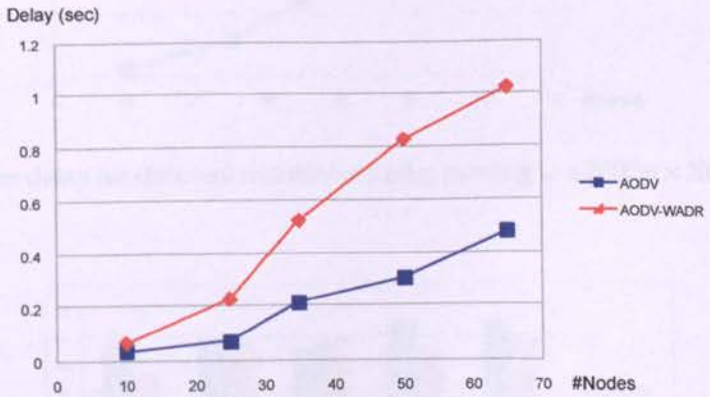


Figure 3.8: The delay for different number of nodes moving in a $1000m \times 1000m$ area (UDP traffic).

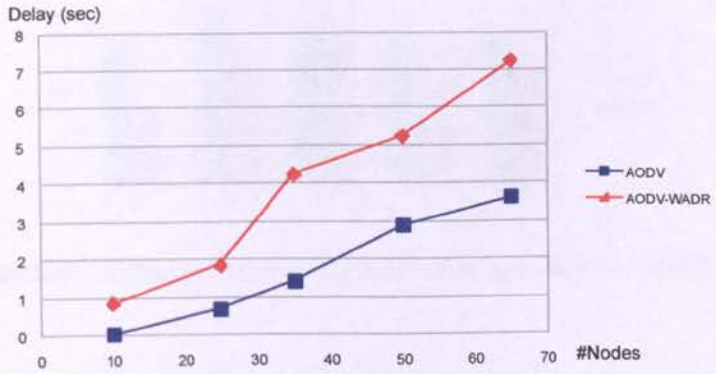


Figure 3.9: The delay for different number of nodes moving in a $2000m \times 2000m$ area (TCP traffic).

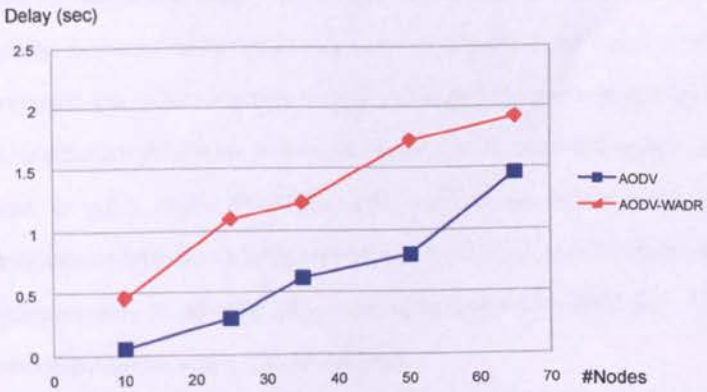


Figure 3.10: The delay for different number of nodes moving in a $2000m \times 2000m$ area (UDP traffic).

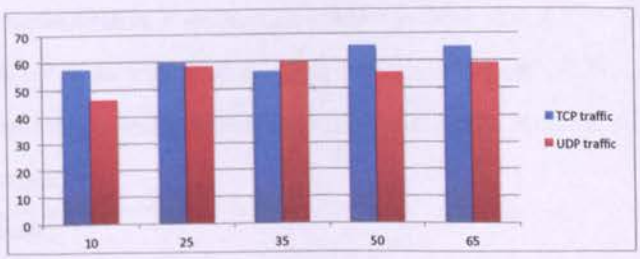


Figure 3.11: The improvement of packet loss for a $1000m \times 1000m$ area.

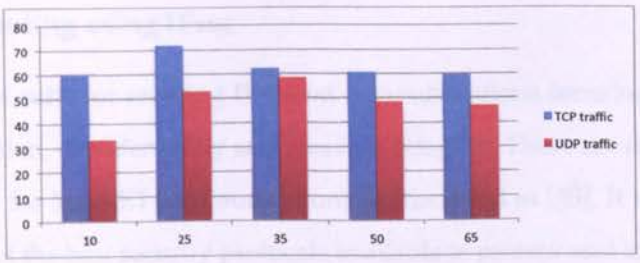


Figure 3.12: The improvement of packet loss for a $2000m \times 2000m$ area.

3.2 Secure routing for emergency MANETs

According to [5], routing in a MANET can be summarised as a multi-hop packet forwarding mechanism that can efficiently adapt to changes in the wireless network topology. This will be mainly beneficial for users situated in areas with inadequate or no pre-existing communication infrastructures. For instance, first responders often have to carry out rescue missions in remote sites or disaster locations where infrastructures may be scarce, incapacitated or even nonexistent. In such cases, MANETs will provide an autonomous IP-based multimedia communication platform to enhance mission critical coordination efforts. MANETs can also be deployed as tactical networks in usually remote battlefields where ad-hoc and autonomous communication setups are required.

In this section, we provide security for CML by using a hybrid version of the *Internet Protocol Security* (IPsec) and evaluate its performance compared to traditional IPsec schemes and the pure CML[3]. To this end, we first apply the same IPsec version over well-known routing protocols for MANETs to evaluate their performance and derive the time and space overheads caused by such a mechanism [8]. Finally, we propose the *Secure ChaMeLeon* (SCML) [9], [10] which provides end-to-end authentication, confidentiality and integrity for MANET messages.

[3]CML without security.

3.2.1 Secure routing using IPsec

IPsec is a protocol suite for securing IP-based communications focusing on message and origin authentication, confidentiality and message integrity. These are also the main security requirements for MANET communications as discussed in [85]. It is widely accepted that IPsec is one of the best security protocols available at present and is mentioned as the most reliable and efficient network layer protocol.

IPsec also offers replay attack prevention and perfect forward secrecy. The significant importance of the aforementioned protocol is that it offers flexibility, which cannot be achieved at higher or lower layer abstractions in addition to the symmetric cryptographic schemes which are appropriate to be used in handheld resource constrained devices such as mobile phones to transmit data.

In this context, several research approaches such as [86] and [87] have concluded that the usage of IPsec is appropriate in MANETs. An intruder who eavesdrops on a wireless communication link has the potential to capture passwords which are being transmitted unencrypted. The malicious node can then use the said password to masquerade as a legitimate mobile user. Using the IPsec protocol, data packets are encrypted and the attacker cannot overhear private information. Additionally, an intruder can spoof his IP address to masquerade as a trusted node when the address-based authentication scheme is used. In that case, IPsec protects against IP spoofing attacks by deploying authentication techniques.

Furthermore, *Denial of Service* (DoS) attacks could be avoided by using IPsec. Specifically, when an intruder is trying for instance to launch a *Transmission Control Protocol* (TCP) *SYNchronous* (SYN) flooding attack by sending a sequence of connection request messages, the available buffer space of the target-victim system is overrun. Due to the authentication that IPsec offers, the intruder launches TCP SYN flooding attacks using its own IP address, revealing its location and identity. Finally, in keeping with the concept of integrity protection that IPsec provides, when the *Integrity Check Value* (ICV) of a packet is valid it receives the appropriate treatment and the nodes decide the next hop node across the path to the destination. If any unauthenticated node changes any data in the IP

datagram or updates the ICV, this node will be detected and the packet will be discarded.

IPsec can achieve its security goals by creating *Security Associations* (SAs) between nodes. An SA contains the addresses of the participating nodes and the type of security to be used along with the algorithms that will be used in each instance. The SA also contains the keys, which will be used by the chosen encryption algorithm. The keys differ in length depending on the type of algorithm used and must be unique. A policy is recorded in the *Security Policy Database* (SPD), which details how the SA is to be implemented. The policy specifies which mode (tunnel or transport) will be used, how, and when it will be used.

In this section a hybrid version of the IPsec protocol [87], [88] is deployed to provide confidentiality, message and origin authentication and message integrity for the MANET communication links. This hybrid version includes both *Authentication Header* (AH) and *Encapsulating Security Payload* (ESP) modes. This choice is taken based on the fact that a potential attacker can perform traffic analysis, examine protocol numbers, modify the destination address, and other IP fields if the only applied protocol is ESP. This occurs since ESP does not protect the IP header of an IP datagram. In addition, according to [87], we have chosen to use only the transport mode of the IPsec protocol in order to avoid high processing power overhead.

Many researchers have argued in favour of a more compact and efficient version of IPsec which will not include the AH, in transport mode. However, ESP offers integrity protection for everything beyond the IP header when AH provides integrity protection for some of the fields of the IP header.

ESP offers confidentiality by encrypting the IP payload using 128-bit symmetric AES keys and AH offers authentication and integrity of transmitted packets. AES uses the Rijndael algorithm which is a symmetric block cipher that supports different key and block sizes of 128, 192 and 256 bits with the AES standardised to be the fixed block size of 128 bits. The most important characteristic of the algorithm is the fact that it combines implementation convenience and simplicity with increased protection against different attacks.

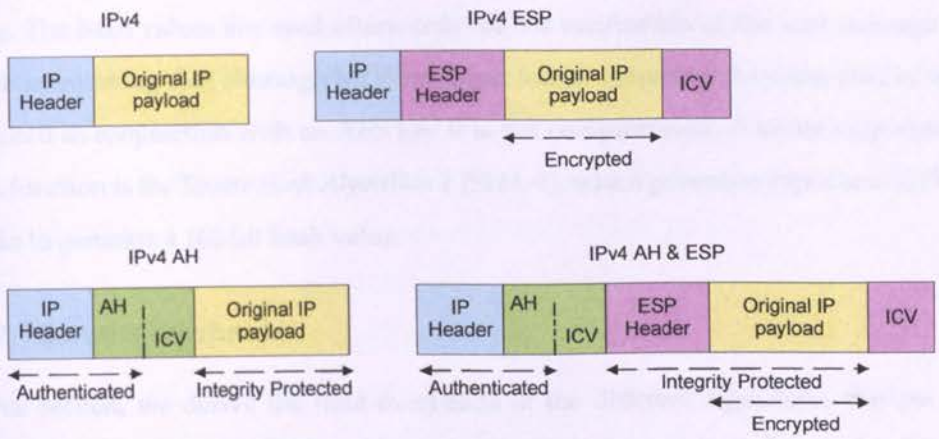


Figure 3.13: Different IPsec setups.

For the ESP protocol we use 128-bit AES symmetric keys due to AES proven strength and its low overhead. According to the *National Institute of Standards and Technology* (NIST), a 128-bit AES key requires a 3072-bit RSA (*Rivest, Shamir and Adleman*) key while 256-bit AES requires an RSA key size of 15,360 bits for equivalent security. Obviously, 15,360 bits will degrade the performance of any system since key size is directly related to computing resources.

In addition, AES is a *Federal Information Processing Standard* (FIPS) certified encryption method described in [89]. A FIPS is a public standard developed by the United States federal government aiming at securing computer systems for any non-military government agency. Due to the critical nature of emergency communications, the aforesaid compliance is required to ensure an adequate security level for encrypting messages in MANETs.

Authentication and integrity are satisfied by the AH protocol that utilises the *Message Digest 5* (MD5) hash algorithm along with a symmetric key to produce an *Hash Message Authentication Code* (HMAC) called HMAC-MD5. We illustrate the different modes of the IPsec protocol in Fig. 3.13.

HMAC is a type of *Message Authentication Code* (MAC) calculated using a cryptographic hash function in conjunction with a secret key. On the other hand, MD5 is a one-way hash function, which processes input text in 512 bit blocks to generate a 128-bit hash

value. The hash values are used afterwards for the verification of the sent message. It is worth mentioning that although MD5 has been found vulnerable to some attacks, when it is used in conjunction with an AES key it is not compromised. Another cryptographic hash function is the *Secure Hash Algorithm 1* (SHA-1), which processes input text in 512 bit blocks to generate a 160-bit hash value.

3.2.2 Security overheads

In this section, we derive the time overheads of the different algorithms that are used by IPsec. The authors in [90] discuss the space[4] and time complexity[5], introduced by the different modes of IPsec, in terms of CPU cycles. In the same work, they find out that the total number of operations required for MD5 processing per 512 bits block is 720 plus 24 operations for initialisation and termination, while for SHA-1 processing is 900 plus 210 operations for initialisation and termination. Consequently, the overhead introduced by HMAC- MD5 is lower. In order to compute the exact time of HMAC-MD5 operation, in terms of processing cycles per packet, for an input of packets n_k and for processor speed c_p the following equation [90] is used

$$t_{HMAC-MD5}(n_k, cp) = [32 + (2 + 744n_k)]/c_p. \tag{3.1}$$

To go a step further, authors in [90] derive the corresponding number of processing cycles required for encrypting one block of data with each one of the three standardised types of AES for different key lengths 6168, 7512 and 8856 number of CPU cycles for 128, 192 and 256 key lengths respectively. For algorithms weaker than AES such as *Data Encryption Standard* (DES) and 3DES, the corresponding overhead is 2697 and 8091 CPU cycles.

The choice of the AES algorithm to generate the symmetric keys, which will be used by ESP to encrypt the payload of the IP datagram has been done based on the fact that the algorithm is one of the fastest and cryptographically strongest. The time overhead of AES

[4]Security related additional information on the transmitted packets increases the bandwidth consumption.
[5]Security processing increases the packet end-to-end delay and the transmission time.

is $T_{encryption} = 6,168$ and $T_{decryption} = 10,992$ CPU cycles according to [90].

IPsec packetisation and ciphering increase the size of transmitted packets. In transport mode, the space overhead of AH equals 24 and ESP equals 10 bytes [91]. Consequently, the space overhead in the case of our hybrid solution is 24+10 = 34 bytes.

We examine scenarios where emergency MANETs have to be deployed to support communications between First Responders (FRs). These are equipped with handheld devices with processing capability which equals 450 *Millions of Instructions Per Second*[6] (MIPS). From the formula 3.1 and the decryption and encryption times, we derive the time overhead per packet for each of HMAC-MD5 and AES algorithms as follows:

- $t_{HMAC-MD5}$ = 1.68 microseconds per block;
- $t_{AES,encryption}$ = 13.7 microseconds per block and;
- $t_{AES,decryption}$ = 24.4 microseconds per block.

It is worth mentioning here that in our overhead we have not included the overhead for key exchange that IPsec requires. Thus, we take into account only the overhead occurred during the communication phase and after the establishment of cryptographic keys.

3.2.3 Simulation results

In this section, we evaluate the performance of IPsec over AODV, OLSR, DYMO by using ns-2. The average pause time of the nodes in the network is varied in order to investigate the effect of varying mobility on routing performance in such environments. It is worth mentioning here that we use CBR traffic of 64kbps to simulate the use of voice data transmission over the network with 10 CBR connections.

Our goal is to evaluate the performance of each of the aforementioned MANET routing protocols during an emergency scenario in a MANET with 20 nodes. In our simulation scenarios, MANET nodes use IEEE 802.11b wireless interfaces and an obstacle-aware *human mobility model* (HUMO) [2] which simulates the movement of FRs during the rescue

[6] 450 MIPS is a realistic value for a well-known PDA (Apple iPhone).

missions. In these scenarios, obstacles are an integral part of the areas where such networks are deployed in order to facilitate communication among FRs. In the proposed mobility model, the nodes of the network move around the obstacles in a natural and realistic way.

3.2.3.1 Throughput

We have illustrated in Fig. 3.14 and 3.15 the throughput which equals the ratio of received by sent data packets and it is a critical QoS metric given as

$$throughput = \frac{average\ received\ data\ packets}{average\ sent\ data\ packets}$$

against different pause time values or else different mobility levels. We clearly notice that for higher node mobility scenarios or else lower average pause time, the throughput is higher for all the protocols. This is explained in [92] where authors prove that high node mobility in MANETs increases data throughput due to reduction of mutual transmission interference and exploitation of multiuser diversity through packet forwarding. In terms of security, we observe that the IPsec hybrid mode introduces time and space overhead without degrading the main routing functionalities of the protocol. We can see in Fig. 3.15 that throughput has been affected by the increased packet size introduced due to IPsec application.

The increased throughput results lead to a higher energy consumption for the mobile devices. Routing load which is illustrated in terms of bytes is also affected when security considerations are concerned due to IPsec space overhead. The increment is still negligible and that is what predicates the IPsec application efficiency.

3.2.3.2 Total routing load

In Fig. 3.16 and 3.17, it can be observed that the total routing load of the routing protocol decreases when mobility decreases. In high mobility networks, the frequent route changes result in DYMO and AODV sending more reactive route discovery routing messages to obtain routes to destinations. DYMO uses additional RERR messages to explicitly alert

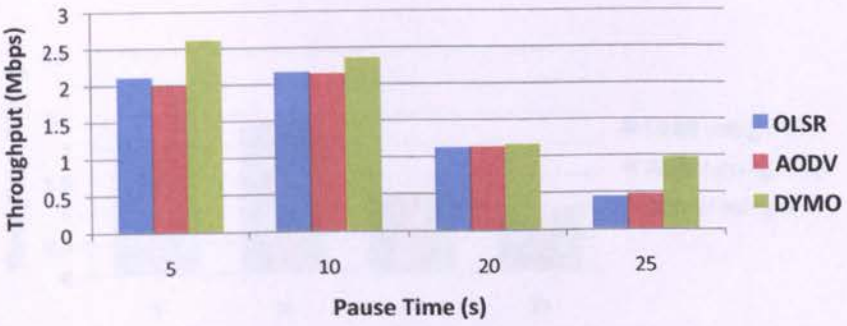


Figure 3.14: The throughput for the different routing protocols.

participating nodes in a route about an unreachable route and therefore it uses more routing load than AODV. In low mobility scenarios where the route changes are less frequent, the difference between DYMO and AODV routing loads is smaller. However, OLSR uses a proactive approach and thus it utilises periodic routing messages without considering the rate of route changes. In Fig. 3.18 we have plotted the extra routing load for the different routing protocols due to the use of IPsec.

3.2.3.3 Average end-to-end packet delay

The average end-to-end packet delay results are shown in Fig. 3.19 and 3.20. The average packet delivery delay in the network decreases when the node pause time increases for all the routing protocols investigated. The average end-to-end delay value for packet delivery corresponds to the time required to find a route to a destination plus the time required for a transmission to take place along such a route and is given by

$$(\textit{end-to-end delay}) = (\textit{route discovery delay}) + (\textit{transmission delay}).$$

The route discovery delay is directly affected by mobility because any originator has to find valid routes in a corresponding frequency. We observe that for secure routing an increment of approximately 67% in the delay is noticeable. This happens due to the time overhead both ESP and AH protocols introduce to the communication links for each transmission.

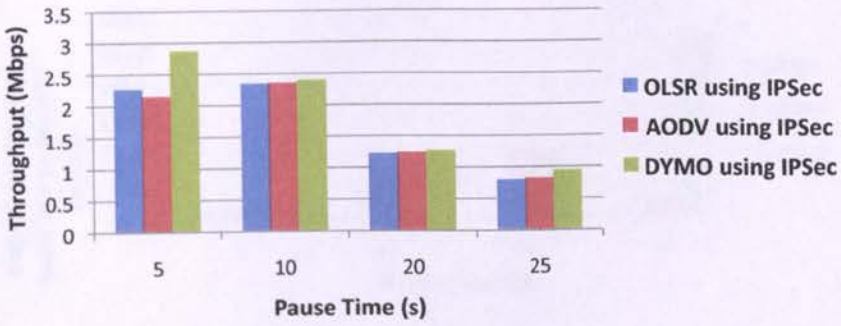


Figure 3.15: The throughput for the different routing protocols using IPsec.

Figure 3.16: The total routing load for the different routing protocols.

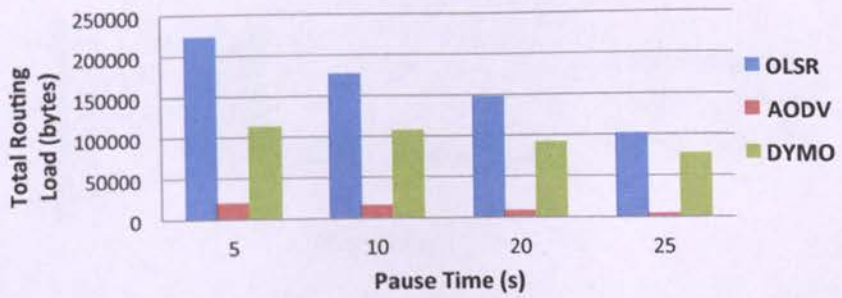


Figure 3.17: The total routing load for the different routing protocols using IPsec.

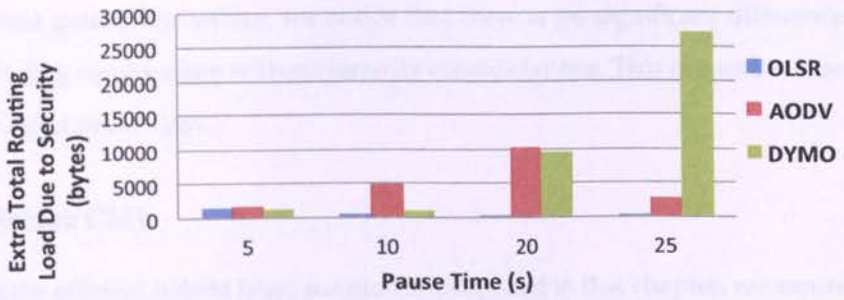


Figure 3.18: The extra routing load for the different routing protocols due to the use of IPsec.

Figure 3.19: The average end-to-end data packet delay for the different routing protocols.

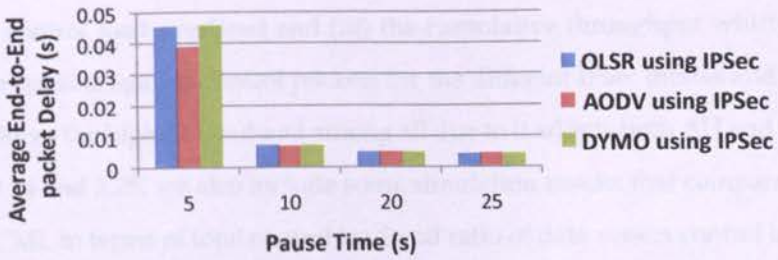


Figure 3.20: The average end-to-end data packet delay for the different routing protocols using IPsec.

Although we have illustrated the ratio of total packets sent to total dropped packets against the different pause time values, we notice that there is no significant difference from the corresponding results taken without security considerations. This occurs because the IPsec does not affect packet loss.

3.2.4 Secure CML

By using the efficient hybrid IPsec solution as proposed in this chapter, we secure the CML routing protocol by proposing *Secure ChaMeLeon* (SCML). In this way, we provide end-to-end authentication, confidentiality and integrity for the MANET messages. We have used simulations to verify the integrity of the proposed mechanisms and showcase the benefits of using our solution. We next use an event based simulator, customised with our implementation of the SCML protocol, to validate the proposed model.

3.2.5 Simulation results

In the following, we illustrate the simulation results, retrieved by ns-2, for the comparison of SCML with CML, CML using IPsec in AH mode and CML using IPsec in ESP mode. The results have shown that the overhead introduced by SCML is negligible compared to the other choices, while at the same time it provides higher level of security as we have previously discussed.

In Fig. 3.21 – 3.23, we illustrate (i) the cumulative packet end-to-end delay, (ii) the cumulative control load overhead and (iii) the cumulative throughput which equals the ratio of data packets against control packets for the different IPsec modes and SCML. The latter introduces the highest overhead among all due to it adopts both AH and ESP modes.

In Fig. 3.24 and 3.25, we also include some simulation results that compare the performance of SCML in terms of total control load and ratio of data versus control load, against a well-know secure routing protocol such as *Secure Ad hoc On-Demand Distance Vector* (SAODV) [46]. This protocol, as we have discussed in Chapter 2 uses digital signatures, asymmetric encryption keys and hash chains.

3.2.5.1 Cumulative packet end-to-end delay

By noticing Fig. 3.21 we see that the cumulative end-to-end delay for the case of SCML is slightly higher than the delay of CML when using the ESP mode whilst it provides both advantages of AH and ESP.

3.2.5.2 Cumulative routing control load

In Fig. 3.22, we illustrate the performance of each case in terms of total control data[7]. We observe that SCML has the highest value of control data in bytes. This is an expected result due to the fact that each SCML packet has an overhead of 192 bits for HMAC-MD5 and 80 bits for AES encryption which equals 272 bits more than conventional CML.

3.2.5.3 Cumulative throughput

In terms of data load versus control data load in bytes, the results illustrated in Fig. 3.23 validate the intuition that the ratio is the highest for CML due to the absence of extra security overhead introduced by the rest of the protocols. In all graphs, we observe that SCML does not introduce unaffordable overhead to CML while it provides adequate level of security. These are enough requirements to highlight the suitability of the protocol for emergency MANETs which require efficient QoS routing solutions.

3.2.5.4 Comparison with SAODV

The simulation results illustrated in Fig. 3.24 and 3.25 and published in [10] show the control load and the ratio of data to control load for different pause times namely for different mobility models. We notice that the routing load of SCML is significantly lower than SAODV's whilst SCML is delivering more data per control load than SAODV. This happens due to the lightweight mechanisms of symmetric cryptography that SCML uses compared to the asymmetric that is used in SAODV. On the other hand, the security level

[7]Routing data.

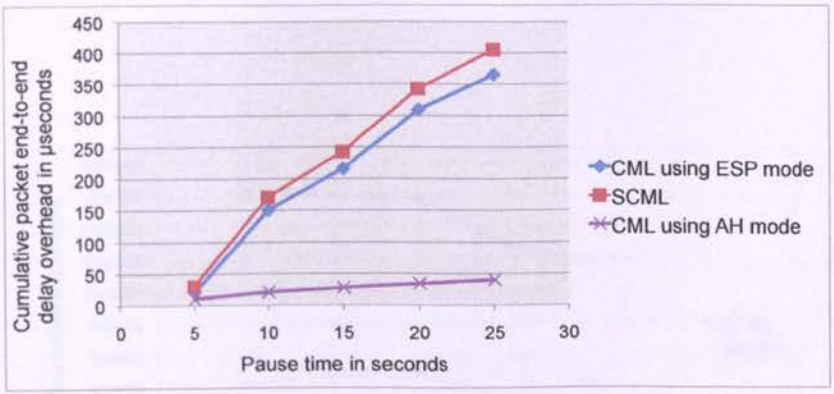


Figure 3.21: Cumulative packet end-to-end delay overhead.

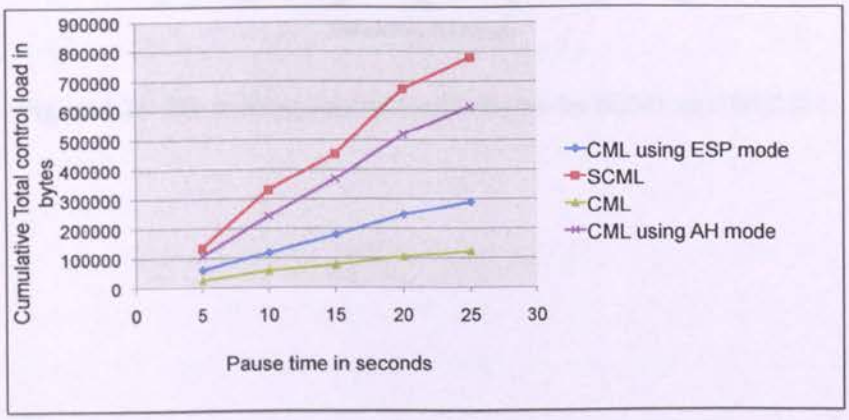


Figure 3.22: Cumulative routing control load in bytes.

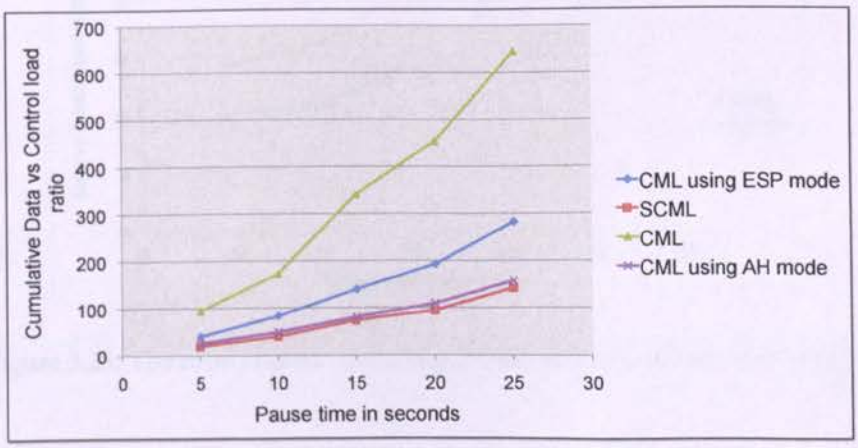


Figure 3.23: Cumulative ratio data against routing control load.

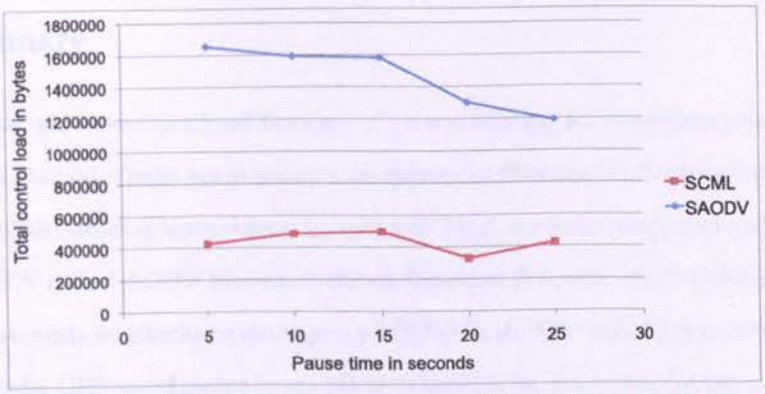


Figure 3.24: The routing control load in bytes for SCML and SAODV.

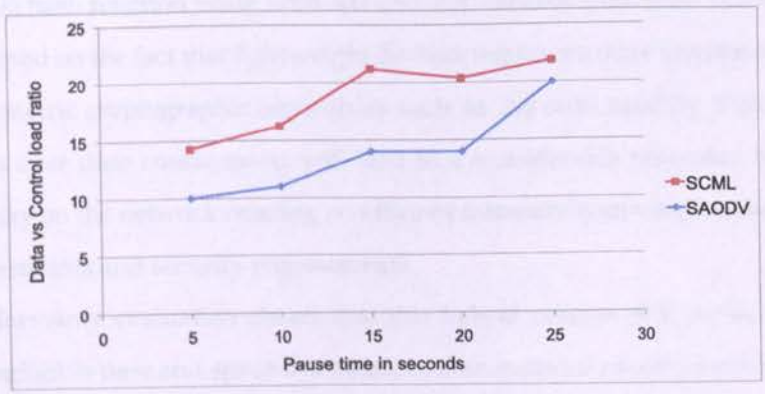


Figure 3.25: The ratio of data vs routing control load for SCML and SAODV.

of SCML is adequate when AES is used and is comparable with asymmetric solutions in terms of security strength.

3.3 Summary

In this chapter, we have examined the case of secure routing for emergency mobile ad-hoc networks (MANETs). These are autonomous networks that can be deployed in emergency cases to establish communication among rescuers. First, we have proposed a secure mechanism for AODV called *AODV Wormhole Attack Detection Reaction* (AODV-WADR) to detect and react to wormhole attacks in emergency MANETs. AODV-WADR does not require statistical methods, GPS coordinates or specialised hardware, since employing such methods or hardware may not be feasible during emergencies. The simulation results show that the performance of AODV-WADR is more efficient than AODV, in terms of packet loss due to the mitigation of wormhole attacks.

We have also taken advantage of the security strength of IPsec to provide network layer security for emergency MANETs. In fact, we have used the *transport* mode of IPsec and we have applied the *Advanced Encryption Standard* (AES) cryptographic algorithm along with the MD5 hash function using both AH and ESP security protocols. The afore choices have been based on the fact that lightweight devices require security implementations that rely on symmetric cryptographic algorithms such as the ones used by IPsec. Using this combination over their counterparts will lead to a considerable reduction in processing time and delay on the network creating an efficient transaction moving towards satisfying resource constraints and security requirements.

The performance evaluation shows that this hybrid version of IPsec in MANETs introduces, negligible time and space overhead, to conventional routing mechanisms while it enables the adequate security level for MANET multimedia communications. We have used the same version of the IPsec on top of the MANET routing protocol *ChaMeLeon* (CML) to provide *confidentiality*, and *integrity* to the transmitted packets by designing the *Secure ChaMeLeon* (SCML) protocol.

Chapter 4

Secure P2P Overlays for Emergency MANETs

"Those whose acquaintance with scientific research is derived chiefly from its practical results easily develop a completely false notion of the mentality of the men who, surrounded by a sceptical world, have shown the way," Albert Einstein

In this chapter we examine how to provide security for peer-to-peer (P2P) overlays in emergency MANETs[1] [31]. Especially, we propose the secure version of the novel peer-to-peer overlay architecture for MANETs, called *Reliable Overlay Based Utilisation of Services and Topology* (ROBUST), discussed in Chapter 2 of this thesis, by securing the *Distributed Hash Tables* (DHT) signalling messages by using symmetric key encryption.

We then present and discuss the performance evaluation results retrieved by developing this DHT architecture in ns-2. We also compare this protocol with the pure ROBUST by evaluating average end-to-end DHT data request delay, overhead and DHT signalling packet loss. The chapter concludes that this protocol introduces affordable overhead hence it can be used when high QoS multimedia communications are required.

The security extensions presented in this chapter consist of the following:

[1] in this chapter from now the terms MANETs and emergency MANETs are interchangeable.

- A *key exchange* phase where ROBUST peers exchange pairwise symmetric key material K_{pwk} with their leafset peers[2] as well as their super peers;
- A *key refresh* phase where peers generate new key material and exchange it with their leafset peers as well as their super peers;
- A *proximity synchronisation* phase where peers that wish to join a new cluster, in order to reduce the delay have to accomplish a secure handshake and exchange key material with their new super peer and leafset peers.

4.1 ROBUST architecture

In ROBUST at any given time we need C clusters where $C = \lceil \frac{N}{\log_2 N} \rceil$ and N is the total number of peers in the network. This gives us a total routing complexity of $O(\log_2 C) + O(1)$ and $O(\log_2 C) \leq O(\log_2 N)$. To address the issue of scalability and refrain any peer from being bottlenecked, more clusters would need to be factored into the DHT as the amount of peers increases.

Peer proximity is central to ROBUST algorithm and the architecture has been designed with this notion in mind. From the start when peers join the overlay they contact the nearest bootstrap peer, which is the nearest super peer. If the number of peers within the cluster is less than $\log_2 N$ the peer will join that cluster after being given a *peerID*, by the super peer, in order to maintain ID space equality.

If the number of peers within the cluster is equal to $\log_2 N$, the super peer will forward the join request to its closest two super peers (the first numerically greater than and less than its own *peerID*). These super peers will then run the same algorithm until the peer has joined a cluster with free space. The maximum number of steps to find a non-full cluster is denoted as $O(\log_2 C) + 2$.

This is explained as follows. The origin peer P_1 sends a message to the destination peer P_2. If P_2 belongs to a different than P_1 cluster then, the message is sent from P_1 to its cluster's

[2] L immediate neighbours in the nodeId space

super peer SP_1. Then, this super peer sends the message to the super peer of the cluster that P_2 belongs to, namely SP_2. The complexity of a search algorithm in a DHT equals the binary tree search complexity [93]. Thus assuming C clusters, the maximum path length from SP_1 to SP_2 is $O(\log_2 C)$. When the message arrives at the destination cluster, SP_2 forwards this to the destination peer P_2 in one logical hop inside this cluster.

The next step is to take into account mobility. When peers move through the physical space, they may be closer physically to another super peer. In order to maintain proximity, a function aptly named *proximity synchronisation* is proposed. This is achieved by super peers periodically broadcasting a beacon to each of the peers within their cluster. These peers then forward the beacon to any peers around them with a one-hop *Time To Live* (TTL). The result of this function is that if a peer moves closer to another super peer, it can ping the newly discovered super peer and compare its latency with the current super peer with which it has established communications. If the newly discovered super peer is closer, the peer sends a move request to the relevant super peer, if the cluster is not full, the peer leaves the overlay with its current ID and rejoins with an ID issued by the new super peer.

In this thesis we consider the following types of signalling messages:

- DHT_{put_req}: this corresponds to a request for putting some data in the DHT.
- DHT_{ping}: this corresponds to any ping message in the DHT.
- DHT_{join_req}: this equates to the join request packet, which is forwarded to the nearest super peer.
- DHT_{ack}: this corresponds to an acknowledgement message required to acknowledge other signalling packets such as DHT_{get}, DHT_{put}, DHT_{sync}, DHT_{ls_up}, DHT_{ping}, DHT_{clsrt_beacon} and DHT_{prox_sync}.

The rest of the signalling messages are described in the next example. In Fig. 4.1 we show a mobility example scenario where a peer P_1 is moving from C_1 to C_2. The box at the top of the figure represents a top down overview of the network, containing two clusters C_1 and C_2. The dashed lines around these clusters represent the broadcast radius of the super

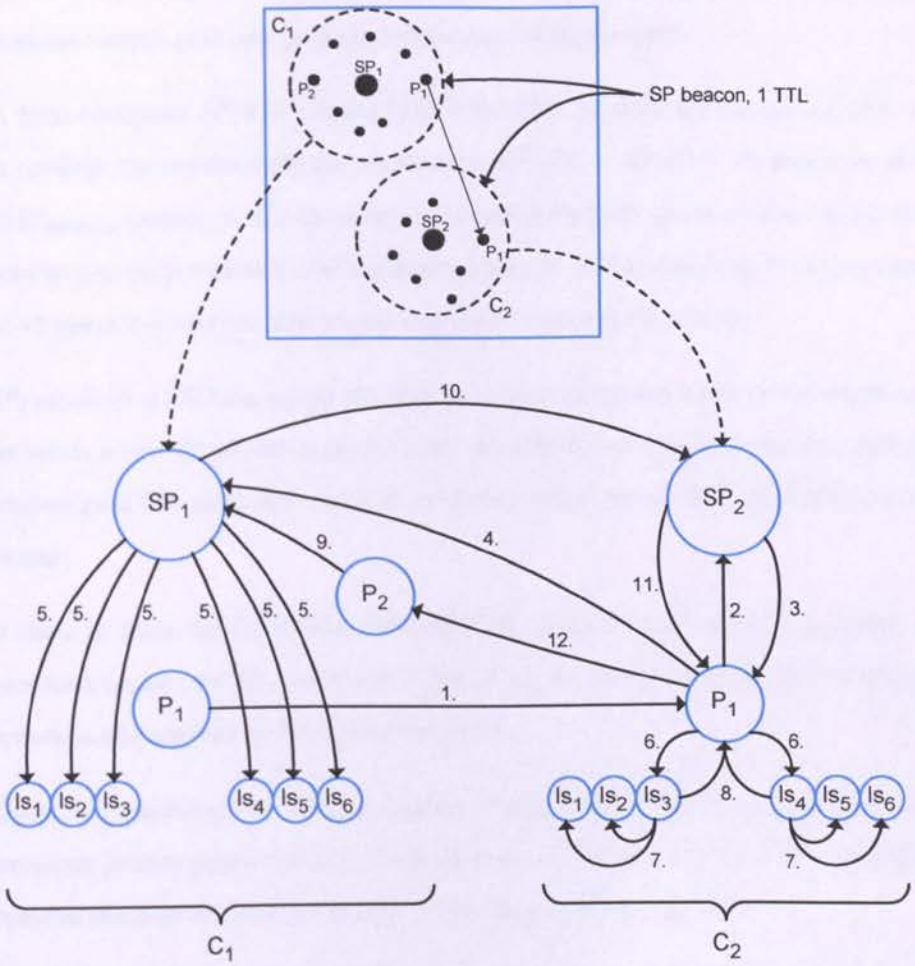


Figure 4.1: An overview of the described DHT architecture.

peers for each cluster SP_1 and SP_2 respectively. Each step of the diagram is explained in detail below:

1. Peer P_1 moves out of transmission range of super peer SP_1 and subsequently into transmission range of super peer SP_2, therefore receiving the DHT_{clstr_beacon} packet from said super peer and gaining knowledge of its presence.

2. P_1 then compares SP_1RTT (*Round Trip Time*) with SP_2RTT over a period of $3 \cdot t_{beacon}$ to confirm the results with the realisation $SP_2RTT < SP_1RTT$. P_1 therefore sends a DHT_{move_req} packet to SP_2 to ascertain whether there is space in the cluster for the peer to join (as previously stated clusters must be within size $\log_2 N$ with a variance of +2 peers in order to maintain an equally distributed ID space).

3. SP_2 sends P_1 a DHT_{move_rep} packet stating if there is indeed room in the cluster and if so, sends a new ID prefix for peer P_1 and also the IPs of P_1's new closest predecessor (closest peer ID lower than P_1) and successor (closest peer ID higher than P_1) in the cluster.

4. If there is space for P_1 to join the cluster C_2, it then sends a DHT_{part} packet to its previous super peer SP_1 notifying it that P_1 is leaving the cluster and subsequently removes all previous nodes from its leafset.

5. Upon SP_1 receiving the DHT_{part} packet, it first sends a DHT_{broad_part} packet to P_1's previous leafset peers notifying them that P_1 has left the cluster, they subsequently remove the peer from all of their DHT routing tables as does SP_1.

6. P_1 then sends a DHT_{ls_up} packet to its predecessor and successor nodes, they add the node to their leafset and reply to P_1 with the leafset peers which fall within P_1's leafset.

7. The leafset nodes of peer P_1 learn of his existence through the leafset update function which runs every t_{ls} period and chooses a random existing leafset peer to sync with.

8. The leafset peers of P_1 run the DHT_{sync} data synchronisation function every t_{sync} interval randomly choosing a leafset peer to synchronise data values for which both the peers are responsible. In this way peer P_1 will receive all of the data values it is responsible for.

9. Peer P_2 of cluster C_1 submits a DHT_{get_req} to its super peer SP_1 whom then compares the ID lookup stored in the request with the IDs of all of the other super peers in the overlay which it knows of.

10. SP_1 then forwards the request to the super peer with the closest peer ID to that of the ID stored in the request which in this case is SP_2.

11. SP_2 receives the DHT_{get_req} and forwards it to the peer within the cluster with the closest peer ID to the ID stored in the request which is P_1.

12. Peer P_1 receives the request and sends the data stored under the specified ID directly back to P_2 using its IP address.

4.2 Security for ROBUST

Within the context of ROBUST, different types of signalling messages have to be exchanged amongst peers during the networks' lifetime as we discussed in the previous section. Thus potential attackers could find a way to exploit security vulnerabilities which appear due to the transmission of these messages.

To give a clear picture of how harmful the existence of malicious peers against the ROBUST DHT could be, we derive the maximum length l of an overlay (logical) route in hops between a source and a destination peer. This equals $\log C + 2$ where C is the number of clusters in the overlay network. Further, $C = \lceil \frac{N}{\log_2 N} \rceil$ which is the maximum length of an overlay route equals

$$l = \log N - \log(\log N) + 2.$$

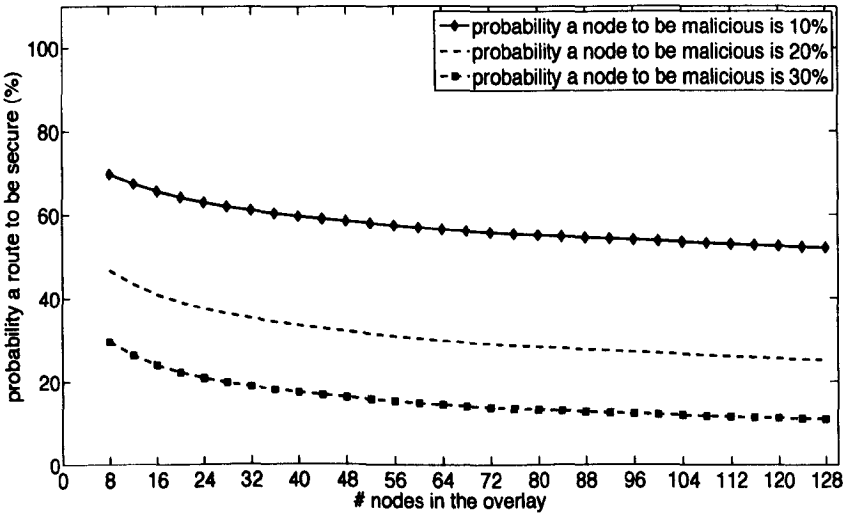


Figure 4.2: The probability of a route to be secure as a function of the overlay peers based on the likelihood for a peer to be malicious.

Assuming that the probability of a peer to be malicious is m, the probability to have a secure route namely a route that consists only of legitimate peers equals

$$P_{secure\_route} = (1-m)^{\log N - \log(\log N)+2}.$$

From this we can derive that the impact of the attacker is severe even for a small fraction of malicious peers. In Fig. 4.2 we have illustrated the likelihood of a secure route for different network sizes. We notice that for higher number of nodes, in the overlay, there is a lower probability for a route to be secure.

To cope with external adversaries the ROBUST DHT needs to be extended in a way that peers will exchange cryptographic material. In the following we describe how peers as well as super peers exchange cryptographic pairwise symmetric keys. These keys will then be used to encrypt ROBUST signalling information in a pairwise manner. This means that each pair of peers, including super peers, will use a specific symmetric key to encrypt the signalling information. We assume that in the beginning of the network's life, a global 128-bit symmetric *Advanced Encrypted Standard* (AES) pre-shared key called a *network wide*

key (K_{nwk}) has been installed in all the devices of the mobile peers. Similarly groups of users who wish to share data securely can use such a pre-shared key much like common security encryption standards use today for example the IEEE 802.11i *pre-shared key* mode (PSK).

The use of K_{nwk} defends a MANET against *man-in-middle* attacks during the exchange of the peers' pairwise symmetric keys. As we have mentioned the use of symmetric rather than asymmetric cryptography is due to asymmetric cryptographic algorithms being slower than symmetric algorithms as well as they introduce higher energy cost [3].

On the other hand, the reason why we do not use the K_{nwk} for the duration of the network's lifetime is due to the ample opportunities for cryptanalysers to retrieve the key material. By exchanging pairwise symmetric keys and refreshing at a certain interval we minimise the risk of successful cryptanalysis activities whilst we prevent compromised peers from reading information exchanged between other peers. We assume that there is a very limited possibility for a peer to be compromised before the exchange of the pairwise symmetric keys. The security extensions for the ROBUST signalling messages between two peers P_i and P_j consist of three main phases as described in the following:

- *key exchange* phase: during this phase ROBUST peers exchange their pairwise 128-bit AES symmetric key K_{pwk} with their leafset peers and their super peers by sending a DHT_{key_exch}. To this end, peers use the K_{nwk} to encrypt the DHT_{key_exch} as well as the ROBUST packet header;

- *key refresh* phase: the task of this phase is for any given peer to generate new key material and exchange it with their leafset peers and super peer by sending them a DHT_{key_refr} every t_{key_refr} seconds. For the encryption and transmission of the new keys, peers use the previous established symmetric keys K_{pwk};

- *proximity synchronisation* phase: during this phase peers move closer to a new super peer SP' and consequently should move to the new cluster by adopting a new ID in the DHT space. In this case, peers must use the K_{nwk} to send their symmetric keys to their new leafset peers in addition to the new super peer. Therefore before they join

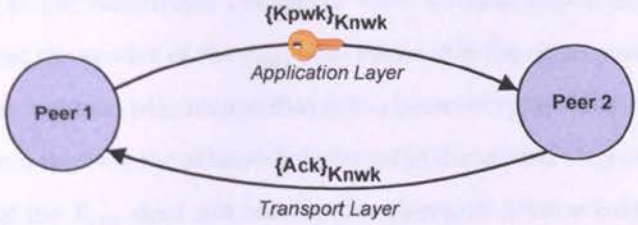


Figure 4.3: The 2-way handshake between two peers which are exchanging a pairwise symmetric key K_{pwk} during the *key exchange* or *proximity synchronisation* phase.

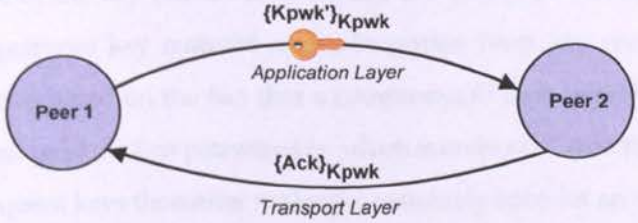


Figure 4.4: The 2-way handshake between two peers which are exchanging a pairwise symmetric key K_{pwk} during the *key refresh* phase.

the new cluster they send a DHT_{part} packet to all of their previous leafset peers and super peer.

All phases consist of a 2-way handshake between two peers as illustrated in Fig. 4.3 and 4.4. It is worth stressing here the following:

- Since the security extension algorithm is distributed, there is a possibility for both peers that participate in a handshake to send their K_{pwk} to each other at almost exactly the same time consequently having two different K_{pwk} at the end of the handshake. To avoid this issue, we assume that both peers keep track of the exact time they send their K_{pwk}. For instance, if P_1 receives a K'_{pwk} from P_2 before it receives an acknowledgement for the previously sent K_{pwk}, it will compare the send time of the received K'_{pwk}, t', with the time they sent the K_{pwk}, t, to the target node. If $t < t'$ P_1 will ignore the key K'_{pwk} and use K_{pwk} for encryption with the target peer following suit;

- The 2 steps in the handshake combined with a round trip timer are adequate to guarantee that the sender of the K_{pwk} will know that the other peer has received the $\{K_{pwk}\}_{K_{nwk}}$ (the notation $\{A\}_K$ means that A has been encrypted with the cryptographic key K), when it receives the acknowledgement in the second step of the handshake. If the sender of the K_{pwk} does not receive the aforesaid acknowledgement within the certain RTT (round trip time), it resends the key packet to the target peer assuming the original packet was dropped;

- The purpose of the key refresh is to harden the ability of a compromised peer to reveal any pairwise key material and information from any encrypted signalling packets. This is based on the fact that a compromised peer would need to overhear the key exchange of the first pairwise key which is encrypted with the K_{nwk} in addition to the subsequent keys thereafter making it extremely hard for an attacker even with the K_{nwk} to decrypt refreshed K_{pwk} messages;

- To satisfy confidentiality for the different DHT signalling packets, as previously presented, we use one of the K_{nwk}, K_{pwk} depending on the type of the ROBUST packet.

In Table 4.1, we summarise the different DHT signalling packets as well as the required keys per packet type regarding the different phases of the proposed security extensions. Authentication and integrity are both satisfied by ROBUST using *Hash-based Message Authentication Code* (HMAC). To this end, a hash function is applied to the ciphertext of the message using the proper symmetric key, depending on the DHT signalling packet type. The receiver of the signalling checks the message digest to verify the authenticity of the sender and to identify whether the message was altered compared to the one sent by the originator due to intermediate MANET nodes routing the packet.

An assumption of this work is that the beacon packet used to advertise super peers' existence in order to estimate proximity to said super peer by a normal DHT peer must always be encrypted by the K_{nwk} due to its broadcast nature. Regarding the *proximity synchronisation* phase we assume that peers joining a cluster communicate the new pairwise

symmetric key for future transactions with their new super peer, as well as their new leafset peers. This is accomplished by using the K_{nwk}, as the overhead required to use existing secure channels[3] is deemed to outweigh the risks.

4.3 Simulation results

In this section, we use simulations to verify the integrity of the proposed model and showcase the benefits of using our proposed solution. We next use an event based simulator, customised with our implementation of ROBUST protocol, to validate the proposed model and optimisation solution. We have developed a simulator module for the packet-level network simulator ns-2. The simulator incorporates all DHT packets and functions needed for a fully implemented DHT and the implementation is based on the ROBUST DHT clustered architecture with dynamic mobility considerations. In addition, the different phases of the security extensions are implemented fully in ns-2 and are utilised in order to route ROBUST packets. Further lower layers are also simulated in the ns-2 simulator and these characteristics are taken into account. The medium access control (MAC) layer protocol implements the IEEE 802.11b *distributed coordination function* (DCF) with a four-way handshaking mechanism [94].

4.3.1 Network setup

The setup of our network comprises of randomly distributed peers throughout an area of $1km^2$. For smaller networks such as ten peers, the peers are considerably closer together in order to stay within transmission range of one another. *Puts*[4] and *Gets*[5] (data transmission and retrieval) are called in the DHT at a rate of one request per second. The number of peers simulated ranges from ten peers to seventy peers with increments of twenty peers.

We specifically chose this amount of peers to represent smaller networks and also

[3]Going through their previous super peer SP for which both the joining peer and the SP' have established pairwise symmetric keys.

[4]Refers to DHT_{put_req}.

[5]Refers to DHT_{get_req}

investigate the scalability of the aforementioned approaches. During tests we found the threshold 90ms to be sufficient to allow peers to change cluster when *SN* RTT is less than $SN'RTT + 90ms$. The threshold is needed so that peers do not move cluster when even a small delay increase is experienced. In addition to the threshold we have also implemented the algorithm to always take the best RTT for the current super peer *SN* and the worst RTT for the new super peer *SN'* over three subsequent RTTs. This ensures that we can guarantee the super peer *SN'* to have a better *Round Trip Time* (RTT) than *SN* for a total duration of $3t_{beacon}$. All simulations were run for a total of 1000 seconds simulation time. This was chosen in order for the DHT and network to stabilise.

In the simulation experimentations regarding the ROBUST DHT we assume static super peers. One of the limitations of our simulations are the fact churn[6] is not simulated per-se. This is due to the fact we have decided to only simulate mobility churn as adding churn would detract from the goal of investigating these results. We consider two main different scenarios in our simulations; one without security extensions (pure ROBUST) and one with security additions for signalling (secure ROBUST). The values for the intervals of the different DHT functions are based on those used in OpenDHT [95]. The list of simulation parameters can be seen in Table 4.2.

The process of packet initialisation to its definitive end is described below:

- Packets are originated from the ROBUST protocol itself and then passed to the ROBUST sent agent which maintains connections and keeps track of packets RTTs using pings;
- Subsequently when a RTT expires after a packet is sent the packet is resent since it is assumed that it has been dropped;
- The sent agent also keeps track of the packet sequence numbers so then the packet sent down the stack to the routing protocol (we have chosen OLSR [17]);

[6]Node arrival and failure.

Table 4.1: List of required signalling robust packets and associated cryptographic keys.

ROBUST signalling packet	**before key exchange phase**	**after key exchange/ before or during refresh phase**	**proximity synchronisation phase**
DHT_{get_req}	K_{nwk}	K_{pwk}	-
DHT_{put_req}	K_{nwk}	K_{pwk}	-
DHT_{ping}	K_{nwk}	K_{pwk}	-
DHT_{beacon}	K_{nwk}	K_{nwk}	-
DHT_{join_req}	K_{nwk}	K_{nwk}	-
DHT_{ack}	K_{nwk}	K_{pwk}	K_{pwk}
DHT_{sync_vals}	K_{nwk}	K_{pwk}	K_{pwk}
DHT_{str_keys}	K_{nwk}	K_{pwk}	K_{pwk}
DHT_{pull_ls}	K_{nwk}	K_{pwk}	K_{pwk}
DHT_{push_ls}	K_{nwk}	K_{pwk}	K_{pwk}
DHT_{move_req}	-	-	K_{pwk}
DHT_{move_rep}	-	-	K_{pwk}
DHT_{part}	-	-	K_{pwk}
DHT_{broad_part}	-	-	K_{pwk}
DHT_{key_exch}	K_{nwk}	-	K_{nwk}
DHT_{key_refr}	K_{nwk}	K_{pwk}	-

- The latter then computes the best route to send the packet and forwards the packet over the intermediate peers of the MANET until it reaches the destination;
- The destination node pushes the packet up the stack thus it is then received by the ROBUST agent which sends an acknowledgement packet back to the source node and computes any information/ data stored in the packet.

Table 4.2: Simulation parameters.

Network size (number of peers)	10, 30, 50, 70
Number of clusters needed (C)	4, 7, 9, 12
Percentage of mobile peers	0%, 25%, 50%
Area size	1000m x 1000m
Data packet payload size	512 bytes
MANET Routing protocol	OLSR
MAC layer	802.11*b*
Link bandwidth	11Mbit/s
Maximum transmission range	250m
Node moving speed	1m/sec
Types of traffic	UDP (All aforementioned DHT and security packets)
Simulation time	1000 sec
DHT data distribution	Random
DHT node ID distribution	Random

4.3.2 End-to-end DHT request delay

The graph in Fig. 4.5 shows the cumulative distribution function of end-to-end DHT_{get_req} request delay for 10-70 peers in a state with and without security when the network has no mobility (all peers are static). One can see from this figure that when there is no mobility, the delay experienced when getting data from the DHT is minimal as for 90% of all cases the end-to-end delay is less than 100ms. We can see that in almost all cases the security and non-security scenarios experience roughly the same delay (within a 5ms variance) except

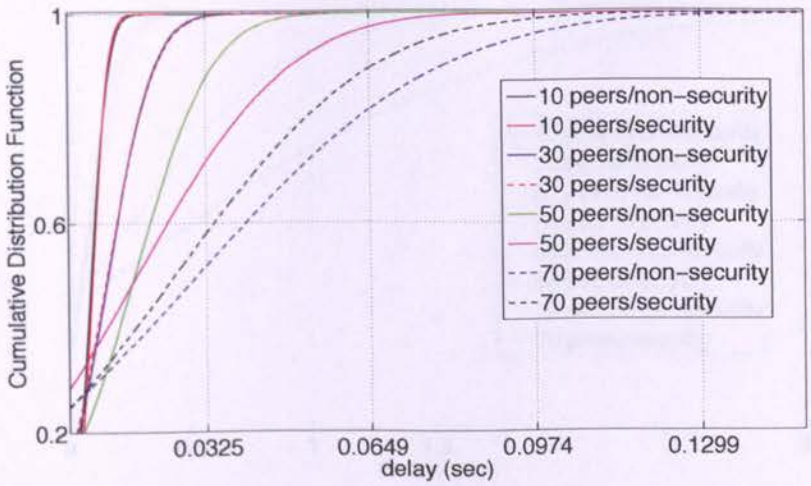


Figure 4.5: The cumulative distribution function of the DHT_{get_req} from transmission to completion of the request for the 8 scenarios where none of the peers are mobile.

for 70 peers where the variance is extended to less than 20ms. The higher experienced delay here for 70 peers without security can be attributed to a slight variation of the distribution of peer and data IDs in the DHT, for example the data IDs are distributed more evenly in the non-security scenario creating more DHT_{sync} packets and higher redundancy, at the cost of slightly higher delay.

Fig. 4.6 demonstrates the cumulative distribution function of end-to-end DHT_{get_req} request delay for 10-70 peers in a state with and without security when the network has 25% mobility (25% of the peers are moving at 1m/sec). As one would expect the delay in smaller networks (10-30 peers) is very small with 80% of the RTTs being less than 70ms due to no congestion, interference and the fact that peers hardly move out of a one-hop range. When the network size is increased to 50 peers where 13 peers are moving, we see slightly higher delay due to broken links causing packet retransmission and more packets being sent over the network increasing congestion (primarily DHT_{prox_sync} packets when a node moves cluster).

We see this evidently more for 70 peers (18 moving) where the delay increases greatly. The

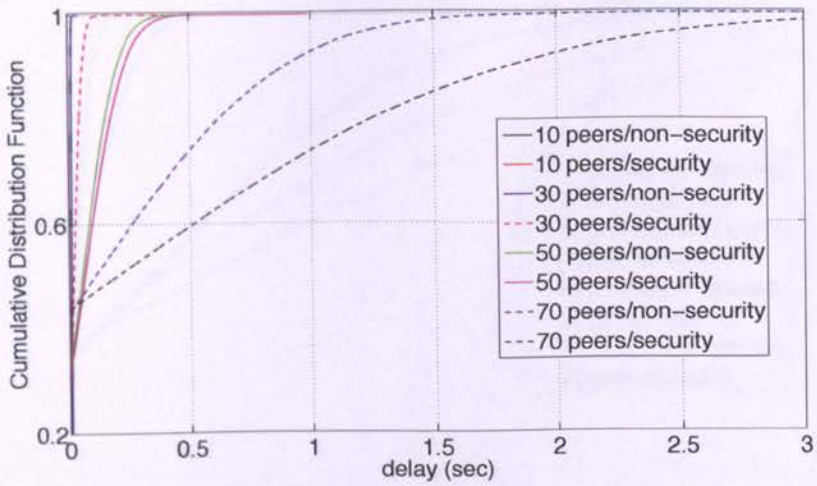


Figure 4.6: The cumulative distribution function of the DHT_{get_req} from transmission to completion of the request for the 8 scenarios with 25% of the peers mobile.

results here show a clear indication that adding the security packets increases delay due to the time the peer has to wait to establish keys before transmitting data, however for 30 and 50 peers this is less than 50ms, whereas for 70 peers this is increased to less than 600ms. The great difference here is due to a much higher rate of peers moving cluster causing higher delays due to packet loss and interference as confirmed in the paper [96]. Packet loss can cause very high delay times in get request RTT such as those experienced here due to the dropped packet timer implemented in ROBUST. Based on the OpenDHT implementation [95] when a packet is sent and a round trip timer is started with an expiry time of the RTT of the last successfully transmitted packet to the specific target peer, if the timer expires the packet is retransmitted and the expiry time is doubled. Due to this the RTT can increase exponentially when experiencing particularly high packet loss.

The graph Fig. 4.7 presents the results of the cumulative distribution function for end-to-end DHT_{get_req} request delay for 10-70 peers in a state with and without security when the network has 50% mobility (50% of the peers are moving at 1m/sec). In keeping with the results for 25% mobility we can see that the smaller network sizes (10-30) experience

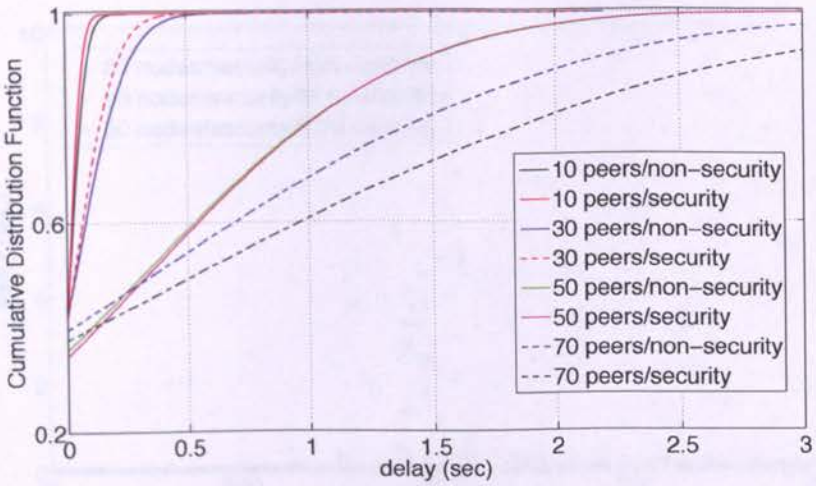


Figure 4.7: The cumulative distribution function of the DHT_{get_req} from transmission to completion of the request for the 8 scenarios with 50% of the peers mobile.

less than 210ms delay for 80% of the requests, while this is significantly higher than the previous results, it is not unexpected due to the increasing volatility of the network. In this scenario the network with 50 peers has a sharp increase in the end-to-end delay compared with Fig. 4.6 due to the aforementioned factors, mainly resultant of peers moving more frequently. One can see again the overhead of security only marginally affecting the delay with a maximum difference with 70 peers of 300ms.

One can see a sample of end-to-end delay for DHT_{get_req} request delay for 50 peers with security extensions enabled in Fig. 4.8. Following the trend of the previous graphs we can clearly see that the delay for 50% of the mobile peers is much more varied than the other two scenarios. It is interesting to note that during the stabilisation period of 200 seconds we do not see high delay for any of the scenarios. However when the peers become mobile around 200 seconds the delay for a small percentage of the DHT_{get_req} requests increases rapidly.

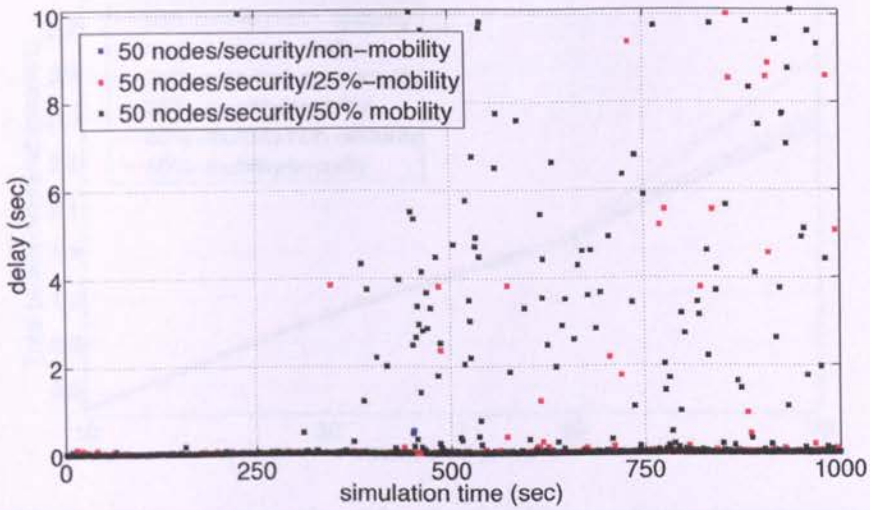


Figure 4.8: The end-to-end DHT_{get_req} delay for 50 peers for the scenarios with 0%, 25% and 50% of the peers mobile with security extensions enabled.

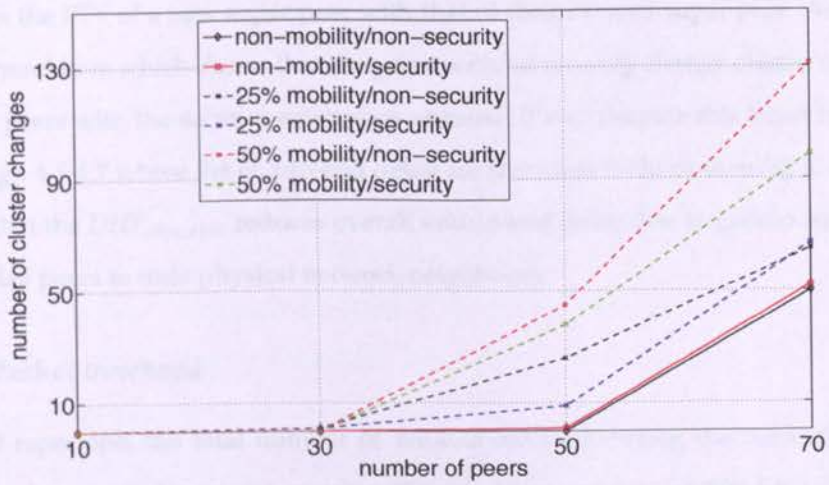


Figure 4.9: The number of peers who change cluster due to the DHT_{prox_sync} function for the number of peers 10-70 for all the above mentioned scenarios.

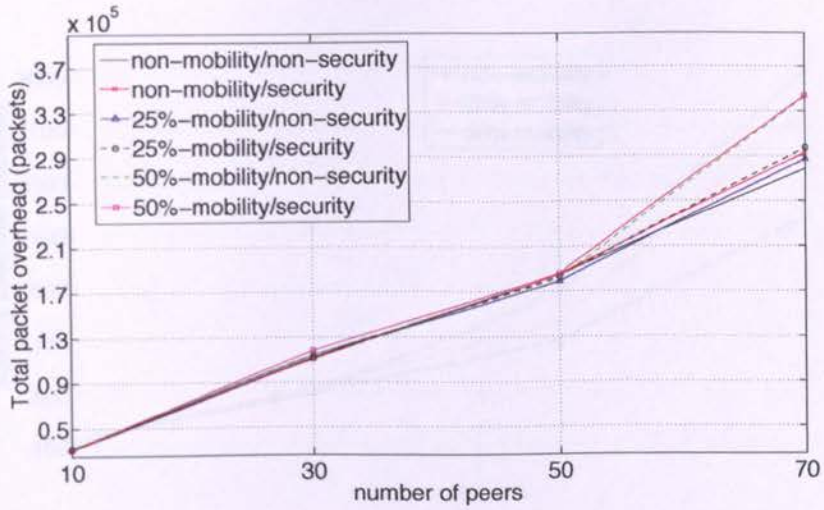


Figure 4.10: The total packet overhead for the 6 mobility and security scenarios for each number of peers.

4.3.3 Cluster roaming

Fig. 4.9 displays the number of peers who change cluster due the DHT_{prox_sync} which compares the RTT of a new super peer with that of their current super peer. We can see a general trend here which shows that the peers without security change cluster more times than the peers with the security extensions enabled. If we compare this trend to what we see in Figs. 4.5-4.7 where the end-to-end delay for scenarios without security is lower, one can see that the DHT_{prox_sync} reduces overall end-to-end delay due to greater proximity of the overlay peers to their physical network neighbours.

4.3.4 Packet overhead

Fig. 4.10 represents the total number of packets received during the networks lifetime during each scenario for a given number of peers. Here one can see that for each scenario the security extensions add a noticeable number of packets in the results, but still not enough to add any real difference in terms of congestion. It is interesting to note that for scenarios 10-50 peers the results are hardly distinguishable from each other. This shows

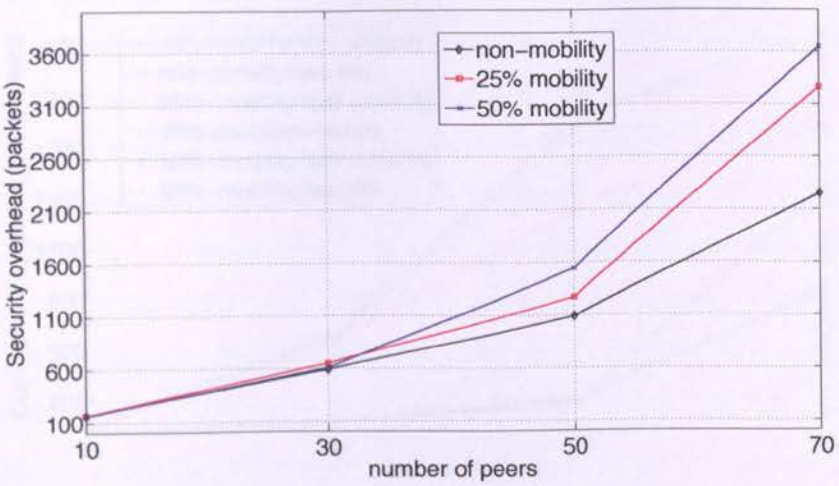


Figure 4.11: The packet overhead experienced due to security extensions for ROBUST for each of the different mobility levels and for all the number of peers.

that the threshold for DHT_{prox_sync} impacts more in the 70 peer network than all of the others due to higher RTT delay variance.

Confirming the notion in Fig. 4.10, in Fig. 4.11 one can determine the actual real number of total security packets received during the networks lifetime to be negligible, with the maximum number of security packets received at 70 peers with 50% mobility as expected due to DHT_{prox_sync}. One can say with clarity that adding 3600 packets to a total over 3×10^5 would not produce any noticeable difference in network behaviour. On the contrary any resulting impact from the security would have to be delay wise, while waiting for a packet to arrive due to the congestion caused by the total number of packets. This is more noticeable with the security extensions as one has to wait for this procedure to complete before transmitting secure data. The results in Fig. 4.11 do not include duplicate packets sent, which might result in more overall packets being sent from the security function.

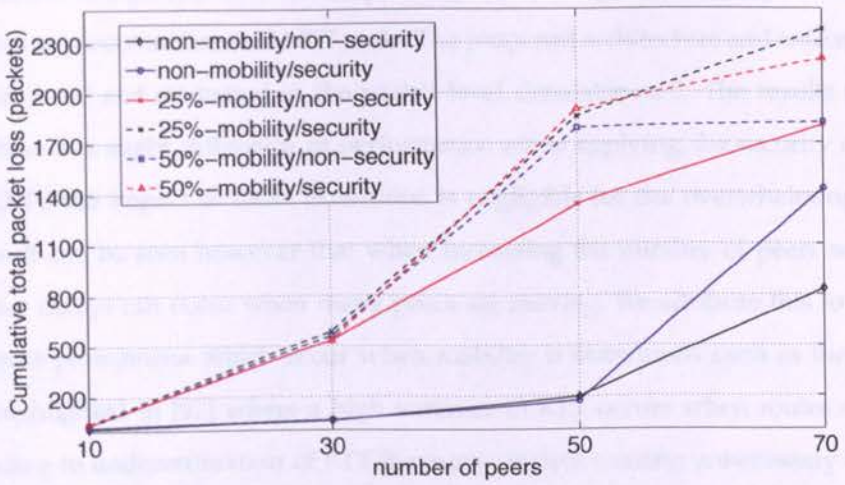


Figure 4.12: The cumulative packet loss experienced for each of the 6 mobility scenarios.

4.3.5 Packet loss

The results in Fig. 4.12 provide insight into the cumulative packet loss experienced during the networks lifetime for any given number of peers simulated for each mobility scenario with and without security. One can gather that while there is packet loss, it is not experienced on a large scale. While the general trend shows that the security scenarios have a slightly higher packet loss, when compared with the total number of packets received this amounts to less than 1 percent. This happens due to frequent route change multiple copies of a single packet can be received, this causes a lot of duplicate packets in the network and a phenomenon we experienced with a high impact when simulating 70 peers with high mobility due to congestion.

4.4 Summary

In this chapter we have extended the *Reliable Overlay Based Utilisation of Services and Topology* (ROBUST) *peer-to-peer* (P2P) overlay to encompass security extensions that provide *confidentiality* and *integrity* in order for all distributed hash table (DHT) transactions to be

authenticated and private between only those participating in the overlay and appear encrypted to any intermediate MANET node. The proposed architecture and extensions have been simulated and evaluated in the packet-level simulator ns-2. The results show that while there is a slight difference in performance when applying the security extensions to the DHT, the impact of these extensions is negligible for the overwhelming majority of cases. It can be seen however that when increasing the number of peers so much as 70, higher delays can occur when many peers are moving. We attribute this to a number of different phenomena which occur when mobility is introduced such as the transport issues highlighted in [97] where a high variance in RTT occurs when routes change often, leading to underestimation of RTT for many packets causing unnecessary duplicates to be sent, further congesting the network and increasing delay.

Chapter 5

Game Theoretic Defence Strategies to Improve Availability in MANETs

"If we knew what it was we were doing, it would not be called research, would it ?", Albert Einstein

This chapter examines how to increase MANET availability in presence of intrusion detection systems, by proposing optimal defence MANET strategies. To achieve such a goal, we first propose the *Game Theoretic MANET Routing* (GTMR) protocol which has been designed based on a non-cooperative game theoretic model. GTMR maximises the utility of the MANET at the Nash Equilibrium ($\mathcal{NE}$). Thorough performance evaluation results have been retrieved by developing GTMR in ns-2. We have compared this protocol with AODV, OLSR, AOMDV, by evaluating the average node lifetime, total routing overhead, average end-to-end packet delay and average intrusion detection energy cost per node. Such results also show that GTMR introduces affordable overhead therefore it can efficiently support QoS multimedia communications. Apart from this routing mechanism, this chapter proposes a non-cooperative game theoretic model to derive the optimal intrusion detection effort (monitoring probability) that must be spent by each MANET node in order to achieve the best balance between intrusion detection cost, for defending the MANET nodes, and detection accuracy therefore proposing an optimal defence MANET strategy.

5.1 Gaming security formalism

Any MANET, that employs IDS techniques, has to guarantee availability of the network resources by keeping the MANET nodes alive and the intrusion detectors in use as long as possible. In this way, the whole security across the MANET is increased. In Section 5.2, we propose a novel routing protocol called *Game Theoretic MANET Routing* (GTMR) to address the above security challenges by minimising the energy spent for intrusion detection on each MANET route. Our work has been based on the non-cooperative, non-zero sum game (Model I) proposed in Section 5.1.1.

In Section 5.1.2 we propose an optimal defence strategy for MANETs by deriving the intrusion detection MANET effort with respect to the energy costs incurred. Such effort is represented as a defending probability distribution which maximises the utility of the MANET at the Nash Equilibrium ($\mathcal{NE}$) of a non-cooperative security game between the MANET and a malicious coalition. Our work has been based on the non-cooperative, non-zero sum game (Model II) proposed in this section.

5.1.1 Model I

In this section, we present the first game theoretic model, called Model I, which formulates a non-cooperative game between a MANET and a malicious coalition. The MANET defends either a route that is used to transmit data from a source to a destination or any other route, depending on the chosen strategy. On the other hand, the malicious coalition (MC) defends either the route which is used to send data or another route. Both MANET and MC might choose to abstain from the spending energy by defending or attacking, correspondingly.

5.1.1.1 Game information

As usually required in game theoretic applications similar to ours, such as [98], in the following we introduce the game information. We assume a non-cooperative game $G_{GTMR} = (S, U)$ as follows:

- **Players**: This game has two players namely; MANET and MC.
- **Strategy space**: $S = \{S_{manet}, S_{mc}\}$ where:
  - $S_{manet} = \{d_{r_i}, d_0, d_{r_{-i}}\}$ is the MANET's strategy space where the strategies are the following:
    - d_{r_i}: MANET defends a route i;
    - d_0: MANET does not defend;
    - $d_{r_{-i}}$: MANET defends any route other than i.
  - $S_{mc} = \{a_{r_i}, a_0, a_{r_{-i}}\}$ is the malicious' coalition strategy space where the strategies are the following:
    - a_{r_i}: MC attacks a route i;
    - a_0: MC does not attack;
    - $a_{r_{-i}}$: MC attacks any route other than i.
- **Cost**: The following are the costs incurred for the players of the game:
  - MANET:
    - $cost_{loss,r_i}$: is the damage incurred due to the loss of data or routing signalling on a route i mainly due to a successful attack.
    - $cost_{d,r_i}$: represents the average cost per node of defending a route i against malicious parties.
  - Malicious coalition:
    - $cost_{a,r_i}$: represents the energy cost of attacking r_i.
- **Gain**: We assume that each route possesses an amount of security asset denoted as V. This represents the gain obtained by protecting the MANET route which equals the loss of security when an attack is successful. Without loss of generality, we assume that all routes have equivalent security assets.

- **Utility**: We define the MANET's utility space as U_{manet} and the malicious coalition's as U_{mc}, where the strategy pairs are the following

$$\{(d_{r_i}, a_{r_i}), (d_{r_i}, a_0), (d_{r_i}, a_{r_{-i}}), (d_0, a_{r_i}), (d_0, a_0), (d_0, a_{r_{-i}}), (d_{r_{-i}}, a_{r_i}), (d_{r_{-i}}, a_0), (d_{r_{-i}}, a_{r_{-i}})\}.$$

then

$$U_{manet} = \begin{pmatrix} u_{manet}(d_{r_i}, a_{r_i}) & u_{manet}(d_{r_i}, a_0) & u_{manet}(d_{r_i}, a_{r_{-i}}) \\ u_{manet}(d_0, a_{r_i}) & u_{manet}(d_0, a_0) & u_{manet}(d_0, a_{r_{-i}}) \\ u_{manet}(d_{r_{-i}}, a_{r_i}) & u_{manet}(d_{r_{-i}}, a_0) & u_{manet}(d_{r_{-i}}, a_{r_{-i}}) \end{pmatrix}$$

and

$$U_{mc} = \begin{pmatrix} u_{mc}(d_{r_i}, a_{r_i}) & u_{mc}(d_{r_i}, a_0) & u_{mc}(d_{r_i}, a_{r_{-i}}) \\ u_{mc}(d_0, a_{r_i}) & u_{mc}(d_0, a_0) & u_{mc}(d_0, a_{r_{-i}}) \\ u_{mc}(d_{r_{-i}}, a_{r_i}) & u_{mc}(d_{r_{-i}}, a_0) & u_{mc}(d_{r_{-i}}, a_{r_{-i}}) \end{pmatrix}$$

5.1.1.2 Utility values

In the following we define the different utility values for all the aforesaid strategy tuples. We have assumed that the MANET's intrusion detection rate equals r_d and the mis-detection rate equals r_m. Therefore we have:

- For (d_{r_i}, a_{r_i}):
  - $u_{manet}(d_{r_i}, a_{r_i}) = r_d V - r_m cost_{loss,r_i} - cost_{d,r_i}$. When MANET defends r_i it gains a proportion of the security asset V of the route defined by the intrusion detection rate ($r_d V$). Also, it loses (i) $cost_{loss,r_i}$ for failing to defend the route with mis-detection rate r_m and (ii) $cost_{d,r_i}$ for spending energy to defend this route.
  - $u_{mc}(d_{r_i}, a_{r_i}) = r_m V - cost_{a,r_i}$. When MC attacks a route i, it gains a profit of $r_m V$ when MANET erroneously mis-detects an attack. Conversely, MC loses $cost_{a,r_i}$ due to the energy spent for attacking route i.
- For (d_{r_i}, a_0):

* $u_{manet}(d_{r_i}, a_0) = V - cost_{d,r_i}$. When MANET defends r_i and MC does not attack, MANET gains the security asset V of the route and it loses $cost_{d,r_i}$ which represents the energy spent defending this route.
* $u_{mc}(d_{r_i}, a_0) = 0$. When MC does not attack, it does not gain any profit.

- For $(d_{r_i}, a_{r_{-i}})$:
  * $u_{manet}(d_{r_i}, a_{r_{-i}}) = V - cost_{d,r_i}$. When MANET defends r_i and MC defends any other route, MANET gains the whole security asset V of the route and it loses $cost_{d,r_i}$ which represents the energy spent defending this route.
  * $u_{mc}(d_{r_i}, a_{r_{-i}}) = -cost_{a,r_{-i}}$. When MC attacks a route r_{-i} that MANET does not defend (this is a route that MANET does not use to transmit data) then there is not any gain for the attacker. The cost for such an attack equals $-cost_{a,r_{-i}}$.
- For (d_0, a_{r_i}):
  * $u_{manet}(d_0, a_{r_i}) = -V$. When MANET does not defend the route i which is being attacked by MC, then MANET loses the security asset V of this route.
  * $u_{mc}(d_0, a_{r_i}) = V - cost_{a,r_i}$. In the same case the MANET's loss is the MC's profit. Also, MC spends $-cost_{a,r_i}$ for attacking this route.
- For (d_0, a_0):
  * $u_{manet}(d_0, a_0) = V$. Since both MANET and MC have no activity, MANET gains the security asset of route i.
  * $u_{mc}(d_0, a_0) = 0$. In this case, MC does not have any profit.
- For $(d_0, a_{r_{-i}})$:
  * $u_{manet}(d_0, a_{r_{-i}}) = V$. Here, although MANET does not defend r_i, MC attacks a different route thereby MANET gains the whole security asset of route i.
  * $u_{mc}(d_0, a_{r_{-i}}) = -cost_{a,r_{-i}}$. MC loses $-cost_{a,r_{-i}}$ to attack the route r_{-i}.
- For $(d_{r_{-i}}, a_{r_i})$:
  * $u_{manet}(d_{r_{-i}}, a_{r_i}) = -V - cost_{d,r_{-i}}$. If MANET defends a route r_{-i} while MC

attacks r_i, then MANET loses the security asset V of route i as well as the energy spent defending the route r_{-i} which is represented by $cost_{d,r_{-i}}$.

* $u_{mc}(d_{r_{-i}}, a_{r_i}) = V - cost_{a,r_i}$. In this case, MC gains as profit the security asset of route i while it loses $cost_{a,r_i}$ to attack.

- For $(d_{r_{-i}}, a_0)$:

  * $u_{manet}(d_{r_{-i}}, a_0) = V - cost_{d,r_{-i}}$. In this case, the MANET gains the security asset of route i due to MC does not attack but it loses $cost_{d,r_{-i}}$ to defend another route.

  * $u_{mc}(d_{r_{-i}}, a_0) = 0$.

- For $(d_{r_{-i}}, a_{r_{-i}})$:

  * $u_{manet}(d_{r_{-i}}, a_{r_{-i}}) = V - cost_{d,r_{-i}}$. In this case, the MANET gains the whole security asset of the route i since MC attacks another route. MANET's loss equals $cost_{d,r_{-i}}$ due to defending a route different than r_i.

  * $u_{mc}(d_{r_{-i}}, a_{r_{-i}}) = -cost_{a,r_{-i}}$. MC does not gain any profit because it does not attack r_i, which is the route used by MANET to transmit data, however it loses some energy represented by $cost_{a,r_{-i}}$, to defend a route else than r_i.

The MANET and malicious coalition's payoff matrices are illustrated in Tables 5.1 and 5.2, correspondingly.

Table 5.1: MANET payoff matrix.

s.t.	$\mathbf{a_{r_i}}$	$\mathbf{a_0}$	$\mathbf{a_{r_{-i}}}$
$\mathbf{d_{r_i}}$	$r_d V - r_m cost_{loss,r_i} - cost_{d,r_i}$	$V - cost_{d,r_i}$	$V - cost_{d,r_i}$
$\mathbf{d_0}$	$-V$	V	V
$\mathbf{d_{r_{-i}}}$	$-V - cost_{d,r_{-i}}$	$V - cost_{d,r_{-i}}$	$V - cost_{d,r_{-i}}$

Table 5.2: Malicious coalition payoff matrix.

$s.t$	$\mathbf{a}_{r_i}$	$\mathbf{a}_0$	$\mathbf{a}_{r_{-i}}$
$\mathbf{d}_{r_i}$	$r_m V - cost_{a,r_i}$	0	$-cost_{a,r_{-i}}$
$\mathbf{d}_0$	$V - cost_{a,r_i}$	0	$-cost_{a,r_{-i}}$
$\mathbf{d}_{r_{-i}}$	$V - cost_{a,r_i}$	0	$-cost_{a,r_{-i}}$

5.1.1.3 Nash Equilibrium

Existence

We must first verify the existence of at least one $N\mathcal{E}$ in the G_{GTMR} security game. From the previous section we can say that this game:

- has a finite strategic form as illustrated in Tables 5.1 and 5.2,
- has finite number of players (MANET, malicious coalition) and,
- has a finite number of pure strategies for each player,

then it satisfies the requirements of Theorem 2.8.1 thereby having at least one $N\mathcal{E}$.

Derivation of Nash Equilibrium

In game theory a zero-sum game highlights a situation in which a player's gain or loss is exactly balanced by the losses or gains of the other players. G_{GTMR} is a non-zero sum game because from the payoff matrices 5.1 and 5.2 we observe that even if the malicious coalition does not attack, the MANET is defending. Therefore, the payoff of the MANET decreases while the payoff of the malicious coalition is steady. The above assumption contradicts with the zero-sum assumption which means that G_{GTMR} is a non-zero sum game.

In order to find the $N\mathcal{E}$ in a non-zero sum game we have to consider the concept of the *dominant strategy*. A strategy is called dominant when it is better than any other strategy for one player, no matter how that player's opponents could play. In terms of mathematics:

For any player i, a strategy $s^* \in S_i$ dominates another strategy $s' \in S_i$ if $\forall\, s_{-i} \in S_i$, $u_i(s^*, s_{-i}) \geq u_i(s', s_{-i})$.

Table 5.3: Payoff matrix of the G_{GTMR}.

s.t.	$\mathbf{a}_{r_i}$	$\mathbf{a}_0$	$\mathbf{a}_{r_{-i}}$
$\mathbf{d}_{r_i}$	$\underline{r_d V - r_m cost_{loss,r_i} - cost_{d,r_i}}$, $\underline{r_m V - cost_{a,r_i}}$	$V - cost_{d,r_i}$, 0	$V - cost_{d,r_i}$, $-cost_{a,r_{-i}}$
$\mathbf{d}_0$	$-V$, $\underline{V - cost_{a,r_i}}$	$\underline{V}$, 0	$\underline{V}$, $-cost_{a,r_{-i}}$
$\mathbf{d}_{r_{-i}}$	$-V - cost_{d,r_{-i}}$, $\underline{V - cost_{a,r_i}}$	$V - cost_{d,r_{-i}}$, 0	$V - cost_{d,r_{-i}}$, $-cost_{a,r_{-i}}$

In the following we find the dominant strategy of the G_{GTMR}.

- For the MANET:
  - When the malicious coalition plays a_{r_i}, d_{r_i} is the best MANET response due to $u_{manet}(d_{r_i}, a_{r_i}) > \max(u_{manet}(d_0, a_{r_i}), u_{manet}(d_{r_{-i}}, a_{r_i}))$ and this is interpreted as follows. When MC attacks the route i the MANET's best response is to defend such a route.
  - When the malicious coalition plays a_0, d_0 is the best MANET response due to $u_{manet}(d_0, a_0) > \max(u_{manet}(d_{r_i}, a_0), u_{manet}(d_{r_{-i}}, a_0))$. In other words, when MC does not attack the best MANET response is not to spend energy for defending.
  - When the malicious coalition plays $a_{r_{-i}}$, d_0 is the best MANET response due to $u_{manet}(d_0, a_{r_{-i}}) > \max(u_{manet}(d_{r_i}, a_{r_{-i}}), u_{manet}(d_{r_{-i}}, a_{r_{-i}}))$. This shows that when MC does not attack the route r_i which is used by MANET to propagate data from a source to a destination then the MANET does not gain any profit by defending. Thereby is more profitable for the MANET to play d_0.

From the above, we see that there is not a dominant strategy for the MANET.

- For the malicious coalition:
  - When MANET plays d_{r_i}, $u_{mc}(d_{r_i}, a_{r_i})$ is the best response due to $u_{mc}(d_{r_i}, a_{r_i}) > \max(u_{mc}(d_{r_i}, a_0), u_{mc}(d_{r_i}, a_{r_{-i}}))$. The best response for MC, when MANET defends the route i is to attack such route so at least it gains $r_m V$ when the intrusion detection of the MANET do not detect any attack.
  - When MANET plays d_0, $u_{mc}(d_0, a_{r_i})$ is the best response due to $u_{mc}(d_0, a_{r_i}) > \max(u_{mc}(d_0, a_0), u_{mc}(d_0, a_{r_{-i}}))$. Namely, when the MANET does not defend, MC prefers to attack the route i to gain the entire security asset V of this route.
  - When MANET plays $d_{r_{-i}}$, $u_{mc}(d_{r_{-i}}, a_{r_i})$ is the best response due to $u_{mc}(d_{r_{-i}}, a_{r_i}) > \max(u_{mc}(d_{r_{-i}}, a_0), u_{mc}(d_{r_{-i}}, a_{r_{-i}}))$.

Thus, *the dominant strategy for the attacker is to attack the route i.* in that case, the best response for the MANET is to defend the route i. Therefore, the strategy pair (d_{r_i}, a_{r_i}) is the $\mathcal{NE}$ of G_{GTMR}. Table 5.3 represents the game's payoff matrix. This equilibrium indicates the stable status of the game and it will be used in Section 5.2 of this thesis to design our novel game theoretic routing protocol. In Table 5.4 we have summarised the notations that have been used in this section.

5.1.2 Model II

We use game theory to model non-cooperative security games between a MANET, which is defended by IDSs operating at each node as well as a group of collaborative malicious nodes called *malicious coalition* (MC).

5.1.2.1 Game information

In the following we assume a non-cooperative game $G_{SG} = (S, U)$ and we discuss the game information as usually required when we examine problems similar to ours.

- **Players**: This game has two players namely; MANET and MC

Table 5.4: Notations of Model I.

G_{GTMR}	GTMR game
S	set of strategies of both MANET and MC
S_{manet}	set of MANET strategies
S_{mc}	set of MC strategies
r_i	a MANET route i
d_{r_i}	MANET defends a route i
d_0	MANET does not defend
$d_{r_{-i}}$	MANET defends any route other than i
a_{r_i}	attackers' coalition attacks a route i
a_0	MC does not attack
$a_{r_{-i}}$	MC attacks any route other than i
$cost_{loss,r_i}$	the damage incurred on a route i due to a successful attack
$cost_{d,r_i}$	average energy per node for defending r_i
$cost_{d,r_{-i}}$	average energy per node for defending any route other than i
$cost_{a,r_i}$	energy cost of attacking r_i
$cost_{a,r_i}$	energy cost of attacking any route other than i
V	security asset of a MANET route
U_{manet}	MANET's utility
U_{mc}	MC's utility
$u_{manet}(d_{r_i}, a_{r_i})$	MANET's utility when MANET plays d_{r_i} and MC plays a_{r_i}
$u_{mc}(d_{r_i}, a_{r_i})$	MC's utility when MANET plays d_{r_i} and MC plays a_{r_i}
r_d	attack detection rate
r_m	misdetection rate
r_f	false alarm detection rate

- **Strategy space**: $S = \{S_{manet}, S_{mc}\}$ where:
  - $S_{manet} = \{d, nd\}$ is the MANET's strategy space where the strategies are the following:
    - d: MANET is defending;
    - nd: MANET does not defend.
  - $S_{mc} = \{a, na\}$ is the MC's strategy space where the strategies are the following:
    - a: MC is attacking the MANET;
    - na: MC does not attack.
- **Cost**: The following are the costs incurred for the players of the game:
  - MANET:
    - $cost_d$: represents the energy cost of intrusion detection when MANET defends;

* $cost_f$: represents the energy cost of a false alarm, for instance energy spent reacting due to a falsely detected attack.

- MC:

* $cost_a$: represents the energy cost of attacking the MANET.

- **Gain**: We assume that each node possesses an amount of security asset. $0 < V_{n_i} \leq 1$ indicates the loss of security when an attack against a node $n_i \in N$ is successful, where N is the set of MANET nodes. For simplicity reasons we assume that $V_{n_i} = V_{n_j} = V, \forall i, j \in N$. This represents the gain obtained by protecting this MANET node which equals the loss of security when an attack is successful. Without loss of generality, we assume that all nodes have equivalent security assets. It is worth mentioning that since the attacker aims at gaining some utility he expects that $cost_a < V$ otherwise he is not motivated to attack the MANET.

- **Utility**: We define the MANET's utility space as U_{manet} and the MC's as U_{mc}, thereby the utility space equals $U_{SG} = \{U_{manet}, U_{mc}\}$, where the strategy pairs are the following

$$\{(d, a), (d, na), (nd, a), (nd, na)\}.$$

then

$$U_{manet} = \begin{pmatrix} u_{manet}(d,a) & u_{manet}(d,na) \\ u_{manet}(nd,a) & u_{manet}(nd,na) \end{pmatrix}$$

and

$$U_{mc} = \begin{pmatrix} u_{mc}(d,a) & u_{mc}(d,na) \\ u_{mc}(nd,a) & u_{mc}(nd,na) \end{pmatrix}.$$

5.1.2.2 Different cases

The goal of the MC is to attack the MANET without being detected whereas that of the MANET is to detect any malicious behaviour. Since there is no cooperation between the two players, the discussed game is characterised as a *non-cooperative* game. When an attack

is indeed in progress one of the following cases may occur:

- the MANET has not detected the attack due to IDSs' limitations. This might happen for instance in cases where the IDS software has not been updated with a known or a new attack or the IDS capabilities are limited;
- the MANET has not recognised the attack due to malfunction;
- the MANET has recognised the attack and triggers an alarm.

In all the above cases the mis-detection rate equals $(1 - r_d)$ where r_d is the attack detection rate. On the other hand, when there is no attack in progress the MANET might produce a false alarm due to malfunctioning or the attack detection mechanism has falsely concluded that an attack was in progress.

5.1.2.3 Utility values

In the following we define the different utility values for all the aforesaid strategy tuples. We have assumed that the MANET's intrusion detection rate equals r_d and r_f is the false alarm rate. Therefore we have:

- For (d, a):
  - $u_{manet}(d, a) = r_d V - r_f cost_f V - cost_d V$. In this case the MANET defends and it gains the proportion of the security asset of the node that it defends which is indicated by the detection rate value. At the same time, MANET loses some proportions of this asset due to false alarms occurred ($r_f cost_f$) and the cost (for instance in terms of energy consumption) for defending this node.
  - $u_{mc}(d, a) = (1 - r_d)V - cost_a V$. In this case the MANET defends a node thus MC receives gain equal to the proportion of the node's security asset that is indicated by the misdirection rate. On the other hand, MC loses some energy to launch an attack against such node.
- For (d, na):

- $u_{manet}(d, na) = V - r_f cost_f V - cost_d V$. The profit of the MANET is almost the same with the previous case apart from the fact that the entire value of the node asset is gained due to the absence of malicious activities.
- $u_{mc}(d, na) = 0$. Since MC does not attack its utility equals zero.

- For (nd, a):
  - $u_{manet}(d, a) = -V$. Since the MANET does not defend, it loses the entire node asset.
  - $u_{mc}(d, a) = V - cost_a V$. Since there is no MANET defence in place, MC gains the entire node security asset minus the energy that loses to attack such a node.

- For (nd, na):
  - $u_{manet}(d, a) = V$. As there is no attack against the MANET, the entire node security asset is preserved while there is not any loss since MANET abstains from defending.
  - $u_{mc}(d, a) = 0$. MC does not earn any profit by not attacking.

In Table 5.5 we show the utility functions of the MANET and the MC for the different strategy tuples;

Table 5.5: Security game's payoff matrix

strategy	a	na
d	$r_d V - r_f cost_f V - cost_d V$ $(1 - r_d)V - cost_a V$	$V - r_f cost_f V - cost_d V$, 0
nd	$-V$, $V - cost_a V$	V 0

We define $P_d = (p_{d,n_1}, p_{d,n_2}, \cdots, p_{d,n_n})$ as the probability distribution over N of MANET defending nodes $1, \cdots, n$ and $P_a = (p_{a,n_1}, p_{a,n_2}, \cdots, p_{a,n_n})$ as the probability distribution

over N of MC attacking nodes $1, \cdots, n$. These satisfy the following constraints

$$\sum_{n_i \in N} p_{d,n_i} \leq P_d, \sum_{n_i \in N} p_{a,n_i} \leq P_a. \tag{5.1}$$

Therefore, the utility values of the two players could be represented as follows:

$$\begin{aligned} U_{manet}(P_d, P_a) = & \sum_{n_i \in N} p_{d,n_i} p_{a,n_i} (r_d V - r_f cost_f V - cost_d V) \\ & + \sum_{n_i \in N} p_{d,n_i} (1 - p_{a,n_i})(V - r_f cost_f V - cost_d V) + \sum_{n_i \in N} (1 - p_{d,n_i}) p_{a,n_i} (-V) \\ & + \sum_{n_i \in N} (1 - p_{d,n_i})(1 - p_{a,n_i}) V = \cdots \\ & = \sum_{n_i \in N} [V[p_{d,n_i}[p_{a,n_i}(1 + r_d) - r_f cost_f - cost_d] - 2p_{a,n_i}] \end{aligned} \tag{5.2}$$

$$\begin{aligned} U_{mc}(P_d, P_a) = & \sum_{n_i \in N} p_{d,n_i} p_{a,n_i} ((1 - r_d)V - cost_a V) \\ & + \sum_{n_i \in N} p_{d,n_i} (1 - p_{a,n_i}) \cdot 0 + \sum_{n_i \in N} (1 - p_{d,n_i}) p_{a,n_i} (V - cost_a V) \\ & + \sum_{n_i \in N} (1 - p_{d,n_i})(1 - p_{a,n_i}) \cdot 0 = \cdots \\ & = \sum_{n_i \in N} V p_{a,n_i} (1 - cost_a - p_{d,n_i} r_d) \end{aligned} \tag{5.3}$$

5.1.2.4 Nash Equilibrium

Existence

Before we derive the $N\mathcal{E}$ solution of the U_{SG}, (P_d^*, P_a^*), we must verify the existence of at least one $N\mathcal{E}$. Recall that a strategy *pure* when a player chooses to take one action with probability 1. Mixed strategy is a strategy which chooses randomly between possible moves. In other words, this strategy is a probability distribution over all the possible pure strategy profiles. Since G_{SG}

- has a finite strategic form highlighted in Table 5.5,

- has finite number of players (MANET, MC), and
- has a finite number of pure strategies for each player: two for the MANET[1] and two for any MC[2].

This satisfies the requirements of Theorem 2.8.1. Thus, it has at least one $\mathcal{NE}$.

Derivation of Nash Equilibrium

In the following we derive the $\mathcal{NE}$ point of G_{SG}. In this way, we find the strategies of both the MANET and MC at the $\mathcal{NE}$ which is the solution (P_d^*, P_a^*) of the G_{SG}, where $P_d^* = \underbrace{\{p_d^*, \cdots, p_d^*\}}_{n}$ and $P_a^* = \underbrace{\{p_a^*, \cdots, p_a^*\}}_{n}$.

Lemma 5.1.1 *At $\mathcal{NE}$, MC attacks any MANET node with the same likelihood thereby the probability of the malicious coalition to attack any node equals p_a^* where*

$$p_a^* = p_{a,n_i}^* = p_{a,n_j}^* \; \forall \, i, j \in N \; s.t. \; p_{d,n_i}^*, \; p_{d,n_j}^* > 0. \tag{5.4}$$

and at the $\mathcal{NE}$ point, the MANET defends any node with the same likelihood p_d^* such as

$$p_d^* = p_{d,n_i}^* = p_{d,n_j}^* \; \forall \, i, j \in N \; s.t. \; p_{a,n_i}^*, p_{a,n_j}^* > 0. \; \blacksquare \tag{5.5}$$

Proof: We will prove this lemma by using the contradiction method. The proof has been split in two part. We will first prove that Eq. (5.4) holds at $\mathcal{NE}$. Then, we will prove that Eq. (5.5) holds at $\mathcal{NE}$.

Assuming that Eq. (5.2), (5.4) and (5.5) hold. We then have that

$$\begin{aligned} 0 \leq p_{a,n_i}^*(1 + r_d) - r_f cost_f - cost_d &= p_{a,n_j}^*(1 + r_d) - r_f cost_f - cost_d \\ &= p_a^*(1 + r_d) - r_f cost_f - cost_d. \end{aligned} \tag{5.6}$$

[1] *defending, non-defending*
[2] *attacking, non attacking*

and for any $n_k \in N$ s.t. $p^*_{d,n_k} = 0$ holds

$$p^*_{a,n_i}(1 + r_d) - r_f cost_f - cost_d \geq p^*_{a,n_k}(1 + r_d) - r_f cost_f - cost_d. \tag{5.7}$$

If (P^*_d, P^*_a) is not a $\mathcal{NE}$ then at $\mathcal{NE}$ one of the following must hold:

- $p^*_{a,n_i}(1 + r_d) - r_f cost_f - cost_d < 0$. In this case the MANET has incentive to change its strategy by change its probability to defend, p^*_{d,n_i}, to zero to avoid gaining negative utility. This contradicts the definition of $\mathcal{NE}$ presented in Section 2.8.3.

- $0 \leq p^*_{a,n_i}(1 + r_d) - r_f cost_f - cost_d \leq p^*_{a,n_j}(1 + r_d) - r_f cost_f - cost_d$. In this case the MANET has incentive to change its strategy by decreasing its probability to defend p^*_{d,n_i} and increase p^*_{d,n_j} as it gains higher utility when it defends node $n_j \in N$. This contradicts the definition of $\mathcal{NE}$.

- $0 \leq p^*_{a,n_i}(1 + r_d) - r_f cost_f - cost_d \leq p^*_{a,n_k}(1 + r_d) - r_f cost_f - cost_d$. In this case the MANET has incentive to change its strategy by adding the defending probability p^*_{d,n_i} to p^*_{d,n_k} and set $p^*_{d,n} = 0$. This happens due to gaining higher utility when it defends the node $n_k \in N$. This contradicts the definition of $\mathcal{NE}$.

Thus at $\mathcal{NE}$ Eq. (5.4) is true.

From Eq. (5.3), (5.4) and (5.5) we have that

$$0 \leq 1 - cost_a - p^*_{d,n_i} r_d = 1 - cost_a - p^*_{d,n_j} r_d = 1 - cost_a - p^*_d r_d. \tag{5.8}$$

and for any $n_k \in N$ s.t. $p^*_{a,n_k} = 0$ holds

$$1 - cost_a - p^*_{d,n_i} r_d \geq 1 - cost_a - p^*_{d,n_k} r_d. \tag{5.9}$$

If (P^*_d, P^*_a) is not a $\mathcal{NE}$ then at $\mathcal{NE}$ one of the following must hold:

- $1 - cost_a - p^*_{d,n_i} r_d < 0$. In that case MC chooses to change its probability to attack node n_i to zero to avoid negative utility. This contradicts the definition of $\mathcal{NE}$.

- $0 \leq 1 - cost_a - p^*_{d,n_i} r_d \leq 1 - cost_a - p^*_{d,n_j} r_d$. In this case MC has incentive to change its strategy by decreasing its probability to attack node n_i and increase p^*_{a,n_j} as it gains higher utility when it defends node $n_j \in N$. This contradicts the definition of $\mathcal{NE}$.

- $0 \leq 1 - cost_a - p^*_{d,n_i} r_d \leq 1 - cost_a - p^*_{d,n_k} r_d$. In this case MC has incentive to change its strategy by adding the probability p^*_{d,n_i} to attack node n_i to p^*_{d,n_k} and set $p^*_{d,n_i} = 0$, due to MC gains higher utility by defending n_k. This contradicts the definition of $\mathcal{NE}$.

Thus at $\mathcal{NE}$ Eq. (5.5) is true. ∎

5.1.2.5 MANET defence strategy based on Model II

In this section we derive the optimal MANET defence strategy in terms of intrusion detection effort or else energy cost incurred due to intrusion detection across a MANET. Such strategy is represented by a probability distribution which indicates how much effort a MANET must put to defend each node. Parameters such as intrusion detection rate, attacking cost, defending cost, false alarm detection rate and false alarm cost affect this distribution probability. At $\mathcal{NE}$ the utility functions of the MANET (Eq. (5.2)) and the malicious coalition (Eq. (5.3)) become

$$U_{manet}(P^*_d, P^*_a) = |n|V[p^*_d[p^*_a(1 + r_d) - r_f cost_f - cost_d] - 2p^*_a],$$

$$U_{mc}(P^*_d, P^*_a) = |n|Vp^*_a(1 - cost_a - p^*_d r_d).$$

To find the stationary point (this is an input to a function where the derivative is zero) which maximises the utility functions of the MANET and the malicious coalition at $\mathcal{NE}$ we have the following[3]

$$\frac{dU_{manet}(P^*_d, P^*_a)}{dP^*_d} = 0 \Leftrightarrow p^*_a(1 + r_d) - r_f cost_f - cost_d = 0$$
$$\Leftrightarrow p^*_a = \frac{r_f cost_f + cost_d}{1 + r_d}.$$

[3]We use Leibniz's notation for the first derivative.

Table 5.6: Notations of Model II.

G_{SG}	security game
S	set of strategies of both MANET and MC
S_{manet}	set of MANET strategies
S_{mc}	set of MC strategies
d	MANET is defending
nd	MANET does not defend defending
a	MC is attacking the MANET
na	MC does not attack
$cost_d$	energy cost of intrusion detection when MANET defends
$cost_f$	energy cost of a false alarm
$cost_a$	energy cost of attacking the MANET
V	security asset of a MANET node
U_{manet}	MANET's utility
U_{mc}	MC's utility
U_{SG}	utility space of G_{SG}
$u_{manet}(d,a)$	MANET's utility when MANET plays d and MC plays a
$u_{mc}(d,a)$	MC's utility when MANET plays d and MC plays a
r_d	attack detection rate
r_f	false alarm detection rate
N	set of MANET nodes
$\|n\|$	total number of nodes
n_i	a node i
p_{d,n_i}	probability to defend a node n_i
p_{d,n_i}	probability to attack a node n_i
P_d	probability distribution over N of MANET defending nodes $n_1, \cdots, n_n$
P_a	probability distribution over N of MC attacking nodes $n_1, \cdots, n_n$

$$\frac{dU_{mc}(P_d^*, P_a^*)}{dP_a^*} = 0 \Leftrightarrow 1 - cost_a - p_d^* r_d = 0$$
$$\Leftrightarrow p_d^* = \frac{1 - cost_a}{r_d}.$$

At the $\mathcal{NE}$ point, both players (MANET and malicious coalition) reach a unique point $(P_d^*, P_a^*) = (\underbrace{\{p_d^*, \cdots, p_d^*\}}_{n}, \underbrace{\{p_a^*, \cdots, p_a^*\}}_{n})$ where they do not consume all of their available energy. We notice that the malicious coalition does not have any profit at $\mathcal{NE}$ even if it decreases its attack cost. This happens because, in such a case, the MANET will increase its monitoring probability reducing the utility of the malicious coalition to zero. The profit of the malicious coalition can be measured as the degree of damage caused to the MANET when an attack is successfully launched. This occurs when an attack is not detected by the MANET due to IDS malfunction or IDS limited capabilities.

The results about the probability distributions align with the fact that the legitimate

MANET nodes are equally important for the network's operation and the attacker realises that a successful attack against any MANET node will equally harm the network.

5.1.2.6 Numerical results

In this section, numerical results have been illustrated showing the MANET utility, at the $\mathcal{NE}$, as a function of the *packet size*, the *intrusion detection rate* and the *mobility*. We have considered two different types of MANETs: a *wireless personal area network* (WPAN) and a *tactical MANET* (for example emergency, military). Both network types use the same air interface. The difference between these two types is that in the case of tactical MANETs we are interested in applying high level of security even if the energy consumption is high while for WPANs, we are more interested in saving energy rather than applying the same level of very high level of security.

In Fig. 5.1, we illustrate the MANET utility loss at the $\mathcal{NE}$ point, in terms of mJoules, as a function of the packet size. The MANET utility loss depends on the energy spent for intrusion detection namely the MANET has to spend some energy resources to monitor the traffic within the network and recognise malicious activities. From Fig. 5.1 we notice that the higher the network size is, the higher the MANET utility loss is, for both network types. This was expected due to the MANET utility is the cumulative utility of all the MANET nodes. Thereby, higher number of nodes implies higher MANET utility loss for certain packet sizes. In the same figure, we also see that for a tactical MANET the utility loss is higher than for a WPAN due to the higher required security level. Furthermore, larger packet size introduces higher MANET utility loss due to higher energy consumption to apply intrusion detection algorithms.

In Fig. 5.2 we have depicted the MANET utility loss against the intrusion detection rate which is an indicator of the MANET's intrusion detection capability. We observe that for increasing intrusion detection rate, the MANET utility loss is decreasing because more attacks are prevented thus more nodes are not damaged. We additionally see that the same trend is followed with the case of Fig. 5.1 regarding different types of networks and

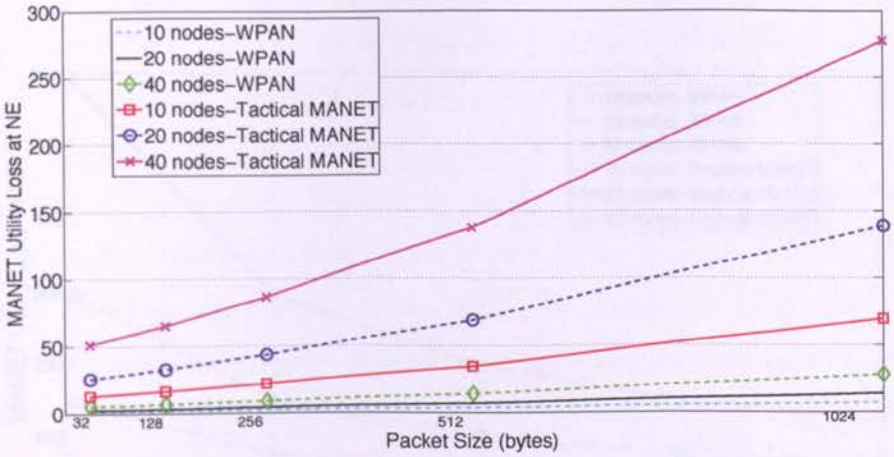


Figure 5.1: The MANET utility loss at $\mathcal{NE}$ against the packet size for different network types and sizes.

different network sizes while in WPANs, the MANET utility loss is less than in tactical MANETs. In addition, a higher network size introduces higher MANET utility loss due to the participation of more devices in the intrusion detection. From Fig. 5.2 we also notice that in the case where the intrusion detection rate has very small value (for example 0.2) the MANET utility loss is significantly high (for example 600 units for 40 nodes tactical MANET) showing that intrusion detection rate strongly indicates the level of the MANET utility.

Fig. 5.3 shows the MANET utility at $\mathcal{NE}$ for different node mobility levels indicated by different pause times. We notice that MANET utility loss increases when mobility increases. This happens due to higher number of link breakages caused by nodes movement outside the transmission range of each other. IDSs might assume that these packet errors are due to malicious activities (such as dropping due to a blackhole attack). Thus, energy is spent defending against a non-existing attack. On the other hand, low mobility makes the detection of an attack easier as IDSs can collect and analyse more information regarding a certain node which, due to the low mobility, stays within the range of its neighbours for longer period.

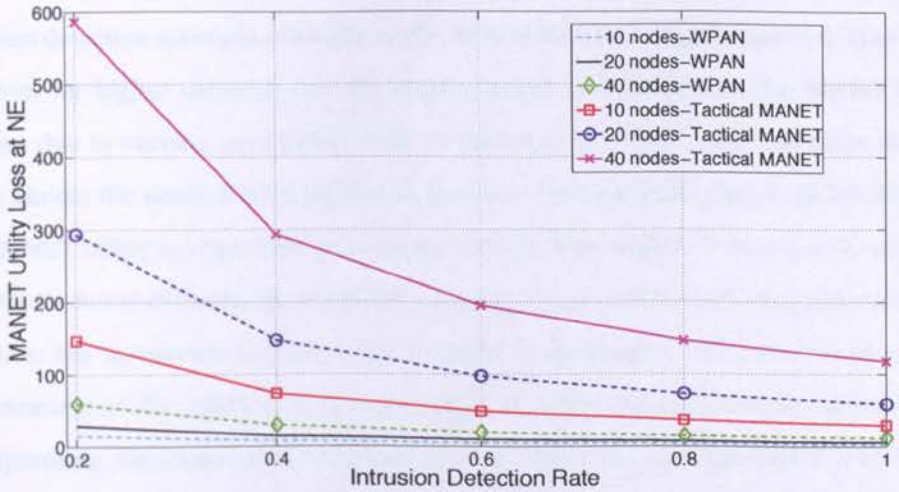


Figure 5.2: The MANET utility loss at $\mathcal{NE}$ against the intrusion detection rate for different network types and sizes.

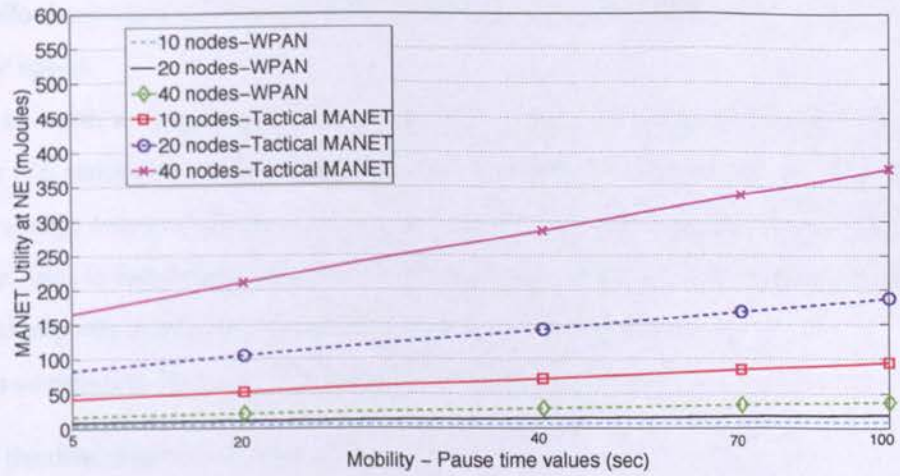


Figure 5.3: The MANET utility loss at $\mathcal{NE}$ as a function of the nodes' mobility level for different network types and sizes.

The results show that for all the different network sizes the average change in the MANET utility is the same for all the different parameters. This can be explained as intrusion detection takes place locally or else within the same neighbourhood. This implies that even for higher network size the improvement or detriment of the MANET utility function due to varying parameters such as packet size, mobility and intrusion detection rate is almost the same. For incremental detection rate (for example 20, 40, 60, 80, 100%) the MANET utility is improved, in average, by 30%. This implies that when the quality of the IDSs (in terms of hardware or software) is improved thereby detecting more malicious activities, the increment in the MANET utility is significant. For incremental mobility the detriment of the utility is approximately 23% whilst for incremental packet size the corresponding detriment approximately equals 30%. This signifies that the changes in mobility and packet size during the network's lifetime do not equally affect the MANET utility.

The high impact of the packet size indicates that applications must be carefully chosen to support nodes' communication in a tactical MANET. On the other hand, the smaller value of utility's detriment in the case of changing mobility shows that intrusion detection will afford any gradual changes in the pause time of the MANET nodes or higher level of nodes' speed.

It is worth mentioning that, we were anticipating the negative $U_{manet}(P_d^*, P_a^*)$'s value at the $N\mathcal{E}$ point due to the energy spent by the IDSs. In addition, we see that spending more energy resources (in the case of incremental $cost_d$) causes degradation of the MANET utility. Also, to reduce the damage caused by attacks, MANET has to improve its intrusion detection performance by increasing the intrusion detection rate.

To summarise, $U_{manet}(P_d^*, P_a^*)$ increases in the following cases:

- the detection rate increases;
- the false alarm detection decreases;
- the intrusion detection cost decreases and;

- the false alarm cost decreases.

5.2 GTMR - A game theoretic approach to reduce the overall intrusion detection cost in MANETs

In this section we describe our novel routing protocol, entitled *Game Theoretic MANET Routing* (GTMR) which reduces the total energy spent for intrusion detection, to defend MANET routes, based on Model I described in Section 5.1.1. This protocol decides upon routes to extend the network's lifetime, alleviate network segmentation (for example the situation where some nodes have "died" and there are no paths from source to destination) and improve availability by increasing the lifetime of the IDSs operated by MANET nodes. GTMR is an extension of our solution published in [13] with the following main differences:

- we extend the utility function of the MANET, the cost of defending a route and the cost of attacking a route;
- to calculate the MANET utility we take into account the intrusion detection and misdirection rates r_d and r_m;
- we add the d_0 strategy which is the case that MANET does not defend in order to reserve battery power;
- we conduct more simulations to evaluate several parameters related to the availability of MANET resources;
- we undertake comparisons with *Ad hoc On demand Distance Vector* (AODV) [4], *Ad hoc On-demand Multipath Distance Vector* (AOMDV) [20] and *Optimized Link State Routing* (OLSR) [17] protocols.

In the rest of this section we describe the GTMR functionalities and packet formats. Then, we present the simulation results which show that GTMR:

- enables more energy efficient host-based intrusion detection than conventional routing protocols increasing the MANET security level by extending the availability of the network resources,
- supports longer network-wide intrusion detection,
- respects the *Quality-of-Service* (QoS) of delay sensitive data.

5.2.1 Cost analysis

We define the metric of density for a node n_k as σ_{n_k}. This symbolises the node density within the transmission range of n_k. The $cost_{loss,r_i}$ of the route i can be expressed as the energy cost of retransmitting a piece of data due to a route error caused by an attack. This cost multiplied by the misdirection rate r_m equals

$$r_m cost_{loss,r_i} = \frac{r_m V}{|n_{r_i}|} E_{loss} \sum_{n_k \in n_{r_i}} \sigma_{n_k}. \tag{5.10}$$

The value of $cost_{loss,r_i}$ changes as a function of the density of the MANET nodes that constitute the route i. We define the metric of density for each node n_k as follows:

$$\sigma_{n_k} = \frac{T_{R_{n_k}} \pi}{A} |neigh_{n_k}|. \tag{5.11}$$

and substituting in Eq. (5.12) we have that

$$cost_{loss,r_i} = \frac{\pi}{A} \frac{1}{|n_{r_i}|} \sum_{n_k \in n_{r_i}} T_{R_{n_k}} |neigh_{n_k}| E_{loss}. \tag{5.12}$$

Assuming that all nodes in the MANET have equal transmission range, T_R from (5.12) we have that

$$\begin{aligned} cost_{loss,r_i} &= \frac{\pi}{A} |n_{r_i}| \frac{1}{|n_{r_i}|} T_R \sum_{n_k \in n_{r_i}} |neigh_{n_k}| E_{loss} \\ &= \frac{\pi}{A} T_R \sum_{n_k \in n_{r_i}} |neigh_{n_k}| E_{loss}. \end{aligned} \tag{5.13}$$

More precisely, the cost of defending a route i against a malicious node is the cost of operating the IDS in the nodes which constitute this route as well as in their one-hop neighbours. The latter are overhearing the transmissions within their transmission range due to they are operating in promiscuous mode participating in the intrusion detection. More details about the energy costs operating in the promiscuous mode can be found in [99].

The value of $cost_{d,r_i}$ represents the average cost per node of defending a route i against malicious nodes. This value depends on the values of $|neigh_{n_k}| \; \forall \; n_k \in n_{r_i}$ and n_{r_i} and it is given by the next formula

$$cost_{d,r_i} = (\sum_{n_k \in n_{r_i}} |neigh_{n_k}| + |n_{r_i}|)E_{ids}. \tag{5.14}$$

When a packet is forwarded through a route which has higher $cost_{d,r_i}$ value than another route, the cost of defending the former route is higher due to the participation of more intrusion detection nodes. One skilled in the art could suppose that $cost_{d,r_i}$ depends on the degree of importance of each route, too. However, for reasons of simplicity and without loss of generality, we suppose that all the routes have equivalent degree of importance.

5.2.2 Design challenges

Depending on which route is selected to enable communication between a source and a destination node there is a different number of nodes which carry out the intrusion detection activities. In that case, if the same routes are constantly used, due to for instance their high QoS provision or other routing parameters, there is a high risk for the detection nodes which monitor this route to spend their residual energy faster than in the case where a more distributed assignment of intrusion detection would be in place. As a result, the MANET will be "unprotected" for a longer period of time as well as network fragmentation might occur.

The challenge is to design and develop a routing protocol which will respect the energy spent due to intrusion detection along a MANET route. In the following we describe how

GTMR addresses this challenge by maximising the utility of the MANET at the $\mathcal{NE}$ of the non-cooperative game proposed in Model I. GTMR therefore increases the MANET security by extending the lifetime of the intrusion detectors and prolong the availability of the network resources.

5.2.2.1 AODV extensions

GTMR has been designed by adding some functionalities to AODV as described next. One of the main characteristics of AODV is that the selection of a route is mainly based on the number of hops from n_S to n_D as well as the RREP receiving time. The energy spent for intrusion detection is not taken into account upon route selection. GTMR addresses such a deficiency by:

- changing the routing packets' format (both RREQ and RREP) to take into account the number of neighbours of each node (these act as intrusion detectors);
- extending the routing table to store the *utility per route* derived by Model I,
- updating the reverse route, whenever a RREQ is received, with the one which has the highest utility value,
- updating the forward route, whenever a RREP is received, with the one which has the highest utility value.

In a nutshell, our methodology extends both RREQ and RREP messages in AODV, and proposes a new MANET routing decision algorithm. by choosing the route with the highest utility according to G_{GTMR}. Such route improves MANET security by increasing the IDSs lifetime and the availability of the network resources by taking into account the energy consumption, due to intrusion detection, on a route.

5.2.2.2 Functionality

We assume that a requester node n_S wants to find a route to a destination node n_D. If there no such a route cached then n_S broadcasts a RREQ which includes a *critical field* to hold the

sum of the number of neighbours, of all nodes on route i, that have sent or forwarded this RREQ. This value equals $\sum_{n_k \in n_{r_i}} |neigh_{n_k}|$.

The node which receives a RREQ caches in its routing table the critical value and based on that, it constructs the reverse route back to the source of the RREQ. The destination node n_D or an intermediate node which has a route to n_D sends a RREP using the reverse path towards n_S. This RREP has the same format as in AODV but it also includes the *critical field* $\sum_{n_k \in n_{r_i}} |neigh_{n_k}|$ where r_i is the forward route. The forward and reverse routes' refresh happens periodically in certain timeouts defined by AODV in [4].

The *critical field* equals the number of intrusion detection nodes thereby, when the source node n_S of a RREQ receives a GTMR RREP packet, it will be aware of the cumulative number of detection nodes along a route towards n_D.

5.2.2.3 Packets' format

In the following we present the RREQ and RREP packet formats in the GTMR protocol:

GTMR RREQ

{Type, ···, Hop Count, RREP ID, Destination IP Address, Destination Sequence Number, Originator IP Address, Originator Sequence Number, $\sum_{n_k \in n_{r_i}} |neigh_{n_k}|$*}.*

GTMR RREP

{Type, ··· , Hop Count, RREQ ID, Destination IP Address, Destination Sequence Number, Originator IP Address, Originator Sequence Number, Lifetime, $\sum_{n_k \in n_{r_i}} |neigh_{n_k}|$*}.*

Thereafter, the construction of a requested forward route towards a n_D, allows n_S to decide which route will be used to transmit its data. The final goal is to maximise the utility value $u_{manet_{11}} = r_d V - r_m cost_{loss,r_i} - cost_{d,r_i}$ of the MANET at the $\mathcal{NE}$.

5.2.2.4 Route utility

Without loss of generality, we assume that the detection and false alarm rates of all the intrusion detectors are equivalent across the MANET, therefore the challenge is to find the

route which optimally minimises the values of $cost_{loss,r_i}$ and $cost_{d,r_i}$. To this end, we first define the following utility function for each route i as

$$u_{r_i} = \frac{1}{\sum_{n_k \in n_{r_i}} |neigh_{n_k}| + |n_{r_i}|}. \tag{5.15}$$

GTMR aims at choosing the route with the highest utility, called R_{GTMR}.

A set of routes from n_S to n_D is defined as

$$R_{n_S n_D} = \{r_1, r_2, \cdots, r_{|R_{n_S n_D}|}\},$$

and it is constructed using all the received RREPs. These indicate all the forward routes that the routing protocol finds from n_S to n_D, let them be

$$r_1, r_2, \cdots, r_{n_S n_D},$$

with utility values

$$u_{r_1}, u_{r_2}, \cdots, u_{r_{n_S n_D}}.$$

We define R_{GTMR} as the route with the highest utility thus

$$R_{GTMR} =: \{r_x \in R_{n_S n_D} : u_{r_x} \geq u_{r_i}, \forall\, r_i \in R_{n_S n_D} - r_x\}. \tag{5.16}$$

It is worth stressing here that the source of a RREQ does not wait until it receives all the possible routes to a destination to find $GTMR_{route}$ but it starts using the first route that it retrieves from the first RREP. Thereafter, each time a RREP is received n_S must check $GTMR_{route}$ must be updated with the route associated to this RREP. This substitutions happens when the latter has higher utility than the currently in use route.

The algorithms (3) and (4) describe the main functionalities of the GTMR protocol as they have been described in this section.

Table 5.7: Notations of GTMR.

r_d	attack detection rate
r_m	misdetection rate
n_k	node k
σ_{n_k}	density for a node n_k
$cost_{loss,r_i}$	the damage incurred on a route i due to a successful attack
V	security asset of a MANET route
n_{r_i}	set of nodes on r_i
$\|n_{r_i}\|$	number of nodes that r_i traverses
$\overline{E_{loss}}$	average energy loss due to a successful attack
$T_{R_{n_k}}$	transmission range of n_k
$neigh_{n_k}$	set of one-hop neighbours of n_k
$\|neigh_{n_k}\|$	number of n_k's
A	geographical MANET size
T_R	transmission range
$cost_{d,r_i}$	average energy per node for defending r_i
E_{ids}	nodal average energy spent for intrusion detection
n_S	source node
n_D	destination node
$u_{manet_{\mathcal{NE}}}$	the utility of the MANET at the $\mathcal{NE}$
r_i	a MANET route i
u_{r_i}	utility value of r_i
$R_{n_S n_D}$	set of routes from n_S to n_D
$\|R_{n_S n_D}\|$	number of routes from n_S to n_D
$U_{R_{n_S n_D}}$	set of utility values of routes belong to $R_{n_S n_D}$
R_{GTMR}	the route with the highest utility, chosen by GTMR

5.2.3 Simulation results

In this section, we use simulations to verify the integrity of the proposed model and showcase the benefits of using our proposed solution. We have used an event based simulator, for the packet-level network simulator ns-2, customised with our implementation of GTMR protocol, to validate the proposed model and optimisation solution. The simulator incorporates all the energy parameters needed for evaluating the efficiency of different protocols in terms of energy cost, space and time overhead. The implementation takes into account variable number of nodes and dynamic mobility scenarios. Further lower layers are also simulated in the ns-2 simulator to achieve more realistic simulation results.

We have focused our simulation studies on the improvement of the energy across the MANET when IDSs are used and we have also examined the impact of GTMR in terms of QoS. Table 5.8 summarises the parameters of our simulation studies. In this table the different energy values have been retrieved from the manufacturers specifications of the Dell DW 1520 WLAN 802.11n half mini-card.

Algorithm 3 Request a route to a destination

1: n_S seeks for a route to a destination node n_D by broadcasting a $RREQ_{n_D}$
2: **if** a node n_A receives a $RREQ_{n_D}$ **then**
3: n_A caches the reverse route (including the critical field) in its routing table
4: **if** $n_A \neq n_D$ **then**
5: **if** n_A does not have a route to n_D **then**
6: n_A broadcasts the $RREQ_{n_D}$
7: **else**
8: n_A sends a $RREP_{n_D}$ to n_S using the reverse route
9: **end if**
10: **else**
11: n_A is the destination node n_D
12: n_D sends a $RREP_{n_D}$ to n_S using the reverse route
13: **end if**
14: **end if**

Algorithm 4 Selecting the GTMR route

1: n_S receives a $RREP_{n_D}$ which includes a route i to the destination
2: **if** n_S does not have any other forward active route **then**
3: n_S sets the $R_{GTMR} := r_i$
4: n_S sends data to n_D using the R_{GTMR}
5: **else**
6: n_S compares r_i with R_{GTMR}
7: **if** $u_{r_i} < u_{R_{GTMR}}$ **then**
8: n_s keeps using the current R_{GTMR}
9: **else**
10: n_S sets the $R_{GTMR} := r_i$
11: **end if**
12: **end if**

We have conducted extensive simulations to evaluate the effectiveness of GTMR and compare them with other MANET routing protocols such as AODV, AOMDV and OLSR. In these simulations, nodes are randomly deployed inside a rectangular area of 1000m x 1000m, and each mobile node moves according to the random waypoint model [100], which can be characterised by the following two parameters: the minimum velocity and the maximum velocity. We use the following scenarios to investigate the effects of mobility [100]; min velocity 4.5 m/s – max velocity 5.5 m/s, min velocity 7.5 m/s – max velocity 8.5 m/s. The *medium access control* (MAC) layer protocol implements the IEEE 802.11b *distributed coordination function* (DCF) with a four-way handshaking mechanism [94]. The link data

Table 5.8: Simulation parameters.

Parameter	Value
Network size (number of nodes)	10, 20, 30, 40, 50, 60
Data packet payload size	512 bytes
Transmission data rate	64kb/s
Area size	1000m x 1000m
MAC Layer	IEEE 802.11b
Maximum transmission range	250 m
Maximum number of traffic connections	No. nodes / 2
Speed	0-5 m/s
Simulation time	1000s
Types of traffic	UDP, CBR
Mobility model	Random Waypoint
Initial nodal energy	4000 Joules
Power Supply	3.3Volts
Idle power (P_{idle})	25mA = 0.0825W
Receiving power (P_{rec})	468mA = 1.544W
Transmission power (P_{trans})	572mA = 1.8876W

rate is 54Mb/s, the data packet size is 512 bytes and the transmission rate of data is 64kb/s CBR. The maximum transmission range is 250m. Inside the transmission range, the channel errors are characterized using the two-ray ground propagation model.

We have illustrated the following results for 10, 20, 30, 40, 50 and 60 nodes, for each routing protocol; AODV, GTMR, AOMDV and OLSR we repeated the simulations for mobility levels 4.5-5.5 m/s, 7.5-8.5 m/s and 10.5-11.5 m/s:

- GTMR extra average node lifetime for different network sizes and MANET routing protocols.
- cumulative MANET lifetime for different network sizes and MANET routing protocols[4];
- total routing overhead (packets) for different network sizes and MANET routing protocols;
- average end-to-end packet delay for different network sizes and MANET routing protocols;

[4]Time to deplete the entire initial energy.

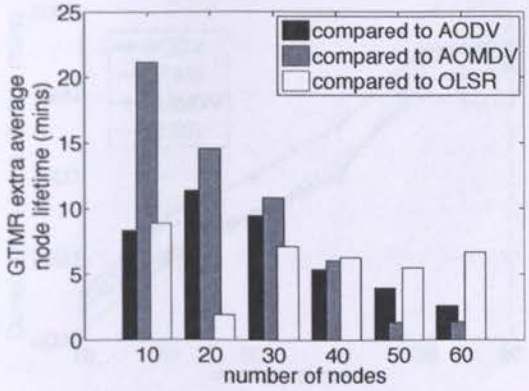
- less average intrusion detection energy cost per GTMR node.

In Fig. 5.4(a) we have illustrated the extra average node lifetime of GTMR compared to different MANET routing protocols and for different network sizes. According to this graph, GTMR outperforms the rest of the protocols. We notice that the examined parameter is erratic for the other routing protocols (AODV, AOMDV, OLSR) in the sense that none of them comes second consistently. Additionally, none of them outperforms GTMR and has 6.8, 14.2, 6.04 minutes extra average node lifetime than AODV, AOMDV and OLSR for different network sizes.

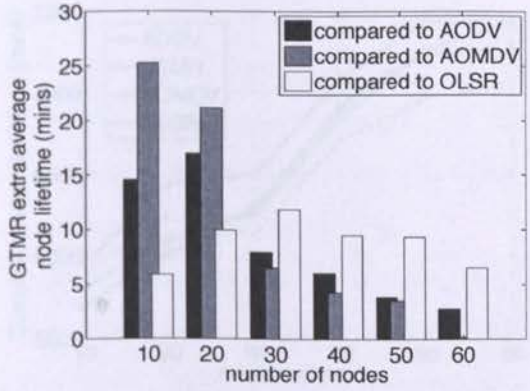
Fig. 5.4(b) depicts the same results for different mobility level, namely 7.5-8.5m/s. We observe that the performance of GTMR has increased as mobility level has been raised. GTMR still outperforms the different routing protocols providing 8.6, 10.1 and 8.8 minutes extra average node lifetime compared to AODV, AOMDV and OLSR, respectively. In Fig. 5.4(c), we have plotted the same parameter for 10.5-11.5 m/s mobility level noticing that GTMR introduces 7.18, 11.8 and 8.6 minutes extra average node lifetime than AODV, AOMDV and OLSR.

To show the extra actual network lifetime which is measured in terms of usable energy to maintain the network operative (for example data transmissions, voice and video.) we have plotted the cumulative lifetime for different network sizes and routing protocols in Fig. 5.5. In Fig. 5.5(a) we observe that GTMR consistently outperforms the other protocols due to the maximisation of the MANET utility as it has been analysed in the previous section. GTMR provides 193.4, 202.5 and 210.7 minutes extra average network lifetime than AODV, AOMDV and OLSR. Fig. 5.5(b) validates the same findings for higher mobility level with the outperformance of GTMR to be more pronounced. In this case, the GTMR extra network lifetime is 219.08, 203.64 and 308.09 minutes compared to AODV, AOMDV and OLSR. Similar trend is followed by the different protocols for mobility level 10.5-11.5m/s as shown in Fig. 5.5(c) with 177.6, 217.9 and 334.1 minutes extra GTMR average network lifetime than AODV, AOMDV and OLSR.

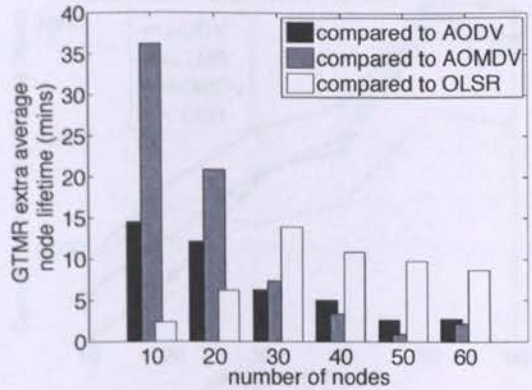
The trend in Fig. 5.6 shows that GTMR has the highest packet overhead among all the



(a) Mobility level 4.5-5.5 m/s

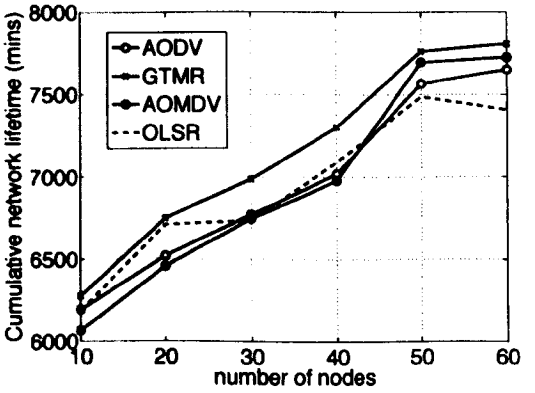


(b) Mobility level 7.5-8.5 m/s

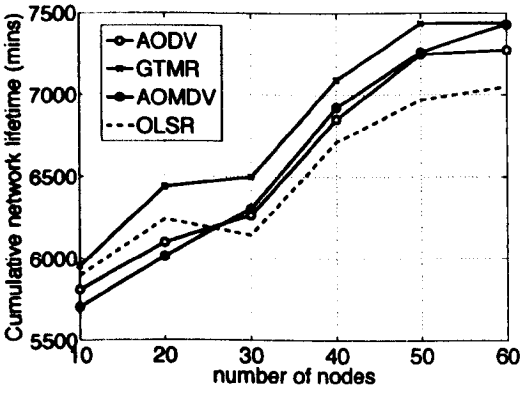


(c) Mobility level 10.5-11.5 m/s

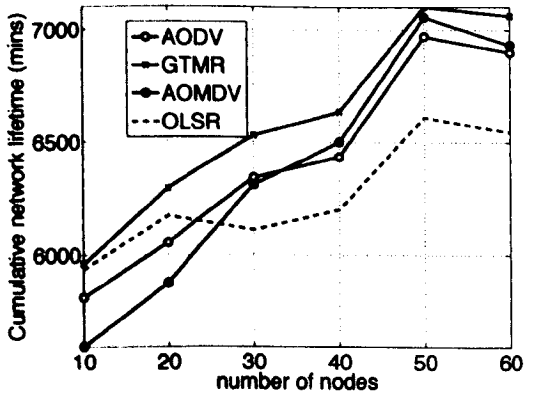
Figure 5.4: Extra average lifetime per GTMR node.



(a) Mobility level 4.5-5.5 m/s



(b) Mobility level 7.5-8.5 m/s



(c) Mobility level 10.5-11.5 m/s

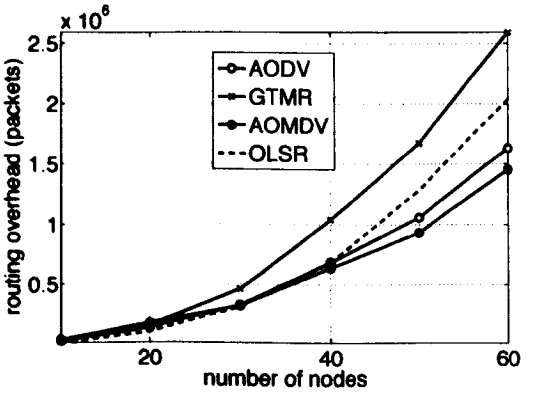
Figure 5.5: Cumulative lifetime of the entire network.

routing protocols simulated. This happens due to the GTMR routing algorithm which requires a higher route refresh rate to update the route energy levels for different routes. However the fact that GTMR maintains better energy efficiency compounds the effectiveness of the algorithms. This also provides a promising avenue for future research to lower the overhead which will further improve the energy efficiency characteristics. With the increment of the mobility level link breakages increase and the difference of GTMR with regards to the rest of the protocols, in terms of routing overhead, is slightly higher. This occurs due to GTMR discovering more link breakages because of the higher route refresh rate.

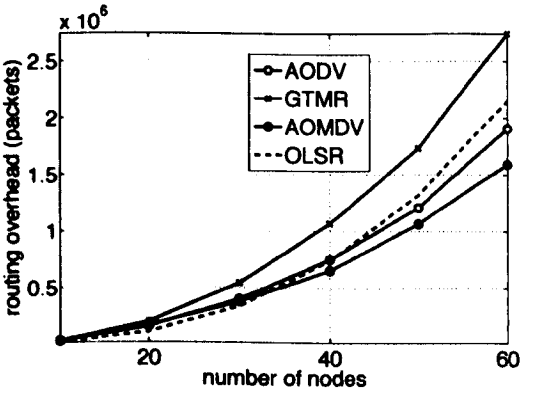
Fig. 5.7 illustrates the end-to-packet delay for the different MANET routing protocols considering data packets. This is an important parameter assuming MANETs will be used for delay sensitive applications such as multimedia communications. We notice that GTMR mostly introduces approximately equivalent or less delay than the other protocols apart from AOMDV which is anyway tailored to reduce such a parameter. In Fig. 5.7(a), 5.7(b) and 5.7(c), we observe that higher mobility increases this delay without increasing the difference between the performance of all the protocols.

Finally, in Fig. 5.8, we have plotted the GTMR less average node IDS energy consumption per second compared to the rest of the protocols. For mobility level 4.5-5.5 m/s, we notice from Fig. 5.8(a) that AODV, AOMDV and OLSR introduce in average 8.845, 7.396 and 11.4 mJoules/sec more average IDS energy cost, per MANET node, than GTMR, respectively. In Fig. 5.8(b), we see that for higher mobility (7.5-8.5 m/s) this difference is more pronounced for GTMR which has 10.5, 8.27 and 17.76 mJoules/sec more average node IDS energy cost than AODV, AOMDV and OLSR, correspondingly.

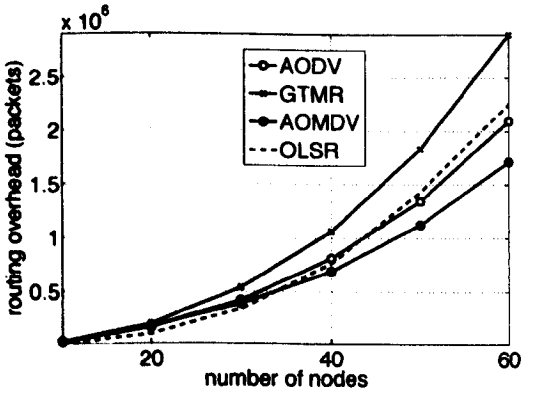
By increasing the mobility level to the range of 10.5 – 11.5 m/s, Fig. 5.8(c) shows that the differences in terms of the same parameter among the different protocols remains approximately the same with the average differences of GTMR compared to AODV, AOMDV and OLSR to be 7.38, 5.62 and 20.44 mJoules/sec.



(a) Mobility level 4.5-5.5 m/s

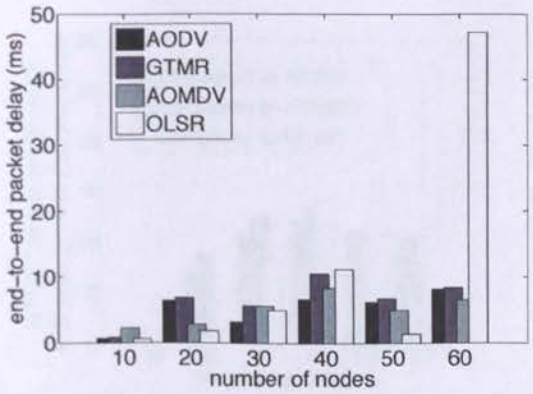


(b) Mobility level 7.5-8.5 m/s

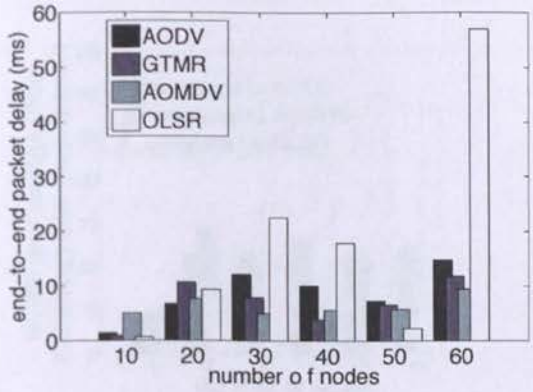


(c) Mobility level 10.5-11.5 m/s

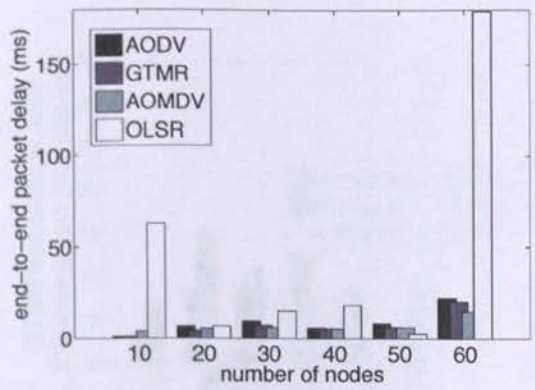
Figure 5.6: Routing packet overhead.



(a) Mobility level 4.5-5.5 m/s

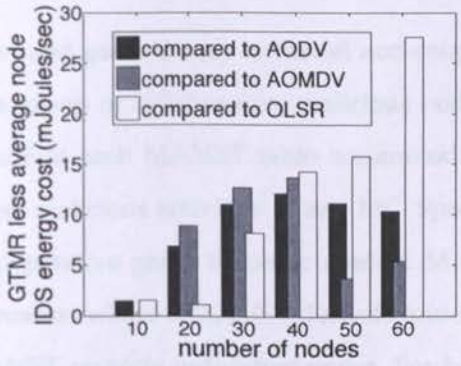


(b) Mobility level 7.5-8.5 m/s

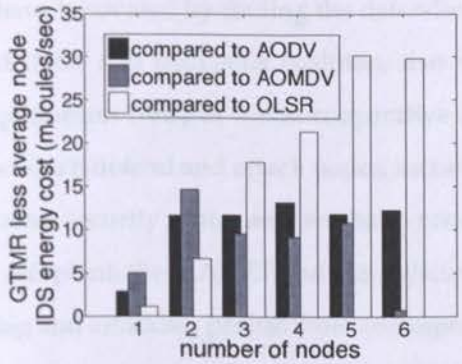


(c) Mobility level 10.5-11.5 m/s

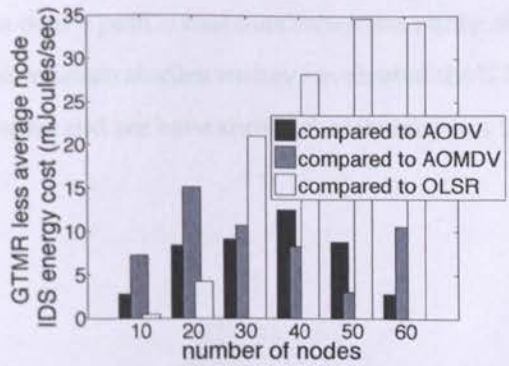
Figure 5.7: End-to-end packet latency.



(a) Mobility level 4.5-5.5 m/s



(b) Mobility level 7.5-8.5 m/s



(c) Mobility level 10.5-11.5 m/s

Figure 5.8: Less average IDS energy cost per GTMR node.

5.3 Summary

In this chapter we have used game theory to model non-cooperative security games between a MANET and a group of collaborative malicious nodes called *malicious coalition* (MC). We have assume that each MANET node accommodates an intrusion detection system in order to detect malicious activities of any MC. Specifically, we have proposed two substantive non-cooperative game theoretic models. Model I, presented in Section 5.1.1, formulates the situation where a MANET defends routes whilst Model II examines the case where the MANET protects individual nodes. For both games we have proven proven the existence of a $\mathcal{NE}$. Thereafter, we have derived this equilibrium and we have calculated when the MANET utility is maximised.

In Section 5.1.2 we have innovated by finding the defending and attacking probability distributions, of any MANET and malicious coalition, that maximise the utility of the players at the Nash Equilibrium ($\mathcal{NE}$) of a non-cooperative security game between the aforementioned entities which defend and attack nodes, accordingly. We have derived the $\mathcal{NE}$ of the non-cooperative security game and we have proven its validity. In fact, we have shown that at the $\mathcal{NE}$ point, the MANET and the malicious coalition have to equally distribute their defending and attacking probabilities correspondingly.

In Section 5.2, we have proposed the *Game Theoretic MANET Routing* (GTMR) protocol to increase MANET availability by reducing the network-wide intrusion detection cost based on a non-cooperative game theoretic model. According to GTMR, any source node chooses to route its data over a path r_i that maximises the utility of the MANET at $\mathcal{NE}$. By undertaking thorough simulation studies we have evaluated the GTMR performance under varying MANET topologies and we have shown that it compares favourably to traditional routing protocols.

Chapter 6

Conclusions and Future Work

"When I examine myself and my methods of thought, I come to the conclusion that the gift of fantasy has meant more to me than any talent for abstract, positive thinking.", Albert Einstein

In this chapter we present the research achievements and limitations of the work undertaken in this thesis. We also provide several suggestions for future work.

The overall goal of this thesis is to propose solutions for secure Mobile Ad-hoc NETwork (MANET) communications. Some of these solutions are concerned with emergency MANETs, required by the setting of the EU FP7 PEACE project.

We started our investigation by looking at the main research areas of MANET security. We identify that the main issues pertaining to MANET communications are the provision of integrity, confidentiality and availability by investigating secure routing, secure peer-to-peer overlays and game theoretic intrusion detection mechanisms.

Our first contribution falls within the area of secure routing for emergency MANETs. We have proposed a secure mechanism for AODV called *AODV Wormhole Attack Detection Reaction* (AODV-WADR) to detect and react to wormhole attacks.

One of the limitations of this contribution is the assumption of a symmetric pre-shared network-wide key which are hard-coded in each mobile device prior to the establishment of the network. This was a strong assumption in the scenarios defined by PEACE based on emergency cases where first responders could be securely equipped with such a device prior

to the network setup. Future work must provide a more sophisticated key management mechanism which will overcome the need for the existence of a pre-shared key and might also further improve the efficiency of our protocol.

Another limitation of this protocol is that the detection of a wormhole attack currently takes place by identifying delays in a communication path from a source to a destination. In future work, a combination of the existing technique and a behaviour-based intrusion detection model would enhance detection accuracy. However, one must think carefully how such a model would affect the overall network performance in terms of QoS metrics such end-to-end delay and jitter.

We then propose a hybrid version of IPsec tailored to satisfy the special requirements of emergency MANET communications. The performance evaluation shows that this hybrid version of IPsec introduces negligible time and space overhead to conventional routing mechanisms while it enables the adequate security level for MANET multimedia communications. We have used the same version of IPsec on top of CML routing to provide confidentiality, and integrity to the transmitted packets by designing the SCML protocol.

A limitation of this contribution is that each node must cache a different pair of symmetric keys for each of the associated MANET nodes. In SCML, this happens in order to avoid each node to be able to overhear the content of the transmitted packets when such a node is not the anticipated destination. In future, this limitation could be addressed by investigating a more efficient technique based on secret sharing and other tools, that have been out of scope for our work.

Recently, other secure MANET routing protocols have been suggested in the literature such as [101], [102], [103], [104], [105], [106] and [107]. Some future work could evaluate SCML compared to these. Furthermore, a testbed implementation would have been ideal to act as a proof of concept in order to validate SCML outperforming other routing protocols which use asymmetric cryptography.

With regards to secure peer-to-peer overlays for MANETs, we have extended the ROBUST peer-to-peer (P2P) overlay to encompass security extensions that provide confi-

dentiality and integrity in order for all distributed hash table (DHT) transactions to be authenticated and private between only those participating in the overlay and appear encrypted to any intermediate MANET node. The resulting contributions from this work are important for a future design and implementation of P2P protocols for MANETs, especially in the cases where data security and confidentiality is of high importance.

Again here, the symmetric key management used by the peers of the overlay is a limitation of this contribution. Such a key management sits on top of the corresponding network layer key management to enable secure peer-to-peer communications rather than securing packets only on the network layer. In the same context, a more advanced key management scheme would avoid peers caching different key pairs for each of their predecessors and successors. Such a scheme could take more advantage of the clustered-based ROBUST's topology to reduce the size of the required cached cryptographic information.

Further work could include comparisons of secure ROBUST with other structured peer-to-peer overlay approaches for MANETs and to assert that ROBUST is indeed a very efficient peer-to-peer overlay technique. Future work in the area of secure P2P for MANETs must also address the scalability issues experienced when a high number of peers are mobile. While ROBUST goes some way to addressing this problem with proximity synchronisation, it is clear that a lot of the encountered discrepancies stem from an inefficient transport protocol which should be addressed.

Moreover, a real time testbed implementation of the secure ROBUST DHT will benefit our research and it might initiate the first standardisation activities within the realm of peer-to-peer networking for MANETs. We believe that by using such a peer-to-peer overlay architecture in conjunction with multi-secret sharing techniques, we can increase the security of the communications keeping at the same time the incurred space and time overhead to an acceptable level.

The last contribution of this thesis is the use of game theoretic applications for enhancing intrusion detection in MANETs. Specifically, we have used game theory to model non-cooperative security games between a MANET and a group of collaborative mali-

cious nodes called malicious coalition (MC). We have proposed two independent non-cooperative game theoretic models. Model I formulates the situation where a MANET defends routes whilst Model II examines the case where the MANET protects individual nodes. For both games we have proven proven the existence of a Nash Equilibrium and we have also derived it.

More importantly, we have designed and developed the GTMR protocol to increase MANET availability by reducing the network-wide intrusion detection cost based on the non-cooperative game theoretic Model I. According to GTMR, any source node chooses to route its data over a path that maximises the utility of the MANET at the Nash Equilibrium. By undertaking thorough simulation studies we have evaluated the GTMR performance under varying MANET topologies and we have shown that it compares favourably to traditional routing protocols.

One limitation of our scenarios when testing GTMR, by using the network simulator ns-2, is that we have not defined and investigated a specific threat model. This leads to the absence of an actual malicious coalition in the network. Neither, we have developed a specific intrusion detection mechanism in ns-2, but we have considered and added an appropriate energy cost for carrying out intrusion detection capabilities in each node. Thereby, any future work will benefit from the development of such an attacker model and an intrusion detection mechanism operated in each node. In this case, we will be able to evaluate how GTMR behaves in the presence of an MC in terms of packet loss, delay and other network parameters.

By using Model II, we have innovated by finding the defending and attacking probability distributions, of a MANET and MC, that maximise their utility at the Nash Equilibrium of a non-cooperative security game between such players which defending and attacking nodes, accordingly. We have derived the Nash Equilibrium of this non-cooperative security game and we have proven its validity. In fact, we have shown that at the Nash Equilibrium, the MANET and the malicious coalition have to equally distribute their defending and attacking probabilities correspondingly.

The next step, regarding Model II is the implementation of a network simulator which will take into account a specific threat model and appropriate intrusion detection techniques running in each of the nodes. Our plans for future work includes simulation of scenarios where malicious nodes launch attacks against the MANET nodes whilst the latter are using intrusion detection techniques to recognise such attacks spending faster their residual energy. In such a work we will focus on maximising the intrusion detection sampling rate using the results of this thesis to achieve an efficient balance between intrusion detection as well as the implied energy consumption.

In [108] we have proposed a novel and simple method to provide recipients' anonymity in multihop ad-hoc networks. Although this work is not included in this thesis due to its preliminary nature, future work within the field of MANET security can be based on this anonymity method. Compared to anonymous methods that are solely based on hiding users identities with a hash, our proposal is more robust. In particular, identities change in every lookup so attackers cannot profile nodes in the network in addition to the fact that dictionary attacks are not possible since they usually require more time than the lifetime of a certain identity.

To conclude, the work undertaken in this thesis is an important contribution to comprehensive security frameworks for mobile ad-hoc networks. Such frameworks will likely to be included in future networking paradigms, when ubiquitous networking will be the case rather than the exception.

Bibliography

[1] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, "Mobile ad hoc networking," *Wiley-IEEE Press*, Aug. 2004.

[2] C. Papageorgiou, K. Birkos, T. Dagiuklas, and S. Kotsopoulos, "An obstacle-aware human mobility model for ad hoc networks," *in Proc. IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), London, UK*, pp. 1–9, Sep. 2009.

[3] F. Anjum and P. Mouchtaris, *Security for wireless ad hoc networks*. Wiley-Blackwell, Mar. 2007.

[4] C. Perkins, E. Belding-Royerand, and S. Das, "Ad hoc on-demand distance vector (aodv) routing," *IETF, RFC 3561*, Jul. 2003.

[5] T. Ramrekha, E. Panaousis, and C. Politis, "Standardisation advancements in the area of routing for mobile ad-hoc networks," *The Journal of Supercomputing, Springer*, pp. 1–26, 2011.

[6] G. Millar, E. Panaousis, and C. Politis, "Distributed hash tables for peer-to-peer mobile ad-hoc networks with security extensions," *Journal of Networks, Special Issue: Recent Advances in Information Networking, Services and Security*, vol. 7, no. 2, pp. 288–299, Feb. 2012.

[7] E. Panaousis, L. Nazaryan, and C. Politis, "Securing aodv against wormhole attacks in emergency manet multimedia communications," *in Proc. International Mobile Multimedia Communications Conference, ICST, London, UK*, pp. 34:1–34:7, Sep. 2009.

[8] E. Panaousis, T. Ramrekha, and C. Politis, "Secure routing for supporting adhoc extreme emergency infrastructures," *in Proc. Future Network and MobileSummit, IEEE, Florence, Italy*, pp. 1–8, Jun. 2010.

[9] E. Panaousis, T. Ramrekha, G. Millar, and C. Politis, "Adaptive and secure routing protocol for emergency mobile ad hoc networks," *International Journal of Wireless and Mobile Computing*, vol. abs/1005.1740, pp. 62–78, May 2010.

[10] E. Panaousis, C. Politis, K. Birkos, C. Papageorgiou, and T. Dagiuklas, "Security model for emergency real-time communications in autonomous networks," *Information Systems Frontiers, Springer Netherlands*, vol. 14, pp. 541–553, 2012.

[11] E. Panaousis, G. Millar, C. Politis, and E. Pfluegel, "A game theoretic approach to reduce the overall intrusion detection cost in manets (to be submitted)," *Journal of Computer and System Sciences, Elsevier*, Nov. 2012.

[12] E. Panaousis and C. Politis, "Non-cooperative games between legitimate nodes and malicious coalitions in manets," *Proc. Future Network and MobileSummit, IEEE*, Jun. 2011.

[13] ——, "A game theoretic approach for securing aodv in emergency mobile ad hoc networks," *in Proc. IEEE Conference on Local Computer Networks (LCN), Zurich, Switzerland*, pp. 985–992, Oct. 2009.

[14] S. Corson and J. Macker, "Mobile ad hoc networking (manet): Routing protocol performance issues and evaluation considerations," *IETF, RFC 2501*, Jan. 1999.

[15] J. Burbank, P. Chimento, B. Haberman, and W. Kasch, "Key challenges of military tactical networking and the elusive promise of manet technology," *IEEE Communications Magazine*, vol. 44, no. 11, pp. 39–45, Nov. 2006.

[16] M. Conti and S. Giordano, "Multihop ad hoc networking: The reality," *IEEE Communications Magazine*, vol. 45, no. 4, pp. 88–95, Apr. 2007.

[17] T. Clausen and P. Jacquet, "Optimized link state routing protocol (olsr)," *IETF, RFC 3626*, Oct. 2003.

[18] D. Johnson, Y. Hu, and D. Maltz, "The dynamic source routing protocol (dsr) for mobile ad hoc networks for ipv4," *IETF, RFC 4728*, Feb. 2007.

[19] T. Cormen, H. Leiserson, E. Charles, and R. Ronald, "The bellman-ford algorithm," *MIT Press and McGraw-Hill*, pp. 651–655, 2009.

[20] M. Marina and S. Das, "On-demand multipath distance vector routing in ad hoc networks," *in Proc. 9th International Conference on Network Protocols*, pp. 14–23, Nov. 2001.

[21] T. Ramrekha and C. Politis, "A hybrid adaptive routing protocol for extreme emergency ad hoc communication," *in Proc. International Conference on Computer Communications and Networks (ICCN), Zurich, Switzerland*, pp. 1–6, Aug. 2010.

[22] D. Eastlake, "Domain name system (dns) iana considerations," *IETF, RFC 6195*, Mar. 2011.

[23] D. Bryan, B. Lowekamp, and C. Jennings, "Sosimple: A serverless, standards-based, p2p sip communication system," *in Proc. 1st International Workshop on Advanced Architectures and Algorithms for Internet Delivery and Applications (AAA-IDEA), Orlando, FL*, pp. 42–49, Jun. 2005.

[24] E. Levy and A. Silberschatz, "Distributed file systems: Concepts and examples," *ACM Computing Surveys*, vol. 22, no. 4, pp. 321–374, Dec. 1990.

[25] M. Bisignano, G. Di Modica, O. Tomarchio, and L. Vita, "P2p over manet: a comparison of cross-layer approaches," *in Proc. Database and Expert Systems Applications (DEXA), IEEE, Regensburg, Germany*, pp. 814–818, Sep. 2007.

[26] H. Pucha, S. M. Das, and Y. C. Hu, "Ekta: An efficient dht substrate for distributed applications in mobile ad hoc networks," *in Proc. IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), Lake District, UK*, pp. 163–173, Dec. 2004.

[27] R. Schollmeier, I. Gruber, and F. Niethammer, "Protocol for peer-to-peer networking in mobile environments," *in Proc. International Conference on Computer Communications and Networks (ICCN), Texas, USA*, pp. 121– 127, Oct. 2003.

[28] M. Conti, E. Gregori, and G. Turi, "A cross-layer optimization of gnutella for mobile ad hoc networks," *in Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), Urbana-Champaign, IL, USA*, pp. 343–354, May 2005.

[29] B. Tang, Z. Zhou, A. Kashyap, and T. Chiueh, "An integrated approach for p2p file sharing on multi-hop wireless networks," *in Proc.of IEEE International Conference on Wireless And Mobile Computing, Networking And Communications (WiMob), Montreal, Canada*, vol. 3, pp. 268–274, Aug. 2005.

[30] T. Zahn and J. Schiller, "Madpastry: A dht substrate for practicably sized manets," *in Proc. Applications and Services in Wireless Networks (ASWN) Conference, Paris, France*, Jun. 2005.

[31] G. Millar, E. Panaousis, and C. Politis, "Robust: Reliable overlay based utilisation of services and topology for emergency manets," *in Proc. Future Network and Mobile-Summit, Florence, Italy*, pp. 1–8, Jun. 2010.

[32] K. Nadkarni and A. Mishra, "Intrusion detection in manets the second wall of defense," *in Proc. Annual Conference of the IEEE Industrial Electronics Society (IECON)*, vol. 2, pp. 1235–1238, Nov. 2003.

[33] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," *in Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), Boston, Massachusetts, USA*, pp. 275–283, Aug. 2000.

[34] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *in Proc.ACM MOBICOM*, pp. 255–265, 2000.

[35] W. Yu, Y. Sun, and K. Liu, "Hadof: defense against routing disruptions in mobile ad hoc networks," *in Proc. IEEE International Conference on Computer Communications (INFOCOM), Miami, FL, USA*, vol. 2, pp. 1252–126, Mar. 2005.

[36] J. Cabrera, C. Gutierrez, and R. Mehra, "Infrastructures and algorithms for distributed anomaly-based intrusion detection in mobile ad-hoc networks," *in Proc. IEEE Military Communications Conference (MILCOM), New Jersey, USA*, vol. 3, pp. 1831–1837, Oct. 2005.

[37] C. Xenakis, C. Panos, and I. Stavrakakis, "A comparative evaluation of intrusion detection architectures for mobile ad hoc networks," *Computers & Security, Elsevier*, vol. 30, no. 1, pp. 63–80, 2011.

[38] S. Şen and J. Clark, *Intrusion Detection in Mobile Ad Hoc Networks.* Springer, 2009, pp. 1–28.

[39] C. Papageorgiou, K. Birkos, T. Dagiuklas, and S. Kotsopoulos. Mission critical mobility model for mobile ad hoc networks in network simulator ns-2. [Online]. Available: http://www.wltl.ee.upatras.gr/humo/

[40] Y.-C. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defence against wormhole attacks in wireless networks," *in Proc. IEEE International Conference on Computer Communications (INFOCOM), California, USA*, vol. 3, pp. 1976–1986, Mar. 2003.

[41] J. Eriksson, S. Krishnamurthy, and M. Faloutsos, "Truelink: A practical countermeasure to the wormhole attack in wireless networks," *in Proc.IEEE ICNP*, pp. 75–84, Nov. 2006.

[42] F. Nait-Abdesselam, "Detecting and avoiding wormhole attacks in wireless ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 127–133, Apr. 2008.

[43] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," *in Proc. Network and Distributed System Security Symposium, San Diego, US*, Feb. 2004.

[44] H. S. Chiu and K.-S. Lui, "Delphi: wormhole detection mechanism for ad hoc wireless networks," *in Proc. 1st International Symposium on Wireless Pervasive Computing, Phuket, Thailand*, p. 6 pp., Jan. 2006.

[45] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," *in Proc. IEEE International Conference on Computer Communications (INFOCOM), Anchorage, Alaska, USA*, pp. 107–115, May 2007.

[46] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," *in Proc. 1st ACM workshop on Wireless security (WiSE), Atlanta, GA, USA*, pp. 1–10, Sep. 2002.

[47] S. Eichler and C. Roman, "Challenges of secure routing in manets: A simulative approach using aodv-sec," *in Proc. IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS), Vancouver, BC*, pp. 481–484, Oct. 2006.

[48] K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "Authenticated routing for ad hoc networks," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 23, no. 3, pp. 598–610, Mar. 2005.

[49] S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad hoc routing for wireless networks," *in Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), California, USA*, pp. 299–302, Oct. 2001.

[50] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," *in Proc. SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, Texas*, vol. 31, pp. 193–204, Jan. 2002.

[51] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *Wireless Networks, Kluwer Academic Publishers*, vol. 11, no. 1-2, pp. 21–38, Jan. 2005.

[52] S. Zhao, A. Aggarwal, S. Liu, and H. Wu, "A secure routing protocol in proactive security approach for mobile ad-hoc networks," *in Proc. IEEE Wireless Communications and Networking Conference (WCNC), Las Vegas, USA*, pp. 2627–2632, Apr. 2008.

[53] L. Buttyán and I. Vajda, "Towards provable security for ad hoc routing protocols," *in Proc. 2nd ACM workshop on Security of Ad hoc and Sensor Networks, Washington, USA*, pp. 94–105, Oct. 2004.

[54] A. Adnane, R. de Sousa, C. Bidan, and M. Ludovic, "Analysis of the implicit trust within the olsr protocol," *International Federation for Information Processing Digital Library, Trust Management, Springer Boston*, vol. 238, pp. 75–90, 2007.

[55] J. Cho, A. Swami, and I. R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys Tutorials*, vol. 13, no. 4, pp. 562–583, Quart. 2011.

[56] C. Adjih, T. Clausen, A. Laouiti, P. Muehlethaler, and D. Raffo, "Securing the olsr protocol," *in Proc. 2nd IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), Mahdia, Tunisia*, pp. 25–27, Jun. 2003.

[57] U. Herberg and T. Clausen, "Security issues in the optimized link state routing protocol version 2 (olsrv2)," *International Journal of Network Security & Its Applications*, pp. 162–181, May 2010.

[58] A. Hafslund, A. T¿nnesen, R. B. Rotvik, J. Andersson, and ¯ivind Kure, "Secure extensions to the olsr protocol," *In OLSR Interop Workshop, San Diego, USA*, Aug. 2004.

[59] *Olsr daemon*, 2012 (accessed Jan 30, 2012). [Online]. Available: http://www.olsr.org/

[60] D. Raffo, C. Adjih, T. Clausen, and P. Mühlethaler, "An advanced signature system for olsr," *in Proc. 2nd ACM workshop on Security of ad hoc and sensor networks (SASN), New York, USA*, pp. 10–16, 2004.

[61] B. Kannhavong, H. Nakayama, and A. Jamalipour, "Sa-olsr: Security aware optimized link state routing for mobile ad hoc networks," *in Proc. IEEE International Conference on Communications (ICC), Beijing, China*, pp. 1464–1468, May 2008.

[62] A. Fourati and K. Agha, "A shared secret-based algorithm for securing the OLSR routing protocol," *Telecommunication Systems, Springer*, vol. 31, no. 2-3, pp. 213–226, Mar. 2006.

[63] A. Hegland, P. Spillin, L. Nilsen, and ¯. Kure, "Hybrid protection of solsr," *in Proc. Workshop on Cryptography for Ad hoc Networks (WCAN), Venice, Italy*, Jul. 2006.

[64] M. Pužar, J. Andersson, T. Plagemann, and Y. Roudier, "Skimpy: A simple key management protocol for manets in emergency and rescue operations," *Security and Privacy in Ad-hoc and Sensor Networks, Springer*, vol. 3813, pp. 14–26, 2005.

[65] A. Fourati, K. Agha, and T. Claveirole, "Securing olsr routes," *Technologies for Advanced Heterogeneous Networks, Springer Berlin / Heidelberg*, vol. 3837, pp. 183–194, 2005.

[66] P. Papadimitratos and Z. J. Haas, "Secure link state routing for mobile ad hoc networks," *in Proc. Symposium on Applications and the Internet Workshops (SAINT), IEEE, Orlando, FL, USA*, pp. 379–383, Jan. 2003.

[67] D. Chopra, H. Schulzrinne, E. Marocco, and E. Ivov, "Peer-to-peer overlays for real-time communication: security issues and solutions," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, pp. 4–12, First Quarter 2009.

[68] Y. Mao, V. Narayanan, A. Swaminathan, and I. Qualcomm, "Threat analysis for peer-to-peer overlay networks," *IETF, Internet-Draft*, Sep. 2009.

[69] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," *in Proc. IEEE International Conference on Computer Communications (INFOCOM), Barcelona, Spain*, pp. 1–13, Apr. 2006.

[70] A. Banerjee and C.-T. King, "Building ring-like overlays on wireless ad hoc and sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 11, pp. 1553–1566, Nov. 2009.

[71] M. Osborne and A. Rubinstein, *A course in game theory*. The MIT press, 1994.

[72] N. Nisan, T. Roughgarden, E. Tardos, and V. V. Vazirani, *Algorithmic Game Theory*. New York, NY, USA: Cambridge University Press, 2007.

[73] J. Nash, "Non-cooperative games," *Annals of mathematics*, vol. 54, no. 2, pp. 286–295, 1951.

[74] A. Patcha and J. Park, "A game theoretic approach to modeling intrusion detection in mobile ad hoc networks," *in Proc.IEEE IWIA*, pp. 280–284, Jun. 2004.

[75] ——, "A game theoretic formulation for intrusion detection in mobile ad hoc networks," *Int. Journ. of Netw. Sec.*, vol. 2, no. 2, pp. 131–137, 2006.

[76] A. Agah, K. Basu, and S. Das, "Security enforcement in wireless sensor networks: A framework based on non-cooperative games," *Pervasive and Mobile Computing, Elsevier*, vol. 2, no. 2, pp. 137–158, 2006.

[77] Y. Liu, C. Comaniciu, and H. Man, "A bayesian game approach for intrusion detection in wireless ad hoc networks," *in Proc. International Conference on Game Theory for Networks (GAMENETS), Pisa, Italy*, p. Article 4, Oct.. 2006.

[78] ——, "Modelling misbehaviour in ad hoc networks: A game theoretic approach for intrusion detection," *Int. Journ. Security Netw.*, vol. 1, no. 7, pp. 243–254, Jun. 2006.

[79] H. Otrok, M. Debbabi, C. Assi, and P. Bhattacharya, "A cooperative approach for analyzing intrusions in mobile ad hoc networks," *in Proc. IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW), Washington, USA*, Jun. 2007.

[80] N. Marchang and R. Tripathi, "A game theoretical approach for efficient deployment of intrusion detection system in mobile ad hoc networks," *in Proc. International*

Conference on Advanced Computing and Communications (ADCOM), India, pp. 460–464, Dec. 2007.

[81] N. Santosh, R. Saranyan, K. Senthil, and V. Vetriselvi, "Cluster based co-operative game theory approach for intrusion detection in mobile ad-hoc grid," *in Proc. International Conference on Advanced Computing and Communications (ADCOM), IEEE, Chennai, Bangalore*, pp. 273–278, Dec. 2008.

[82] M. Seredynski and P. Bouvry, "Evolutionary game theoretical analysis of reputation-based packet forwarding in civilian mobile ad hoc networks," *in Proc. IEEE International Parallel & Distributed Processing Symposium (IPDPS), Rome, Italy*, pp. 1–8, May 2009.

[83] H. Otrok, N. Mohammed, L. Wang, M. Debbabi, and P. Bhattacharya, "A game-theoretic intrusion detection model for mobile ad hoc networks," *Computer Communications, Elsevier*, vol. 31, no. 4, pp. 708–721, 2008.

[84] J. Daemen and V. Rijmen, *The Design of Rijndael AES - The Advanced Encryption Standard*. Springer-Verlag New York, 2002.

[85] H. Yin and H. Wang, "Building an application-aware ipsec policy system," *IEEE/ACM Transactions on Networking*, vol. 15, no. 6, pp. 1502–1513, Dec. 2007.

[86] L. DaSilva, S. Midkiff, J. Park, G. Hadjichristofi, N. Davis, K. Phanse, and T. Lin, "Network mobility and protocol interoperability in ad hoc networks," *IEEE Communications Magazine*, vol. 42, no. 11, pp. 88–96, Nov. 2004.

[87] A. Hegland and E. Winjum, "Securing qos signalling in ip-based military ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 42–48, Nov. 2008.

[88] S. Kent and K. Seo, "Security architecture for the internet protocol," *IETF, RFC 4301*, Dec. 2005.

[89] "Fips 197: Advanced encryption standard (aes)," *Federal Information Processing Standards Publication*, vol. 197, pp. 441–0311, Nov. 2001.

[90] C. Xenakis, N. Laoutaris, L. Merakos, and I. Stavrakakis, "A generic characterization of the overheads imposed by ipsec and associated cryptographic algorithms," *Computer Networks, Elsevier North-Holland, Inc.*, vol. 50, no. 17, pp. 3225–3241, 2006.

[91] O. Elkeelany, M. Matalgah, K. Sheikh, M. Thaker, G. Chaudhry, D. Medhi, and J. Qaddour, "Performance analysis of ipsec protocol: encryption and authentication," *in Proc. IEEE International Conference on Communications (ICC), NY, USA*, vol. 2, pp. 1164–1168, Apr. 2002.

[92] M. Grossglauser and D. Tse, "Mobility increases the capacity of ad hoc wireless networks," *IEEE/ACM Transactions on Networking*, vol. 10, no. 4, pp. 477–486, 2002.

[93] Y. Joung, L. Yang, and C. Fang, "Keyword search in dht-based peer-to-peer networks," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 25, no. 1, pp. 46–61, Jan. 2007.

[94] "Ieee standard 802.11-1007, wireless lan medium access control (mac) and physical layer (phy) specifications," *LAN MAN Standards Committee, IEEE Computer Soc.*, 1999.

[95] S. Rhea, D. Geels, T. Roscoe, and J. Kubiatowicz, "Handling churn in a dht," *in Proc. Annual conference on USENIX Annual Technical Conference (ATEC). , Boston, MA*, Jun. 2004.

[96] L. Barolli, M. Ikeda, F. Xhafa, and A. Duresi, "A testbed for manets: Implementation, experiences and learned lessons," *IEEE Systems Journal*, vol. 4, no. 2, pp. 243–252, Jun. 2010.

[97] D. Kim, H. Bae, and C. K. Toh, "Improving tcp-vegas performance over manet routing protocols," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 1, pp. 372–377, Jan. 2007.

[98] W. Yu and K. Liu, "Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 5, pp. 507–521, May 2007.

[99] L. M. Feeney, "An energy consumption model for performance analysis of routing protocols for mobile ad hoc networks," *Mobile Networks and Applications*, vol. 6, no. 3, pp. 239–249, 2001.

[100] J. Yoon, M. Liu, and B. Noble, "Sound mobility models," *in Proc. ACM Annual International Conference on Mobile Computing and Networking (MobiCom), San Diego, California, USA*, pp. 205–216, Sep. 2003.

[101] C. Li, C. Yang, and M. Hwang, "A secure routing protocol with node selfishness resistance in manets," *International Journal of Mobile Communications*, vol. 10, no. 1, pp. 103–118, 2012.

[102] A. Banerjee, D. Bose, A. Bhattacharyya, H. Saha, and D. Bhattacharyya, "Administrator and trust based secure routing in manet," *in Proc. International Conference on Advances in Mobile Network, Communication and its Applications (MNCAPPS)*, pp. 39–45, 2012.

[103] S. Zhao, R. Kent, and A. Aggarwal, "An integrated key management and secure routing framework for mobile ad-hoc networks," *in Proc. 10th IEEE Annual International Conference on Privacy, Security and Trust (PST), Paris, France*, pp. 96–103, 2012.

[104] D. Bose, A. Banerjee, A. Bhattacharyya, H. Saha, D. Bhattacharyya, and P. Banerjee, "An efficient approach to secure routing in manet," *Advances in Computing and Information Technology*, pp. 765–776, 2012.

[105] P. John and P. Vivekanandan, "A framework for secure routing in mobile ad hoc networks," 2012, pp. 453–458.

[106] S. Dabideen and J. Garcia-Luna-Aceves, "Secure routing in manets using local times," *Wireless Networks*, pp. 1–16, 2012.

[107] M. Bansal and C. Pujara, "Secure routing of data packets in manet on basis of fidelity concept," *International Journal of Research in Computer Engineering & Electronics*, vol. 1, no. 1, 2012.

[108] H. R. Pous, E. Panaousis, and C. Politis, "Recipients' anonymity in multihop ad-hoc networks," *IEICE Transactions on Information Systems, Special section on Trust, Security and Privacy in Computing and Communication Systems*, vol. E95-D, no. 1, pp. 181–184, Jan. 2012.