OPTIMAL PLACEMENT AND POWER ALLOCATION FOR JAMMERS IN WIRELESS MESH NETWORKS

by

Shruti Lall

Submitted in partial fulfillment of the requirements for the degree

Master of Engineering (Electronic Engineering)

in the

Department of Electrical, Electronic and Computer Engineering
Faculty of Engineering, Built Environment and Information Technology
UNIVERSITY OF PRETORIA

August 2015

SUMMARY

OPTIMAL PLACEMENT AND POWER ALLOCATION FOR JAMMERS IN WIRELESS MESH NETWORKS

by

Shruti Lall

Supervisor(s):	Prof. B. T. Maharaj and Prof. A. S. Alfa
Department:	Electrical, Electronic and Computer Engineering
University:	University of Pretoria
Degree:	Master of Engineering (Electronic Engineering)
Keywords:	jammer placement, jammer power allocation, optimisation, wireless jammers, wireless mesh networks, wireless network security

Wireless networks are gaining widespread use and popularity because of their progressive increase in affordability and convenience. Owing to the improved facilitation of communication and data transfer, wireless networks are being deployed in numerous modalities, ranging from wireless local area networks, to mesh and sensor networks. Wireless Mesh Networks (WMNs) have numerous applications in both civilian and military based environments. The main disadvantage of WMNs is its susceptibility to interference and eavesdroppers that are able to intercept, and listen in on the communication between devices in the networks. Eavesdroppers can act as non-lethal weapons to combatants at war and can have dire consequences if vital information is obtained by the adversaries. As a result of the emerging and prevalent use of WMNs in military domains, protecting information contained in networks is of utmost importance in this information driven age.

This study proposes a novel physical-layer based security method that utilises jammers to generate additional interference for devices that are eavesdropping on wireless network communication. The most popular method for ensuring data confidentiality is through the use of cryptographic techniques; however, as a result of the decentralised nature and power limited network nodes of WMNs, the protection scheme precludes the use of any cryptographic techniques and is only physical-layer based. The scheme involves the intelligent placement of continuous jammers in order to achieve maximum protection and data confidentiality for WMNs with multiple eavesdroppers, sources and destinations. Furthermore, the scheme is optimised in terms of the transmitting power associated with each jammer, so that the energy expended by the jammers is kept at a minimum.

The security method is modelled as a minimisation mixed integer non-linear problem, and is approximated as the sequential solution of two linear optimisation sub-problems relating to the placement, and power allocation of the wireless jammers. The proposed security model is subject to constraints which ensure that sufficient interference is generated for malicious devices that seek to obtain confidential information, while legitimate communication within the network is not affected. The placement of the jammers takes the form of a multiple demand multi-dimensional knapsack problem with a minimisation objective. The power allocation problem is modelled as a linear real-valued minimisation optimisation problem. The branch-and-cut method, and the simplex method are the algorithms used for solving the placement and power allocation problems respectively. In the effort to reduce the computation time associated with solving the linear integer jammer placement problem, an alternating control tree based heuristic is also developed. The performance of the proposed security method and heuristic are evaluated through appropriate simulations conducted on random network instances.

The performance of the proposed security scheme is shown for a number of different scenarios with varying parameters. The branch-and-cut algorithm is used to solve various cases of the jammer placement sub-problem while altering parameters such as the grid size, the number of legitimate nodes, the number of malicious eavesdropping nodes and the locations of potential jammers. The heuristic is successfully applied to large networks, demonstrating the scalability of the implementation. The performance in terms of the solution provided and the computation time associated with use of the heuristic, in comparison to the branch-and-cut algorithm, is also shown. The heuristic can perform up to 60 times faster than the branch-and-cut method depending on the particular network instance, while returning a solution that is within 10% of the optimal solution. The use of the heuristic proves to be imperative in real-life large network scenarios, where an acceptable solution needs to be obtained with a low execution time. It can therefore be concluded, that for small network scenarios, where optimality in terms of the number of jamming devices required to protect an area is critical, the branch-and-cut method should be implemented. However, in scenarios where the execu-

tion time is critical, the heuristic can be used to obtain a reasonable solution within a small time limit.

OPSOMMING

OPTIMALE PLASING EN KRAGTOEKENNING VIR STOORSENDERS IN DRAADLOSE MAASNETWERKE

deur

Shruti Lall

Studieleier(s):	Prof. B. T. Maharaj and Prof. A. S. Alfa
Departement:	Elektriese, Elektroniese en Rekenaar-Ingenieurswese
Universiteit:	Universiteit van Pretoria
Graad:	Magister in Ingenieurswese (Elektroniese Ingenieurswese)
Sleutelwoorde:	stoorsenderplasing, stoorsenderkragtoekenning, optimering, draadlose stoorsenders, draadlose maasnetwerke, draadlose-netwerksekuriteit

Draadlose netwerke is gewild en word algemeen gebruik, omdat hulle bekostigbaar en gerieflik is. Danksy die verbeterende fasilitering van kommunikasie en data-oordrag, word draadlose netwerke in talle modaliteite, wat wissel van plaaslike-areanetwerke tot maas- en sensor-netwerke, ontplooi. Draadlose maasnetwerke het in beide burgerlike en militêr-gebaseerde omgewings talle toepassings. Die grootste nadeel van maasnetwerke is hulle vatbaarheid vir inmenging en afluisteraars, wat in staat is om na kommunikasie tussen toestelle op die network te luister en inligting so te onderskep. Afluisteraars kan optree as nie-dodelike wapens in die oorlog en ernstige skade aanrig deur belangrike inligting aan die vyand bekend te maak. As gevolg van die ontwikkeling en algemene gebruik van draadlose maasnetwerke vir militêre toepassings in hierdie inligting-gedrewe tyd, is die beskerming van inligting vervat in hierdie netwerke van die uiterse belang.

Hierdie studie stel 'n nuwe fisiese laaggebaseerde sekuriteitsmetode voor wat gebruik maak van stoorsenders om inmenging teen toestelle wat afluister op die netwerk te veroorsaak. Die gewildste metode om vertroulikheid van data te verseker, is die gebruik van kriptografiese tegnieke, maar as gevolg van die gedesentraliseerde aard van die draadlose maasnetwerke en hul kragbeperkte netwerknodes kan kriptografiese tegnieke nie gebruik word nie, daarom word dit beperk tot fisiese laaggebaseerde beskerming. Die skema behels die strategiese plasing van intelligente, deurlopende stoorsenders om maksimum beskerming en vertroulikheid van data vir draadlose maasnetwerke - met verskeie afluisteraars, bronne en bestemmings - te verseker. Die skema is verder geoptimeer met betrekking tot die transmissiekrag van elke stoorsender, om die minimum energieverbruik te verseker.

Die sekuriteitsmetode is gemodelleer as ’n minimerende, gemengde-heelgetal-, nie-lineêre probleem en word benader as die opeenvolgende oplossing van twee lineêre optimeringsubprobleme met betrekking tot die plasing en die kragtoekenning van die stoorsenders. Die voorgestelde sekuriteitsmodel is onderhewig aan beperkings, wat verseker dat voldoende inmenging genereer word teen kwaadwillige toestelle wat poog om vertroulike inligting te bekom, terwyl wettige kommunikasie binne die netwerk onaangeraak bly. Die plasing van die stoorsenders neem die vorm van ’n meervoudigevraag-, multi-dimensionele knapsakprobleem aan, met ’n verminderingsdoelwit. Die kragtoekenningprobleem is gemodelleer as ’n lineêre, reëlwaardige minimering-optimeringprobleem. Die tak-en-snymetode en die simpleksmetode is die algoritmes wat onderskeidelik gebruik word om die oplossings van die plasing- en kragtoekenningprobleem te verkry. Om die berekeningstyd van die oplossing vir die lineêre heelgetalstoorsenderplasingprobleem te verminder, is ’n wisselende beheerboomgebaseerde heuristiek ook ontwikkel. Die werksverrigting van die voorgestelde sekuriteitsmetode en heuristiek is geëvalueer deur geskikte simulasies op ewekansige netwerkvoorbeelde uit te voer.

Die werksverrigting van die voorgestelde sekuriteitskema word getoon vir ’n aantal verskillende gevalle met wisselende grense. Die tak-en-sny-algoritme word gebruik om verskeie gevalle van die stoorsenderplasingsubprobleem op te los, terwyl grense soos die grootte van die rooster, die aantal wettige nodes, die aantal kwaadwillige meeluisteringnodis en die posisies van potensiële stoorsenders verander word. Die heuristiek is suksesvol aangewend op groot netwerke en illustreer dus die skaalbaarheid van die oplossing. Die werksverrigting van die oplossing en die berekeningstyd, wat verband hou met die gebruik van die heuristiek, in vergelyking met die tak-en-sny-algoritme, word ook getoon. Die heuristiek kan tot 60 keer vinniger as die tak-en-snymetode bereken, afhangend van die spesifieke netwerk, en lewer ’n oplossing wat binne 10% van die optimale oplossing is. Die gebruik van die heuristiek is noodsaaklik vir groot netwerke in die werklike lewe waar ’n aanvaarbare oplossing binne ’n kort tyd verkry moet word. Gevolglik moet die tak-en-snymetode vir klein netwerke geïmplementeer word, waar optimaliteit van die aantal storingtoestelle wat nodig is om ’n gebied te

beskerm van kritieke belang is. In gevalle waar die uitvoertyd belangrik is, kan die heuristiek gebruik word om 'n redelike oplossing in 'n kort tydperk te kry.

ACKNOWLEDGEMENTS

I would like to extend my sincerest gratitude to the following people and organisations for their assistance:

- My supervisor and mentor, Prof B.T. Maharaj for his expert guidance and support.
- My co-supervisor and advisor, Prof A.S. Alfa for his invaluable insight and guidance.
- The Sentech Chair in Broadband Wireless Multimedia Communication (BWMC) at the University of Pretoria, and the South African Research Chairs Initiative (SARChI) for their financial support.
- My friends and colleagues of the BWMC group for their insightful suggestions and support.
- My parents and sister, Khushi, for their unconditional love and encouragement.

LIST OF ABBREVIATIONS

ACT	Alternating Control Tree
AODV	Adhoc On Demand Distance Vector
CVaR	Conditional Value-at-Risk
DO	Distributed Operation
DoS	Denial of Service
HWMP	Hybrid Wireless Mesh Protocol
IP	Internet Protocol
JPP	Jammer Placement Problem
MAC	Media Access Control
MAP	Mesh Access Point
MP	Mesh Point
MPP	Mesh Portal
MSDU	MAC Service Data Units
NCW	Network Centric Warfare
OLSR	Optimized Link State Routing
PERR	Path Error
PMK	Pairwise Master Key
PREP	Path Reply
PREQ	Path Request
RA-OLSR	Radio aware optimized link state routing
RANN	Root Announcement
SAE	Simultaneous Authentication of Equals
SIR	Signal-to-Interference Ratio
SNR	Signal to Noise Ratio
STA	Station
VaR	Value-at-Risk
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WMN	Wireless Mesh Network
WSN	Wireless Sensor Network

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

Wireless networks are gaining widespread use and popularity because of their progressive increase in affordability and convenience. Owing to the improved facilitation of communication and data transfer, wireless networks are being deployed in numerous modalities, ranging from wireless local area networks to mesh and sensor networks [1]. Wireless networks are often seen as a more attractive option to their wired network counterpart due to their increased mobility, expandability, cost efficiency and ease of integration. As a result of the need for mobility, data is broadcast using radio technology, which implies that any unintended receiver in range will be able to listen in on the transmission and thus compromise network confidentiality.

Wireless Mesh Networks (WMNs) have numerous applications in both civilian and military based environments. They are ideal for the formation of communication networks in rural areas where there is a lack of infrastructure because of its low set-up cost and easy scalability. In the military domain, WMNs offer an efficient solution for the deployment of military tactical networks. The networks need to be resilient and be able to withstand harsh propagation channels and interference, as well as constant changes in the network topology. The primary application of WMNs is for sending out information related to troops positions and conditions; this is termed as situational awareness communications. WMNs are rapidly gaining popularity in military functional areas including intelligence, war fighting and logistics, to exchange vital information between separate small units and operation centers in a quick and optimal way.

The main disadvantage of WMNs is its susceptibility to interference and eavesdroppers that are able to intercept and listen in on the communication between the devices in the networks. Eavesdroppers can act as non-lethal weapons to combatants at war and can have dire consequences if vital information is obtained by the adversaries. Owing to the emerging and prevalent use of WMNs in military domains, protecting the information contained in the networks is of utmost importance in this information driven age. A physical layer based protection mechanism is achieved through the deployment of jammers which are used to ensure private communication within networks.

The security method proposed in this study is used to maintain data confidentiality in WMNs through the use of protective jammers which generate interference for eavesdroppers, thereby preventing them from obtaining any meaningful information. The proposed scheme seeks to overcome the weaknesses evident in cryptographic based protection methods by strategically placing protective jammers in order to enhance the security of WMNs. The efficiency of the scheme is increased by minimising the number of jammers required to protect an area and reducing the power consumption levels of the jamming devices. The proposed security model is subject to constraints which ensure that sufficient interference is generated for malicious devices that seek to obtain confidential information, while legitimate communication within the network is not affected. In the effort to reduce the computation time associated with the implementation of the proposed method, an alternating control tree (ACT) search based heuristic is also developed for solving the jammer placement problem.

1.2 RESEARCH OBJECTIVE

Protecting communication within networks is of utmost importance especially in environments where information is critical, and loss thereof can result in disastrous consequences. Although cryptographic techniques are able to provide authentication and confidentiality in wireless ad hoc networks, a prominent challenge in securing WMNs, as opposed to other ad hoc networks, is accounting for the numerous different technologies in the network nodes as well as dealing with the heterogeneous nature of the network. With the emergence of ad hoc and decentralised networks, providing security at the physical layer, in contrast to cryptographic techniques which are applied at the higher layers, has been of interest [2]. Another reason why physical layer security has been gaining attention is that the wireless nodes are not completely immune to the effects of eavesdroppers or relay attacks when encryption methods are utilised; this is because the network can still be eavesdropped upon during the key exchange process, thereby defeating the purpose of encryption.

Physical layer security aims to maximise the rate of reliable information from the source to the destination while maintaining data confidentiality against eavesdroppers. The maximum reliable rate is termed as the "secrecy capacity". The secrecy capacity of a communication channel can be improved by increasing the signal to noise ratio (SNR) of the destination node or by decreasing the SNR of the eavesdropper. The SNR at the destination node can possibly be improved by shortening the distance between source and destination, however this is generally not feasible. Thus, in order to reduce the SNR at the eavesdropper, a suitable method would be the deployment of jamming devices which are capable of inducing controlled inference in the eavesdropper's channel.

In this case, the jamming is termed as being *friendly* or *protective*. Friendly jammers are used as a way of providing physical layer security by protecting the wireless networks against information leakage. In the literature studied relating to the use of friendly jammers and the minimisation of their power consumption, it was assumed that the friendly jammers were placed far enough from the receivers or destination nodes to have any detrimental effect on the communication channel in which, the data that it wishes to protect, resides. It is simply considered as a trade-off in the power allocation strategies for friendly jammers [3]. However, in practical scenarios, there is bound to be induced interference from the friendly jammer and it is not always possible to control it so that the SNR at the destination is maintained, especially in multiple source, eavesdropper and destination scenarios. The placement and the effect that the friendly jammers have on legitimate communication needs to be taken into account.

The primary objective of this work is to develop a novel physical-layer based security scheme that is able to provide data confidentiality for WMNs with multiple sources, destinations and eavesdroppers. The scheme utilises friendly jammers that are optimally placed to offer WMNs protection against interspersed malicious devices that seek to obtain confidential information from communicating nodes. The scheme also involves optimisation for the power consumption of the jammers. By carefully placing jammers to protect a particular WMN, the number of jammers can significantly be reduced while still being able to provide high levels of security. The power consumption of each jammer is also subject to a number of constraints so that the legitimate communication within the network is not affected by the jammers. Optimising the power levels associated with each jammer lowers the cost and increases the efficiency of the scheme. The development of the scheme involves the formulation of accurate mathematical models that encapsulate all related parameters and constraints. The efficiency of the scheme is greatly influenced by the algorithms and techniques used to solve the corresponding optimisation models. The study also aims to propose and develop suitable methods and heuristics for solving the associated mathematical programming models.

1.3 CONTRIBUTION

A novel method of utilising jammers to protect WMNs against eavesdropper nodes in a multi-hop network with multiple sources, destinations and eavesdroppers is proposed. A mathematical model is developed for the joint optimal placement and power allocation of the wireless jammers. The model takes into account not only the effect that the jammers have on the malicious nodes, but also the impact they have on the communicating nodes. Measures are taken to prevent the jammers from having any ill-effect on the communication channels they are protecting. This is achieved through the careful placement of the jammers so that network continuity is maintained, while the principal purpose of degrading the eavesdroppers channel through controlled interference, is accomplished. The jammers are used to exploit the physical characteristics of the wireless channel in order to provide secure communication. The protection scheme precludes the use of any cryptographic techniques and is only physical-layer based.

Focus has been placed on the ease of practical implementation of the proposed scheme as no additional computation or complexity is required from the legitimate communication nodes; only the intelligent placement of simple continuous jammers is needed to achieve maximum protection. The scheme is further optimised in terms of the transmitting power associated with the jammers so that the energy expended through use of the jammers is kept at a minimum. This work is largely targeted for protecting wireless networks in military domains which are very flexible and uncertain. Furthermore, a heuristic for solving the jammer placement sub-problem, which is modelled as a multiple demand multi-dimensional knapsack problem with a minimisation objective, is proposed to increase the efficiency of the proposed security scheme. To the best of our knowledge, there has not been any work to date, jointly addressing protective jammer placement and power allocation which is used for the effective and efficient protection of multi-hop military-based networks with multiple sources, destinations and eavesdroppers.

1.4 DISSERTATION OUTLINE

A novel physical-layer based security method that utilises jammers to generate additional interference for devices that are eavesdropping on wireless network communication is proposed in this dissertation. The security method is modelled as a minimisation mixed integer non-linear problem and is approximated as the sequential solution of two linear optimisation sub-problems relating to the placement and power allocation of the wireless jammers. The placement of the jammers takes the form of a multiple demand multi-dimensional knapsack problem with a minimisation objective. The power allocation problem is modelled as a linear real-valued minimisation optimisation problem. The branch-and-cut method and simplex method are the algorithms used for solving the placement and power allocation problems respectively. In the effort to reduce the computation time associated with solving the integer linear jammer placement problem, an alternating control tree based heuristic is developed. The performance of the proposed security method and heuristic are evaluated through appropriate simulations conducted on random network instances.

Chapter 2 gives an overview of WMNs and their various applications. The IEEE 802.11s standard detailing the protocol for WMNs, as well as the usage scenarios relating to both civilian and military environments, are discussed. Aspects relating to the routing protocol, the mesh architecture and the current security mechanisms recommended by the standard are explained. The security methods make use of cryptographic techniques that reside in the network layer. The work presented in this dissertation, however, aims to overcome the weaknesses inherent with the use of cryptographic techniques by enhancing the security of WMNs through a physical-layer based method. The method is designed with emphasis placed on applications of WMNs in military environments where the value of the tactical information is considerably higher. The designed method can also easily be applied in civilian applications, given that the most difficult of the environments to protect is in a military domain. The importance and various uses of WMNs in military environments are further elaborated upon in this chapter. The principles of network centric warfare (NCW) related to maintaining information superiority are discussed.

Chapter 3 reviews literature pertaining to the placement and power allocation of jammers. The need for the protection of WMNs is highlighted as a result of the application in environments where security is of utmost importance. Current methods of protecting wireless networks are presented. The most popular method for ensuring data confidentiality is through the use of cryptographic techniques; however, as a result of the decentralised nature and power limited network nodes of WMNs, physical-layer based methods such as jamming are considered. Literature on optimisation techniques used with regard to the placement and the power allocation of jammers is also further elaborated upon.

Chapter 4 provides a mathematical formulation, based on optimisation theory, of the proposed method of protecting wireless networks against malicious nodes that seek to obtain confidential information. The problem is modelled as a non-linear minimisation problem that jointly addresses the optimal placement and power allocation of wireless jammers in a multi-hop network with multiple sources, eavesdroppers and destinations. The network environment upon which the problem is modelled after, is one which aims to closely represent the highly mobile, non-deterministic nature of WMNs in military battlefields. This was described in the usage scenarios of the IEEE 802.11s standard in chapter 2. Owing to the difficulty and computational intensive nature of non-linear problems, the problem is linearised by approximating the joint non-linear problem as two separate linear problems that are sequentially solved. The first of which, is used to address the problem of determining and placing a minimum number of jammers to protect a multiple source and destination network. This jammer placement sub-problem is modelled as a multiple demand multi-dimensional knapsack problem.The power allocation sub-problem is a real valued linear minimisation problem with constraints ensuring the power values allocated to the jammers, are sufficient to protect the wireless network without the need of any additional wireless jammers.

In chapter 5, the different optimisation techniques that are used in solving the optimisation problems formulated in chapter 4, are discussed. The simplex method, which is the most popular and efficient method for solving linear real-valued problems, is used for solving the power allocation problem. Exact algorithms associated with solving integer optimisation problems, are discussed. The method selected for solving the integer jammer placement sub-problem is the branch-and-cut method; this method seeks to improve upon the popular branch-and-bound method with the additional use of cutting planes. Furthermore, a heuristic for solving the integer jammer placement sub-problem is developed in order to increase the efficiency of the proposed security scheme. Although the branch-and-cut method is fairly effective in obtaining the optimal solution for integer optimisation problems, the computational complexity and execution time associated for solving large problems, decreases the efficiency of the algorithm. In military environments especially, it is necessary to obtain solutions in a fast manner given the criticality associated with the information exchanged. An alternating control tree (ACT) structure based heuristic is developed for solving the multiple demand multi-dimensional knapsack problem with a minimisation objective that is associated with the placement of the wireless jammers.

Chapter 6 illustrates the performance of the proposed security scheme for a number of different scenarios with varying parameters. The branch-and-cut algorithm is used to solve various cases of the jammer placement sub-problem while altering parameters such as the grid size, the number of legitimate nodes, the number of malicious eavesdropping nodes and the locations of potential jammers. The results pertaining to solving the jammer placement sub-problems using the ACT-based heuristic are shown for large network sizes. The performance in terms of the solution provided and the computation time associated with use of the heuristic, in comparison to the branch-and-cut algorithm, is graphically shown. The results of optimising the transmitting power of the selected wireless jammers are shown for varying networks where the placement of jammers have been determined through the application of the jammer placement sub-problem. The performance of the entire scheme, which involves the optimal placement and power allocation, are shown for a number of different random network scenarios. The proposed security scheme is also compared to similar work regarding protective jammer placement.

1.5 PUBLICATIONS

This section describes a list of peer reviewed conference and institute for scientific information accredited web of science journal papers. The publications deal with the optimal placement and power allocation of jammers in wireless mesh networks.

1.5.1 Conference Proceedings

The following conference paper has been published in the proceedings for the IEEE Vehicular Technology Conference (VTC2015-Fall).

S. Lall, A. S. Alfa and B. T. Maharaj, "Optimal Placement and Power Allocation for Jammers in Wireless Mesh Networks," in*Proc. IEEE Vehicular Technology Conference*, Boston, MA, Sep. 2015.

1.5.2 Journal Article

The following journal article was submitted to the *Wireless Personal Communications* journal for publication. The work presented in this paper is based on the work presented in this research project.

S. Lall, A. S. Alfa and B. T. Maharaj, "Optimal Placement and Power Allocation for Jammers in Wireless Mesh Networks," *Wireless Personal Communications*, Aug. 2015, in review.

CHAPTER 2

WIRELESS MESH NETWORKS

2.1 INTRODUCTION

WMNs are networks which consist of peer-to-peer wireless mobile node interconnections that collectively form an intelligent, large-scale and broadband wireless network. These networks are ad hoc in nature with no fixed infrastructure and as a result, the wireless mesh nodes are self-organising and self-configuring. The wireless mesh nodes are responsible for maintaining connectivity amongst each other and can serve as both the transmitter and receiver. A typical WMN is shown in figure 2.1. The network is made up of numerous mesh clients in the form of PCs and mobile devices, as well as a collection of wireless access routers. WMNs are therefore heterogeneous and consist of two types of nodes, namely, mesh clients and mesh routers. The wireless communication standard that is most often used between the wireless nodes is based on the IEEE 802.11 standard. The routing of packets occurs through multiple intermediary hops, as opposed to long distance forwarding. There are a number of routing algorithms that have been proposed for routing packets across mesh networks which fall into proactive, reactive or hybrid categories. A proactive routing protocol is one in which each node maintains, at all times, a routing table containing possible routes. Alternatively, a reactive protocol discovers routes only when needed. A hybrid routing protocol is proactive when routing packets over short distances and reactive over long distances. As with clients in any type of network, wired or wireless, end-to-end communication services of applications are provided by transport layer protocols.

As a result of the lack of infrastructure, such networks are easy to deploy and maintain [4]. Connections between nodes are formed based on the node's coverage area. The coverage area is the area around the node in which it is able to transmit and receive data directly to or from another node. Depending on whether the nodes are equipped with omnidirectional or directional antennas, the coverage area will differ. If another wireless node is within the coverage area, a direct link is formed and so, the ad hoc wireless mesh topology is generated. In comparison to traditional wireless networks which make use of a base station to disseminate information through the network, the larger area coverage that can be achieved by spreading the mesh nodes will be attained at a lower transmission power [5]. The nodes in the network can utilise various wireless access technologies such as wireless fidelity (Wi-Fi) or worldwide interoperability for microwave access (WiMAX).

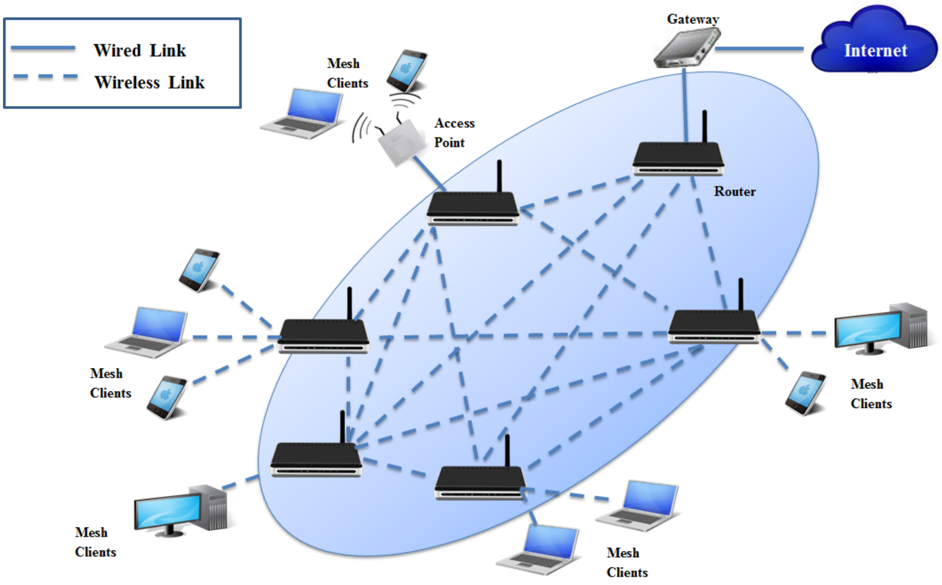

Figure 2.1: Typical wireless mesh network

2.2 APPLICATIONS

WMNs have numerous applications in both civilian and military based environments. As a result of its low-cost set-up and scalability, they are ideal for the formation of communication networks in rural areas where there is a lack of infrastructure [6]. It can also be used as alternative means of providing network services to clients in metropolitan areas [7]. Security surveillance systems can be configured as a WMN which are able to effectively transfer security relevant multimedia content amongst the mesh clients [8]. WMNs are suited for areas in which wired and standard WLANs are not feasible, such as in the industrial domain, in which WMNs can be used to connect machinery in rough surroundings [9]. Rapidly changing areas, such as disaster or emergency prone areas where communication becomes vital, the need for a quick and efficient set-up of a network arises. WMNs prove to be pivotal in such a scenario as it is able to provide more bandwidth resources than other wireless or mobile ad hoc networks [10].

In the military domain, WMNs offer an efficient solution for the deployment of military tactical networks [11]. The networks need to be resilient and be able to withstand harsh propagation channels and interference, as well as constant changes in the network topology. The primary applications of WMNs are for sending out information related to troops positions and conditions; this is termed as situational awareness communications. Before the use of WMNs in the military, critical orders and battlefield information were relayed through the use of line-of-sight radios and voice communications; however, as a result of the earth's terrain and other obstructions, it did not prove to be a viable solution. The U.S. Military uses WMNs as a way of overcoming the problems inherent with the use of line-of-sight devices [12]. Mesh networks are also being used for providing the U.S. armys logistics and sustainment personnel with high-speed, robust communication capabilities. WMNs are rapidly gaining popularity in military functional areas including intelligence, war fighting and logistics, to exchange vital information between separate small units and operation centers in a quick and optimal way.

The main disadvantage of WMNs is its susceptibility to interference and eavesdroppers that are able to intercept and "listen" in on the communication between the devices in the networks. Eavesdroppers can act as non-lethal weapons to combatants at war and can have dire consequences if vital information is obtained by adversaries. Owing to the emerging and prevalent use of WMNs, protecting the information contained in the networks is of utmost importance in this information driven age.

2.3 PROTOCOL OVERVIEW: IEEE 802.11S

WMNs are defined by IEEE through an amendment to the IEEE 802.11 standard termed as the IEEE 802.11s standard [13]. The amendment integrates mesh networking service and protocols with the IEEE 802.11 standard for WLANs at the media access control (MAC) layer. The amendment details the architecture and protocols that supports the creation of a wireless distribution system with automatic topology learning and wireless path configuration [14].

WMNs are basically formed when neighbouring nodes directly connect to one another, rather than being routed through centralised control equipment. The task group responsible for standardising the technologies required for WMNs was formed in 2004. The standardisation procedure required the creation of usage scenarios and the formation of the requirements necessary for selecting the technologies proposed.

The need for such an amendment arose because of the limitations placed on the IEEE 802.11 standard for WLANs which is the preferred solution for low cost data services. The major limitation is the coverage or range of the transmitting wireless nodes because of the imposed regulatory transmission power limitations. This restrains the size of the WLANs, and with the increasing demand for wireless networks spanning large areas ranging from office campuses to city-wide deployment, WMNs were viewed as a viable choice in place of WLANs [15]. WMNs allow data packets to traverse over multiple hops as opposed to the single hop limitation of WLANs. Bridging is traditionally used to connect end stations of WLANs to enable a multi-hop system; however, this relies on a wired structure which in turn, increases costs and decreases flexibility. Another problem which is addressed through the IEEE 802.11s standard, is the dependence of WLANs on a centralised structure to disseminate information through the network; this structure does not work well with newer applications. WLANs typically operate under a fixed topology, which prevents wireless nodes from adapting and choosing different and alternate paths if the need arises. The task group responsible for the formation of the IEEE 802.11s standard aims to address these problems by proposing a MAC-based WMN solution. In essence, the standard describes a mesh network as two or more nodes that are interconnected via IEEE 802.11 links which communicate via mesh services and constitute an IEEE 802.11-based wireless distribution system [13]. There are five main areas that the standard addresses, namely, WMN architecture, mesh routing, MAC enhancements, internetworking and WMN security [16]. Aspects relating to the architecture, mesh routing and WMN security will be further elaborated upon as these are more relevant in understanding the network environment used for the development of the proposed security model.

2.3.1 Mesh Architecture

The architecture refers to the different types of wireless nodes that constitute a mesh network. Some of the key terms used in describing the operation of WMNs according to the standard is given as [13]:

- Mesh Facility: The set of enhanced functions, channel access rules, frame formats, mutual authentication methods, and managed objects used to provide data transfer among autonomously operating stations that may not be in direct communication with each other over a single instance of the wireless medium.

- Mesh Point (MP): Wireless node that implements mesh facility.

- Station (STA): Legacy WLAN stations that have no mesh facility.

- Mesh Access Point (MAP): Performs functions of a MP and supports access to STAs.

- Mesh Portal (MPP): A MP at which a mesh network is connected to an external network. It serves as an entry and exit point for MAC service data units (MSDUs).

- Mesh Link: The communication channel between a mesh station and its neighbouring mesh station.

- Mesh Path: A set of mesh links from one particular source mesh station to a destination mesh station.

A small WMN illustrating the roles of each of the different types of nodes, is shown in figure 2.2. The STAs can be any client node such as a Wi-Fi enabled laptop; the MAPs route the frames through the network where a MP can be a next-hop node; the MPP serves as a gateway to the external network and is connected to it via a wired infrastructure.

2.3.2 Mesh Routing

There are several routing protocols that have been proposed for WMNs, most of which, bear close resemblance to routing protocols proposed for mobile ad hoc networks because of the similarities in their structure [17]. The routing protocols are responsible for discovering,

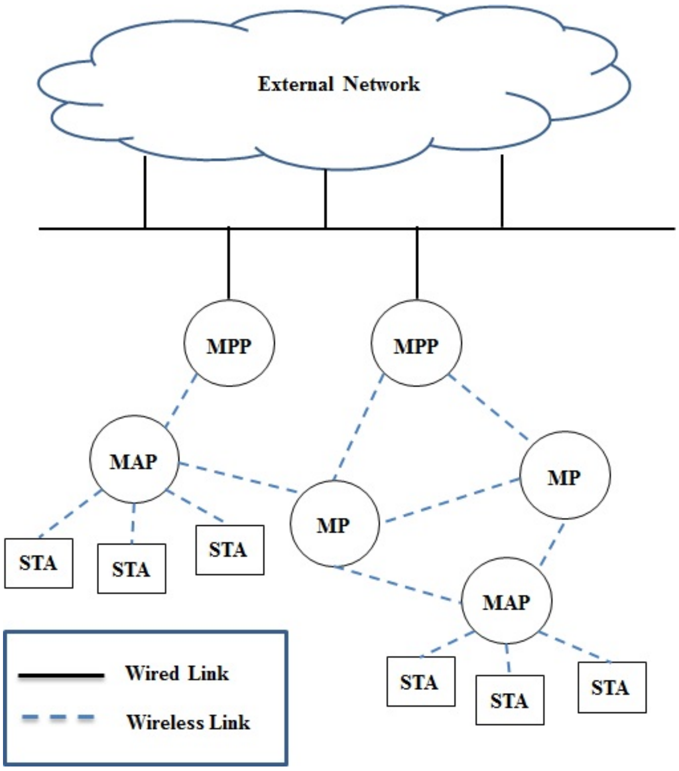

Figure 2.2: Small WMN showing role of the various types of wireless nodes

establishing and maintaining routes within networks so that information can be exchanged between nodes. In general, the protocols can be divided into three categories, namely, proactive routing protocols, reactive routing protocols and hybrid routing protocols. A proactive routing protocol is one in which each node maintains, at all times, a routing table containing possible routes. These routing protocols rely on the periodic dissemination of control packets which increases network bandwidth; however, it does facilitate quick retrieval of route information as a routing table is always maintained. Some examples of proactive protocols are the Destination-Sequenced Distance Vector Routing protocol, the Wireless Routing Protocol and the Optimized Link State Routing (OLSR) protocol. Alternatively, a reactive protocol discovers routes only when needed. This reduces network overhead as compared to a network employing a proactive routing protocol, but at the cost of a route start-up delay. There have been a number of such routing protocols proposed, such as the Dynamic MANET On-Demand protocol, the Dynamic Source Routing protocol and the Adhoc On Demand Distance Vector (AODV) protocol. A hybrid routing protocol is a combination of proactive and reactive routing; examples include the Zone Routing Protocol, Zone-based Hierarchical Link State protocol and the Distributed Spanning Trees protocol. All these aforementioned protocols are employed in the network layer of the nodes, which prevents the accurate capture of the wireless link. As a result, the IEEE 802.11s task group developed a MAC layer based routing protocol [15].

The default routing protocol for WMNs, as specified by the IEEE 802.11s standard, is the Hybrid Wireless Mesh Protocol (HWMP) [13]. This routing protocol utilises a hybrid path selection scheme which uses MAC addresses for forwarding frames. The network layer does not concern itself with the specifics of the routing, and views all nodes in the WMNs as direct neighbours; it is oblivious of the fact that it may take several hops to reach a particular node. WMNs generally utilise the network or internet protocol (IP) layer for enabling multi-hop communication; this means that the IP layer needs to derive the appropriate metrics from the MAC layer in order to accurately get an overview of the radio environment. This compromises the accuracy of the acquired link metrics [18]. To combat this inaccuracy, the IEEE 802.11s proposed a standard which introduces routing capabilities at the link layer.

The protocol combines the flexibility of reactive on-demand routing with a proactive tree based routing. The reactive part of the HWMP is based on the AODV protocol [19] and is adapted for MAC address-based path selection and link metric awareness. There are two supported methods of operations according to the IEEE 802.11s standard [13], namely, the on-demand mode and proactive tree building mode. These methods are not exclusive and operate concurrently, resulting in the hybrid mode. With regard to the on-demand mode, there are three different control packets that are used for path selection. These are the path request (PREQ), path reply (PREP) and path error (PERR) packets. The PREQ packet is broadcast when a particular node in the WMN needs to send a message. When an intermediate node receives the PREQ packet, it creates or updates the path to the source node, and if it cannot, it simply forwards it until it reaches the destination node. Upon reception of the PREQ node by the destination node, a unicast PREP is sent back to the source node. The PERR packets are broadcast to notify nodes that the originator does not support certain routes. In the proactive tree building node, a particular mesh node, most often a MPP, is selected as the root node. This root node periodically broadcasts PREQs through the network, and a PREP packet is sent back to the root node by all nodes that received the PREQ. This enables the formation of a proactive tree, so that the root node has a routing table with all possible destination nodes in the network. A fourth type of packet, the root announcement (RANN) packet is disseminated through the network to notify the mesh nodes about the presence of a root node. In the hybrid mode, both the on-demand mode and the proactive tree building mode run concurrently, thereby making the protocol suitable for various different network configurations. The proactive mode is more suitable for fixed network configurations and the reactive mode is more effective in a mobile ad hoc environment.

The default metric that is used in determining path cost is termed the airtime metric, which takes into account the data rate, frame error rate and overhead as is shown in equation 2.1.

$$C_a = [O_{ca} + O_p + B_t][r/(1 - e_{pt})] \tag{2.1}$$

where O_{ca} represents the overhead of accessing the channel, O_p is the protocol overhead, B_t is the number of bits in the test frame, r is the bit rate (Mb/s) and e_{pt} represents the frame error rate. This routing metric is more efficient and sophisticated than the metrics used in other network layer based routing protocols, because of the inclusion of radio-aware metrics [20].

An optional proactive protocol that is specified by the IEEE 802.11s standard, is the Radio aware optimized link state routing (RA-OLSR) protocol. This is largely based on the OLSR protocol [21] and differs in the type of address and metric used for routing. The OLSR protocol uses IP addresses whereas the RA-OLSR protocol uses MAC addresses; furthermore, RA-OLSR supports the use of arbitrary routing metrics such as the earlier defined airtime metric [13].

2.3.3 Mesh Security

WMN protection and security is thoroughly discussed in the proceeding chapter, therefore only the security measures specified in the IEEE 802.11s standard are briefly discussed. The standard proposes using the Simultaneous Authentication of Equals (SAE) algorithm for authentication and encryption [13]. It makes use of the same link level authentication model that is utilised by IEEE 802.11 WLANs, which is specified in the IEEE 802.11i amendment, and includes authentication, key distribution and encryption of management frames. There is, however, a major difference in that the MPs have to act as both the authenticator and supplicant [22]. The node that is joining the network acts as the supplicant, while the MP that it is connecting to, acts as the authenticator; there is no need for a central authentication server which is otherwise difficult to establish in a mesh network. SAE is based on the Diffie-Hellman key exchange and makes use of finity cyclic groups. SAE also provides the two nodes with a pairwise master key (PMK) for encryption purposes. This provides link encryption as each link is secured independently; no end-to-end encryption is provided by IEEE 802.11s [15]. As a result, if data needs to be broadcast, the broadcasting stations need to establish a secure peering connection with every node in the network before broadcasting packets.

SAE authenticates the two peer nodes by first deriving a number from the shared PMK, which they then send to each other along with an identifier. This type of message is termed as a commitment exchange message and is used to verify that each side has the same shared PMK. It achieves this by ensuring that the same number is derived when using the identifier that was received in the commitment exchange message. A confirmation exchange message is then sent by either node once both nodes have committed and verified that they have the same PMK. The algorithm terminates at this point having established authentication.

There are two other mesh link security protocols that are defined in the standard, namely, the authenticated peering exchange and the mesh group key handshake. These protocols are dependent on the common PMK that is known to the peer MPs. The authenticated peering exchange ensures that an authenticated peering using the exchanged PMKs is established, and that session keys for protecting unicast traffic between the peers is provided. It is also responsible for exchanging group keys, which are used for offering protection to broadcast and multicast traffic. The mesh group key handshake then allows a mesh node to update its group key [23].

2.4 WMNS IN MILITARY ENVIRONMENTS

WMNs have numerous properties that makes them a preferable choice for the deployment of networks for military and combat usage. The ability for WMNs to adapt and perform well in environments lacking infrastructure, makes them particularly well-suited for military usage. WMNs are typically considered a sub-class of ad hoc networking, and differ from mobile ad-hoc networks as the routing nodes are traditionally stationary. The main distinguishing feature of WMNs from other traditional wireless networks, is that WMNs are dynamically self-organised and self-configured. This implies that wireless nodes are able to automatically establish and maintain network connectivity. As a result of this prudent characteristic, there is increased robustness and improved service coverage; both of which are beneficial for networks in environments where military related activities take place. There are also the added benefits of low installation costs, easy maintenance, increased network capacity and ease of integration of WMNs with existing wireless networks [24]. Another beneficial characteristic of WMNs is the speed of deployment. The rapid exchange of critical information pertaining to areas regarding logistics, intelligence and war-fighting is achieved through the deployment of WMNs.

The functions of military forces is not limited to traditional state or nation defence and the execution of war, but also involves additional sanctioned and non-sanctioned functions within a society. This includes operations related to the promotion of political agenda, emergency services, humanitarian relief, prevention of terrorist activities and natural disaster relief [24]. Communication between members prove to be pivotal and protection thereof is extremely important given the extensive impact and critical nature of the tasks. One example of an existing use of WMNs in military scenarios is for Distributed Operation (DO). Essentially, DO entails providing squad-size units with the means of communicating critical information with higher units. WMNs also prove to be especially useful in humanitarian assistance and disaster relief operations, where there is a lack of proper telecommunications infrastructure; perhaps as a result of being damaged as an aftermath of a disastrous event or simply being non-existent as would be the case in rural areas.

2.4.1 Network Centric Warfare

The use of computer equipment and networked communications technology to enhance military operations is termed as network centric warfare (NCW). The use of networks to disseminate information, communicate intelligence, send orders and report back vital information has had a significant impact on the way the military perform their tasks. The purpose of NCW is to address the inherent changes to the military strategic environment that occur because of the unavoidable transition from the industrial age to the information age, where information is the most pivotal asset. NCW promises to deliver a significant advantage over adversaries because of the shared situational awareness that results from the use of networks. It is applicable at the three levels of warfare, namely, strategic, operational and tactical. It is also suited for various military operations, ranging from major combat to stability and peacekeeping operations [25]. Essentially, networking allows allied members within the force to link to each other and increase awareness of the situation. This increases the effectiveness of the decision making at the various levels, thereby, significantly increasing the impact of the actions. According to the U.S. Office of Force Transformation [25], a well networked force improves information sharing, which in turn enhances the quality of information and shared situational awareness. The implications of high-quality situational awareness are collaboration and self-synchronisation between the various nodes in the network. Self-synchronisation means that an augmentation to sustainability and speed of command will be observed; ultimately, increasing the effectiveness of military operation.

With this shift from the industrial age to the information age, it is reasonable to assume that potential adversaries are analysing vulnerabilities and ways of destroying NCW. Thus, it is imperative to consider ways of protecting this integral part of warfare. The principles of NCW that aid in the execution of military operations in the information age, are given as [25]:

1. Information superiority
2. Shared awareness
3. Speed of command
4. Dispersed forces
5. Demassification
6. Deep sensor reach
7. Fast alteration of initial conditions
8. Compressed operations

The first and foremost principle relating to information superiority, involves ensuring that adversaries have reduced ability to access information and to raise their uncertainty. This is extremely critical as a result of the widely varied types of data which is disseminated through the network; whether it be in text, real-time video or voice format, and originating from a number of different sources, ranging from terrestrial forces and sensors, satellites, unmanned aerial vehicles, and a diverse set of centralised and distributed information assets. As military operations are becoming increasingly reliant on networked technology owing to the advantages that it provides; and also so that they are able to keep up with their multinational partners and their adversaries, maintaining data confidentiality is a key issue in modern warfare. If adversaries can gain access to this vast amount of information that is being exchanged, they can manipulate or plan their course of action appropriately, thereby eliminating the advantage that NCW promises to deliver. Any form of information leakage, where the value of the tactical information is considerably higher in the military domain, can have disastrous consequences and should be avoided at all costs.

Some examples of the existing use of NCW in actual military scenarios, include the invasion by the U.S. of Afghanistan in 2001. Co-ordination largely depended on data and voice links that created a rapid, effective situational understanding, where data relating to the troops positions, target locations and tactical plans were exchanged. This was performed in efforts of synchronising military equipments and personnel to perform a particular task effectively [26]. An example of NCW to effectively integrate different platforms such as C2, ISR, tankers, space, ground and sea-based systems is the Air Force Command and Control Constellation network [27]. Another successful implementation of NCW was employed during Operation Iraqi Freedom, to monitor and control the movement of the U.S. Army, U.S. Marine, U.S. Special Forces, and British ground forces during the conflict. Numerous sensors were used for locating units on the battelfield and effective networking was used to communicate this information to various officers and head-quarters [28]. A more recent application of NCW is through the conception of the Tactical Digital Information Link J system. This system is essentially responsible for supporting information exchange between tactical command, control, communications, computers and intelligence systems [29]. This system has been applied during operations conducted in countries such as Libya, Bosnia, Iraq and Afghanistan.

2.4.2 Military Applications of WMNs

Initial networking with military applications took the form of simple ad hoc topologies, in which individual single-radio nodes were directly connected to other nearby nodes within the network. Even though this configuration was relatively well-suited for low-demand environments, the reliance on single channel communication and the limited abilities of the radio nodes, reduced the overall efficiency of the network. Therefore, developers were forced to create more sophisticated mesh networking technology that is able to meets the requirements of higher data rates and effective real-time protocols. In essence, as highlighted by numerous developers of such technology, there are four key requirements namely, mobility, high performance for real-time protocols, distributed frequency agility and distributed network topology formation [30].

A usage scenario was contributed to the IEEE 802.11s standard specifically relating to military application. It was stated that military usage of mesh networks can be divided into two categories: non-combat usage and combat operational usage [11]. Non-combat usage refers to scenarios in the military that resemble application of mesh networking in usage cases for office areas and campus/community/public access networks. In such cases, the requirements for mesh network technology would be to enable low-cost, easily deployable networks that are able to provide reliable coverage and performance. The types of equipment that can possibly be used for non-combat applications include PCs, laptops, PDAs, printers, mobile and desktop phones as well as any other devices found in office environments [31]. Other non-combat usage may resemble a campus/community/public access usage scenario where requirements such as seamless connectivity over large geographic areas, rapid connectivity in wired-free areas, easy scalability as well as location based services should be met.

On the other hand, combat operational usage differs from non-combat usage in factors such as node mobility, heavy reliance on fully automated network management and sensitivity to energy conservation. Combat operations are not geographically limited and can take place indoors and outdoors. A key requirement for the mesh clients in this case, is the ability for it to act as a mesh access point so that it is able to route traffic for troops that are the forward point of the operation. The access points can be placed inside various forms of transport such as ships or vehicles as well as being mounted on the backpacks of military personnel themselves [31]. A graphic illustration of a simple WMN on a battlefield is shown in figure

2.3; the mesh clients whether they are the tanks, trucks or military personnel, may need to act as an access point if the need arises.

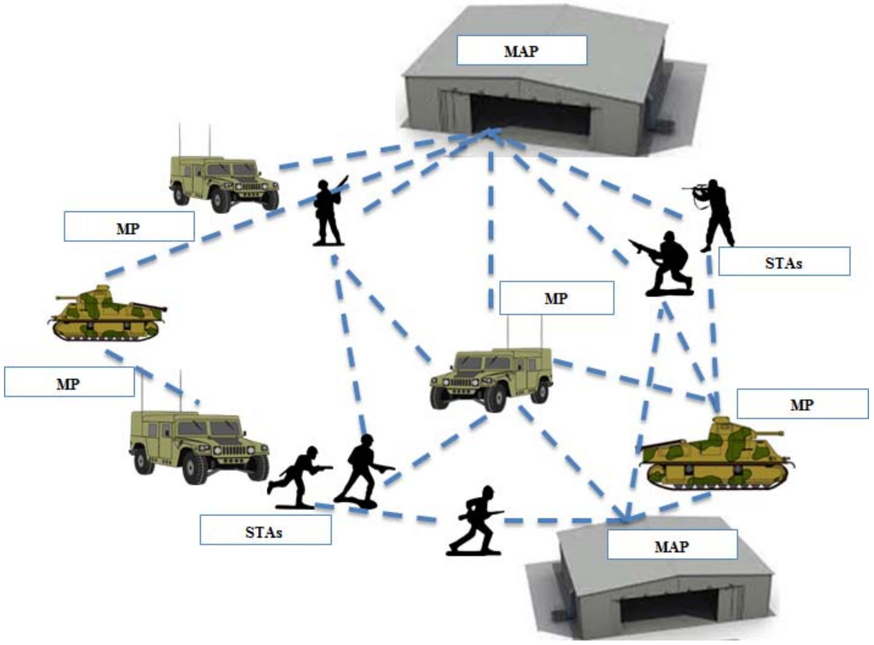

Figure 2.3: Example of a WMN for a military based scenario

As has been pointed out, NCW's primary role is to increase situational awareness which can range from voice, text and video communication that is used for reporting troops positions and conditions to a combat operations center. Situational awareness traffic can also be the data reported from sensing devices through text form or video feeds such as automated surveillance devices. The combat operations center can also disseminate tactical overviews to the engaged troops. Military applications depend largely on broadcast/multicast as well as unicast methods of delivering traffic. It is the most uncertain and flexible of the usage models described in the amendment. In both non-combat and combat scenarios, securing the network is vital owing to the nature of information that is exchanged in such scenarios.

2.5 CONCLUDING REMARKS

This chapter provided an overview of WMNs and their numerous applications. The IEEE protocol written for such networks is given as an amendment to IEEE 802.11 standard [13]. The protocol and aspects relating to the mesh architecture, routing, security, which are most pertinent with reference to the work presented in this thesis, were also discussed. The importance and various uses of WMNs in military environments were elaborated upon. NCW refers to the use of computer equipment and networked communications technology to enhance military operations. The first and foremost principle of NCW that aids in the execution of military operations is related to maintaining information superiority. This involves ensuring that adversaries have reduced ability to access information and to raise their uncertainty. The way in which WMNs are used for disseminating information, communicating intelligence, sending orders and reporting vital information, has had a significant impact on the way the military perform their tasks. Any form of information leakage, where the value of the tactical information is considerably higher in the military domain, can have disastrous consequences and should be avoided at all costs.

CHAPTER 3

WIRELESS NETWORK PROTECTION

3.1 INTRODUCTION

The main disadvantage of WMNs is its susceptibility to interference and eavesdroppers that are able to intercept and "listen" in on the communication between the devices in networks. Eavesdroppers can act as non-lethal weapons to combatants at war and can have dire consequences if vital information is obtained by the adversaries. Owing to the emerging and prevalent use of WMNs, protecting the information contained in the networks is of utmost importance in this information driven age. As a result of the open and shared broadcast medium, information theft is a rising concern in wireless networks. WMNs suffer from two main problems; one which relates to routing and multi-hop technology, and the other, which relates to the security of the networks. There is little attention being paid to securing WMNs as opposed to the large amount of literature dedicated to providing solutions for routing problems [32]. However, as a result of the numerous similarities between WMNs and wireless sensor networks (WSNs), the security solutions provided for WSNs can possibly be adapted for WMNs [32]. WSNs consist of sensor nodes that collect data about the environment and report it to one or more gateway nodes. Both types of networks are prone to similar interference attacks and confidentiality comprising situations.

3.2 WIRELESS NETWORK PROTECTION

3.2.1 Cryptographic Methods

Confidentiality relates to preventing information leakage and securing messages that are exchanged between the nodes, in order to prevent eavesdroppers from obtaining any critical information. Cryptographic techniques are primarily used for encrypting data between the source and destination nodes in which the key used to decrypt the data, is known by the destination node only. The cryptographic techniques involve the application of traditional algorithms such as Diffie-Hellman, RSA and elliptic curve cryptography [33]. Other cryptographic methods that have been adapted especially for wireless ad hoc networks include the use of threshold cryptography in ad hoc networks to develop a key management service [34], extensible authentication protocol-transport layer based security authentication with the use of asymmetric cryptography [35], public-key cryptosystems based on chaotic dynamics [36] as well as self-generated-certificate public key encryption for wireless ad hoc networks [37]. There are, however, several shortcomings related to public key cryptography such as increased complexity in protocol design, vulnerability to denial of service (DoS) attacks during the four-step handshake as well as the lack of effective user identity protection mechanisms [38]. As a result, identity based encryption methods that do not involve maintenance of public key certificates were developed. He and Agrawal [39] proposed a scheme which makes use of identity-based cryptography for key agreement and mutual authentication for WMNs. Similarly, cryptographic algorithms based on the Sakai-Kasahara key construction for maintaining data confidentiality in IEEE 802.11s mesh networks is proposed by Boudguiga and Laurent [40].

Although cryptographic techniques are able to provide authentication and confidentiality in wireless ad hoc networks, a prominent challenge in securing WMNs, as opposed to other ad hoc networks, is accounting for the numerous different technologies in the network nodes as well as dealing with the heterogeneous nature of the network. Cryptographic tools lie in the upper layers and they would thus have to be adapted for the different access technologies of the nodes. Also, as there is a lack of a centralised trusted authority, distributing the public key for encryption purposes becomes difficult. As it stands, these techniques have high memory and energy requirements and with the application to WMNs, there is added complexity and cost [33]. With the emergence of ad hoc and decentralised networks, providing security at the physical layer, in contrast to cryptographic techniques which are applied at the higher layers, has been of interest [2]. Another reason why physical layer security has been gaining attention, is that complete immunity against eavesdroppers or relay attacks is not provided to wireless nodes when encryption methods are utilised. This is because the network can still be eavesdropped upon during the key exchange process, and as such, the purpose of encryption is defeated.

3.2.2 Physical-layer Based Methods

Physical layer security aims to maximise the rate of reliable information from the source to the destination while maintaining data confidentiality against eavesdroppers. The maximum reliable rate is termed as the *secrecy capacity*. The notion of exploiting the nature of the wireless medium to strengthen security in wireless networks was first introduced by Wyner [41]. Wyner proposed that perfect secrecy can be achieved in wireless communication links without the use of any encryption methods. It was proven that when the eavesdropper's channel is a degraded version of the communication channel, which it wants to eavesdrop upon, the source and destination are able to ensure privacy of their messages. This is achieved through stochastic encoding of the additive noise that is used to impair the eavesdropper's channel. Through this method, there is an equivocation that is induced at the eavesdropper, and by setting the equivocation rate to be arbitrarily close to the message rate, perfect secrecy can be obtained. As a follow up, Csiszár and Kroner [42] generalised Wyner's approach to a non-degraded discrete memoryless broadcast channel. Other authors have extended the work by Wyner by addressing multi-user scenarios [43] and different channel models such as the Gaussian wiretap channel model [44], quasi-static fading models [45] and ergodic fading channels [46].

The secrecy rate of a communication channel can be improved by increasing the SNR of the destination node or by decreasing the SNR of the eavesdropper. The SNR at the destination node can possibly be improved by shortening the distance between source and destination; however, this is generally not feasible. In order to reduce the SNR at the eavesdropper, a suitable method would be the deployment of jamming devices that are capable of inducing controlled inference in the eavesdropper's channel [47].

Jamming is typically considered as a malicious activity that seeks to deny service to legitimate users by generating signals, noise or malicious packets in an effort to disrupt communication services [48]. The device that transmits jamming pulses, signals and packets to disrupt the service is known as a jammer or a jamming node. A jamming attack is classified as being effective when it is energy efficient, has a low probability of being detected and has a high level of undesirable impact on network operation. There are a number of different types of jamming attacks, namely constant jamming, deceptive jamming, random jamming, reactive jamming, and scheduled jamming.

Constant jamming is the simplest kind of jamming attack in that it continually transmits an interference signal, so as to degrade the capacity of the wireless channel [49]. It disregards the protocols in the physical and link layers of the nodes. The main disadvantage of constant jammers is that the energy consumption is excessive, as it continually transmits high-power noise. This causes significant interference which prevents the reliable delivery of data packets on the channel [50]. Deceptive jamming is an attack in which the jammers continually inject legitimate packets with valid headers into the channel. As a result, the receiving node thinks that it is receiving a legitimate packet and will therefore be restricted to the receiving mode. As with constant jamming, deceptive jamming is a continuous jamming attack and as such, it expends a large amount of energy to continually send out these packets. In addition, continuous jammers are easy to detect as a result of the constant presence of these high-power interference signals.

Random jamming addresses the large energy expenditure of constant and deceptive jamming by alternating the jammer between sleep mode and jamming mode. The random jammer performs the attack for a random period after which it shuts down for an arbitrary amount of time before continuing the attack. However, random jamming attacks are not as effective in degrading the performance of the network as continuous jamming attacks [51]. Reactive jamming involves listening to the network transmissions, deciphering the packets and reacting to the subsequent network state [52]. This type of attack proves to be more difficult to implement than other attacks as it requires the ability to decode the packet information and react accordingly with malicious intent. The primary advantage of a reactive jammer is that it is more difficult to detect; however, it does not conserve significantly less energy than continuous jammers as it constantly needs to listen to the channel. Scheduled jammers send out bursts of jamming packets for a specific period of time, based on a predefined schedule [53]. This type of attack does not require packet decoding capabilities or reactive intelligence. It is also significantly more energy efficient than both continuous and reactive jammers. The effectiveness of this attack depends on the pre-set schedule of the jamming packet bursts.

3.3 OPTIMISATION SCHEMES FOR JAMMING

3.3.1 Friendly Jamming and Power Allocation

Even though jamming is typically used for degrading the performance of networks, it has found application as a way of enhancing the security of a network by causing interference to the eavesdroppers in order to reduce its ability to decode the source's information [54]. In this case, the jamming is termed as being *friendly* or *protective*. Friendly jammers are used as a way of providing physical layer security by protecting the wireless networks against information leakage. A large portion of literature is dedicated to the use of intermediate relays to act as friendly jammers that are used to generate artificial noise or interference directed at eavesdroppers, thereby degrading the channel capacity between the source and eavesdropper. Lai and El Gamal [55] made use of intermediate relay nodes for performing co-operative jamming by ensuring communication confidentiality from eavesdroppers. The work is based on Wyner's proposition that if the eavesdropper's channel is less noisy than the main communication channel, then perfect secrecy cannot be achieved [41] . The relay nodes are used to send codewords that are independent of the source message in order to confuse the eavesdropper and reduce its SNR. Similarly, co-operative jamming was studied in a multiple antenna scenario by Goel and Negi [56]. Al-nahari proposed and investigated a jamming scheme that creates interference at the eavesdropper during the decode-and-forward phase [57]. The interference can also be generated during the cooperative phase as suggested by Dong *et al.* [58].

It is assumed that the relays are trusted third parties unlike the work considered by Zhang *et al.* [59] in which external friendly jammers are used to protect the messages sent from the source to the destination against the relay which is used to forward the message. This is achieved through the formulation of a Stackelberg game [60] between the source and friendly jammers so that an optimal power allocation scheme for the friendly jammers is obtained. Traditional optimisation methods and the use of game theory are used to for determining the power values allocated to the friendly jammers given that there is a power constraint that the jammers have to adhere to [54], [61]-[63]. Vilela *et al.* [47] investigated the performance of different types of friendly jammers in a quasi-static fading environment in which a single transmitter and receiver want to exchange messages in the presence of an eavesdropper. The jamming strategies considered include blunt jammers (continually emits white Gaussian noise), cautious jammers (opportunistically jams when the transmitter has a better channel to the eavesdropper than to the receiver) and adaptive jamming (a threshold value for the channel quality is set above which it will stop jamming).

In the literature relating to the use of friendly jammers, it was assumed that the jammers were placed far enough from the receivers or destination nodes to not have any detrimental effect on the communication channel, in which the data that it wishes to protect, resides. It is simply considered as a trade-off in the power allocation strategies for the friendly jammers [3]. However, in practical scenarios, there is bound to be induced interference from the friendly jammer and it is not always possible to control it so that the SNR at the destination is maintained, especially in multiple source, eavesdropper and destination scenarios. Bayat *et al.* [3] considered a scenario with multiple source-destination pairs, with multiple jammers but a single eavesdropper. The authors propose an algorithm based on matching theory that matches every source and destination pair with a particular jammer. Although the authors propose a generalised scenario in comparison to the majority of literature which deals with single source-destination scenarios [54]-[63], the jammers are assumed to have no effect on the legitimate communication link and only a single eavesdropper is considered.

A more realistic scenario with multiple eavesdroppers and topologies in which source and destination nodes are not paired, should be considered. Shen *et al.* [64] proposed a technique called "Ally Friendly Jamming" in which connectivity between the source and destination is maintained even when the jamming signals affect the source and destination pair, as well as the eavesdropper. This is achieved through the removal of the interference caused by the jammers to the legitimate receiver through signal processing techniques that utilise secret keys, which is only known to the receiver and not the eavesdropper. The problem of the key possibly being leaked to the eavesdropper during the key exchange process, is analogous to that experienced in networks utilising cryptographic methods for preserving data confidentiality. There is also added computation that needs to be performed at the receiver to remove the interference which increases the latency and is not preferable, especially in military and emergency scenarios where time is of utmost importance. It is therefore beneficial to consider the effect of jammer placement and power allocation in preventing eavesdroppers from intercepting network communication, while not disrupting the legitimate communication taking place between the source and destination nodes.

3.3.2 Jammer Placement

A possible way of providing protection and security for a network is through the use of jammers. The number and placement of jammers in a particular network has a significant impact on the performance and cost of the jamming scheme. Even though there is vast literature available for optimisation in telecommunications, the area of work dedicated to determining the optimal set and behaviour of jammers, has received little attention by the research community [65].

Commander *et al.* [66] were one of the first authors to tackle the problem of determining the optimal number and placement for a set of jamming devices to neutralise the enemy's communication network. This is termed as "The wireless network jamming problem". Two approaches were used for determining the optimal set which included using graph theory to model the target network as an undirected graph, as well as using coverage formulations in which several integer programming models were proposed and solved to determine the number and placement of jamming devices. The set of discrete points that constitute possible locations of where to place jammers was determined by superimposing a uniform grid over the target area where the intersection points correspond to possible locations for a jammer placement. The authors also incorporated risk measures in situations where it may be appropriate to only jam a certain percentage of the adversary's networks. The Value-at-Risk (VaR) and Conditional Value-at-Risk (CVaR) percentile measures were used to set up the jamming placement problem with percentile constraints. Although the CVaR measure is suited for stochastic and uncertain environments, it can also be applied to deterministic situations, as was performed by Commander *et al.* [66]. It was found to be significant more computationally efficient than the VaR counterpart.

Another similar coverage formulation was proposed by Ying-chun *et al.* [67]. The authors determined the placement of crane-umbrella jammers in order to cover a given target area. The scenario describes the dropping of these crane-umbrella jammers, where each jammer has a circular area of influence, over an enemy's network to interfere with the communication antennas. The placement of a fixed number of jammers is achieved through the application of the genetic algorithm. The proposed algorithm determines where to place jammers to disrupt communication in order to cover a discrete set of points. It starts by randomly placing jammers in an area after which the genetic algorithm is employed to perform generation replacement operations to replace the old population of jammers with a new one. The only simulation performed by the authors showed 100% coverage of a 20 km by 20 km area with 45 discrete points after 256 generation replacements. The number of jammers was fixed to 25 which covered the area by a relatively high 92.32% before the genetic algorithm was performed. It differs from geometric disk coverage used for placing sensor nodes as the collaborative effect of the jammers is not considered. In the case of jamming, the effect that multiple jammers has on a certain area should be analysed, whereas with sensor nodes, if a device is placed in the coverage area of a single sensor node then the goal is met.

Guan *et al.* [68] provided heuristics to effectively allocate electronic attack devices i.e. jammers, to target known devices of the adversarial network. The jamming devices are allocated from a set of possible jammer locations to destroy the operations of an enemy's wireless network in which both the transmitting and receiving device locations are known. The branch-and-bound method is suggested as the approach to solve the integer linear program that arises from the formulation of the problem. The use of the genetic algorithm, as was employed by Ying-chun *et al.* [67], was also considered as an alternative approach. It was found that the two-stage decoupled optimisation approach using the branch-and-bound method, generated a solution that was more effective and less costly than the solution obtained using the genetic algorithm.

An extension of the work presented by Commander *et al.* [66] was proposed by Vadlamani *et al.* [69] in which a bi-level programming model was used for solving the problem of placing jammers in a multi-hop multi-channel network in which the jammers have directional antennas instead of omnidirectional antennas. The approach was based on work presented by Brown *et al.* [70] in which the network interdiction problem is modelled as a bi-level attacker-defender mixed integer program. A min-max problem is formulated where the network is depicted as a directed graph, and jammers, which are seen as attackers, are placed to destroy the arcs thereby minimising the expected throughput of the network. The formulation attempts to minimise the throughput of the network from the attacker's perspective and maximise the throughput from the operator's perspective. The paper also discusses the role of the defender when being attacked by the jammers and proposes a channel hoping strategy based on a Nash Equilibrium mixed game [71].

It is important to note the studies related to jammer placement that have been discussed, analyse the problem in deterministic environments where the target devices are known. Uncertainty is a factor that has largely not been investigated even though it better reflects real-life scenarios, and would therefore be more suitable for applications in a military battlefield. Commander *et al.* [72] extended their own work to study the jammer placement problem in networks under complete uncertainty. The problem then reduces to jamming all points in a given area to suppress communication within that area. The paper deals with the sub-problem of covering a square area with a grid where jamming devices are located at the intersection points of the grid. The authors argue that finding a global optimal solution for any given area is difficult and the solution to the sub-problem will provide a feasible solution to the general problem. The objective of the work is to derive the maximum grid step size of where to place jammers with a given circular coverage area. An upper and lower bound, as well a convergence result, is also provided.

An alternative model for solving "The wireless network jamming problem" that is based on the explicit use of signal-to-interference ratio (SIR) quantities, was recently proposed by D'Andregiovanni [73]. A robust cutting-plane algorithm was also developed to address the uncertain nature of the placement problem. The author highlighted a strong correlation with classical wireless network design and as a result, adopted a testpoint model to represent coverage and jamming conditions.

Sankararaman *et al.* [74] studied jammer placement and power allocation for friendly jammers under a storage/fence model. Contrary to other work on the placement of jammers to destroy an entire network [66]-[69], [72]; the communication network that the jammers are protecting against eavesdroppers is taken into account. The placement of jammers are such that it protects the communication network and does not necessarily destroy an entire enemy's network. The storage/fence environment assumes that legitimate communication takes place in the storage, which is a geographic region physically secured by a fence, where eavesdroppers may not enter. There is a minimum gap assumed between the storage and the fence which is termed as the jammer space. The friendly jammers can reside in this space and are used to transmit artificial noise so as to create sufficient interference and prevent reception for the eavesdroppers, while not disrupting any legitimate communication inside the storage area. This work is targeted for protecting data stored on radio-frequency identification tags and where geographically restricting a network is feasible.

Sankararaman *et al.* [74] propose algorithms targeted towards optimising the power consumption and number of jammers needed to reduce the SNR of eavesdroppers to below a threshold without jeopardising network performance. With regard to the basic linear power assignment problem, the authors proposed an ϵ-approximation algorithm for the case when the storage and eavesdropper areas are continuous. The ϵ-approximation algorithm involves computing a discrete set of points in the storage and fence area so that the problem reduces to a linear program with a finite number of constraints. The jammer placement problem has an added number of complexities because of the integer constraints, as well the difficulty in algebraically characterising the jammer placement as a function of the distance between the storage area and the fence. The authors solve this problem by applying a heuristic approach. As with the power allocation problem, a similar ϵ-approximation algorithm is given to discretise the fence and storage areas when there is a pre-determined set of candidate jammer locations. A near-optimal algorithm is proposed for the case when the fence area is assumed to be convex and the storage area is a connected region of any shape. Essentially, a greedy algorithm is proposed in which an arbitrary eavesdropper location, with a certain visibility region, is chosen. The visibility region is defined as the area in the jammer space, in which a jammer must lie to successfully decrease the SNR of the eavesdropper to a value below its threshold. Another eavesdropper location is then chosen by "walking" along the fence until there is no common region of visibility. A jammer is then placed at this location. This method is repeated for all possible eavesdropper locations. The algorithm is very specific to this problem and does not involve any known techniques even though it bears some resemblance to the traditional set-covering problem.

3.4 CONCLUDING REMARKS

In conclusion, literature pertaining to the placement and power allocation of jammers have been investigated and reviewed. The need for the protection of WMNs was highlighted as a result of the application in environments where security is of utmost importance e.g. in the military. The most popular method for ensuring data confidentiality is through the use of cryptographic techniques; however, as a result of the decentralised nature and power limited network nodes of WMNs, it is important to consider physical-layer based methods such as jamming. The physical-layer methods can also be used in conjunction with cryptographic techniques for enhancing the security of a WMN. Friendly jammers are used to prevent eavesdroppers from intercepting vital network communication. Several papers presented algorithms, mostly based on game theory methods, to determine the optimal transmitting power of the friendly jammers [61]-[64]. With regard to the optimisation of jammer placement, the locations of jammers were determined so as to minimise the throughput of an entire enemy's network. Methods for determining the jammer locations involved relaxing or adapting certain constraints such as discretising the jamming area [72],[74] and requiring prior information about the network to jam [66], [68], [69]. Sankaraman *et al.* [74] jointly addressed the problem of allocating power values and placing friendly jammers through the development of heuristics that were specific for a particular environment (storage/fence model). The method of discretising the area has a large effect on the placement of jammers and consequently, on the effectiveness of the jamming scheme. The approach was targeted for protecting data stored on RFID tags in a storage area. There has not been work aimed at the development of optimisation schemes for friendly jammers that are protecting WMNs which address both power and placement of the jammers.

CHAPTER 4

PROBLEM FORMULATION

4.1 INTRODUCTION

A novel method of utilising jammers to protect WMNs against eavesdropper nodes in a multi-hop network with multiple sources, destinations and eavesdroppers is proposed. A mathematical model is developed for the joint optimal placement and power allocation of the wireless jammers. The model takes into account not only the effect that the jammers have on the malicious nodes, but also the impact it has on the communicating nodes. Measures are taken to prevent the jammers from having any ill-effect on the communication channels they are protecting. This is achieved through the careful placement of the jammers so that network continuity is maintained, while the principal purpose of degrading the eavesdropper's channel through controlled interference, is accomplished. The protection scheme precludes the use of any cryptographic techniques and is only physical-layer based. Focus has been placed on the ease of practical implementation of the proposed scheme as no additional computation or complexity is required from the legitimate communication nodes; only the intelligent placement of simple continuous jammers is needed to achieve maximum protection. The scheme is further optimised in terms of the transmitting power associated with the jammers so that the energy expended through use of the jammers, is kept at a minimum. This work is largely targeted for protecting wireless networks in military domains which are very flexible and uncertain.

4.2 NETWORK ENVIRONMENT

The environment used for simulating and testing the optimisation problems is one which aims to closely represent the application of WMNs in military battlefields, as has been described in the usage scenarios for the IEEE 802.11s standard. In such a situation, wireless nodes can be placed indoors or outdoors and are not limited to specific areas. It differs largely from WMNs deployed in office/campus or civilian-based applications in the fact that there is often some geographical restriction placed on the locations of the wireless nodes in those environments. In a military battlefield scenario, there are no such limitations placed except for possible terrain restrictions. Predicting and modelling terrain restrictions is quite difficult because of the randomness associated with this. Thus, all wireless nodes are completely randomly placed to capture certain aspects of the terrain restrictions as well as the non-deterministic nature of the environment.

Malicious nodes are used to describe the adversarial wireless nodes that have been placed to eavesdrop on network communication. The legitimate nodes refer to the wireless communication nodes that are protected against the malicious nodes with the use of jammers. Such a military based network environment would make it difficult to physically prevent malicious nodes from entering the mesh network. Figure 4.1 illustrates a typical WMN is a military environment where eavesdroppers can be found in the midst of the network. The eavesdroppers can take the form of any device that is able to intercept the wireless channels. The jammers are placed interspersed amongst the legitimate nodes and the malicious nodes in such a way so as to prevent the malicious nodes from gaining any information, while not jeopardizing the communication between the legitimate nodes.

4.2.1 Assumptions

The jamming devices are assumed to be fitted with omnidirectional antennas and generate random noise. The legitimate communication nodes are also assumed to be fitted with omnidirectional nodes and function as both transmitters and receivers. The jammers are placed to ensure data confidentiality and cannot prevent the malicious nodes from deliberately altering or causing interference to legitimate communication. The jamming nodes are assumed to be fully cooperative, which means that the effect of all jammers on a particular node is taken

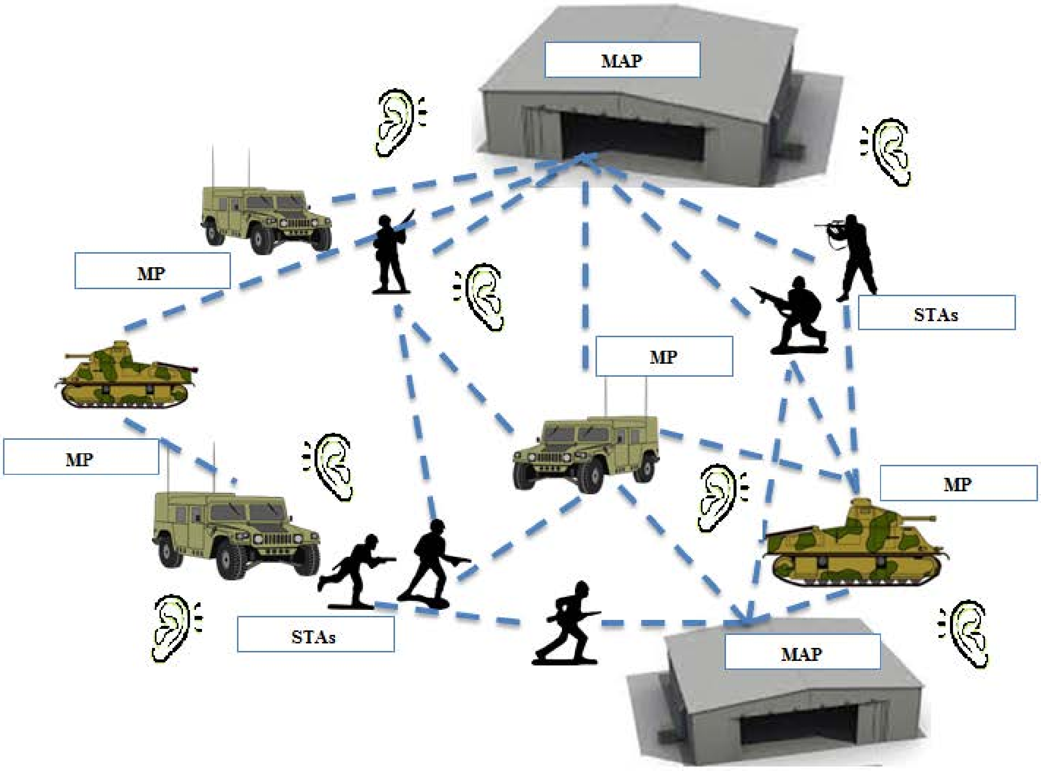

Figure 4.1: Example of WMN with eavesdroppers in military environment

into account. It is also assumed that the channel gain values are known for all channels, including those associated with the eavesdroppers.

Given a set of potential jamming locations, the goal of the scheme is to select the minimum number of jamming locations at which the jammers can be placed, such that there is interference free reception by legitimate receivers, and no malicious nodes are able to gain information as a result of a decrease in its SNR. A node is considered jammed if the combined jamming effectiveness of all jammers on that particular node is above some threshold value.

4.2.2 Jamming Effectiveness

The jamming effectiveness is modelled by the variable q_k^j and depends on the power of its electromagnetic emission which is inversely proportional to the squared distance from the jamming device, j, to the node being jammed, k [66]. This is shown as:

$$q_k^j = \frac{\lambda_j}{(X_k - X_j)^2 + (Y_k - Y_j)^2} \tag{4.1}$$

Where $\lambda_j \in \Re$ is a constant that relates to the transmitting power of the jamming device, (X_k, Y_k) and (X_j, Y_j) are the coordinates of the jamming device and the node being jammed respectively.

For a particular jammer, the radiation intensity should be above some threshold value for effectively jamming a node. The radiation intensity for a simple omnidirectional antenna can be calculated as:

$$\frac{P_T}{\pi R^2} \tag{4.2}$$

where P_T is the transmitting power and R is the radius of the circular coverage area. For any type of antenna, the λ value is directly proportional to the transmitting power, P_T; therefore, λ is used to represent the transmission power.

4.3 MATHEMATICAL PROGRAMMING

4.3.1 Overview

Mathematical optimisation is the branch of mathematics that deals with solving problems in which resources need to be effectively allocated in complex, dynamic and uncertain conditions. The optimisation problem involves the maximisation or minimisation of some function on sets defined by linear and non-linear constraints. The term *Operations Research* or *Decision Science* is used to largely describe the scientific subject that refers to the study of decision problems regarding controlling complex systems and phenomena. Optimisation tools and mathematical methods are employed in the decision making process. Even though its roots can be traced to problems occurring in early civilisations, it was formally identified as a subject in the 1940s during the peak of World War II. There was a need for the British and U.S. military to hire scientists from different disciplines to tackle several problems related to aspects such as finding optimal ways to construct convoys while minimising the affect of adversaries, as well as finding the best ways of covering certain areas with radar equipment given its scarce availability [75]. Operation research teams were extremely important in devising ways for optimally transporting convoys, tracking submarines and allocating supplies to allied forces. In fact, this subject was first referred to as *Military Operations Research*, however as a result of the wide range of applications of these developed techniques in several fields, the word *military* was dropped. Since its conception, it has grown at a rapid and unprecedented pace for most scientific accomplishments while having application in a wide variety of areas relating to business, industrial, military, and public-sector problems.

Mathematical programming, also known as mathematical optimisation, is used for making decisions by modelling the problem mathematically. Essentially, it deals with optimally allocating limited resources among competing activities, while being imposed by a set of constraints inherent with the nature of the problem being studied [76]. The use of mathematical models as an aid for taking decisions, has been increasingly implemented since the conclusion of World War II. Operations research was the term used by the military during World War II, to formally describe the application of scientific methods, techniques and tools to problems involving the operation of a system in order to provide those in command with optimal solutions [77].The need for allocating resources to derive maximum profit at a minimum cost resulted in a collaboration of the military with the scientific community. After the successful application of such tools (the operations research teams were said to be instrumental in winning the air battle of Britain, the island campaign in the Pacific, the battle of North Atlantic and so forth [78]), it became evident that operations research would prove to be beneficial for solving problems over a wide-variety of areas such as business, industrial and the public-sector.

Mathematical programming is seen as the most developed and principal area of operations research. There are a number of different types of mathematical programming which includes linear programming, non-linear programming, dynamic programming and integer programming among others. Mathematical programming is defined as the technique for determining the values of a set of decision variables that optimise a mathematical objective function and conform to a given set of mathematical constraints [77]. The first mathematical programming problem was formulated as a transportation problem and can be attributed to Hitchcock, who proposed the formulation in 1941, and Koopmans, who later discussed the problem in detail in 1947. A transportation problem is essentially used to determine an optimal transportation scheme between warehouses and outlets, subject to specified supply and demand constraints. An efficient way of solving this problem was proposed by Dantzig, who also later generalised the transportation problem to what is now called linear programming [79]. There have been numerous techniques and methods that have since been formulated and proposed for providing solutions to different types of linear programming problems.

A mathematical model will be used to represent the optimal jammer placement and power allocation problem such that appropriate optimisation techniques can be applied and an informed decision can be made. Traditionally, the scientific approach to decision making involves the use of one or more mathematical models [80]. Optimisation models are typically characterised by three components, namely, objective function(s), decision variables and constraints. Theses models are used to determine the values for the decision variables which either minimise or maximise the objective function(s) while being subject to a number of constraints. The region which constitutes all values of the decision variables that satisfy all constraints, is termed as the feasible region. The optimal solution is any point in the feasible region that results in a maximum, or minimum, objective function depending on if it is a maximisation or minimisation optimisation model. An optimisation model can further be characterised as being static or dynamic; linear or non-linear; integer or non-integer; and deterministic or stochastic. A brief description of these models are given as follows:

- Static and dynamic models: A static optimisation model is one which takes place at a fixed point in time rather than over an interval, as would be the case for a dynamic optimisation model. Dynamic models involve sequences of decisions in finally determining the values of the decision variables; a more "one-shot" approach is followed for static problems.

- Liner and non-linear models: Linear models are characterised by their linear objective functions and their linear constraints. Non-linear models, on the other hand, do not exhibit the linearity present in the objective functions or constraints, and are in general more difficult to solve.

- Integer and non-integer models: In some scenarios, it may be necessary that the decision variable take on integer values only; this is known as an integer model. Models without this integer restriction are non-integer models. The integer restriction of the decision variables does, however, add to the difficulty of solving the problem.

- Deterministic and stochastic models: If for any value of the decision variable, the value of the objective function and whether all constraints are satisfied is known with certainty, then the model is deterministic. A stochastic model does not exhibit this property.

4.3.2 Computational Complexity

Associated with optimisation problems, is a level of difficulty which determines whether the problem is "easy" or "hard" to solve. A particular algorithm is defined as being a polynomial time algorithm if its running time is bounded by a polynomial in the size of the input. An algorithm is said to be of $O(I^p)$ with a bounding polynomial of order p in the size, I of the input data. An exponential time algorithm is used to refer to an algorithm that is not bounded by a polynomial in the length of the input [81]. With regard to operations research, the optimisation problems are divided into two categories, namely class P problems which can be solved in polynomial time and class NP problems which can be solved by a non-deterministic algorithm in polynomial time. A class NP problem is easily verifiable but difficult to solve, whereas a class P problem is relatively easy to solve. Within class NP problems, those that are most difficult to solve are termed as NP-complete. A special aspect relating to such problems is that every problem in NP can be polynomially transformed to every other problem in NP-complete. A particular problem is said to be polynomially transformable to a problem, if the polynomial time algorithm would imply a polynomial time algorithm for the transformed problem. Since, $P \subseteq NP$, it means that if a polynomial time algorithm could be developed for a single NP-complete problem, then every problem in the class NP can be solved with a polynomial time algorithm thus making P equal to NP. However, equating class NP problems to class P problems remains to be the single greatest unsolved problem in theoretical computer science.

4.3.3 Problem Formulation

A mathematical model is used to represent the problem of optimally placing and allocating power to wireless jammers. Thereafter, optimisation techniques and tools will be applied to this model so that decisions can be made regarding the locations and power transmission values of the wireless jammers.

The model needs to address two different factors; one which pertains to determining where to place the jammers, and the other, which deals with what their transmitting power values should be such that eavesdropping nodes are unable to obtain any information from the communicating channels. Essentially, the aim is to cause sufficient interference to the malicious nodes while not jeopardizing communication between the legitimate nodes. There are no geographical restrictions placed on the locations of either the legitimate nodes or the malicious nodes; this aims to best imitate military battlefield type environments. The idea of utilising protective jammers is derived from physical-layer security mechanisms, which aim to maximise the rate of reliable information from the source to the destination, while maintaining data confidentiality against eavesdroppers. It is based on the work conducted by Wyner [41], in which he proposed that perfect secrecy can be achieved without the use of any encryption methods if the eavesdropper's channel is a degraded version of the communication channel, which it wants to eavesdrop upon, then the source and destination are able to ensure privacy of their messages.

The secrecy rate of a communication channel can be improved by increasing the SNR of the destination node or by decreasing the SNR of the eavesdropper. The SNR at the destination node can possibly be improved by shortening the distance between source and destination; however, this generally is not feasible. In order to reduce the SNR at the eavesdropper, a suitable method would be the deployment of jamming devices which are capable of inducing controlled inference in the eavesdropper's channel [47]. The mathematical model seeks to represent a protection scheme that utilises protective jammers to protect randomly distributed networks against randomly dispersed malicious eavesdropping devices. The efficiency of the scheme is increased by minimising the number of jammers required to protect an area and reducing the power consumption levels of the jamming devices.

The mixed integer non-linear problem regarding the optimal jammer placement and power allocation is formulated as:

$$Min. \;\; z = \sum_{k=1}^{N} (c_k + \rho\lambda_k) x_k \tag{4.3}$$

s.t.

$$\sum_{k=1}^{N} q_k^j x_k \leq \delta_L, \;\; j = 1, 2, ..., m \tag{4.4}$$

$$\sum_{k=1}^{N} q_k^j x_k \geq \delta_M, \;\; j = m+1, m+2, ..., m+w \tag{4.5}$$

$$\lambda_k x_k \leq \lambda_{max}, \;\; \forall k \tag{4.6}$$

$$\lambda_k \geq 0, \;\; \forall k \tag{4.7}$$

$$x_k \in \{0,1\}, \;\; \forall k \tag{4.8}$$

Where

- c_k: The cost of installing a jamming device at location k. In a battlefield scenario, it may be risky to place a jammer very close to a malicious node, thus the associated installation cost will be higher.

- ρ: Factor that makes the cost of providing power be the same units as the cost of locating jammers.

- λ_k: The decision variable which is associated with the transmitting power of the jammers.

- x_k: The binary decision variable where 1 indicates that a jamming device is installed at location k and 0 indicates no jamming device at that location.

- N: The number of potential jamming locations.

- δ_L: Jamming threshold value for the legitimate nodes.

- δ_M: Jamming threshold value for the malicious eavesdropping nodes.

- λ_{max}: Maximum value for λ_k.

- m: The number of legitimate communication nodes.

- w: The number of eavesdropper nodes.

- q_k^j: The jamming effectiveness, as given in equation (4.1), experienced by node j from the jammer placed at location k. j is used to denote all the legitimate communication nodes and all the eavesdropper nodes in the wireless network. Nodes $j = 1$ to m denote the legitimate communication nodes, and nodes $j = m+1$ to $m+w$ denote the eavesdropper nodes.

In addition, we define a vector $\mathbf{x} = \{x_1, x_2, ..., x_N\}$ which represents the solution to the problem.

4.3.3.1 Objective Function

There are two decision variables that the objective function, given in equation 4.3, seeks to ultimately minimise. The decision variable associated with the transmitting power of jammer k is λ_k while x_k is the binary decision variable, where 1 indicates that a jamming device is installed at location k, and 0 indicates no jamming device at that location. The factor ρ in the objective function is used to equate the units pertaining to the cost of placing the jammers to the cost of providing power. An associated cost, c_k, of placing a jammer at a particular location is also taken into account in the objective function. The number of potential jamming locations is given as N, and the objective function seeks to minimise both the number of jammers required to protect a particular network, while also minimising the transmitting power. Thus, the product of the sum of the cost and the transmitting power with the binary decision variable, x_k, is given as the objective function and serves as an accurate mathematical model for the problem.

4.3.3.2 Constraints

There are two main constraints related to this problem:

1. Ensuring that the jamming signals sent by the jammers placed at the potential locations do not affect the communication taking place between the legitimate nodes. This is modelled by equation 4.4 which seeks to ensure that the jamming effectiveness, given by q_k^j, that affects the legitimate nodes, nodes 1 to m, is less than the threshold value δ_L.

2. Ensuring that the jamming signals sent by the jammers placed at the potential locations are able to jam the malicious nodes so that they are unable to extract any valid information from the communication channels. This is as a result of the increased noise that it receives from the jammers, thereby reducing its SNR. This is modelled by equation 4.5 which seeks to ensure that the jamming effectiveness experienced by the malicious nodes, nodes $m + 1$ to w, is greater than the threshold value δ_M.

The constraint given in equation 4.6 is used to ensure that the transmitting power for a selected wireless jammer, k, is less than a maximum transmitting power, λ_{max}. This can be attributed to hardware constraints.

Equations 4.7 and 4.8 are constraints placed on the two decision variables, λ_k and x_k, respectively. As λ_k represents the transmitting power associated with the jammer, it has to be a positive real number. The variable associated with the selection of jammer, x_k, has to be a binary variable, where a 0 indicates that the jammer is not selected and a 1 indicates that the jammer is selected.

4.3.3.3 Non-linearity

The problem as defined is non-linear owing to the term $\lambda_k x_k$ which appears in the objective function, equation 4.3, and in the constraints given in equation 4.6 and equation 4.7. λ_k is obtained from the jamming effectiveness equation which is shown again in equation 4.9. The squared terms which are inversely proportional to λ_k makes the λ_k term non-linear.

$$q_k^j = \frac{\lambda_j}{(X_k - X_j)^2 + (Y_k - Y_j)^2} \tag{4.9}$$

In order to solve linear problems, the linear constraints are sketched and a feasible region is obtained, after which, an optimal solution is found at one of the corner or extreme points of the region. However, non-linear problems are significantly more difficult to solve than linear problems. There are a number of reasons for this which includes not being able to distinguish between local and global optimum for a particular non-linear problem, the presence of multiple disconnected feasible regions as well as an uncertainty associated with the outcome of a non-linear problem. For linear programming models, there are typically only a few definite outcomes: the model is feasible and a global optimum solution can be found, or that the model is feasible but unbounded or quite simply, the model is infeasible. However, there are uncertainties associated with outcomes of non-linear models. These include the fact that it is difficult to be sure that the solution found is definitely an optimum solution and not just a local optimum, or that the model is indeed bounded and feasible. Also, as a result of the non-linear constraints and non-linear objective function, there are no corner or extreme points at which the optimal solution can be found. Owing to the wide range of characteristics associated with non-linear problems, there are various different types of algorithms targeted at solving very specific types of non-linear problems. There are, however, very few commercially implemented algorithms available because of the numerous complexities associated with non-linear problems.

The problem, as shown in equations 4.3 to 4.8, is computationally intractable and highly complex as a result of the aforementioned difficulties related to non-linear problems. Adding to the difficulty of solving the problem, is determining the factor ρ that is used to equate the units pertaining to the cost of placing the jammers to the cost of providing power. Therefore, an alternate approach is taken. The problem is decomposed into two sub-problems which serve as an approximation and the decision is then made sequentially. By this we mean that the number of jammers and their locations are first determined, and then the power allocation sub-problem associated with the selected jammers is solved. Essentially, an initial value, or a maximum transmitting power is set for all jammers; once the minimum number of jammers required to protect a certain network is established, the transmitting power is further decreased to an amount that satisfies all constraints thereby saving energy and increasing cost efficiency.

The decomposition of the problem into the linear sub-problems eliminates the non-linearity caused by the λ_k value, which is a quadratic function of the legitimate and malicious node's positions. As the jammer placement problem is implemented first, the positions of the malicious nodes become known and as a result, λ_k is simply the required jamming effectiveness multiplied by a constant.

4.3.4 Jammer Placement Sub-problem

The jammer placement sub-problem is modelled as a multiple demand multi-dimensional knapsack problem. A typical knapsack problem is an integer linear program consisting of an objective function with binary decision variables and a single constraint with positive coefficients. The problem can be seen as choosing a subset of items, with an associated profit and weight, such that the overall profit is maximised while not exceeding the knapsack capacity. It is analogous to a hitch-hiker needing to fill a knapsack for a trip. There are N total items available for selection, and each item, x, has a profit value p, which represents the degree of usefulness of the item, as well as an associated size or weight w. The aggregated weight of all selected items cannot exceed the maximum capacity, c, of the knapsack. Thus, the objective of the hitch-hiker is to select a subset of items such that the overall value of the knapsack is maximised while not violating the knapsack's capacity constraint. The general form of a knapsack problem is given as:

$$Max. \;\; z = \sum_{k=1}^{N} p_k x_k \tag{4.10}$$

s.t.

$$\sum_{k=1}^{N} w_k x_k \leq c \tag{4.11}$$

$$x_k \in \{0,1\}, \;\; \forall k \tag{4.12}$$

Knapsack problems are known to be difficult to solve and are considered *NP*-hard [82]. *NP*-hard, which stands for Non-deterministic polynomial-time hard, is a term used to describe the computational complexity of finding solutions to particular computational problems. A polynomial-time algorithm refers to an algorithm where the corresponding running time is bounded by a polynomial in input size. *NP*-hard problems essentially means that it is highly improbable that polynomial-time algorithms can be devised for solving the problems. There are no exact solution techniques for solving the NP-hard knapsack problem other than by a possible complete enumeration of the solution space. The following are some of the techniques or tools used for reducing the difficulty in solving knapsack problems:

- Branch-and-bound method: This technique is especially effective for solving *NP*-hard optimisation problems. It basically searches the solution space until the best solution is found. However, complete enumeration is not possible as a result of the exponential increasing number of potential solutions, and as a result, bounds for the objective function are used to implicitly search parts of a solution space.

- Dynamic programming: This technique searches the solution space in a breadth-first fashion rather than depth-first as with the branch-and-bound technique. It can also evolve into "advaced" forms of the branch-and-bound method if bounding tests are added. There is also the addition of dominance rules in this programming technique.

- State space relaxation: This is a dynamic programming relaxation in which the coefficients are scaled by a particular value in effort to reduce the time and space complexity, but at the cost of a loss in optimality.

- Pre-processing: This involves fixing certain decision variables a-priori at their optimal values based on the results of certain bounding tests that are used to exclude certain values for the decision variables.

This sub-problem aims to find the minimum number of jammers from N potential jamming locations such that the interference caused by the jammers do not affect the communication taking place between the legitimate nodes, but reduces the SNR of the malicious eavesdropping nodes so that they are unable to obtain any information from the communicating nodes. The problem formulation is given as:

$$Min. \;\; z = \sum_{k=1}^{N} c_k x_k \tag{4.13}$$

s.t.

$$\sum_{k=1}^{N} q_k^j x_k \leq \delta_L, \;\; j = 1, 2, ..., m \tag{4.14}$$

$$\sum_{k=1}^{N} q_k^j x_k \geq \delta_M, \;\; j = m+1, m+2, ..., m+w \tag{4.15}$$

$$x_k \in \{0, 1\}, \;\; \forall k, \tag{4.16}$$

where the parameters are defined as for the main problem (equations 4.3 to 4.8). The solution to this sub-problem will be a vector $\mathbf{x}^* = \{x_1^*, x_2^*, ..., x_N^*\} \in \{0,1\}^N$. We also define L to represent the number of optimal jammer locations as $L = \sum_{k=1}^{N} x_k^*$. Further let $\mathcal{L} = \{i_1, i_2, ..., i_L\}$ where $x_{i_v}^* = 1$.

This problem is modelled as a multiple demand multi-dimensional knapsack problem. There are numerous variations and extensions of the classic knapsack problem which are used to model different scenarios. A popular variation is the inclusion of demand constraints which in terms of the knapsack analogy, can be seen as representing the minimum capacity of the knapsack. The knapsack constraint is a less-than-or-equal-to constraint, as shown in equation 4.1, whereas a demand constraint is a greater-than-or-equal-to constraint. If the classic knapsack problem, as shown in equations 4.10 to 4.12, has a set of dimensions, then it is referred to as a multi-dimensional knapsack problem. A multi-dimensional problem is defined by the same set of N items but with m dimensions. The knapsack capacity constraint limits the capacity in each dimension, j, denoted by c^j. As with the classic case, each item x_k, has a profit value p_k with an associated weight, w_k^j, for each dimension. Adding the demand constraints to the multi-dimensional knapsack problem results in the formation of the multiple demand multi-dimensional knapsack problem. With m capacity constraints and q demand constraints, the general form of a multiple demand multi-dimensional knapsack problem is given as:

$$Max. \;\; z = \sum_{k=1}^{N} p_k x_k \tag{4.17}$$

s.t.

$$\sum_{k=1}^{N} w_k^j x_k \leq c^j, \;\; j = 1, 2, ..., m \tag{4.18}$$

$$\sum_{k=1}^{N} w_k^j x_k \geq c_M, \;\; j = m+1, m+2, ..., m+q \tag{4.19}$$

$$x_k \in \{0, 1\}, \;\; k = 1, 2, ..., N \tag{4.20}$$

It can be seen that the jammer placement sub-problem, shown in equations 4.13 to 4.16, is written in the form of a multiple demand multi-dimensional knapsack problem, except that it has a minimisation objective function as opposed to the maximisation objective function that is associated with knapsack problems.

4.3.5 Power Allocation Sub-problem

The optimisation sub-problem related to the power allocation of the jammers is formulated as:

$$Min. \;\; z = \sum_{k \in \mathcal{L}} \lambda_k \tag{4.21}$$

s.t.

$$\sum_{k \in \mathcal{L}} q_k^j \leq \delta_L, \;\; j = 1, 2, ..., m \tag{4.22}$$

$$\sum_{k \in \mathcal{L}} q_k^j \geq \delta_M, \;\; j = m+1, m+2, ..., m+w \tag{4.23}$$

$$\lambda_k \leq \lambda_{max}, \;\; \forall k \tag{4.24}$$

$$\lambda_k \geq 0, \;\; \forall k, \tag{4.25}$$

where the parameters are as previously defined. The solution to this sub-problem will be a vector $\boldsymbol{\lambda}^* = \{\lambda_1^*, \lambda_2^*, ..., \lambda_L^*\}$.

This problem does not have an integer constraint, as is in the case for the jammer placement problem. Techniques for solving real-valued linear problems can be used to obtain the values associated with the chosen jammers given in the $\mathcal{L}$ set.

4.3.6 Comparison of Non-linear and Linear Formulations

For ease of reference, the non-linear problem's objective function is shown again in equation 4.26.

$$Min. \;\; z = \sum_{k=1}^{N} (c_k + \rho\lambda_k)x_k \tag{4.26}$$

The non-linearity of the problem is as a result of $\lambda_k x_k$ term, which is obtained by solving the jamming effectiveness equation shown in equation 4.9. A way of linearising the non-linear problem so that it is computationally tractable and can be solved in polynomial time, is by approximating the problem as a linear one. Although this may seem as the most probable route for eliminating the non-linearity in the problem, an additional parameter, ρ present in the objective function, further increases the complexity of the problem. This parameter is a factor that serves as means of equating the units of the cost related to the transmitting power of the jammers, to the cost of placing the jammers. In order to address these difficulties, an alternate approach is taken in which the non-linear problem is decomposed into two separate linear problems. These two formulations are solved sequentially resulting in an approximate solution to the non-linear problem.

As is inherent in the nature of the problem itself, the optimal placement and power allocation of the jammers can be seen as two separate sub-problems. Following suite, the non-linear problem is approximated by two linear sub-problems; the first of which pertains to the optimal placement of the jammers, and the second is related to the transmitting power values of those jammers. These problems are solved sequentially, meaning that the jammers to be placed for protecting a particular network, are chosen from a set of potential jammer locations, and then the allocation of the transmitting power values are performed on those chosen jammers.

As is seen in equations 4.13 to 4.16, which models the jammer placement sub-problem, the objective function involves the cost of placing the jammers, c_k, and the binary jammer variable, x_k; the non-linear variable, $\lambda_k x_k$, which relates the transmission power of the variables is absent thus making the problem completely linear. The value for λ_k, which is required for calculating the jamming effectiveness, is set to a constant, which will be minimised in the subsequent solving of the power allocation sub-problem. The value that λ_k is set to for the jammer placement sub-problem should be large enough so that when jammers are placed at all potential jamming locations, they should be able to cover the entire network area. However, the value should not be too large, otherwise there would be numerous possibilities of different sets of jammer locations with the same minimum number of jammers. The amount of overlapping coverage areas by the jammers will not have an effect in solving the problem as the power allocation problem aims to minimise this area. However, if λ_k is selected to be too large, there would be an increase in the number of possible solutions all yielding the same minimum number of jammers. A particular set of jammers may result in a better transmitting power reduction after implementing the second sub-problem which serves to optimise the power allocation for a particular set of jammers. This can possibly compromise the overall optimality achieved in solving the linear approximations. Therefore, setting the coverage radius to be equal to the maximum step size between the potential jammer locations is found to be ideal. All the constraints for the linear jammer placement sub-problem is equivalent to the constraints for the non-linear problem formulation, except for the constraint related to the value of λ_k; this is handled in the power allocation sub-problem.

The power allocation sub-problem is a linear non-integer optimisation problem that serves to minimise the λ_k value which is directly related to the transmitting power of a set of pre-selected jammers. The constraints related to this problem are the same as the constraints for the non-linear problem formulation, except that the x_k binary variable which is used to select jammers, is not a decision variable in this sub-problem and thus, does not feature in the constraints of this problem. Once the optimal set of jammers is selected from solving the jammer placement sub-problem, the optimisation of the transmission power values of the selected jammers is performed.

In essence, the non-linear problem formulation addressing the optimal placement and power allocation of wireless jammers, is decomposed into two separate linear problems that are solved sequentially. There is no loss in optimality faced by approximating the non-linear formulation as two separate linear formulations; this is achieved by eliminating the $\lambda_k x_k$ non-linear term in the two sub-problems. The first linear integer sub-problem only concerns itself with the optimisation of the number of jammers required to protect an area. In the second linear non-integer sub-problem, the term λ_k, appears in the objective function in which it is minimised for a pre-selected group of jammers, as determined in the solution of the jammer placement sub-problem. This decomposition can be viewed as the separation of the non-linear $\lambda_k x_k$ variable, into x_k and λ_k decision variables thereby eliminating the non-linearity of the problem. Additionally, this decomposition eliminates the difficulty in determining the ρ factor that is used for equating the cost units for the placement and power allocation of the jammers in the original non-linear problem.

4.4 CONCLUDING REMARKS

The method of protecting wireless networks against malicious nodes that seek to obtain confidential information through the strategic placement of wireless jammers, is formulated as a mathematical programming problem. The problem is modelled as a non-linear optimisation problem that jointly addresses the optimal placement and optimal power allocation of wireless jammers in a multi-hop network with multiple sources, eavesdroppers and destinations. The network environment upon which the problem is modelled after, aims to closely represent the deployment of WMNs in military battlefields. There are no restrictions on the geographical placement of the jammers. They are placed interspersed amongst the legitimate nodes and the malicious nodes in such a way so as to prevent the malicious nodes from gaining any information, while not jeopardizing the communication between the legitimate nodes.

Owing to the difficulty and computational intensive nature of non-linear problems, the problem is linearised by approximating the joint non-linear problem as two separate linear problems that are sequentially solved. The first of which is used to address the problem of determining and placing a minimum number of jammers to protect a multiple source and destination network. This jammer placement sub-problem is modelled as a multiple demand multi-dimensional knapsack problem. A default value is assumed to be used for representing the transmitting power for the wireless jammers in the jammer placement sub-problem. Once the optimal placement of the jammers have been determined, the transmitting power values are optimised upon for those wireless jammers. The power allocation sub-problem is modelled as a non-integer linear minimisation problem with constraints ensuring the power values allocated to the jammers, are sufficient to protect the wireless network without the need of any additional wireless jammers. The further optimisation of the transmitting power of the wireless jammers seeks to improve the efficiency of the security model and is performed on those jammers that have been selected by the jammer placement sub-problem. There is no loss in optimality faced by approximating the non-linear formulation as two separate linear formulations. This is because this decomposition can be viewed as the separation of the non-linear $\lambda_k x_k$ variable, into x_k and λ_k decision variables thereby eliminating the non-linearity of the problem. Furthermore, this decomposition also eliminates the difficulty in determining the ρ factor that is used for equating the cost units for the placement and power allocation of the jammers in the original non-linear problem.

CHAPTER 5

OPTIMISATION TECHNIQUES

5.1 INTRODUCTION

Algorithms for solving optimisation problems are divided into two categories, namely, exact algorithms and heuristics. Using an exact algorithm to solve an optimisation problem guarantees that an optimal solution will be found upon termination. Heuristics, on the other hand, place emphasis on finding high quality solutions in a much shorter time than exact algorithms; however, optimality is not guaranteed. Most non-trivial instance of problems in class NP cannot be solved by exact algorithms, and so the need for the development of efficient heuristics to solve real world instances arises.

5.2 EXACT ALGORITHMS

The most popular exact algorithm employed to solve linear real-valued optimisation problems is the simplex method. This is the method used to solve the power assignment sub-problem. With regard to linear integer problems, the branch-and-bound method is typically used. A variation of this method is the branch-and-cut algorithm which is employed as the exact algorithm for solving the jammer placement sub-problem.

5.2.1 Simplex Method

The simplex method was developed by George B. Dantzig in 1947 for solving linear programming problems as a part of the Scientific Computiation of Optimum Programs research group of the U.S. Air Force. It is consistently ranked as the one of the top ten most important algorithms of the 20th century. The simplex algorithm is widely used in several modelling languages and proves to be very efficient in solving problems with tens of thousand or more of variables and constraints [83].

Essentially, the simplex method obtains an optimal solution by moving from one feasible solution to another in effort to improve the objective function value. There is a termination that occurs after a finite number of movements. The simplex method is robust in that it solves any linear program, it is able to detect redundant constraints, while being able to identify instances of the linear program which result in unbounded objective values. It is also able to solve problems with multiple optimal solutions. This method is self-initiating which means that it uses itself to obtain a feasible solution which is used for the commencement of this algorithm. Not only does the simplex method return the optimal solution, it also indicates how the optimal solution changes according to the values of the cost coefficients, constraint coefficients and the right-hand side data. This is used to relate the original linear program to its dual problem. The simplex method also provides the optimal solution of this dual problem.

It is necessary to transform the linear programming problem into canonical form, after which the simplex method is applied to obtain the optimal solution. The following steps are required to transform a general linear programming problem into its canonical form:

1. For every decision variable that is unconstrained in sign, replace it by a difference between two non-negative variables. This should be done for all constraint equations as well as in the equations for the objective function.

2. Replace all inequalities with equalities. This is achieved through the use of surplus and slack variables. For $\leq$ inequalities, a non-negative surplus variable is used to represent the amount by which the left-hand side exceeds the right-hand side; and for $\geq$ inequalities, a non-negative slack variable is used to represent the amount by which the right-hand side exceeds the left-hand side.

3. Multiply equations with a negative right-hand side coefficient by -1.

4. In order to isolate basic variables in each constraint, add a non-negative artificial variable variable to those equations that do not have an isolated basic variable. The reason

for the isolation of the basic variables is discussed in the summary of the simplex algorithm that follows.

The simplex algorithm can be summarised as follows:

1. The linear programming problem is written in canonical form with positive decision variables, equality constraints, positive right-hand side coefficients and a single decision variable isolated in each constraint. The decision variable that is isolated in each constraint is termed as a basic variable. In general, setting the k^{th} basic variable isolated in constraint k equal to the right-hand side of the k^{th} constraint, and setting the remaining variables, termed as non-basic variables, to zero yields a basic feasible solution. In a maximisation problem, the basic feasible solution maximises the objective function over the feasible region if every non-basic variable has a negative coefficient in the objective function.

2. Corresponding to a basic feasible solution, a tableau is formed. In general, if the basic variables are $x_1, x_2, ..., x_m$, the simplex tableau takes the form as shown in table 5.1.

Table 5.1: General form of a simplex tableau

x_1	x_2	...	x_m	x_{m+1}	x_{m+2}	...	x_j	...	x_n	RHS
1	0	...	0	$a_{1,m+1}$	$a_{1,m+2}$	...	$a_{1,j}$	...	$a_{1,n}$	b_1
0	1	...	0	$a_{2,m+1}$	$a_{2,m+2}$	...	$a_{2,j}$	...	$a_{2,n}$	b_2
0	0	...	0	$a_{i,m+1}$	$a_{i,m+2}$	...	$a_{i,j}$	...	$a_{i,n}$	b_i
0	0	...	1	$a_{m,m+1}$	$a_{m,m+2}$	...	$a_{m,j}$	...	$a_{m,n}$	b_m
0	0	...	0	c_{m+1}	c_{m+2}	...	c_j	...	c_n	$(-z)$

3. From the table, if each $c_j \geq 0$, then the current basic feasible solution is optimal. The method will then get terminated.

4. In order to determine which non-basic variable should become the basic variable, select q such that $c_q < 0$.

5. The ratios $b_i/a_{i,q}$ are calculated for $a_{i,q} > 0, i = 1, 2, ..., m$. If there are no values for which $a_{i,q} > 0$, then the problem is unbounded. Otherwise, the value of p is selected as the index i corresponding to the minimum ratio as shown in equation 5.1.

$$\frac{b_p}{a_{p,q}} = min_i \left\{ \frac{b_i}{a_{i,q}}; \quad a_{i,q} > 0 \right\} \tag{5.1}$$

6. Pivot on the pq^{th} element, and update all rows.

5.2.2 Branch-and-bound Method

Integer programming models arise in practically every area of application of mathematical programming. While the simplex method is the most popular method used for solving non-integer optimisation problems, integer optimisation problems are significantly more difficult to solve. In general, the different methods available for solving these problems can be divided into three groups: enumeration techniques, cutting-plane techniques and group-theoretic techniques. In effort to improve the computational efficiency of solving integer programming problems, several composite procedures that combine numerous techniques have been proposed. The branch-and-bound technique [84] is an enumeration method and refers to a large family of methods all having a general "divide and conquer" approach. The exact steps to be carried out differ according to the problem that needs to be solved, and the available software tools.

Solving integer optimisation problems does not simply involve rounding the corresponding linear optimisation problem's solution. The rounded solutions may not be close to the optimal solution, let alone be feasible. There can also be numerous different rounded solutions. The branch-and-bound method is based on the idea of systematically partitioning the feasible region into smaller manageable regions, and performing appropriate assessments on these regions. As there are numerous possible ways of performing this dividing of the region, there are a number of different branch-and-bound algorithms.

The basic procedure of the branch-and-bound method makes use of the fact that for a maximisation problem, the solution to the linear problem without the integer constraints (the relaxed optimisation problem), provides an upper bound on the optimal integer-programming problem's objective. In addition, the solution to the integer maximisation problem provides a lower bound on the solution of the corresponding relaxed maximisation problem. For a minimisation problem, a lower bound is provided by the solution of the relaxed non-integer problem, and the solution to the integer minimisation problem provides an upper bound. This observation is used for partitioning the feasible region. At first, the feasible region is kept intact, the integer constraints are removed, and the associated relaxed linear programming problem is solved to obtain a solution, z^0. If a maximisation problem is assumed, z^0 gives an upper bound on the optimal solution, z^*. The dividing of the feasible region is guided by the fractional solution obtained when solving the relaxed linear programming problem. If, for example, the solution to one of the variables yields a value of 2.25, then when taking into account the integer constraints, this value should either be less than 2 or greater 3. Therefore, the first subdivision can be dividing the region into values ≤ 2 and ≥ 3. An enumeration tree can be used to represent this division. For each branch in this tree, the solution is obtained and analysis for further division takes place; this process is known as fathoming. The sub-problem is fathomed into the following cases:

1. The optimal solution of the sub-problem satisfies all the constraints of the integer optimisation problem, and the objective function values of both the integer problem and the relaxed problem are equal. This is known as fathoming by integrality.

2. The relaxed sub-problem yields an infeasible solution. This implies that the unrelaxed integer sub-problem is also infeasible. This is known as fathoming by infeasibility.

3. The relaxed sub-problem has an optimal solution that is worse than the current best known solution. This is known as fathoming by bounds.

Once all branches are fathomed, the algorithm can be terminated and no further subdivision is required. To summarise, the branch and bound method involves the following steps:

1. Solve the associated linear problem without any integrality constraints. For a maximisation problem, the upper bound is provided by this solution. Set this solution as $\bar{z}$. Set the value of the best known feasible solution as $\underline{z}$.

2. Analyse the solution. If the linear sub-program solution is infeasible, then the optimal solution is set as $z^* = \underline{z}$ and the algorithm is terminated. If the solution is found to be all integer values, then the method is also terminated if it is better than the best known solution.

3. The previous step is performed for every sub-problem which is determined by dividing the feasible region as guided by the fractional value obtained for a particular decision variable.

5.2.3 Cutting Plane Technique

The cutting plane method [85] is used to find solutions to integer optimisation problems by modifying linear non-integer optimisation problems until an integer solution is obtained. It differs from the branch-and-bound method as no partitioning is involved; instead, additional constraints are successively added to the linear non-integer optimisation problem. The process of adding new constraints essentially cuts or reduces the feasible region until an optimal integer solution is obtained. The process of generating the additional constraints or cuts until an integer solution is obtained can be quite taxing. It was shown by R. Gomory in 1958 that an integer problem can be solved by an associated linear problem with a finite number of added constraints of cuts [75]. Even though a finite number of cuts need to be added, the number tends to be quite large, and practically makes it infeasible to utilise. Although this algorithm is known to perform worse than the branch-and-bound method, it has provided means of determining more efficient algorithms for solving integer optimisation problems [75]. This is evident in the branch-and-cut method that is subsequently discussed and utilised for solving the jammer placement sub-problem.

5.2.4 Branch-and-cut Method

The branch-and-cut method [86] is a complicated method for solving mixed integer linear problems. In general, the branch-and-cut method solves a sequence of linear programming relaxations of the integer programming problem. The cutting plane method improves the relaxation of the problem to more closely approximate the integer programming problem, and then the branch-and-bound algorithms use a sophisticated divide and conquer approach to solve the problem. As has been discussed, it is not usually possible to efficiently solve a general integer optimisation problem using only the cutting plane method, thus branching in addition to using the cutting place method results in the branch-and-cut algorithm. Solving the integer problem with only the branch-and-bound method can considerably be sped up with the use of the cutting plane which significantly reduces the enumeration tree. The cutting plane method can be employed either at the top of the enumeration tree, or at each node in the tree. The branch-and-cut algorithm has been used to solve a number of combinatorial optimisation problems including linear ordering problems, scheduling problems, packing problems, network design problems, maximum cut problems and finding maximum planar subgraphs. The best known application of the branch-and-cut algorithm is to solve the travelling salesman problem [87].

The branch-and-cut algorithm used for solving the integer jammer placement problem is given as:

1. Initialisation: denote the initial jammer placement integer problem as ILP^0 and set the active nodes to be $L = \{ILP^0\}$. Set the upper bound of the total number of jammers to be $\overline{z} = +\infty$. Select one problem $1 \in L$ and set its lower bound to be $\underline{z_1} = -\infty$.

2. Termination: If $L = \emptyset$, then the solution x^* which yielded the incumbent objective value z is optimal. If no such x^* exists $(z = +\infty)$ then the integer linear program is infeasible.

3. Problem selection: Select and delete a problem ILP^1 from L.

4. Relaxation: Solve the linear programming relaxation of ILP^1. If the relaxation is infeasible, set $\underline{z_1} = +\infty$ and go to step 6. If the relaxation is feasible, then let z_1 denote the optimal objective value of the relaxation if it is finite and let x^{1R} be an optimal solution; otherwise set $\underline{z_1} = -\infty$.

5. Add cutting planes: Search for cutting planes that are violated by x^{1R}; if any are found, add them to the relaxation and return to Step 4.

6. Fathoming and pruning: If $\underline{z_1} \geq \overline{z}$ then go to Step 2. Otherwise if $\underline{z_1} < \overline{z}$ and x^{1R} is integral feasible, update $z = z_1$, delete from L all problems with $z_1 \geq z$, and go to Step 2.

7. Partitioning: Let S^{1j} be a partition of the constraint set S^1 of problem ILP^1. Add problems ILP^{1j} to L where ILP^{1j} is ILP^1 with feasible region restricted to S^{1j} and $\underline{z_{1j}}$ for $j = 1, 2, ..., k$ is set to the value of $\underline{z_1}$ for the parent problem 1. Go to step 2.

5.3 ALTERNATING CONTROL TREE BASED HEURISTIC

The intriguing combinatorial structure of the integer jammer placement sub-problem makes it challenging to solve using traditional integer linear programming methods such as the branch-and-cut method. The multiple demand multi-dimensional knapsack problem is an NP-complete problem as the subset sum problem reduces to satisfying two conflicting binary constraints [88]. The associated knapsack constraints force a large number of variables to be set to zero, whereas the demand constraints stipulate that a certain number of variables be set to one. This makes it difficult to even identify a feasible solution of the problem. A heuristic method is thus proposed as a more computationally efficient method than the branch-and-cut method for solving the jammer placement problem (JPP).

5.3.1 Heuristic Overview

The heuristic is based on the method proposed by Hvattum *et al.* for solving traditional multi-dimensional knapsack problems with a maximisation objective [89]. The method operates by transferring control successively to three components: ACT-1, ACT-2 and ACT-3. An initial integer feasible solution, x^{UB} is assumed to be known with associated value z^{UB}, for the original JPP. If no starting solution is known, z^{UB} is equated to $N + 1$, where N is the number of potential jamming locations.

The first component relaxes the problem by ignoring the integer constraint and a solution, x' with objective value, z' is obtained. The method terminates if the linear relaxation has no feasible solution or if $z' \geq z^{UB}$. If x^{UB} was selected as a feasible solution then the heuristic terminates with this being the solution to the JPP problem, otherwise JPP is proved to have no feasible solution. Control is given to ACT-2 if a feasible solution to the relaxed JPP is found to be less than z^{UB}.

ACT-2 distinguishes between three types of values of the solution x': a) values between 0 and 1; b) 1's and c) 0's. An integer sub-problem is defined where both type b and type c variables are kept fixed, and the other variables are forced to take on either a 0 or 1 such that the overall objective value is reduced by 1. If a feasible solution is found to this sub-problem, and it is better than the current z^{UB}, then this solution is recorded as the new x^{UB}, z^{UB}. After this, control shifts to ACT-3.

ACT-3 essentially adjoins inequalities to the JPP to prevent the relaxed linear problem in ACT-1 from creating a situation where a currently selected assignment set (as selected in ACT-2), can duplicate any assignment set previously chosen. In a similar manner, the inclusion of these inequalities prevent the solution to the sub-problem in ACT-2 from duplicating any solution previously obtained.

The process is a cyclic one which moves from ACT-3 back to ACT-1 and proceeds through the different components until the method is forced to terminate by the conditions stipulated in ACT-1. The heuristic can be viewed as an iterative one in which the problem is continuously altered by the components of the framework, in effort to improve the solution while searching the entire solution space. With each iteration of the ACT framework, a subsection of the entire solution space, S, is explored. This is illustrated in figure 5.1. For a particular iteration, i, let the subspace $S_i \subset S$ be the feasible region for the current sub-problem defined in ACT-2. The added inequalities in ACT-3 ensure that the subsets are disjoint for consequent iterations of the ACT-framework. The solution space consists of a finite, but typically large, number of subsets that cover the solution space S. In essence, the ACT heuristic operates by breaking up the solution space into smaller sets which are iteratively selected, and is governed by the solution found to the relaxed linear problem in ACT-1.

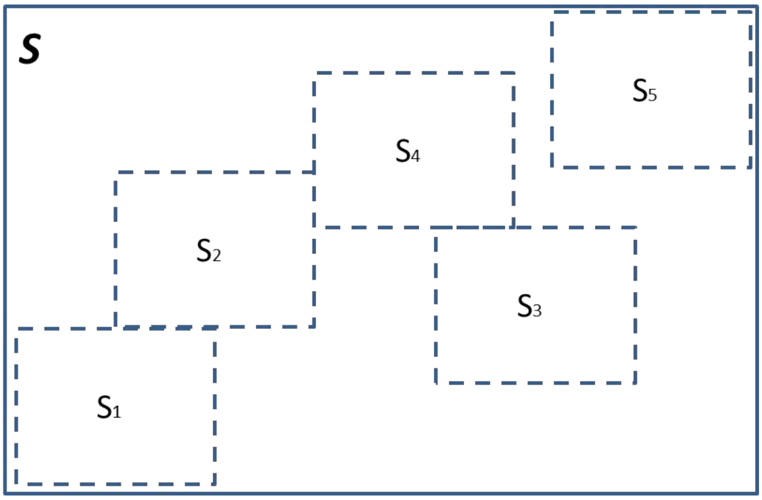

Figure 5.1: Subsections of solution space as performed in ACT-2

Summary of what each component is responsible for:

- ACT-1: Removes integer constraint. Guides the process of selecting the subset of the solution space that will be explored. Terminates solution based on certain conditions.

- ACT-2: Improves solution by fixing certain variables (both the 0's and the 1's) and solving the corresponding sub-problem so that the objective value is lower than the recorded best solution, z^{UB}. Updates z^{UB}.

- ACT-3: Adjoins inequalities that prepares the JPP for the next iteration by ensuring that a different part of the solution space is explored.

5.3.2 Algorithm

The heuristic operates by transferring control successively to three components: ACT-1, ACT-2 and ACT-3. An initial integer feasible solution to the JPP, x^{UB} is assumed to be known with associated value z^{UB}. If no starting feasible solution is known, then z^{UB} is equated to $N+1$, where N is the number of potential jamming locations. The three components are explained as follows:

ACT-1

1. Solve the linear programming relaxation LP-JPP of the JPP to obtain solution x' with value z'.

2. If LP-JPP has no feasible solution, or if $z' \geq z^{UB}$, then the method terminates with one of the following conclusions:

   (a) If $0 \leq z^{UB} \leq N$ then x^{UB} is optimal for the original JPP.

   (b) Otherwise, JPP is proven to have no feasible solution.

ACT-2

1. With reference to the solution x' of LP-JPP, let $\mathbf{N}^0(x') = \{k|x'_k = 0\}$, $\mathbf{N}^1(x') = \{k|x'_k = 1\}$, and $\mathbf{N}^F(x') = \{k|0 < x'_k < 1\}$.

2. Choose an assignment set $\mathbf{N}^{\#}(x')$ as the set which is the union of the subsets $\mathbf{N}^0(x')$ and $\mathbf{N}^1(x')$. Define the sub-problem SUB-JPP to be the current JPP, subject to $x_k = x'_k$ for $k \in \mathbf{N}^{\#}(x')$ and

$$\sum_{k\in\mathbf{N}} c_k x_k \leq z^{UB} - 1 \tag{5.2}$$

3. Apply some method to solve SUB-JPP. If a feasible solution x^{SUB} is found, the solution yields $z^{SUB} < z^{UB}$, and this solution is recorded as the new x^{UB}, z^{UB}.

ACT-3

1. For the part of the assignment set, $\mathbf{N}^{\#}(x')$, that is a subset of $\mathbf{N}^0(x')$, adjoin the following constraint to the system:

$$\sum_{k\in\mathbf{N}^0(x')} x_k \geq 1 \tag{5.3}$$

Or, alternatively, for part of the assignment set $\mathbf{N}^{\#}(x')$ which is a subset of $\mathbf{N}^1(x')$, adjoin the following constraint to the system:

$$\sum_{k\in\mathbf{N}^1(x')} x_k \leq |\mathbf{N}^1(x')| - 1 \tag{5.4}$$

2. Return to ACT-1 to solve the resulting new version of the JPP.

5.3.3 Additional Comments

1. The sub-problem SUB-JPP has the form:

$$Min.\ \ z = \sum_{k\in\mathbf{N^{SUB}}} c_k x_k + c^{SUB} \tag{5.5}$$

s.t.

$$\sum_{k\in\mathbf{N^{SUB}}} q_k^j x_k \leq \delta_L^{SUB},\ \ j = 1, 2, ..., m \tag{5.6}$$

$$\sum_{k\in\mathbf{N^{SUB}}} q_k^j x_k \geq \delta_M^{SUB},\ \ j = m+1, m+2, ..., m+w \tag{5.7}$$

$$x_k \in \{0, 1\},\ \ k \in \mathbf{N^{SUB}} \tag{5.8}$$

where $c^{SUB} = \sum_{k\in\mathbf{N}^{\#}(x')} c_k x'_k$, $\delta_L^{SUB} = \delta_L - \sum_{k\in\mathbf{N}^{\#}(x')} q_k^j x'_k$ for $j = 1, 2, ..., m$, $\delta_M^{SUB} = \delta_M - \sum_{k\in\mathbf{N}^{\#}(x')} q_k^j x'_k$ for $j = m+1, m+2, ..., m+w$, and $\mathbf{N^{SUB}} = \mathbf{N}\backslash\mathbf{N}^{\#}$.

2. The constraints added in ACT-3 prevent the LP-JPP solution in ACT-1 from creating a situation where a currently selected assignment set $\mathbf{N}^{\#}(x')$ was previously chosen. In the same way, the inclusion of these constraints within the SUB-JPP (as inherited from the current JPP) prevents the duplication of the assignment set. This also ensures that the heuristic is finite.

3. The heuristic will lead to an exact solution because an exact algorithm, the branch-and-cut method, is used to solve the SUB-JPP in ACT-2.

4. The method is exhaustive if the entire solution space is explored through the iterative implementation of the different components. However, given that the use of the heuristic is to primarily reduce the computation time, the number of iterations are terminated if a worse solution to the current best solution is found after adjoining the constraints given in ACT-3. This implies that the search is not entirely exhaustive and there is a trade-off between an optimal solution and the time taken to find it. This termination rule is highlighted in point 2 of the ACT-1 component.

5.4 CONCLUDING REMARKS

The different optimisation techniques that are used in solving the optimisation problems formulated in the previous chapter are discussed. The non-linear optimisation problem that jointly addresses the optimal placement and power allocation of wireless jammers was decomposed into two linear problems. The selection of wireless jammers is modelled as a zero-one multiple demand multi-dimensional knapsack problem with a minimisation objective. This is an integer optimisation problem which is significantly more difficult to solve than linear non-integer problems. The second sub-problem relating to the power allocation of selected jammers, is modelled as a linear minimisation problem with no integrality constraints. The most popular method for solving such a problem is through the application of the simplex method. The simplex method is a simple way of obtaining the solution to a real-valued optimisation problem. It basically moves along the edges of the polytope defined by the constraints, from vertex to vertex with successively smaller values of the objective function, until the minimum is reached. The branch-and-cut method, which is the method used for solving the integer jammer placement sub-problem, is a more complicated method for solving mixed integer linear problems. In general, the branch-and-cut method solves a sequence of linear programming relaxations of the integer programming problem. The cutting plane method improves the relaxation of the problem to more closely approximate the integer programming problem, and the branch-and-bound algorithms use a sophisticated divide and conquer approach to solve the problem.

Furthermore, a heuristic for solving the jammer placement sub-problem is developed in order to increase the efficiency of the proposed security scheme. Although the branch-and-cut method is fairly effective in obtaining the optimal solution for integer optimisation problems, the computational complexity and execution time associated for large problems decreases the efficiency of the algorithm. In military environments especially, it is necessary to obtain solutions in a fast manner given the criticality associated with the information exchanged. An ACT structure based heuristic is developed for solving the multiple demand multi-dimensional knapsack problem with a minimisation objective that is associated with the placement of the wireless jammers. The method operates by transferring control successively to three components: ACT-1, ACT-2 and ACT-3. The process is a cyclic one which moves from ACT-3 back to ACT-1 and proceeds through the different components until the method is forced to terminate by the conditions stipulated in ACT-1. The heuristic can be viewed as an iterative one in which the problem is continuously altered by the components of the framework in effort to improve the solution while searching the entire solution space.

CHAPTER 6

RESULTS AND DISCUSSION

6.1 INTRODUCTION

The joint placement and power allocation for protective jammers was formulated as a non-linear optimisation problem in chapter 4. Owing to the difficulty and computational intensive nature of non-linear problems, the problem was linearised by approximating the joint non-linear problem as two separate linear problems that are sequentially solved. The exact algorithms and heuristic developed in the previous chapter are used for solving the sub-problems as is shown in the flow chart in figure 6.1. The jammer placement sub-problem obtained from the joint placement and power allocation non-linear problem is solved either using an exact algorithm or the developed ACT-based heuristic. Once the optimal set of jammers have been obtained, the associated linear minimisation power allocation problem is solved using the simplex method.

The solutions to the developed optimisation models are obtained using the IBM ILOG CPLEX software platform [90]. The branch-and-cut exact algorithm is used to solve various cases of the jammer placement sub-problem while altering a number of parameters related to the network. The results pertaining to solving the jammer placement sub-problems using the ACT-based heuristic are shown for large network sizes. The performance in terms of the solution provided and the computation time associated with use of the heuristic, in comparison to the branch-and-cut algorithm, is graphically shown. The results of optimising the transmitting power of the selected wireless jammers are shown for varying networks where the placement of jammers have been determined through the application of the jammer placement sub-problem. The performance of the entire scheme, which involves the optimal placement and power allocation, are shown for a number of different random network scenarios.

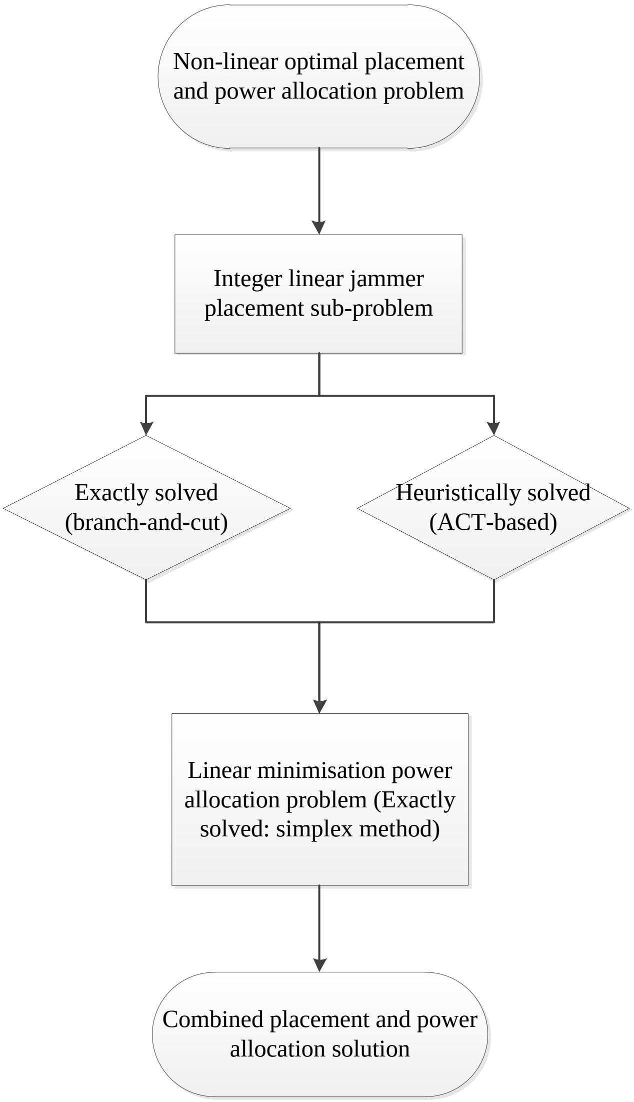
Non-linear optimal placement and power allocation problem
Integer linear jammer placement sub-problem
Exactly solved (branch-and-cut)
Heuristically solved (ACT-based)
Linear minimisation power allocation problem (Exactly solved: simplex method)
Combined placement and power allocation solution

Figure 6.1: Flow chart illustrating the problem formulation and decomposition

6.2 EXACT ALGORITHMS

6.2.1 Jammer Placement Sub-problem

The jammer placement optimisation problems are solved using the IBM ILOG CPLEX solver [90]. The positions of the legitimate nodes and the malicious eavesdropping nodes are randomly generated. The parameters that are used for evaluating the protection scheme is given in table 6.1. Once the random legitimate and malicious nodes have been placed, the co-ordinates are used as input to the optimisation model which solves the problem of minimising the total number of jammers needed to protect an area while adhering to the constraints. The set of discrete points that constitute possible locations of where to place jammers was determined by superimposing a uniform grid, with a grid-space of 0.5, over the target area where the intersection points correspond to possible locations for placing a jammer. The threshold values were experimentally determined and were chosen to be within an acceptable 15% of the λ_j value. The transmitting power as represented by λ_j for the nodes, is set at a constant value of 1. The cost for the placement of the jammers is also set at a uniform value of 1.

To give a visual overview of what is achieved by solving the jammer placement sub-problems, figure 6.2 to figure 6.6 show where jammers have been placed to provide the randomly generated networks with protection from all randomly placed eavesdroppers. There are 20 randomly placed legitimate and 20 randomly placed malicious nodes in each scenario. No internal communication is affected in any way by the placement of these jammers which were obtained by solving the appropriate optimisation problems using the branch-and-cut algorithm. The average number of jammers to protect the networks against 20 malicious nodes for these scenarios is approximately 9.

Table 6.1: Simulation Parameters

Parameter	**Value**
N	441
δ_L	1.15
δ_M	0.85
λ_j	1.0
Area	10x10
c_k for all jammers	1.0

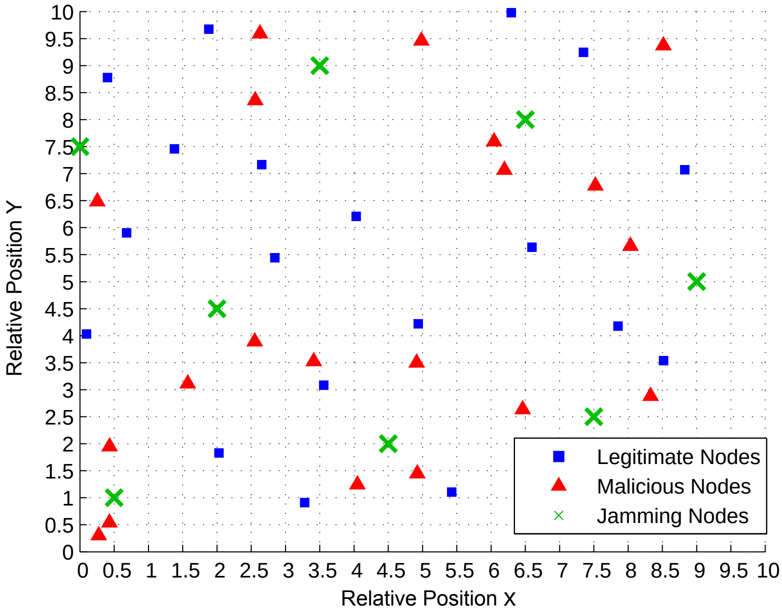

Figure 6.2: Example of a random scenario showing the optimised number of jammers and their locations for protecting the network.

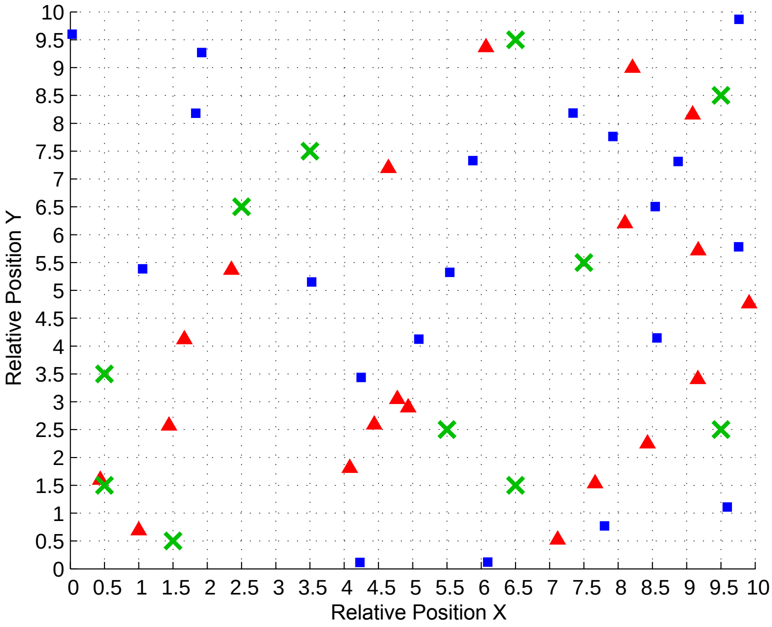

Figure 6.3: Example of a random scenario showing the optimised number of jammers and their locations for protecting the network.

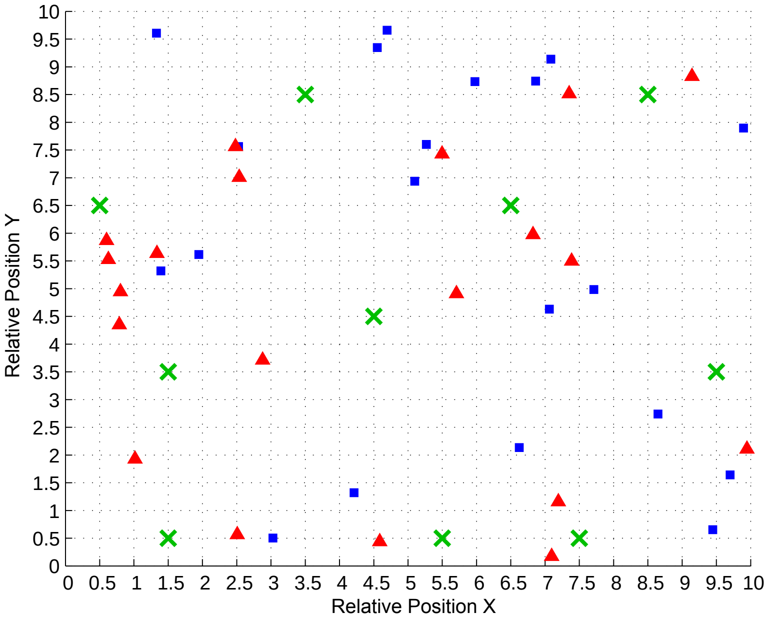

Figure 6.4: Example of a random scenario showing the optimised number of jammers and their locations for protecting the network.

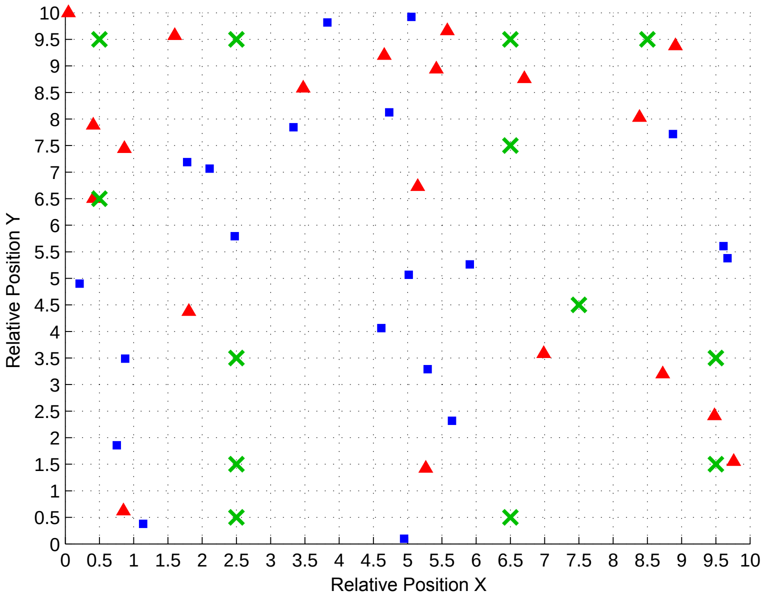

Figure 6.5: Example of a random scenario showing the optimised number of jammers and their locations for protecting the network.

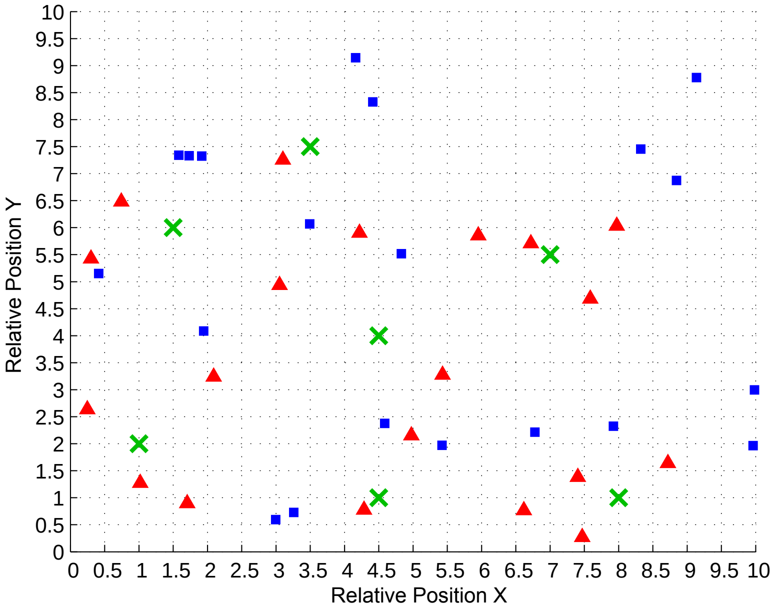

Figure 6.6: Example of a random scenario showing the optimised number of jammers and their locations for protecting the network.

6.2.1.1 Effect of Varying the Number of Malicious Nodes

The effect of varying the number of malicious nodes on the average number of jammers required to protect a network with 20 randomly dispersed communicating nodes is shown in figure 6.7. An average of over a 100 simulation runs were obtained for the varying number of malicious nodes. As can be seen from figure 6.7, there is an overall decrease in the rate at which the average number of jammers increase. This can be attributed to the fact that the area of the network remains the same as the number of malicious nodes increase thereby making the network more densely packed.

6.2.1.2 Effect of Varying the Number of Legitimate Nodes

On the other hand, as seen in figure 6.8, increasing the number of legitimate nodes while keeping the number of malicious nodes constant at 20, exhibits a fairly linear relationship with regard to the number of jammers needed to protect the network. This is a result of the added restrictions on the placement of the jammers due to the increase in the legitimate communication nodes; more jammers need to be placed closer to the malicious nodes thereby

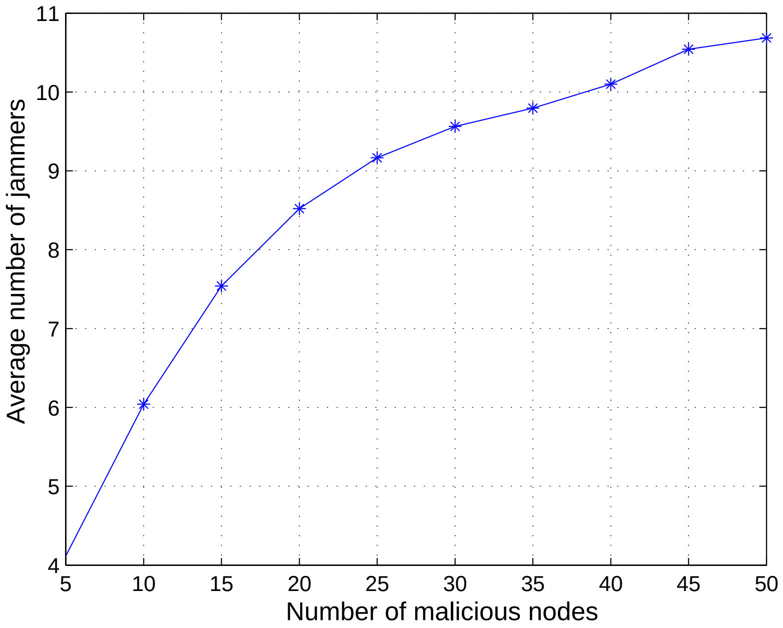

Figure 6.7: The effect of the number of malicious eavesdropping nodes on the average number of jammers required to protect an area.

increasing the jammers to malicious nodes ratio. There is, however, an exponential increase observed in the percentage of infeasible solutions obtained as the number of legitimate nodes increase as shown in figure 6.9. The constraint related to the legitimate nodes is a capacity constraint which is substantially difficult to meet than a demand constraint. Almost 60% of the scenarios with 50 legitimate nodes result in infeasible solutions for the current constraints.

6.2.1.3 Effect of Varying the Number of Potential Jamming Locations

The effect of the number of potential jammer locations on the average number of jammers required to protect a 20-node network against 20 malicious nodes, with the parameters as given in table 6.1, is shown in figure 6.10. 100 different random scenarios for each number of potential locations were implemented and the average thereof was obtained. The number of jammer locations range from 36 potential jammer locations to 784 potential jammer locations and correspond to uniform intervals at which the jammers are placed ranging from 0.35 to 2. An exponential decrease in the number of jammers required to protect an area is observed as the number of potential locations increase. This means that an environment that closely

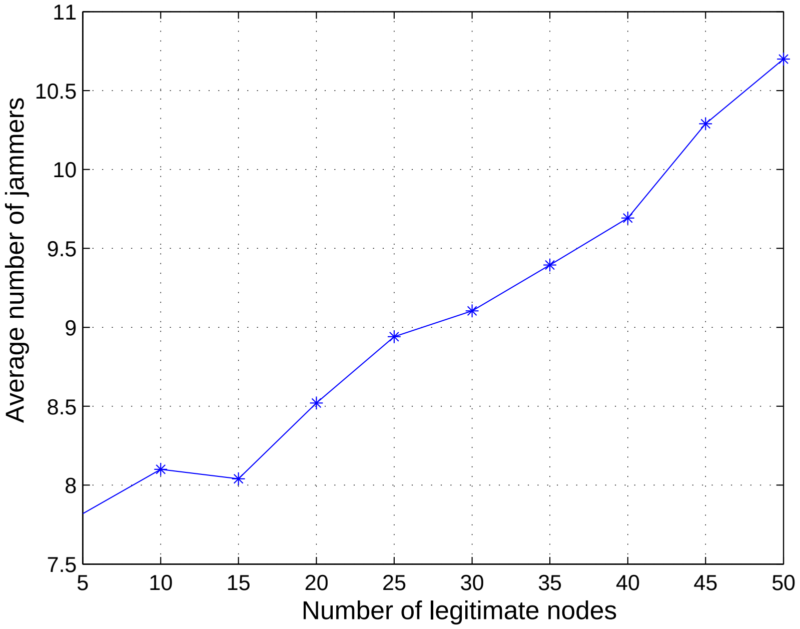

Figure 6.8: The effect of the number of legitimate communication nodes on the average number of jammers required to protect an area.

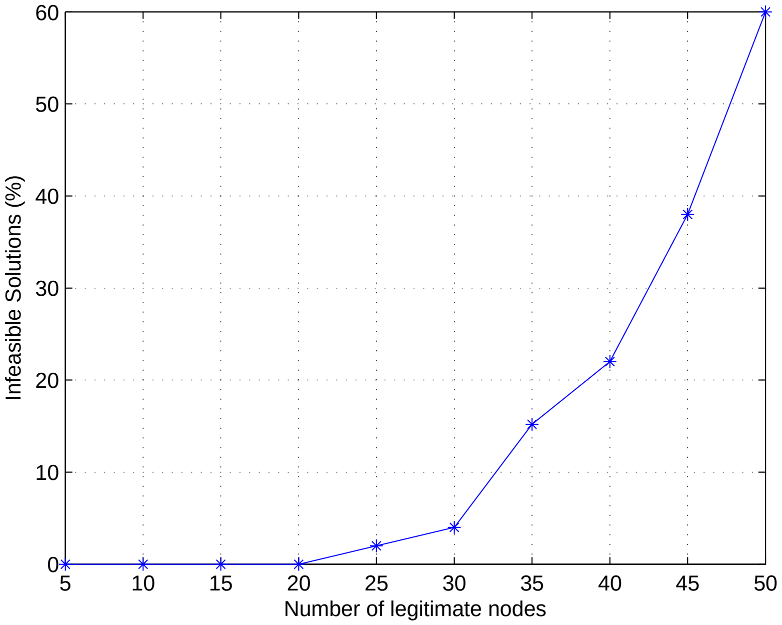

Figure 6.9: Percentage of infeasible solutions obtained against the number of legitimate nodes.

mimics a continuous domain with regard to potential jammer locations performs better; however, after a certain point, the average number of jammers begin to exhibit behavior that is independent to the number of potential jammer locations. Thus, from approximately 450 potential jammer locations onwards for this scenario, increasing the number of jammer locations proves to be futile in improving the result.

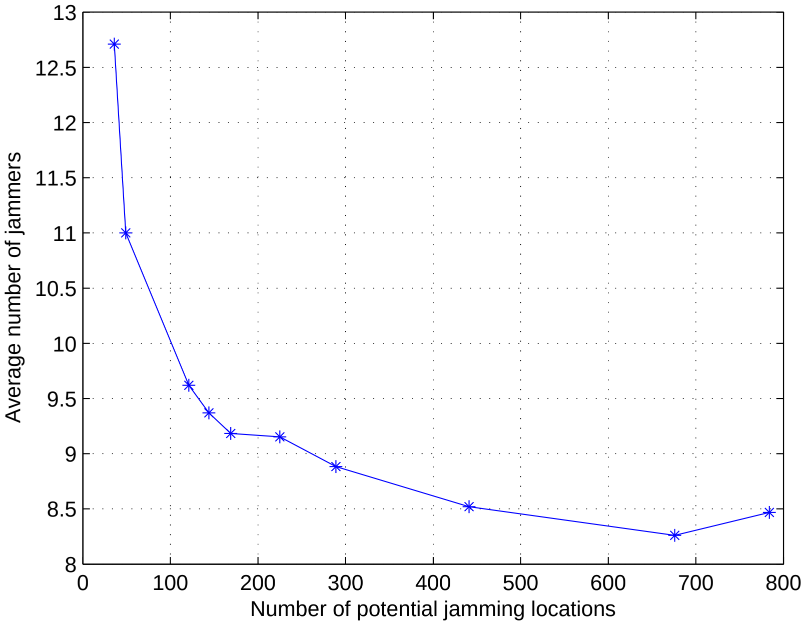

Figure 6.10: The effect of the number of potential jammer locations on the average number of jammers required to protect an area.

6.2.2 Jammer Power Allocation Sub-problem

The transmitting power which is directly proportional to λ_j can be optimised for a particular scenario by minimising λ_j associated with each jammer, while ensuring that it is still able to cause sufficient interference to the malicious nodes. For the initial jammer placement problem, λ_j is set to 1 for all the jammers and thus $\lambda_{max} = 1$ for the associated power allocation sub-problem.

As an example, the random network scenario shown in figure 6.6, is used to gauge the performance of the power allocation optimisation model for each placed jammer. The results of the optimal λ_j value for each jammer as determined by solving the associated jammer power allocation sub-problem, is given in table 6.2. A total power reduction of 11.86% was observed for the entire protection scheme.

Table 6.2: Optimisation of transmitting power of wireless jammers for network shown in figure 6.6.

Jammer Number	**Jammer Location**	λ_j	**Power Reduction (%)**
1	(1.0, 2.0)	1.0	0
2	(1.5, 6.0)	1.0	0
3	(3.5, 7.5)	0.794	20.6
4	(4.5, 1.0)	0.671	32.9
5	(4.5, 4.0)	1.0	0
6	(7.0, 5.5)	0.746	25.4
7	(8.0, 1.0)	0.960	4

A plot of the total power reduction for 50 random scenarios over a 10x10 grid with 20 legitimate nodes and 20 malicious nodes is shown in figure 6.11. It can be seen that the power reduction fluctuates for the varying network scenarios. The percentage reduction strongly depends on the topology, with as high as a 27% reduction and as low as 2% reduction being observed.

The varying percentages of the power reduction is independent of the grid size, number of malicious nodes, number of legitimate nodes and also number of potential jamming locations. A plot of the overall power reduction of 20 random scenarios with twice as many malicious nodes is shown in figure 6.12. Figure 6.13 shows the overall power reduction for 20 random scenarios with twice as many legitimate nodes.

Table 6.3 gives a brief statical analysis of the overall power reductions of the random scenarios for the general case, as shown in figure 6.11, the increased number of malicious nodes as shown in figure 6.12 as well as the increased number of legitimate nodes as shown in figure 6.13. There is no evident connection between varying the number of nodes and the overall power reduction. This further validates the notion that the power reduction is largely dependent on the geographical layout of the networks and their corresponding jammer locations.

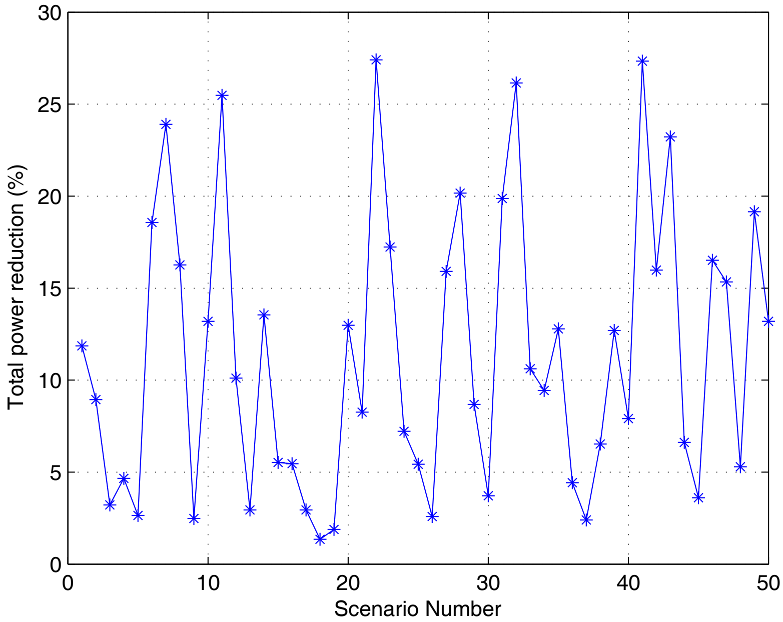

Figure 6.11: Total jammer power reduction for 50 random scenarios with 20 legitimate nodes and 20 malicious nodes.

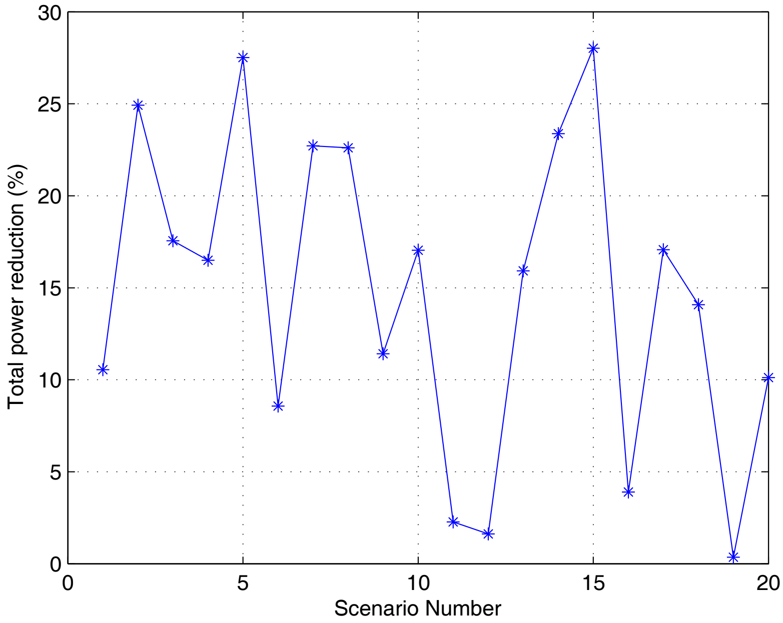

Figure 6.12: Total jammer power reduction for 20 random scenarios with 20 legitimate nodes and 40 malicious nodes.

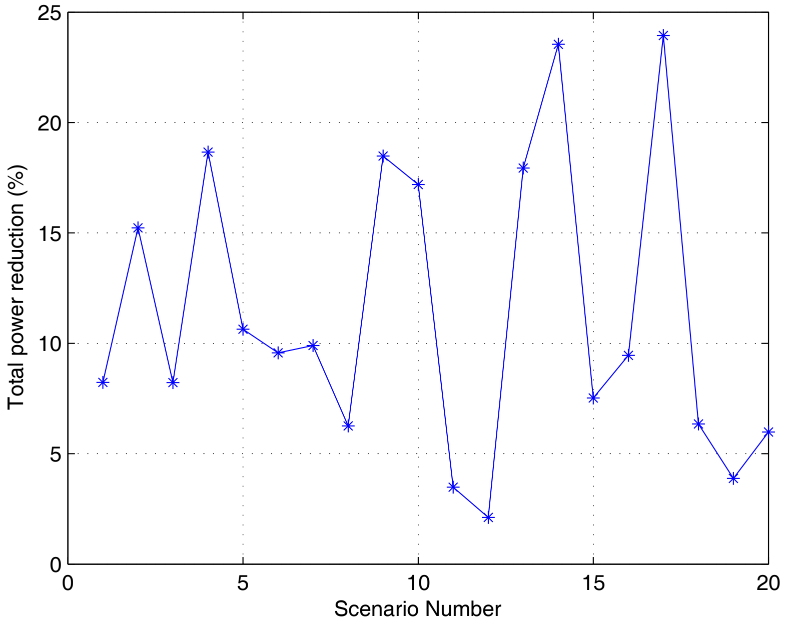

Figure 6.13: Total jammer power reduction for 20 random scenarios with 40 legitimate nodes and 20 malicious nodes.

Table 6.3: Statistical Analysis of power allocation results

Scenario Type	**Mean**	**Median**	**Variance**	**Standard Deviation**
General	11.2713	9.7750	57.5216	7.5843
Increased Malicious Nodes	14.8059	16.2078	74.0471	8.6051
Increased Legitimate Nodes	11.3288	9.5110	43.7116	6.6115

6.3 HEURISTIC RESULTS

The use of the heuristic allows larger jammer placement sub-problems, of more than 1000 potential jammer locations, eavesdropper and malicious nodes, to be solved within a relatively small time limit. In military battlefield scenarios, where the execution time is extremely critical, it is probable to expect very large wireless networks which require protection, and therefore the placement of the jammers needs to be determined quickly. The performance of the heuristic is analysed in terms of the solutions provided for very large jammer placement sub-problems, that would otherwise, take more than 120 minutes to solve when using the branch-and-cut method; this execution time is unacceptable in real-life scenarios. Also, the time advantage gained as a result of solving using the heuristic is shown for small jammer placement problems consisting of 441 potential jamming locations. The objective function values obtained thorough the implementation of the heuristic is compared to the values returned by the branch-and-cut method for particular scenarios. The trade-off between the execution time and the optimality of the problem is then analysed. The parameters used for evaluating the performance of the heuristic for the jammer placement sub-problems is shown in table 6.4.

Table 6.4: Parameters used for Heuristic implementation

Parameter	**Value**
δ_L	1.15
δ_M	0.85
λ_j	1.0
c_k for all jammers	1.0
Number of Legitimate Nodes	20
Number of Malicious Nodes	20

6.3.1 Heuristic Performance Analysis

The results for wireless network configurations in which there are 1681 potential jammers in a 10x10 grid with 20 randomly dispersed legitimate nodes and 20 randomly dispersed malicious nodes, is shown in table 6.5 and continued in table 6.6. The time taken for each of the three ACT components in shown in the table as well as the extra time required if more iterations were required. The number of constraints for this particular large problem is 3401 with 70602 non-zero coefficients. The solution to problems this large is completed well under 2s using the branch-and-cut method to solve the SUB-JPPs.

The heuristic works efficiently for large areas as well. The execution times and objective function values for a 20x20 grid area with 25921 potential jammer locations, 51882 constraints and 1088682 non-zero coefficients related to the 20 randomly dispersed malicious nodes and

20 randomly dispersed legitimate nodes, is shown in table 6.7 and continued in table 6.8. The average time for solving problems of this size is only 16.5064s; as opposed to taking more than 3 hours for problems of this size when using the branch-and-cut method to solve.

6.3.2 Comparison to Branch-and-cut Method

A comparison of the execution times and the optimal solutions provided when implementing the branch-and-cut method versus implementing the heuristic, is shown in figures 6.14 and 6.15. This is for a small network with 441 potential jammer locations in a 10x10 grid with 20 legitimate and 20 malicious nodes.

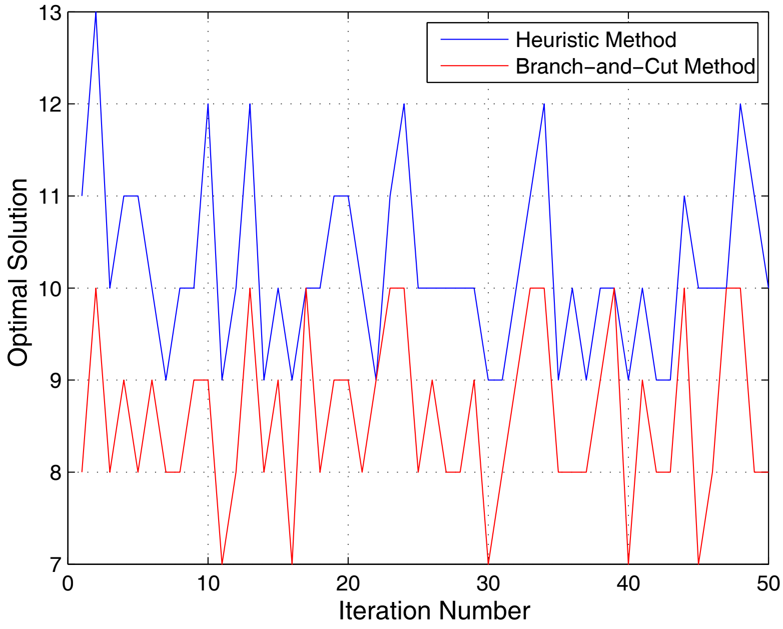

Figure 6.14: Comparison of heuristic method versus branch-and-cut method for 50 different scenarios in terms of the optimal solutions obtained.

The branch-and-cut method was compared to the heuristic method in terms of the solution provided and the computation time for 50 random scenarios with 441 potential jammer locations. The execution times when using the branch-and-cut method is greatly dependent on the particular network topology, and is very inconsistent, ranging from obtaining the solution in well under 1s to over 130s. On the other hand, the execution time when using the heuristic for the very same scenarios remains consistently below 2s. Although, the heuristic returned a higher objective function value for most cases, the maximum difference was of an

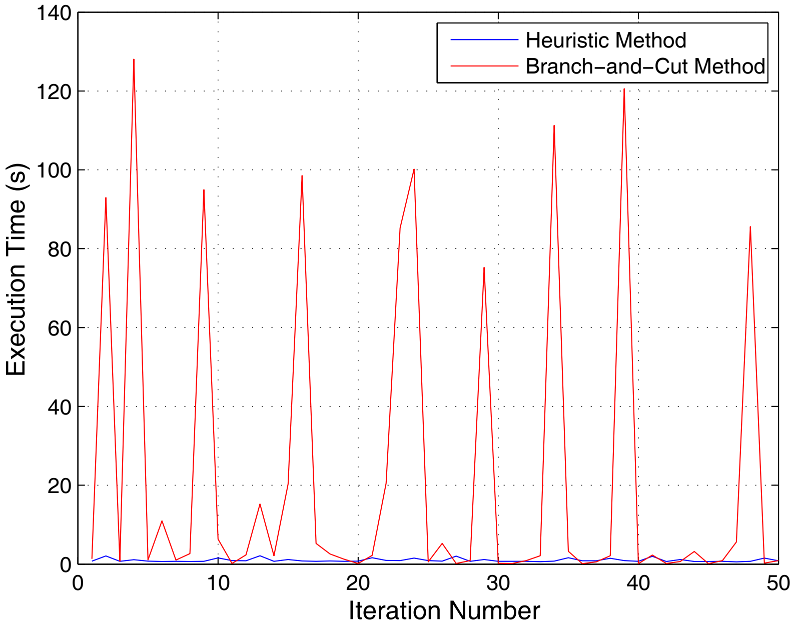

Figure 6.15: Comparison of heuristic method versus branch-and-cut method for 50 different scenarios in terms of the execution time.

acceptable 2 jammers. It can therefore be concluded that for small network scenarios, where optimality in terms of the number of jamming devices required to protect an area is critical, the branch-and-cut method should be implemented. However, in scenarios where execution time is critical, the heuristic can be used to obtain an acceptable solution within a small time limit.

Table 6.5: Execution time and solutions for heuristic implementation for a 10x10 grid network

Run Number	**ACT-1 Time (s)**	**ACT-2 Time (s)**	**ACT-3 Time (s)**	**Number of Iterations**	**Time for extra iterations (s)**	**Objective Function Value**	**Total Time (s)**
1	0.5460	0.468	0.5772	1	-	10	1.5912
2	0.5616	0.39	0.5304	2	0.9205	11	2.4025
3	0.5772	0.6552	0.5616	1	-	10	1.794
4	0.4992	0.6084	0.4680	1	-	10	1.5756
5	0.5304	0.3744	0.5928	2	0.8588	10	2.3564
6	0.4368	0.4368	0.6240	1	-	11	1.4976
7	0.5772	0.4056	0.5616	1	-	11	1.5444
8	0.5304	0.4212	0.5460	1	-	9	1.4976
9	0.4992	0.3900	0.4836	1	-	9	1.3728
10	0.5772	0.6396	0.4836	2	0.9680	10	2.6684
11	0.4826	0.4500	0.5234	1	-	10	1.4560
12	0.5213	0.4231	0.5773	1	-	9	1.5217
13	0.4790	0.6432	0.5923	1	-	10	1.7145
14	0.5520	0.6198	0.4780	1	-	9	1.6498
15	0.5771	0.4112	0.5918	2	0.7546	10	2.3347

,

Table 6.6: Execution time and solutions for heuristic implementation for a 10x10 grid network (continued)

Run Number	ACT-1 Time (s)	ACT-2 Time (s)	ACT-3 Time (s)	Number of Iterations	Time for extra iterations (s)	Objective Function Value	Total Time (s)
16	0.4921	0.4120	0.5321	1	-	11	1.4362
17	0.5239	0.5991	0.4981	1	-	9	1.6211
18	0.5671	0.3870	0.5112	1	-	10	1.4653
19	0.5812	0.6001	0.6105	1	-	11	1.7918
20	0.5446	0.4018	0.4150	2	0.7678	10	2.1292
21	0.4890	0.4270	0.5133	1	-	10	1.4283
22	0.5128	0.4126	0.4887	2	0.8871	11	2.3012
23	0.4998	0.3980	0.4981	1	-	9	1.3959
24	0.5091	0.4012	0.5430	1	-	10	1.4533
25	0.5100	0.6213	0.4213	2	0.9912	10	2.5438
26	0.5290	0.3910	0.5772	1	-	10	1.4972
27	0.4891	0.5987	0.5304	1	-	9	1.6182
28	0.5310	0.6189	0.4923	1	-	10	1.6422
29	0.5214	0.6001	0.4169	1	-	11	1.5384
30	0.4997	0.3214	0.5536	1	-	10	1.3747
Average	**0.5249**	**0.4842**	**0.5264**	**1.2333**	**0.8783**	**10.0**	**1.7190**

Table 6.7: Execution time and solutions for heuristic implementation for a 20x20 grid network

Run Number	ACT-1 Time (s)	ACT-2 Time (s)	ACT-3 Time (s)	Number of Iterations	Time for extra iterations (s)	Objective Function Value	Total Time (s)
1	5.9904	4.3368	6.1152	1	-	11	16.4424
2	6.0216	4.3056	6.2088	1	-	10	16.5360
3	6.0372	4.3524	6.0840	1	-	8	16.4736
4	6.0216	4.3524	6.3804	1	-	11	16.4736
5	6.1776	4.6176	6.1776	1	-	10	16.9728
6	5.8256	4.2315	6.1181	1	-	9	16.1752
7	6.5213	3.9995	6.0025	1	-	10	16.5233
8	6.2315	4.3515	6.1155	1	-	9	16.6985
9	6.0021	4.5815	5.8125	1	-	10	16.3961
10	5.8562	4.2153	5.9923	1	-	8	16.0638
11	5.9904	4.3368	6.1152	1	-	11	16.4424
12	6.0216	4.3056	6.2088	1	-	10	16.5360
13	6.0372	4.3524	6.0840	1	-	8	16.4736
14	6.0216	4.3524	6.3804	1	-	11	16.4736
15	6.1776	4.6176	6.1776	1	-	10	16.9728

Table 6.8: Execution time and solutions for heuristic implementation for a 20x20 grid network (continued)

Run Number	**ACT-1 Time (s)**	**ACT-2 Time (s)**	**ACT-3 Time (s)**	**Number of Iterations**	**Time for extra iterations (s)**	**Objective Function Value**	**Total Time (s)**
16	6.1776	3.8713	6.0471	1	-	10	16.0960
17	6.5147	4.6712	6.1542	1	-	10	17.3401
18	6.0012	4.4712	6.0724	1	-	9	16.5448
19	5.9912	4.1209	6.2190	1	-	9	16.3311
20	6.3210	4.4170	6.1841	1	-	11	16.9221
21	5.9012	3.9102	6.1254	1	-	10	15.9368
22	6.4122	3.8914	6.0012	1	-	8	16.3048
23	6.2322	4.2091	6.1254	1	-	9	16.5667
24	6.0021	4.1278	6.4219	1	-	9	16.5518
25	6.5001	4.0034	5.7812	1	-	10	16.2847
26	6.2421	4.3365	6.1146	1	-	8	16.6932
27	5.9981	4.3129	6.2213	1	-	11	16.5323
28	6.1776	4.5192	5.8164	1	-	10	16.5132
29	5.9120	4.6391	6.0021	1	-	10	16.5532
30	6.0012	4.5145	5.9612	1	-	8	16.4769
Average	**6.1137**	**4.3007**	**6.092**	**1**	**-**	**9.53**	**16.5064**

6.4 COMPARISON OF PROTECTIVE JAMMING SCHEMES

In this section, a comparison to the only other similar work on utilising protective jammers and exploiting their geographic location to provide protection, is presented. As was discussed in chapter 3, Sankararaman *et al.* [74] studied jammer placement and power allocation for protective jammers under a storage/fence model. Contrary to other work on the placement of jammers to destroy an entire network [66]-[69], [72]; the communication network that the jammers are protecting against eavesdroppers is taken into account. The storage/fence environment assumes that legitimate communication takes place in the storage, which is a geographic region physically secured by a fence, where eavesdroppers may not enter. There is a minimum gap assumed between the storage and the fence which is termed as the jammer space. The protective jammers can reside in this space and are used to transmit artificial noise so as to create sufficient interference and prevent reception for the eavesdroppers, while not disrupting any legitimate communication inside the storage area. This work is targeted for protecting data stored on radio-frequency identification tags and where geographically restricting a network is feasible.

Sankararaman *et al.* [74] proposed algorithms targeted towards optimising the power consumption and number of jammers needed to reduce the SNR of eavesdroppers to below a threshold without jeopardising network performance. With regard to the basic linear power assignment problem, the authors proposed an ϵ-approximation algorithm for the case when the storage and eavesdropper areas are continuous. The ϵ-approximation algorithm involves computing a discrete set of points in the storage and fence area so that the problem reduces to a linear program with a finite number of constraints. The jammer placement problem has an added number of complexities because of the integer constraints, as well as the difficulty in algebraically characterising the jammer placement as a function of the distance between the storage area and the fence. The authors solve this problem by applying a heuristic approach. As with the power allocation problem, a similar ϵ-approximation algorithm is given to discretise the fence and storage areas when there is a pre-determined set of candidate jammer locations. A near-optimal algorithm is proposed for the case when the fence area is assumed to be convex and the storage area is a connected region of any shape. Essentially, a greedy algorithm is proposed in which an arbitrary eavesdropper location, with a certain visibility region, is chosen. The visibility region is defined as the area in the jammer space, in which a jammer must lie to successfully decrease the SNR of the eavesdropper to a value below its threshold. Another eavesdropper location is then chosen by "walking" along the fence until there is no common region of visibility. A jammer is then placed at this location. This method is repeated for all possible eavesdropper locations. The algorithm is very specific to this problem and does not involve any known techniques.

This work differs significantly to the security method and optimisation schemes presented in this dissertation. Sankararaman *et al's* proposed security scheme is for a network model which mimics a storage/fence environment; however, the novel aspect related to this work is the network model utilised, which imitates a military battlefield scenario. There are no geographical restrictions placed on any of the nodes. In the storage/fence model, there are geographical restrictions placed on the legitimate nodes (limited to only appear in the storage area), eavesdropper nodes (can only appear outside the storage) and the jamming devices (limited to being placed in between the storage and fence area only). Despite the differences, the fundamental principle and related constraints ensuring that the legitimate communication is not affected in any way while causing sufficient interference to the eavesdroppers, remains the same.

In effort of comparing the two schemes, the network model is altered so that the geographical locations of the legitimate nodes are confined to a storage area scenario as presented in the paper by Sankararaman *et al.* [74]. The distribution of the malicious and legitimate nodes is controlled as the legitimate nodes are distributed in a smaller 6x6 grid which is surrounded by malicious nodes. The malicious nodes are distributed in the area that borders the 6x6 grid which is placed in the centre of the larger 10x10 grid. Two examples of such a scenario are shown in figure 6.16 and figure 6.17. The average number of jammers to protect 20 legitimate nodes against 20 malicious nodes was approximately 8.26 over 100 simulations. This shows that there is no significant decrease in the number of jammers needed to protect this area as opposed to the environment where there are no restrictions placed on the locations of the legitimate and malicious nodes.

The authors in [74] presented results for the number of jammers that need to be placed in the jammer space area while altering the fixed power transmitting power values of the jammers, λ_j. A square grid of 50x33 units with an irregularly shaped storage area contained in a centrally placed rectangular grid of dimensions of 40x23 units is used by Sankararaman *et*

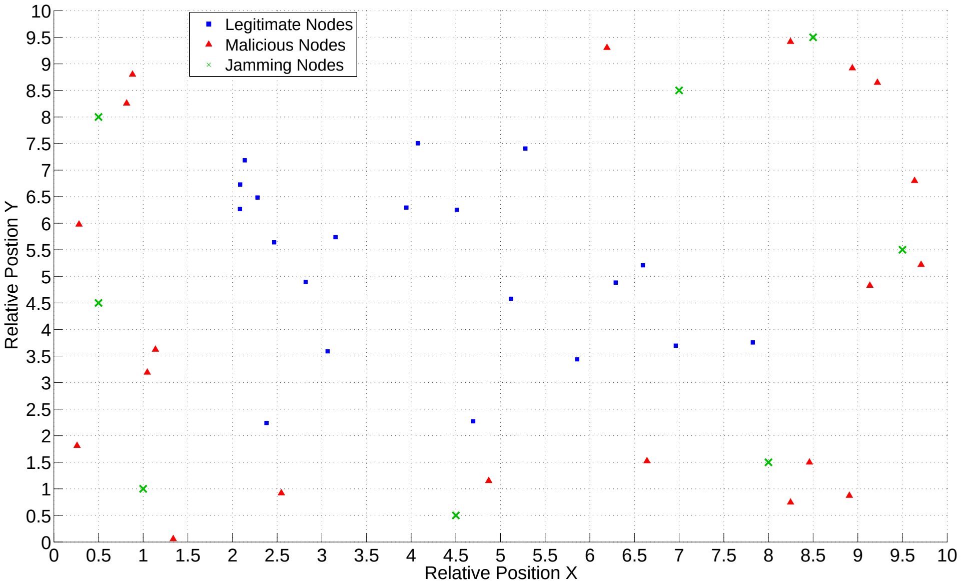

Figure 6.16: Example of a random scenario showing the optimised number of jammers and their locations for protecting a network in a storage/fence environment.

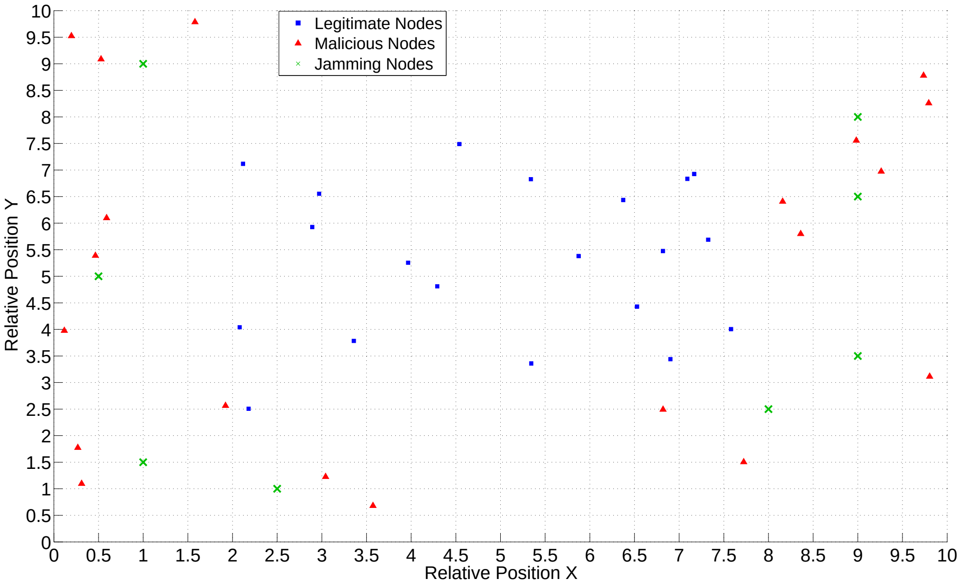

Figure 6.17: Example of a random scenario showing the optimised number of jammers and their locations for protecting a network in a storage/fence environment.

al. [74] for evaluating the performance of their proposed heuristic. Ten random points were chosen for the placement of 10 malicious eavesdropping nodes in the area between the storage and fence, this is termed as the jammer space. Figure 6.18 shows the concept of the storage, fence and jammer space area with random legitimate and malicious nodes.

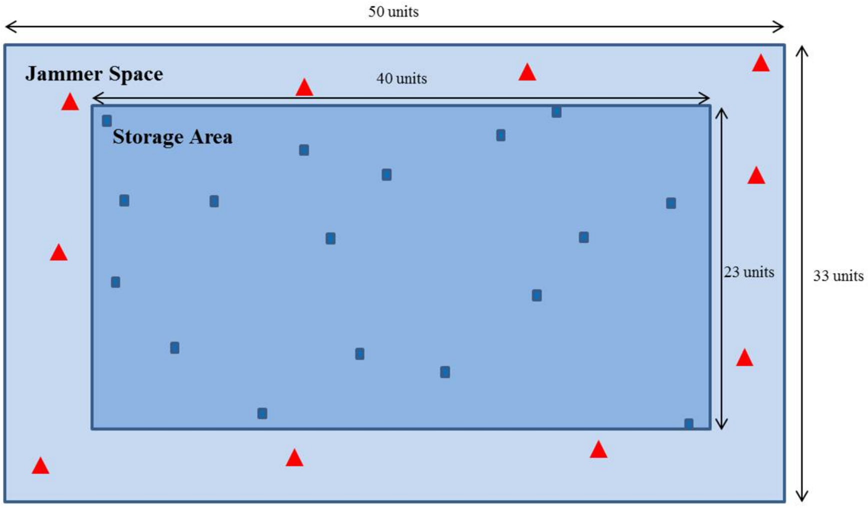

Figure 6.18: Storage/fence scenario with randomly placed legitimate nodes (blue squares) and malicious nodes (red triangle).

The results for the number of jammers required to protect a scenario guided by the dimensions as shown in figure 6.18, is shown in comparison to the results obtained by Sankararaman *et al.* [74]. The authors provided results while altering the jammer power, λ_j, from values of 1 to 5 while the threshold values for both the legitimate and malicious nodes were kept at a constant value of 1. The comparison of our proposed scheme with Sankararaman *et al.*'s scheme is shown in figure 6.19. The graph shows the average number of jammers over 100 simulation runs for each different λ_j value. It can be seen that the number of jammers is comparable to the number obtained by Sankararaman *et al.*, with the average number being slightly less for $\lambda_j = 1$, $\lambda_j = 2$ and $\lambda_j = 3$. A general decrease in the number of jammers is observed for increasing λ_j values. This is to be expected as the higher the transmitting power of the jammers, the fewer the number of jammers are required to cause sufficient interference for the malicious devices. For $\lambda_j = 3$ and onwards, the number of jammers required to protect the area using the proposed method is independent of the transmitting value for such a small scenario.

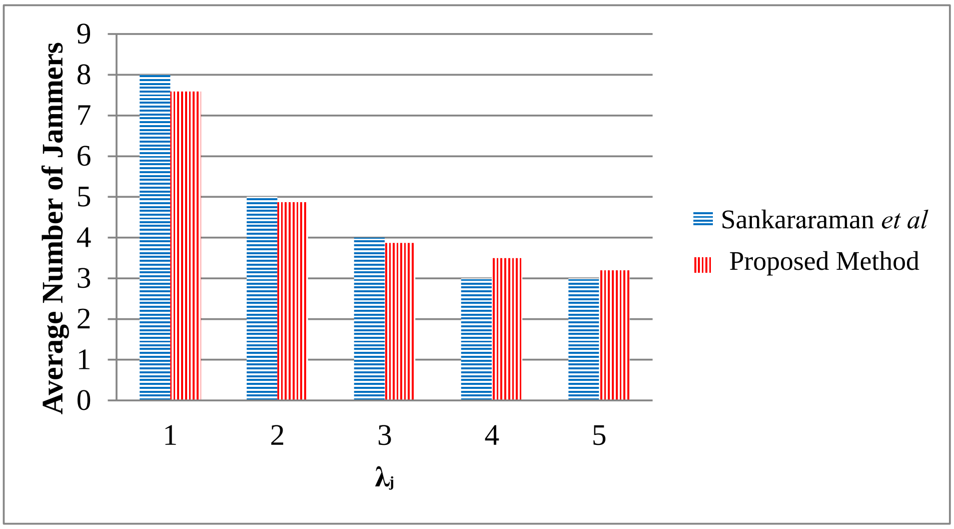

Figure 6.19: Comparison of proposed method with results obtained by Sankararaman *et al.* [74] for varying jammer transmitting power values.

6.5 CONCLUDING REMARKS

The branch-and-cut algorithm was used for solving the jammer placement sub-problem and the simplex algorithm was employed for solving the power allocation sub-problem. In order to reduce the computational complexity associated with solving the linear integer jammer placement sub-problem, an ACT based search heuristic was also developed. The effect of varying the number of legitimate communication nodes and the number of malicious eavesdropping nodes were analysed. In worst case scenarios, approximately 11 jammers were required to protect a 50 node network against 20 eavesdropper nodes. After optimising the transmitting power for the jammers, it was found that the total percentage power reduction was highly dependent on the topology and jammer placement. The performance of the proposed heuristic method was evaluated in terms of the execution time and solutions provided for large network scenarios. The heuristic was also compared to the branch-and-cut method for smaller network scenarios. As a result of the inconsistent execution times for the branch-and-cut method, the heuristic can perform up to 60 times faster than the branch-and-cut method for certain network cases, while returning an acceptable solution that is within 10% of the optimal solution obtained by the exact branch-and-cut algorithm. The use of the heuristic proves to be imperative in real-life large network scenarios where a feasible and reasonable solution needs to be obtained with a low execution time. The proposed security model also displayed comparable results when applied to a storage/fence environment as performed by Sankararaman *et al.* [74] for protective jammer placement.

CHAPTER 7

CONCLUSION

The need for protecting communication within networks is of utmost importance especially in environments where information is critical and loss thereof can result in disastrous consequences. The most popular method for ensuring data confidentiality is through the use of cryptographic techniques; however, as a result of the decentralised nature and power limited network nodes of WMNs, it is important to consider physical-layer based methods such as jamming. Friendly jammers are used to protect the communication of wireless network from eavesdroppers trying to gain access to the information. A protection scheme utilising friendly jammers to protect randomly distributed networks against randomly dispersed malicious eavesdropping devices was proposed in this dissertation. The efficiency of the scheme is increased by minimising the number of jammers required to protect an area and reducing the power consumption levels of the jamming devices. By carefully placing jammers to protect a particular WMN, the number of jammers can be significantly reduced while still providing high levels of security. The power consumption of each jammer is also subject to a number of constraints so that the legitimate communication within the network is not affected by the jammers. Optimising the power levels associated with each jammer lowers the cost and increases the efficiency of the scheme. The solution to the modelled non-linear optimisation problem was approximated as the sequential solution to two linear sub-problems. The branch-and-cut algorithm was used for solving the jammer placement sub-problem and the simplex algorithm was employed for solving the power allocation sub-problem. In order to reduce the computational complexity associated with solving the linear integer jammer placement sub-problem, an ACT based search heuristic was also developed.

7.1 SUMMARY

A novel physical-layer based security method that utilises jammers to generate additional interference for devices that are eavesdropping on wireless network communication was proposed in this dissertation. The scheme involves the intelligent placement of continuous jammers in order to achieve maximum protection and data confidentiality for WMNs with multiple eavesdroppers, sources and destinations. Furthermore, the scheme is optimised in terms of the transmitting power associated with each jammer so that the energy expended by the jammers is kept at a minimum. The protection scheme precludes the use of any cryptographic techniques and is only physical-layer based. The security method is modelled as a minimisation mixed integer non-linear problem, and is approximated as the sequential solution of two linear optimisation sub-problems relating to the placement and power allocation of the wireless jammers. The placement of the jammers takes the form of a multiple demand multi-dimensional knapsack problem with a minimisation objective. The power allocation problem is modelled as a linear real-valued minimisation optimisation problem. The branch-and-cut method and simplex method are the algorithms used for solving placement and power allocation problems respectively. In effort to reduce the computation time associated with solving the linear integer jammer placement problem, an ACT based heuristic is developed. The performance of the proposed security method and heuristic are evaluated through appropriate simulations conducted on random network instances.

Chapter 2 gave an overview of WMNs and their various applications. The IEEE 802.11s standard for WMNs protocol and the usage scenarios relating to both civilian and military environments were discussed. Aspects relating to the routing protocol, the mesh architecture and the current security mechanisms recommended by the standard were explained. The security methods make use of cryptographic techniques that reside in the network layer. The work presented in this dissertation, however, aims to overcome the weakness inherent with the use of cryptographic techniques and enhance the security of WMNs using a physical-layer based method. The method is designed with emphasis placed on applications of WMNs in military environments where the value of the tactical information is considerably higher. The designed method can also easily be applied to civilian applications given that the most difficult of the environments to protect, is in a military domain. This is because such networks are very unpredictable and there are no geographical restrictions placed on any of the nodes.

The importance and various uses of WMNs in military environments were further elaborated upon in this chapter. The use of computer equipment and networked communications technology to enhance military operations is referred to as network centric warfare (NCW). The first and foremost principle of NCW is related to maintaining information superiority. This involves ensuring that adversaries have reduced ability to access information and to raise their uncertainty. The way in which WMNs are used for disseminating information, communicating intelligence, sending orders and reporting vital information has had a significant impact on the way the military perform their tasks. Any form of information leakage, where the value of the tactical information is considerably higher in the military domain, can have disastrous consequences and should be avoided at all costs.

Chapter 3 reviewed literature pertaining to the placement and power allocation of jammers. The need for the protection of WMNs was highlighted as a result of the application in environments where security is of utmost importance. The most popular method for ensuring data confidentiality is through the use of cryptographic techniques; however, as a result of the decentralised nature and power limited network nodes of WMNs, it is important to consider physical-layer based methods such as jamming. The physical-layer methods can also be used in conjunction with cryptographic techniques for enhancing the security of a WMN. Friendly jammers are used to prevent eavesdroppers from intercepting vital network communication. Several papers presented algorithms, mostly based on game theory methods, to determine the optimal transmitting power of the friendly jammers. With regard to the optimisation of jammer placement, the locations of jammers were determined so as to minimise the throughput of an entire enemy's network. Methods for determining the jammer locations involved relaxing or adapting certain constraints such as discretising the jamming area and requiring prior information about the network to jam. There has not been work aimed at the development of optimisation schemes for friendly jammers that are protecting WMNs which address both power and placement of the jammers.

Chapter 4 provided a mathematical formulation, based on optimisation theory, of the proposed method for protecting WMNs against malicious nodes that seek to obtain confidential information. The problem was modelled as a non-linear minimisation problem that jointly addressed the optimal placement and optimal power allocation of wireless jammers in a multi-hop network with multiple sources, eavesdroppers and destinations. The network environment upon which the problem was modelled after, is one which aims to closely represent

WMNs in military battlefields. The application of WMNs in military domains was described in the usage scenarios for the IEEE 802.11s standard in chapter 2. Owing to the difficulty and computational intensive nature of non-linear problems, the problem was linearised by approximating the joint non-linear problem as two separate linear problems that are sequentially solved. The first of which was used to address the problem of determining and placing a minimum number of jammers to protect a multiple source and destination network. This jammer placement sub-problem was modelled as a multiple demand multi-dimensional knapsack problem. The second sub-problem, related to the power allocation of the jammers, was modelled as a non-integer linear minimisation problem with constraints ensuring the power values allocated to the jammers, are sufficient to protect the wireless network without the need of any additional wireless jammers.

In chapter 5, the different optimisation techniques that were used for solving the optimisation problems formulated in chapter 4, were discussed. The simplex method, which is the most popular and efficient method for solving linear non-integer problems, was the technique chosen for solving the power allocation problem. This method was discussed, along with the branch-and-bound method and the cutting plane technique, which are used for solving integer programming problems. The method selected for solving the integer jammer placement sub-problem was the branch-and-cut method, which seeks to improve upon the typical branch-and bound-method using cutting planes. Furthermore, a heuristic for solving the jammer placement sub-problem was developed to increase the efficiency of the proposed security scheme. Although the branch-and-cut method is fairly effective in obtaining the optimal solution for integer optimisation problems, the computational complexity and execution time associated for large problems decreases the efficiency of the algorithm. In military environments especially, it is necessary to obtain solutions in a fast manner given the criticality associated with the information exchanged. An ACT structure based heuristic was developed for solving the multiple demand multi-dimensional knapsack problem with a minimisation objective that is associated with the placement of the wireless jammers.

Chapter 6 illustrated the performance of the proposed security scheme for a number of different scenarios with varying parameters. The branch-and-cut algorithm was used to solve various cases of the jammer placement sub-problem while altering parameters such as the grid size, the number of legitimate nodes, the number of malicious eavesdropping nodes and the locations of potential jammers. The results pertaining to solving the jammer placement sub-problems using the ACT-based heuristic, was also shown for large network sizes. The performance in terms of the solution provided and the computation time associated with use of the heuristic, in comparison to the branch-and-cut algorithm, was graphically shown. The results of optimising the transmitting power of the selected wireless jammers, were shown for varying networks where the placement of jammers were determined through the application of the jammer placement sub-problem. The performance of the entire scheme, which involves the optimal placement and power allocation, were shown for a number of different random network scenarios. The proposed security model also displayed comparable results when applied to a storage/fence environment as performed by Sankararaman *et al.* [74] for protective jammer placement.

7.2 FUTURE RESEARCH

Based on the findings of this study, the author recommends that further research be conducted on the following topics:

- An additional optimisation of the proposed technique takes place with the sequential solution of the power allocation sub-problem associated with a particular scenario. The results indicated a large dependence on the selected jammers and their location with respect to the eavesdroppers. Further investigation should take place on developing a power allocation model that is, within limits, independent of the eavesdropper locations. This can possibly be achieved through the creation of probabilistic models, that guarantee a certain level of protection based on several power values allocated to the jammers, and potential eavesdropper locations around that particular jammer. It is, however, challenging to eliminate this large distance dependence based on the current proposed model; a reformulation will be required.

- Cryptographic techniques are still primarily used as a method for maintaining data confidentiality in wireless networks. Using these techniques in conjunction with the proposed physical-layer based technique, can strengthen the security scheme considerably, and also possibly decrease the number of jammers required to protect an area. Further investigation on the utilisation of the cryptographic techniques, and the increased complexity associated with it, should take place.

- The ACT-based heuristic developed in chapter 5 has a modular structure, in that there are three distinct processes that are iteratively applied, until a solution is obtained. In evaluating the performance of the heuristic, the branch-and-cut method was used as a sub-solver for the integer sub-problem in the ACT-2 component. The sub-problem in ACT-2 is significantly smaller than the original integer placement problem, thus justifying the use of the computational and resource intensive branch-and-cut algorithm. However, for extremely large problems, the execution time can significantly increase because of the use of the exact algorithm in ACT-2, and this then defeats the purpose of utilising the heuristic. To alleviate this issue, the structure of the developed heuristic easily lends itself to the application of different heuristics and algorithms as the sub-solver in the ACT-2 component. A tabu search or greedy algorithm can possibly be used to obtain the solution in ACT-2. A more complex game theoretic approach can also be applied. The effects and performance of the heuristic can thoroughly be investigated when using different sub-solvers apart from the branch-and-cut method used in this study.

- Another area of research could be in the modelling of the WMNs and the properties associated with them. This dissertation proposes a method that is independent of any link-layer, network or high-level protocols associated with the wireless nodes. This increases the practical applicability, as in real-life scenarios, information obtained about eavesdroppers and their capabilities are minimal. However, certain assumptions regarding their SNR threshold values are made in this work. A statistical model can thus be developed with associated risk measures, depending on any assumptions made regarding the eavesdropping nodes. This would required extensive research and investigation into various nodes and their eavesdropping related capabilities, so that it can effectively be incorporated into the proposed security scheme. As opposed to a single optimal solution provided based on assumed values, a number of different optimal solutions depending on the assumptions and their associate percentage of occurrence in real-life network scenarios, can be provided.

- A more complex transmission/reception scheme that makes use of spatial correlation can be investigated. Such schemes are currently implemented in commercial Wi-Fi cards and also in the IEEE 802.11n standard. This would involve altering the jamming effectiveness, q_k^j, equation used in the problem formulation; the structure and optimisation problems would remain the same. The effect of channel fading should also be taken into account.

- The mathematical program developed for this security scheme assumes stationary nodes. It is, however, reasonable to assume that the malicious eavesdropping nodes are able to move and react based on locations of the jammers. As a result, a game theoretic approach (such as using a Stackelberg game) can be investigated.

- Focus has been placed on the ease of practical implementation of the proposed scheme as no additional computation or complexity is required from the legitimate communication nodes; only the intelligent placement of simple continuous jammers is needed to achieve maximum protection. There are, however, a number of different types of more energy efficient jammers, such as reactive and scheduled jammers, that can be used. The power savings that are incurred and the costs associated with more complicated jammers, can further be looked into.

- In certain scenarios, it may be sufficient to protect only a certain area of the network, rather than offering 100% protection that is achieved through the designed security scheme. In order to accomplish this, percentile risk constraints can be added to the mathematical formulations developed in chapter 4. Possible risk measures that can be applied and are particularly effective in deterministic environments, are the Value-at-Risk and Conditional-Value-at-Risk measures. The incorporation of these risk measures can be investigated.

- The heuristic developed in chapter 5 can be used to solve any multi-dimensional multiple demand knapsack problem with a minimisation objective. Further performance evaluations on the developed heuristic can be conducted and a valuable contribution to the field of optimisation techniques, can be made.

REFERENCES

[1] W. Xu, W. Trappe, W. Zhang, and T. Wood, “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,” in *Proc. MobiHoc.*, 2005, pp. 46–57.

[2] M. DiRenzo and M. Debbah, “Wireless physical-layer security: The challenges ahead,” in *Proc. Int. Conf. Advance Technologies for Communications*, 2009, pp. 313–316.

[3] S. Bayat, R. H. Y. Louie, Z. Han, and Y. Li, “Physical-layer security in distributed wireless networks using matching theory,” *IEEE Trans. Inf. Forens. Security*, vol. 8, no. 5, pp. 717–732, May 2013.

[4] L.Le, “Multipath Routing Design for Wireless Mesh Networks,” in *Proc. IEEE Global Telecommunications Conference*, 2011, pp. 1–6.

[5] J. H. Huang, L. C. Wang, and C. J. Chang, “Power Fairness in a Scalable Ring- Based Wireless Mesh Network,” in *Proc. IEEE 66th Vehicular Technology Conference Fall*, 2007, pp. 341–346.

[6] S. Jayaprakasam, T. C. Chuah, and S. W. Tan, “Collaborative mesh networking for low cost wireless coverage in rural areas,” in *Proc. IEEE Symp. Industrial Electronics Applications*, 2009, pp. 313–318.

[7] S. Vural, D. Wei, and K. Moessner, “Survey of experimental evaluation studies for wireless mesh network deployments in urban areas towards ubiquitous internet,” *IEEE Communications Surveys Tutorials*, vol. 15, no. 1, pp. 223–239, Feb. 2013.

[8] F. Licandro and G. Schembra, “Wireless Mesh Networks to Support Video Surveillance: Architecture, Protocol, and Implementation Issues,” *EURASIP Journal on Wireless*

Communication and Networking, vol. 2007, no. 1, pp. 1–13, Mar. 2007.

[9] W. Yang, Y. Zhang, and Y. Liu, "Constructing of wireless emergency communication system for underground coal mine based on wmn technology," *Journal of Coal Science and Engineering*, vol. 16, no. 4, pp. 441–448, Dec. 2010.

[10] M. Fouda, H. Nishiyama, R. Miura, and N. Kato, "On efficient traffic distribution for disaster area communication using wireless mesh networks," *Wireless Personal Communications*, vol. 74, no. 4, pp. 1311–1327, Feb. 2014.

[11] D. J. Shyy, "Military Usage Scenario and IEEE 802.11s Mesh Networking Standard," in *Proc. IEEE Military Communications Conf*, 2006, pp. 1–7.

[12] H. Hayes. (2012, Aug. 1) How mesh networks extend military comm. [Online]. Available: http://www.fedtechmagazine.com/article/2012/08/how-mesh-networks-extend-military-comm.

[13] *802.11s-2011 - IEEE Standard for Information Technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 10: Mesh Networking*, IEEE 802.11s Std., 2011.

[14] W. S. Conner, J. Kruys, K. Kim, and J. C. Zuniga, "IEEE 802.11s Tutorial: Overview of the Amendment for Wireless Local Area Mesh Networking," in *IEEE 802 Plenary Tutorials*, 2006.

[15] G. R. Hiertz, D. Denteneer, S. Max, R. Taori, J. Cardona, L. Berlemann, and B. Walke, "IEEE 802.11s: The WLAN Mesh Standard," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 104–111, Feb. 2010.

[16] R. M. Abid, T. Benbrahim, and S. Biaz, "IEEE 802.11s Wireless Mesh Networks for Last-Mile Internet Access: An Open-Source Real-World Indoor Testbed Implementation," *Wireless Sensor Network*, vol. 2, no. 10, pp. 725–738, Oct. 2010.

[17] S. V. Mohan and N. Kasiviswanath, "Routing Protocols for Wireless Mesh Networks," *International Journal of Scientific and Engineering Research*, vol. 2, no. 8, pp. 1–5, Aug.

2011.

[18] I. F. Akyildiz, X. Wang, and W. Wang, “Wireless Mesh Networks: A survey,” *Computer Networks*, vol. 47, no. 4, pp. 445–487, Mar. 2005.

[19] *IETF Ad hoc On-Demand Distance Vector*, RFC3561 Std., 2003.

[20] Y. Zhang, J. Luo, and H. Hu, *Wireless Mesh Networking.* Boca Raton, FL: CRC Press, 2006.

[21] *IETF Optimised Link State Routing*, RFC3626 Std., 2003.

[22] J. D. Camp and E. W. Knightly, “The IEEE 802.11s Extended Service Set Mesh Networking Standard,” *IEEE Communications Magazine*, vol. 46, no. 8, pp. 120–126, Aug. 2008.

[23] D. Raychaudhuri and M. Gerla, *Emerging Wireless Technologies and the Future Mobile Internet.* New York, NY: Cambridge University Press, 2011.

[24] E. Hossain and K. K. Leung, *Wireless Mesh Networks: Architectures and Protocols.* New York City, NY: Springer, 2008.

[25] U. S. Secretary of Defense, “The implementation of network-centric warfare,” Office of Force Transformation, Tech. Rep., 2005.

[26] J. L. Groh, “Network-centric warfare: Leveraging the power of information,” *USAWC Guide to National Security Issues*, vol. 1, pp. 323–338, Jun. 2008.

[27] C. N. Sweet and S. Kanefsky, “The c2 constellation a us air force network centric warfare program,” Electronic Systems Center, C2 Enterprise Planning and Integration, Tech. Rep., 2004.

[28] J. L. Conatser and V. E. Grizio, “Force xxi battle command brigade and below-blue force tracking (fbcb2-bft),” Naval Postgraduate School, Tech. Rep., 2005.

[29] D. Gonzales, J. S. Hollywood, G. Kingston, and D. Signori, *Network-Centric Operations Case Study: Air-to-Air Combat with and without Link 16.* Santa Monica, CA: RAND

Corporation, 2005.

[30] C. Fuzak, W. L. Carper, M. Gmritruk, J. W. Aitkenhead, T. Matoon, and V. J. Monteleon, "C^{4}ISR imperatives- conerstones of a network-centric architecture," Space and Naval Warfare Systems Center, Tech. Rep., 2001.

[31] J. Hauser, D. J. Shyy, and M. Green, "Military Usage Model," in *IEEE P802.11 Wireless LANs Usage Models IEEE P802.11-04/662r13*, 2004.

[32] R. DiPietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, "Security in wireless adhoc networks - A survey," *Computer Communications*, vol. 51, no. 1, pp. 1–20, Sep. 2014.

[33] V. M. Rohokale, N. R. Prasad, and R. Prasad, "Reliable and secure cooperative communication for wireless sensor networks making use of cooperative jamming with physical layer security," *Wireless Personal Communications*, vol. 73, no. 3, pp. 595–610, May 2013.

[34] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, Aug. 2002.

[35] O. Cheikhrouhou, M. Laurent-Makanavicius, and H. Chaouchi, "Security architecture in a multi-hope mesh network," in *Proc. Conf. Safety and Architectures Networks*, 2006, pp. 1–10.

[36] P. Bergamo, P. D'Arco, A. DeSantis, and L. Kocarev, "Security of public-key cyptosystems based on chebyshev polynomials," *IEEE Trans. Circuits Syst. I Reg. Papers*, vol. 52, no. 7, pp. 1382–1393, Jul. 2005.

[37] J. Lai, W. Kou, and K. Chen, "Self-generated-certificate public key encryption without pairing and its applications," *Information Sciences*, vol. 181, no. 11, pp. 2422–2435, Jun. 2011.

[38] Z. Wang, Y. Xing, Q. Wang, and W. Liu, "A wireless mesh network secure access method based on identity-based signature," in *Proc. Wireless Communications Networking and Mobile Computing Conf.*, 2010, pp. 1–4.

[39] B. He and D. P. Agrawal, “An identity-based authentication and key establishment scheme for multi-operator maintained wireless mesh networks,” in *Proc. Int. Conf. Mobile Adhoc and Sensor Systems*, 2010, pp. 71–78.

[40] A. Boudguiga and M. Laurent, “An authentication scheme for ieee 802.11s mesh networks relying on sakai-kasahara id-based cyrptographic algorithms,” in *Proc. Int. Conf. Communications and Networking*, 2012, pp. 1–8.

[41] A. D. Wyner, “The wire-tap channel,” *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[42] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[43] R. Liu, T. Liu, H. V. Poor, and S. Shamai, “Multiple-input multiple-output gaussian broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.

[44] S. K. Leung-Yan-Cheong and M. E. Hellman, “The gaussian wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[45] J. Barros and M. R. D. Rodrigues, “Secrecy capacity of wireless channels,” in *Proc. IEEE Int. Symp. Inf. Theory*, 2006, pp. 356–360.

[46] A. Khisti, A. Tchamkerten, and G. W. Wornell, “Secure broadcasting over fading channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[47] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, “Wireless secrecy regions with friendly jamming,” *IEEE Trans. Inf. Forens. Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.

[48] S. Prasad and D. J. Thuente, “Jamming attacks in 802.11g- a cognitive radio based approach,” in *Proc. IEEE Military Communications Conf.*, 2011, pp. 1219–1224.

[49] F. Xing and W. Wang, “Understanding dynamic denial of service attacks in wireless networks: The case of jammers,” in *Proc. IEEE Military Communications Conf.*, 2006,

pp. 791–802.

[50] E. Altman, K. Avrachenkov, and A. Garnaev, “Jamming in wireless networks under uncertainty,” in *Proc. Int. Symp. Modeling and Optimization in Mobile Ad Hoc and Wireless Networks*, 2009, pp. 1–7.

[51] L. Wang and A. Wyglinski, “A combined approach for distinguishing different types of jamming attacks against wireless networks,” in *Proc. 2011 IEEE Pacific Rim Conf. Commun. Compt. Signal Process*, 2011, pp. 809–814.

[52] F. Xing and W. Wang, “Understanding dynamic denial of service attacks in mobile ad hoc networks,” in *Proc. IEEE Military Communications Conf.*, 2006, pp. 1–7.

[53] M. Balakrishnan, H. Huang, R. Asorey-Cacheda, S. Misra, S. Pawar, and Y. Jaradat, “Measures and countermeasures for null frequency jamming of on-demand routing protocols in wireless ad hoc networks,” *IEEE Trans. Wireless Commun.*, vol. 11, no. 11, pp. 3860–3868, Nov. 2012.

[54] Z. Han, N. Marina, M. Debbah, and A. Hjorungnes, “Physical layer security game: Interaction between source, eavesdropper, and friendly jammer,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, pp. 1–10, Jan. 2010.

[55] L. Lai and H. ElGamal, “The relay-eavesdropper channel: Cooperation for secrecy,” *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[56] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[57] A. Y. Al-nahari, I. Krikidis, A. S. Ibrahim, M. I. Dessouky, and F. E. A. El-Samie, “Relaying techniques for enhancing the physical layer secrecy in cooperative networks with multiple eavesdroppers,” *Trans. Emerging Tel. Tech*, vol. 25, no. 4, pp. 445–460, Apr. 2014.

[58] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Jun. 2009.

[59] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[60] C. Swamy, "The effectiveness of Stackelberg strategies and tolls for network congestion games," *ACM Transactions on Algorithms*, vol. 8, no. 4, pp. 1–19, Sep. 2012.

[61] J. Qu, Y. Cai, J. Lu, A. Wang, J. Zheng, W. Yang, and N. Weng, "Power allocation based on stackelberg game in a jammer-assisted secure networks," in *Proc. Int. Conf. Cyberspace Technology*, 2013, pp. 347–352.

[62] M. Ara, H. Reboredo, F. Renna, and M. R. D. Rodrigues, "Power allocation strategies for ofdm gaussian wiretap channels with a friendly jammer," in *Proc. Int. Conf. Communications*, 2013, pp. 3413–3417.

[63] J. Yang, I. Kim, and D. Kim, "Power-constrained optimal cooperative jamming for multiuser broadcast channel," *IEEE Wireless Commun. Lett.*, vol. 2, no. 4, pp. 411–414, May 2013.

[64] W. Shen, P. Ning, X. He, and H. Dai, "Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time," in *Proc. IEEE Symp. Security and Privacy*, 2013, pp. 174–188.

[65] M. G. C. Resende and P. M. Pardalos, *Handbook of Optimization in Telecommunications.* New York City, NY: Springer, 2006.

[66] C. W. Commander, P. M. Pardalos, V. Ryabchenko, S. Uryasev, and G. Zrazhevsky, "The wireless network jamming problem," *Journal of Combinatorial Optimization*, vol. 14, no. 4, pp. 481–498, Mar. 2007.

[67] H. Ying-chun, L. Xiao-xiao, and L. Hang, "The research on optimal coverage algorithm of crane-umbrella communication jammers," in *Proc. Int. Conf. Intelligent Networks and intelligent Systems*, 2010, pp. 572–575.

[68] K. Guan, R. Ghanadan, S. Dehni, and S. Mo, "Optimal platform placement and configuration in networked electronic warfare (EW)," in *Proc. Military Communications*

Conf., 2010, pp. 1019–1024.

[69] S. Vadlamani, H. Medal, B. Eksioglu, and P. Li, “A bi-level programming model for the wireless network jamming placement problem,” in *Proc. Industrial and Systems Engineering Research Conf.*, 2014, pp. 1003–1011.

[70] G. Brown, M. Carlyle, J. Salmeron, and K. Wood, “Defending critical infrastructure,” *Interfaces*, vol. 36, no. 6, pp. 530–544, Dec. 2006.

[71] S. Heikkila, “On extremal pure Nash equilibria for mixed extensions of normal-form games,” *Nonlinear Analysis: Theory, Methods and Applications*, vol. 66, no. 7, pp. 1645–1659, Apr. 2007.

[72] C. W. Commander, P. M. Pardalos, V. Ryabchenko, O. Shylo, S. Uryasev, and G. Zrazhevsky, “Jamming communication networks under complete uncertainty,” *Optimization Letters*, vol. 2, no. 1, pp. 53–70, Jan. 2007.

[73] F. D’Andreagiovanni, “Revisiting wireless network jamming by sir-based considerations and multiband robust optimization,” *Optimization Letters*, pp. 1–16, 2014. [Online]. Available: http://dx.doi.org/10.1007/s11590-014-0839-2

[74] S. Sankararaman, K. Abu-Affash, A. Efrat, S. D. Eriksson-Bique, V. Polishchuk, S. Ramasubramanian, and M. Segal, “Optimization schemes for protective jamming,” *Mobile Netw. Appl.*, vol. 19, no. 1, pp. 45–60, Feb. 2014.

[75] N. Andreasson, A. Evgrafov, and M. Patriksson, *An Introduction to Continuous Optimization.* Lund, Sweden: Studentlitteratur AB, 2007.

[76] S. P. Bradley, A. C. Hax, and T. L. Magnanti, *Applied Mathematical Programming.* Addison-Wesley, 1977.

[77] B. Lev and H. J. Weiss, *Introduction to Mathematical Programming: Quantitative Tools for Decision Making.* London, England: Edward Arnold, 1982.

[78] F. S. Hillier and G. J. Lieberman, *Introduction to Operations Research.* New York, NY: McGraw-Hill, 2004.

[79] G. B. Dantzig, *Linear Programming and Extensions.* Princeton, NJ: Princeton University Press, 1998.

[80] W. L. Winston and M. Venkataramanan, *Introduction to Mathematical Programming.* Belmont, CA: Brooks/Cole Cengage Learning, 2003.

[81] R. K. Ahuja, T. L. Magnanti, and J. B. Orlin, *Network Flows: Theory, Algorithms, and Applications.* Upper Saddle River, NJ: Prentice Hall, 1993.

[82] H. Kellerer, U. Pferschy, and D. Pisinger, *Knapsack Problems.* Berlin, Germany: Springer, 2004.

[83] R. M. Karp, "George Dantzig's impact on the theory of computation," *Discrete Optimization*, vol. 5, no. 2, pp. 174–185, May 2008.

[84] V. I. Norkin, G. C. Pflug, and A. Ruszczynski, "A branch and bound method for stochastic global optimization," *Mathematical Programming: Series B*, vol. 83, no. 3, pp. 425–450, Nov. 1998.

[85] C. Still and T. Westerlund, "A sequential cutting plane algorithm for solving convex NLP problems," *European Journal of Operational Research*, vol. 173, no. 2, pp. 444–464, Sep. 2006.

[86] P. Kesavan and P. I. Barton, "Generalized branch-and-cut framework for mixed-integer nonlinear optimization problems," *Computers and Chemical Engineering*, vol. 24, no. 2, pp. 1361–1366, Jul. 2000.

[87] P. M. Pardalos and M. G. C. Resende, *Handbook of Applied Optimization.* New York, NY: Oxford University Press, 2002.

[88] P. Cappanera and M. Trubian, "A Local-Search-Based Heuristic for the Demand-Constrained Multidimensional Knapsack Problem," *INFORMS Journal on Computing*, vol. 17, no. 1, pp. 82–98, Feb. 2005.

[89] L. M. Hvattum, H. Arntzen, A. L. kketangen, and F. Glover, "Alternating control tree search for knapsack/covering problems," *Journal of Heuristics*, vol. 16, no. 3, pp. 239–

258, Nov. 2008.

[90] IBM. (2015) IBM ILOG CPLEX Optimizer. [Online]. Available: http://www-01.ibm.com/software/commerce/optimization/cplex-optimizer