
Satish Vadlamani

Follow this and additional works at: https://scholarsjunction.msstate.edu/td

Recommended Citation

This Dissertation is brought to you for free and open access by the Theses and Dissertations at Scholars Junction. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of Scholars Junction. For more information, please contact scholcomm@msstate.libanswers.com.
A mixed-integer programming approach for jammer placement problems for flow-jamming attacks on wireless communication networks

By

Satish Vadlamani

A Thesis
Submitted to the Faculty of Mississippi State University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Industrial and Systems Engineering in the Department of Industrial and Systems Engineering

Mississippi State, Mississippi

December 2015
A mixed-integer programming approach for jammer placement problems for flow-jamming attacks on wireless communication networks

By

Satish Vadlamani

Approved:

Hugh R. Medal
(Major Professor)

Burak Eksioglu
(Committee Member)

Mengqi Hu
(Committee Member)

Pan Li
(Committee Member)

Kari Babski-Reeves
(Graduate Coordinator)

Jason M. Keith
Dean
Bagley College of Engineering
In this dissertation, we study an important problem of security in wireless networks. We study different attacks and defense strategies in general and more specifically jamming attacks. We begin the dissertation by providing a tutorial introducing the operations research community to the various types of attacks and defense strategies in wireless networks. In this tutorial, we give examples of mathematical programming models to model jamming attacks and defense against jamming attacks in wireless networks. Later we provide a comprehensive taxonomic classification of the various types of jamming attacks and defense against jamming attacks. The classification scheme will provide a one stop location for future researchers on various jamming attack and defense strategies studied in literature. This classification scheme also highlights the areas of research in jamming attack and defense against jamming attacks which have received less attention and could be a good area of focus for future research.
In the next chapter, we provide a bi-level mathematical programming model to study jamming attack and defense strategy. We solve this using a game-theoretic approach and also study the impact of power level, location of jamming device, and the number of transmission channels available to transmit data on the attack and defense against jamming attacks. We show that by increasing the number of jamming devices the throughput of the network drops by at least 7%.

Finally we study a special type of jamming attack, flow-jamming attack. We provide a mathematical programming model to solve the location of jamming devices to increase the impact of flow-jamming attacks on wireless networks. We provide a Benders decomposition algorithm along with some acceleration techniques to solve large problem instances in reasonable amount of time. We draw some insights about the impact of power, location and size of the network on the impact of flow-jamming attacks in wireless networks.

Key words: Wireless networks, security, jamming attacks, Benders decomposition
DEDICATION

To my parents.
ACKNOWLEDGEMENTS

First, I would like to thank my committee co-chairs, Dr. Hugh R. Medal and Dr. Burak Eksioglu, without their guidance and assistance, this dissertation would never have been accomplished. Both of them were very patient and were of constant support. I would like to thank Dr. Medal for funding my dissertation. He not only helped me on my dissertation, he was always there to talk and provide continuous support and encouragement. His kind words of advice I will always remember. Without his words of encouragement, this dissertation would not have completed. Dr. Burak has been a constant support from the time I came to Mississippi State for pursuing my M.S. through my dissertation. I will always remember him for his easily approachable nature. He is one person whom I have always looked up to. I would like to sincerely thank the both of them again for everything they have done for me.

Additionally, I would like to thank other members of my dissertation committee: Dr. Mengqi Hu and Dr. Pan Li for their time, effort and feedback that was invaluable to me.

I would also like to thank the Research and Curriculum Unit at Mississippi State for providing me financial support during the initial stages of my dissertation. I would like to extend my gratitude to Lisa Hardjono and Dr. Surya Durbha for everything they have done for me. I have been very fortunate to have great lab-mates. Special thanks to Dr. Mohammad Marufuzzaman, Dr. Gokce Palak, Dr. Md. Roni, Dr. Abdullah Al Khaled,
Apurba Kumar Nandi, Eghbal Rashidi, Hadi Karimi, Zahra Azadi, Adindu Emelogu, Yang Chen and Sushil Poudel. I will cherish the moments we spent in the lab studying for exams and discussing various topics at length.

My heartfelt thanks to my parents for their love, affection and support. I will never forget all the sacrifices they had to go through to get me where I am today. I would also like to thank my sister and grandparents for their support. I would like to thank my wife Sree for her love and support and for always encouraging to be positive and work hard.

Finally, and most importantly, I want to thank God for giving me all that is need to complete my dissertation successfully and giving me the opportunity to be among such wonderful people.
# TABLE OF CONTENTS

DEDICATION ................................................................. ii

ACKNOWLEDGEMENTS ..................................................... iii

LIST OF TABLES .......................................................... viii

LIST OF FIGURES ......................................................... ix

CHAPTER

1. INTRODUCTION ............................................................... 1

2. SECURITY IN WIRELESS NETWORKS: A TUTORIAL ..................... 4
   2.1 Introduction .......................................................... 4
   2.2 About Wireless Networks ............................................ 6
      2.2.1 Types of Wireless Networks and Applications ............... 7
         2.2.1.1 WLAN ..................................................... 7
         2.2.1.2 WSN ...................................................... 8
         2.2.1.3 Ad Hoc .................................................... 9
   2.3 Modeling Constructs ................................................ 10
      2.3.1 Attack Strategies ............................................... 11
         2.3.1.1 Types of Attacks: ........................................ 11
      2.3.2 Defense Strategies ............................................ 13
         2.3.2.1 Defense against Sink-hole Attacks ....................... 13
         2.3.2.2 Defense against Sybil Attack .......................... 13
         2.3.2.3 Defense against Worm-hole Attacks .................... 14
         2.3.2.4 Defense against Jamming Attacks ...................... 14
   2.3.3 Objectives (Performance Metrics) ............................... 15
      2.3.3.1 SINR ...................................................... 15
      2.3.3.2 Packet Send Ratio (PSR) ................................ 16
      2.3.3.3 Packet Delivery Ratio (PDR) ............................ 17
      2.3.3.4 Connectivity Index ..................................... 17
      2.3.3.5 Throughput ............................................... 18
      2.3.3.6 Utilization ............................................... 19
4. A BI-LEVEL PROGRAMMING MODEL FOR THE WIRELESS NETWORK JAMMING PLACEMENT PROBLEM .......................... 70

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Introduction</td>
<td>70</td>
</tr>
<tr>
<td>4.2</td>
<td>Literature Review</td>
<td>72</td>
</tr>
<tr>
<td>4.3</td>
<td>Problem Description and Mathematical Model</td>
<td>73</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Problem Description</td>
<td>75</td>
</tr>
<tr>
<td>4.3.2</td>
<td>Mathematical Model</td>
<td>76</td>
</tr>
<tr>
<td>4.4</td>
<td>Solution Approach</td>
<td>81</td>
</tr>
<tr>
<td>4.5</td>
<td>Numerical Experiments</td>
<td>83</td>
</tr>
<tr>
<td>4.6</td>
<td>Conclusion</td>
<td>86</td>
</tr>
</tbody>
</table>

5. A MIXED-INTEGER PROGRAMMING APPROACH FOR LOCATING JAMMING DEVICES IN A FLOW-JAMMING ATTACK .......................... 87

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Introduction</td>
<td>87</td>
</tr>
<tr>
<td>5.2</td>
<td>Problem Description and Mathematical Model</td>
<td>91</td>
</tr>
<tr>
<td>5.3</td>
<td>Algorithmic Strategy</td>
<td>96</td>
</tr>
<tr>
<td>5.3.1</td>
<td>Benders Decomposition</td>
<td>97</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Accelerating Standard Benders Decomposition</td>
<td>100</td>
</tr>
<tr>
<td>5.3.2.1</td>
<td>Pareto Optimality Cut</td>
<td>101</td>
</tr>
<tr>
<td>5.3.2.2</td>
<td>Trust Region</td>
<td>102</td>
</tr>
<tr>
<td>5.3.2.3</td>
<td>Knapsack Inequality</td>
<td>103</td>
</tr>
<tr>
<td>5.3.2.4</td>
<td>Solution Elimination Constraint</td>
<td>103</td>
</tr>
<tr>
<td>5.4</td>
<td>Computational Results and Analysis</td>
<td>104</td>
</tr>
<tr>
<td>5.4.1</td>
<td>Experimental Results</td>
<td>104</td>
</tr>
<tr>
<td>5.4.1.1</td>
<td>Case 1:</td>
<td>104</td>
</tr>
<tr>
<td>5.4.1.2</td>
<td>Case 2:</td>
<td>110</td>
</tr>
<tr>
<td>5.4.2</td>
<td>Discussion</td>
<td>110</td>
</tr>
<tr>
<td>5.5</td>
<td>Conclusion</td>
<td>114</td>
</tr>
</tbody>
</table>

6. CONCLUSION AND FUTURE WORK .............................................. 116

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Conclusion</td>
<td>116</td>
</tr>
<tr>
<td>6.2</td>
<td>Future Work</td>
<td>117</td>
</tr>
</tbody>
</table>

REFERENCES ................................................................. 118
<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Classification scheme</td>
<td>39</td>
</tr>
<tr>
<td>3.2</td>
<td>Classification scheme</td>
<td>40</td>
</tr>
<tr>
<td>3.3</td>
<td>Classification scheme</td>
<td>41</td>
</tr>
<tr>
<td>4.1</td>
<td>3 Intermediate Nodes</td>
<td>85</td>
</tr>
<tr>
<td>4.2</td>
<td>5 Intermediate Nodes</td>
<td>86</td>
</tr>
<tr>
<td>4.3</td>
<td>9 Intermediate Nodes</td>
<td>87</td>
</tr>
<tr>
<td>5.1</td>
<td>List of mathematical notations</td>
<td>96</td>
</tr>
<tr>
<td>5.2</td>
<td>Jamming device types</td>
<td>107</td>
</tr>
<tr>
<td>5.3</td>
<td>Problem Instances</td>
<td>108</td>
</tr>
<tr>
<td>5.4</td>
<td>Case 1: Computational Results for CMU</td>
<td>109</td>
</tr>
<tr>
<td>5.5</td>
<td>Case 1: Computational Results for MIT</td>
<td>110</td>
</tr>
<tr>
<td>5.6</td>
<td>Case 2: Computational Results for Random</td>
<td>113</td>
</tr>
<tr>
<td>Figure</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>2.1</td>
<td>WirelessLAN</td>
<td>7</td>
</tr>
<tr>
<td>2.2</td>
<td>WSN</td>
<td>9</td>
</tr>
<tr>
<td>2.3</td>
<td>Wireless-ad-hoc</td>
<td>10</td>
</tr>
<tr>
<td>2.4</td>
<td>Single Channel Access Point with one transmitter and one jammer</td>
<td>23</td>
</tr>
<tr>
<td>3.1</td>
<td>Wireless LAN (adapted from [120])</td>
<td>30</td>
</tr>
<tr>
<td>3.2</td>
<td>Wireless Ad Hoc Network (adapted from [120])</td>
<td>31</td>
</tr>
<tr>
<td>3.3</td>
<td>Wireless Sensor Network (adapted from [120])</td>
<td>33</td>
</tr>
<tr>
<td>3.4</td>
<td>Publication trend over the year</td>
<td>35</td>
</tr>
<tr>
<td>3.5</td>
<td>Example of jamming in a network</td>
<td>43</td>
</tr>
<tr>
<td>3.6</td>
<td>Number of papers by wireless network type</td>
<td>64</td>
</tr>
<tr>
<td>3.7</td>
<td>Percentage of the contribution of papers by wireless network type</td>
<td>64</td>
</tr>
<tr>
<td>4.1</td>
<td>Example of jamming in a network</td>
<td>77</td>
</tr>
<tr>
<td>4.2</td>
<td>Jamming in a network of 9 intermediate node</td>
<td>83</td>
</tr>
<tr>
<td>5.1</td>
<td>Network without jamming</td>
<td>93</td>
</tr>
<tr>
<td>5.2</td>
<td>Flow jamming attack with arbitrary jamming device locations</td>
<td>93</td>
</tr>
<tr>
<td>5.3</td>
<td>Flow jamming attack with optimal jamming device locations</td>
<td>94</td>
</tr>
<tr>
<td>5.4</td>
<td>Network Topology of CMU</td>
<td>105</td>
</tr>
<tr>
<td>5.5</td>
<td>Network Topology of MIT</td>
<td>105</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>5.6</td>
<td>Example of jamming device locations</td>
<td>106</td>
</tr>
<tr>
<td>5.7</td>
<td>Effect of network topology on jamming impact</td>
<td>113</td>
</tr>
<tr>
<td>5.8</td>
<td>Effect of network topology on computational time-Random</td>
<td>114</td>
</tr>
</tbody>
</table>
Wireless networks are communication networks that enable transfer of data through air without the use of any cables or wires. Wireless networks like Wireless Local Area Network (WLAN) or more commonly called WiFi have found a place at homes, offices, coffee shops etc [40]. Another type of wireless network mostly found in places where human presence is difficult [83], e.g., deserts, is the Wireless Sensor Network (WSN). These networks collect information such as temperature and send it to the base station where the data is analyzed. Another type of network is the Ad Hoc Network (AHN), which military and the disaster management teams use to communicate when building a communication infrastructure is not feasible [103]. The method of data transfer using air as a medium makes wireless networks easy to use because they allow for movement which is not possible with the traditional networks that were connected by wires. However, along with the ease of access wireless networks also come with a myriad of security issues [46]. Since the data is transferred using air as a medium, it is easy for an adversary to disrupt communication [92].

Among the various attacks in wireless networks such as Worm hole attacks [46], Sybil attacks [143] etc., jamming attacks is the most critical security concern [112]. Jamming
attacks are a kind of Denial of Service (DoS) [92] attack, which denies legitimate users the ability to transfer data in a network by transmitting a signal that is stronger than the legitimate communication signal. Data sent in a network travels through a set of abstract layers before it reached the destination node. Of these abstract layers the DoS attacks on the physical layer are called jamming attacks [17]. However, [117, 128] have studied jamming attacks on the link layer and not just on the physical layer. [114] introduce an new attack called flow-jamming attacks by incorporating higher layer information in jamming attacks and by intelligently assigning jamming devices to flows. They provide a linear programming model for the flow-jamming attacks and also provide certain metrics to evaluate the effect of flow-jamming attacks. In this dissertation, we focus on flow-jamming attack, a topic which has not received much attention in literature.

In the recent years, there has been an increase in optimization problems involving wireless communication networks [32]. With an increase in the usage of wireless networks it is important to tackle these optimization problems to improve the quality and security of communication. In this dissertation, we provide several problems that affect the communication of wireless networks used by the military and disaster management teams. The problems presented are generally hard to solve and take a tremendous amount of time for computation. Furthermore, these problems are of importance in time critical and data sensitive adversarial settings, as compared to conventional setting when time and data may not be very critical. Thus, this dissertation focuses on designing algorithms that solve these complex problems to optimality in a reasonable amount of time.
In a war scenario or disaster situation, it is important to restrict the adversary from disrupting communication and disrupt communication of the adversary. Hence, in this dissertation, we study two class of problems in wireless networks. The first class of problems deals with disrupting or denying communication. The second class of problems deals with defending against attempts to disrupt the communication.

In this dissertation, we first start of by introducing the readers to wireless networks and different attack and defense strategies with a tutorial. Then we provide a comprehensive survey and classification scheme to help better understand a particular class of attack called jamming attack which is the main focus of this dissertation. We then introduce the problems and show that they can be formulated and solved using mathematical programming and optimization methods. For the problems considered we examine the computational complexity and provide algorithmic solution approaches.

The rest of the dissertation is as follows: Chapter 1 provides a tutorial about wireless networks and different types of attacks and defense against these attacks. Chapter 2 provides a comprehensive survey and a classification method for the various papers in the literature. Chapter 3 provides a bi-level mathematical model of an attacker-defender channel hopping jamming attack problem in wireless networks. Finally, in Chapter 4 we solve a mathematical programming model using Benders decomposition for the flow-jamming attacks.
2.1 Introduction

Wireless networks are proving to be a strong opponent to the already established wired networks and have gained more importance over the past few years. Largely because the cost of radio cards has decreased from $1500 to $50 over the past two decades, companies frequently use wireless networks for collecting data in contexts such as supply chain logistics [40]. Companies and enterprises are also using wireless networks for easy collaboration with other colleagues through emails and voice over calls across the globe for low costs. Wireless networks with location based technology helps companies to advertise their product depending on the physical location of the user. In addition to commercial uses, wireless networks have found a place in the home and residential areas too [40]. The installation and use of wireless networks is easy as compared to running cables through the walls, and the mobility provided by wireless network has become an instant hit in homes [40]. The applications of wireless networks are not restricted to commercial and home use only; they are used extensively in military and disaster situations.

The benefits of using wireless networks come at the expense of security. Wireless network are susceptible to various attacks because they use air to transmit and receive data. The most commonly occurring attacks in wireless networks are jamming attacks and de-
nial of service attacks; hence, these types of attacks are most commonly studied. Different defense approaches [4, 5, 39, 95, 100, 108] to cope with the various attacks on wireless networks is an active area of research. While wireless networks are a major research area in the field of electrical engineering (EE), we believe that the field of operations research (OR) can also contribute to the study of wireless network security. In particular, many wireless network security problems involve the allocation of resources, and resource allocation problems [90, 94] have been studied in depth by the OR community. Thus, the purpose of this tutorial is to marry the study of wireless network security and resource allocation.

Specifically, the main aim of this paper is to introduce the topic of network security in wireless networks with more emphasis on jamming attacks to the operations research community. We start by discussing the different types of wireless networks. We also highlight the main attack and defense mechanisms in wireless networks. We discuss some of the important definitions to better understand wireless networks and the security concerns. Finally, a few modeling examples are also provided. We believe that the examples provided along with the definitions will give a good start for the operations research community to see and better understand potential research areas in wireless network security. The rest of the paper is organized as follows. In Section 2 we introduce wireless networks; in Section 3 we provide different modeling components, and define some performance metrics; and in Section 4 we provide some modeling examples from the literature for better understanding wireless network security problems from an operations research view. We provide conclusions in Section 5.
2.2 About Wireless Networks

Although wired networks (e.g., Ethernet) are the most common medium for electronic communication, wireless networks are becoming increasingly popular because of the added mobility they provide. Wireless networks work by sending bits from one device to another through air as a medium. The bits are translated into radio frequency before they are modulated and sent via an antenna. The data received or transmitted goes through the following layers before it reaches its destination. The bottom up hierarchy of each of the layers and their respective function is as shown.

1. **Physical Layer [83]**: Describes the characteristics of the physical connection between devices on the network. The physical connection between devices can be cables, fibers, or wires. The transmission and reception of data is managed by the physical layer. In the case of wireless networks the binary data between computers is translated into electrical signals. The physical layer suffers from radio jamming attacks.

2. **Data Link Layer [83]**: Responsible for communication between the network layer and the physical layer. Also, this layer segments the packets sent by the higher layer to frames that can be sent by the physical layer below. This layer also provides error checking and formatting of the frames of data being sent. The MAC (Medium Access Control) layer is a part of the data link layer and is responsible for moving data packets to and from one node to another across a shared channel. A channel in a wireless network is a frequency at which the nodes send their data. The MAC sublayer uses MAC protocols to ensure that signals sent from different stations across the same channel don’t collide. This layer is susceptible to much more sophisticated jamming and energy efficient jamming than physical layer jamming attacks.

3. **Network Layer [83]**: Responsible for determining the network topology, assigning addresses and routing the data. It acts as a link between the transportation layer below and the data link layer above in the hierarchy.

4. **Transport Layer [83]**: Recovers any lost data and also responsible for retransmission of data. Provides data encryption and reliable data transfer capabilities.

5. **Application Layer [83]**: This layer is responsible for defining the specifications of the data requested by the end user in the network.
2.2.1 Types of Wireless Networks and Applications

2.2.1.1 WLAN

The most common type of wireless network is the wireless local area network (WLAN), more commonly known as Wi-Fi. WLAN has become ubiquitous in many developed countries, with wireless transmitters operating in homes, schools, offices, coffee shops, etc. In a WLAN, computers connect wirelessly to an access point (AP), which connects to the Internet, allowing users to have a wireless connection to the Internet, as long as they are in range of a wireless signal. Figure 2.1 gives an example of a WLAN with one AP and four computers.
2.2.1.2 WSN

A Wireless Sensor Network (WSN) is a collection of a large number of autonomous nodes that share information among themselves. The information shared, for example, can be temperature of a particular area collected every few seconds by the sensors. WSNs are usually deployed by a person or an organization to collect data from places which are difficult for humans to be physically present (e.g., deserts, toxic areas etc.). The person or the organization that uses the data collected by the WSNs is referred to as a user. The user might be interested only in the average temperature of a place and not the temperature data collected every few seconds. In a WSN the data collected is not directly sent to the user; rather the results of the computation (average temperature) is sent, i.e., only the goal of the sensor network is sent to the user and the intermediate data is not sent [97]. A WSN consists of a gateway (base station) that connects the sensor nodes to other sensor networks or to the end user (see Figure 2.2). The data is compressed at the sensor nodes and then transmitted to the base station, which presents the results to the end user [119]. Data packets are often sent to the destination via many intermediate nodes, a process known as hopping. Thus, a WSN is referred to as a multi-hop network. Figure 2.2 shows a WSN with sensors in a sensing area deployed by the end user to collect specific data needed. Data is transmitted from each of the sensors through the network to the base station, which consolidates the data and presents it to the user. The following list includes some of the applications of WSNs [83]:

- **Security**: WSNs are used to detect biological or chemical threats.
- **Environment and habitat monitoring:** WSNs also help in getting information about areas that are difficult to monitor such as deserts, the poles, high altitudes and underwater.

- **Medical monitoring:** Doctors use WSNs to remotely monitor the health of patients.

- **Assistive environments:** The functional capabilities of individuals with disabilities can be improved [98] by equipping the individual with position measuring systems and location information gathering devices with the help of a WSN. WSNs can also help enable cost effective self care and a better quality of life.

![Figure 2.2 WSN](image)

**2.2.1.3 Ad Hoc**

A network is called *ad hoc* if it does not need any pre-existing infrastructure such as cables or access points. Each node (e.g., laptop, cellphone) in an ad hoc network (AHN) participates in the routing of data independently by forwarding data from one node to another without a centralized manager such as an access point (AP). Thus, the nodes in an AHN dynamically decide which node to send the data to next depending on the network connectivity. Figure 2.3 shows a basic setup of an AHN between laptops and phones,
which communicate among themselves without an AP. AHNs are used in the following applications [103, 145]:

- **Military**: Units (e.g., soldiers and tanks) can communicate with each other within a theater, which may have limited functioning infrastructure.

- **Disaster response**: AHNs can also be used for emergency, law enforcement, and rescue missions, provide communication even when the existing telephone and other means of communications are destroyed or disrupted.

- **Meetings**: AHNs are also used in conferences/lectures/meetings and other commercial areas where the load on the network can be very high.

![Figure 2.3: Wireless-ad-hoc](image)

2.3 **Modeling Constructs**

As mentioned in the introduction, wireless security problems often involve the allocation of resources. The field of operations research often uses optimization modeling to
optimize the allocation of resources in a system. In this section we discuss the components that a properly formulated optimization model for wireless network security should have.

2.3.1 Attack Strategies

2.3.1.1 Types of Attacks:

- **Sink-hole attack:** In sink-hole attacks an adversary makes a malicious node attractive to the other nodes in the network, luring all traffic to the malicious node instead of the base station. The adversary fakes the routing table values and makes the compromised nodes look attractive; by showing higher quality links to reach the base station. When neighboring nodes send data through the compromised node, it baits the other legitimate nodes to use the malicious nodes to route data to the base station. This routing of data from all the nodes in the area increases the “strength of influence” [50] of the adversarial node. The adversary can either eavesdrop or even corrupt the data, making this a dangerous threat [50].

- **Sybil attack:** In this type of attack, a single node displays multiple identities to other nodes in the network. This attack reduces the efficiency of the network by causing problems with routing protocols. The legitimate data is sent along a path that has one attacker node, who represents himself as many nodes. This decreases the efficiency of the network and compromises the data [50].

- **Worm-hole attack:** In worm-hole attacks the attacker tunnels the data received from one point in the network over a link with less delays and replays the data from another point in the network. Worm-hole attacks include two distant malicious nodes colluding together to falsify the actual distance from each other, attracting data to be sent through them. The malicious nodes could be very far from the network and be out of bound from a single hop, but they still pretend to be close by using a single long-range directional link. A successful worm-hole attack allows the adversary to eavesdrop or even form a sink-hole [46, 50].

- **Jamming attack:** A jamming attack is the act of intentionally transmitting electromagnetic waves towards a communication network to either disrupt or preclude signal transmission in wireless networks. When the word “jammer” is used we mean a device that has the capacity to jam a network. In WSNs and AHNs jamming attacks interfere with legitimate transmission by using the same radio frequency that the nodes in the network use. Powerful jammers can degrade the functionality of the network. In the case of military and security applications where WSNs and AHNs are extensively used, a jamming attack could mean losing critical information to attackers or terrorists because they can interrupt legitimate data and listen to it. This makes it important to use effective countermeasures against such attacks. The nodes in WSNs and AHNs have limited power, memory resources and low computational capacity, making them easy targets for an unsophisticated attacker. Moreover, these
networks sometimes even have to use insecure channels to transmit data, in the case of an event like a natural disaster where establishing a secure channel could be infeasible, allowing attackers to get easy access to the data by jamming the link the data is being transferred on. Jamming attacks are sometimes referred to as a special case of a Denial of Service (DoS) attack [83]. A successful denial of service attack denies legitimate users from sending data because of the presence of an illegitimate user who transmits false data or radio frequency through the network, giving an impression to the legitimate nodes that the network is busy, forcing them to stop sending data until the network is free again. A jamming device, tuned to the same frequency as the opponent’s receiving equipment and with the same type of modulation, can, with enough power, override any signal at the receiver. Wireless signal jamming devices are most often used to interfere with wireless networks. Advanced and more expensive jamming devices are used to jam satellite communications.

Four classes of jammers have been studied in the literature [83, 136, 92]:

- **Constant Jammer:** The constant jammer continuously emits jamming signals. The signal emitted can be a simple electromagnetic wave or even a random sequence of bits of data and does not follow any protocol or rule that the legitimate nodes in the network follow. This kind of jammer reduces the packet delivery ratio (see Section 2.2.3) by corrupting the bits at the receiver node by interfering with the transmission of a transmitter node. The other objective of the constant jammer can be to reduce the packet send ratio (see Section 2.2.2) by keeping the channels busy and not allowing legitimate nodes to transmit data [92].

- **Deceptive Jammer:** Although deceptive jammers also continuously transmit signals or data, unlike constant jammers deceptive jammers do not use a random bit sequence. As a result, the legitimate nodes in the network believe these bits of data are legitimate, making the attack more effective [92].

- **Random Jammer:** Both constant and deceptive jammers continuously transmit signals, requiring a lot of power. To conserve power, random jammers have sleep cycles. The jammer alternates between jamming and sleeping states randomly [92].

- **Reactive Jammer:** Like the random jammer, reactive jammers do not continuously emit a signal. Rather, they jam the channel when any transmission is detected. These jammers constantly listen to the channel, and when they sense a packet transmission they immediately send a radio signal that jams the channel. The amount of power needed to listen to a channel is much less than the amount of power needed to jam [92].
2.3.2 Defense Strategies

2.3.2.1 Defense against Sink-hole Attacks

- **Trust Management System:** Trust Management and Dynamic Trust Management Systems (DTMS) have been used to protect both ad hoc and wireless networks from attacks. In a trust management system the nodes in the ad hoc network broadcast a trust vector of length of $N$ (number of nodes in the network) and a value of $+0.5$. The trust vector is broadcasted to all nodes in the network at regular time intervals. But, the value in vector changes depending on the experience of the other nodes in the network. If a node drops packets then its trust value is reduced at a very high rate. If a node transfers packets without much loss it earns a positive trust value. However, the rate of increase of trust value is very small. This process is repeated and each node knows the trust value of others, so the nodes with a bad trust value are ignored from the routing [28]. Roy et al. [102] provide a dynamic trust management system to counter sink-hole attacks in WSNs. Unlike ad hoc networks, where there is no central manager who controls the flow of data, in sensor networks the trust vector is sent to the base station at regular intervals, where the decision of which node to trust is made and then the routing plan is decided.

2.3.2.2 Defense against Sybil Attack

- **One-way key chains:** In sensor networks, defense against Sybil attacks is done by a redundancy mechanism [143]. A setup server assigns each sensor a unique identifier prior to operation. The server subsequently assigns each of the unique identifiers a unique id and pairs the sensor with that unique id and unique identifier. The server creates a certificate of binding, and downloads the certificate and the unique information to the sensor node. To successfully receive/transmit data the node must first show its unique id and the unique information to the demand node. If this check is complete then the data is transferred. This way no node can display multiple identities, countering a Sybil attack [143].

- **Radio Resource Testing:** In this approach to defend against Sybil attacks, a node $n$ assigns each of its neighbors a different channel to broadcast some message on. The node $n$ then randomly chooses a channel to listen to; if the neighbor that was assigned that channel is legitimate then node $n$ can hear the message. If on other the hand, $s$ of $n$’s neighbors are Sybil identities then the probability that a randomly chosen channel is not transmitting any data hence successfully detecting a Sybil attack is $\frac{s}{n}$. Conversely, the probability of not detecting a Sybil attack is $\frac{n-s}{n}$. Hence, if this procedure is repeated $r$ times, the probability of not detecting a Sybil attack is $\left(\frac{n-s}{n}\right)^r$. As a result, as the number of rounds increases the probability of not detecting the attack decreases [87].
2.3.2.3 Defense against Worm-hole Attacks

- **Packet Leash:** The packet leash method has two different variants: 1) geographic leash and 2) temporal leash. In a geographic leash the sender sends his location $p_s$, and time of sending $t_s$ along with the packet. The clocks at the transmitter and receiver are loosely synchronized. At the receiver the node calculates its location $p_r$ and the time of receiving $t_r$. Using the time and the location values and knowing the speed of packets, the receiver can calculate the upper bound of the distance between the transmitter and receiver. So, in the presence of a worm-hole, the distance would seem very far from the actual reported value by the transmitter, hence eliminating the route [46]. In a temporal leash the transmitter and the receiver clocks have to be tightly synchronized. The transmitter node includes the time of sending the packet and the receiver, upon receiving the packet, notes the time. Using the time values and the speed of light, the receiver calculates the distance, to see if the packet has traveled a longer distance than it should have. There is another variation of temporal leash in which the transmitter includes the time of sending and an expiration time in the packet after which the receiver should not accept the packet.

2.3.2.4 Defense against Jamming Attacks

- **Transmission power:** A transmitter can use low power to transmit data in the network, making it difficult for the jammer to detect the source of transmission. However, it is better to have a stronger signal power to combat jamming by increasing the SINR (Eq. (4.2)). Therefore, it is important for nodes to be able to vary their power level [83].

- **Frequency Hopping Spread Spectrum (FHSS):** Spread Spectrum (SS) is a modulation technique that spreads the transmitting data across the entire band even though the entire band is not needed to send that data. The spreading of the data beyond the needed limit in the entire band makes the signal resistant to noise, interference and eavesdropping. FHSS is a spread spectrum technique where the transmitting radio rapidly switches between frequency channels. The channel change is done by an algorithm that is shared between both the transmitter and the receiver prior to exchanging data. The channel switching algorithm is kept secret from the jammer [83].

- **Directional Antennas:** Directional antennas transmit and receive data from one direction while omni directional antennas, transmit and receive data from all directions. The use of directional antennas reduces the interference and increases the performance of the network. Directional antennas provide better protection from jamming and eavesdropping. Wireless AHNs use two types of directional antennas: sectored and beamforming antennas or more commonly known as smart antennas [83]. Noubir [89] proposed sectored directional antennas for WSNs. Sectored directional antennas can transmit or receive signals in one particular horizontal direction. The beamforming antennas transmit or receive data in the same direction as the user.
Each user can transmit or receive data from other users in the particular direction of that user by using beamforming antennas.

- **Channel Surfing:** Channel Surfing is similar to FHSS in that both methods evade jamming attacks by quickly changing channels to transmit and receive data between the transmitter and receiver. The difference between the two is that FHSS is on the physical layer and needs special transceivers, whereas channel surfing is a link layer technology and can be applied to wireless nodes. The other difference is that FHSS needs the transmitter and receiver to share an algorithm prior to sending data (as discussed above), and this is not needed in channel surfing [25].

### 2.3.3 Objectives (Performance Metrics)

Some of the objectives or performance metrics used in analyzing wireless networks are presented below.

#### 2.3.3.1 SINR

Signal to Interference plus Noise Ratio (SINR) is the ratio of the power of the signal of interest to the power of all other interfering signals including other nodes in the network, the jammer, and the power of background noise in the channel. The power of a signal (signal of interest, interference from other nodes, and signal from jammer) attenuates in the air with distance. The rate at which electromagnetic waves attenuates in free space is \( \frac{1}{d_{ij}^2} \), where \( d_{ij} \) is the distance from the transmitting node \( i \) to receiving node \( j \). The power of node \( i \) experienced at node \( j \), denoted by \( p_{ij} \), is given by:

\[
p_{ij} = \frac{\lambda}{d_{ij}^2}
\]

where \( \lambda \in \mathcal{R} \) is a proportionality constant; without loss of generality, we can set \( \lambda = 1 \). Now, the SINR in the channel at the receiver node \( D \) is:
\[ \text{SINR} = \frac{p_{TD}}{I_D + \nu} \]  \hspace{1cm} (2.2)

where \( p_{TD} \) is the power of transmitting node \( T \) as experienced at destination node \( D \) and \( I_D \) is the interference from concurrent transmissions of other nodes in the network and the power from the jammer experienced at destination node \( D \); all these powers experience path equation given by Eq. (4.1) and \( \nu \) is the background noise in the channel. The higher the SINR value the better the quality of the data being transferred and vice-versa. The jammer tries to increase the interference power to decrease the SINR and thereby achieve its goal of disrupting the network. There could also be some selfish nodes in the network other than the jammer that try to decrease the SINR by increasing their power of concurrent transmission.

2.3.3.2 Packet Send Ratio (PSR)

PSR is defined as the ratio between the number of packets that are successfully sent by a legitimate transmission node \( T \) and the number of packets it intended to send [136]. If the transmission node intended to send \( n \) packets and the receiving node \( D \) receives only \( m \) (\( m \leq n \)) packets, then the PSR is given as:

\[ PSR = \frac{m}{n} = \frac{\text{Packets sent}}{\text{Packets intended to be sent}} \]

This packet loss is often due to jamming interference. Before transmitting any data node \( T \) senses the channel to be busy, i.e., the channel is already in use, because of the presence
of a jamming signal. This busy channel leads the backlog at node $T$’s processing queue to fill up, blocking all incoming packets, and eventually discarding packets in the queue.

### 2.3.3.3 Packet Delivery Ratio (PDR)

The Packet Delivery Ratio (PDR) metric is the ratio of the number of packets that pass the CRC (Cyclic Redundancy Codes) check to the number of packets received by the receiver. CRC is an error-detecting technique used mainly in computer networks. This method finds the error between the data that is received and the data that is supposed to be received. Suppose receiving node $D$ receives $n$ packets and from that only $q$ packets pass the CRC check; then the PDR is given by the following

$$\text{PDR} = \frac{q}{n} = \frac{\text{Packets that pass the CRC check}}{\text{Packets Received}}$$

In the presence of a jammer the data packets received will not pass the CRC, thereby reducing the PDR. While PSR captures the effectiveness of jamming at the transmitter, PDR measures the effectiveness at the receiver. Note that if no packets are received, i.e., $n = 0$ the PDR is defined to be zero [92, 136].

### 2.3.3.4 Connectivity Index

In wireless AHNs the presence of a jammer can disrupt the routes between the nodes in the network, thereby reducing the connectivity. If there is at least one path between any two nodes of a graph, then the graph is said to be a connected graph [89]. The connectivity index metric was first introduced by Noubir [89] to study the effect of jamming on the connectivity of AHNs. Noubir [89] starts by defining a non-jammed link. Assume $R_n$
is the range of communication between the nodes in the network, $JS$ is the set of all the jammers, and $R_J$ is the range of jammers. A link between nodes $T$ and $D$ is said to be non-jammed if and only if the following expression holds [89]:

$$(d_{TD} < R_n) \land (d_{JD} > R_J) \quad \forall J \in JS$$

(2.3)

where $d_{TD}$ and $d_{JD}$ represents the Euclidean distance between nodes $T$ and $D$ and distance between jammer $J$ and node $D$. Further, let $G = (V, E)$ be the directed connectivity graph representing the multi-hop ad hoc network after removing all jammed links. Let $G' = (V, E')$ be the transitive closure of $G$. The transitive closure $E'$ contains all the node pairs in the graph that have a connection between them [92]. The connectivity index of $G$ is defined as:

$$\text{Connectivity Index} = \frac{|E'|}{\frac{|V|(|V| - 1)}{2}}$$

(2.4)

So, the connectivity index is nothing but the ratio between such pair of nodes that have a connection between them to the number of all possible pairs of nodes in the network. We can see that a connected graph has a connectivity index of 1, while a graph partitioned in two connected sub-graphs of equal size, has a connectivity index of 0.5 [92].

### 2.3.3.5 Throughput

In computer networks throughput is defined as the average rate of successful message delivery in a network over a communication channel. The throughput of a communication channel is given by the Shannon’s rate [38]:
where \( C \) is the channel capacity or maximum theoretical throughput measured in bits/sec, \( B \) is the bandwidth of the channel in Hertz and SINR is given by Eq. (4.2). The throughput of a channel is affected by the presence of a jammer or selfish node because the SINR is reduced as discussed above.

### 2.3.3.6 Utilization

If the rate of arrival (\( \lambda \)) to and departure (\( \mu \)) from a system both follow a Poisson process then the utilization of the system is given by Little's Law [16]:

\[
\rho = \frac{\lambda}{\mu} \tag{2.6}
\]

Similarly, in wireless networks the utilization is measured as the ratio of the rate of arrival of packets at a node to the packet service rate of that node. The presence of a jammer reduces the utilization of the node and overall network by jamming the channels and increasing the service rate.

### 2.3.4 Constraints

In addition to being susceptible to attacks, the other disadvantage of wireless communications is their power requirements. WSNs and AHNs are used in places where it is hard for humans to be and in military situations where a node failing due to lack of power or energy could prove dangerous. Researchers have fairly recently included power constraints
in their models [108]. Power constraints have also been modeled from the attacker’s point of view [108]. In addition, cost is also an important consideration when designing wireless networks, especially if new technologies are used.

2.3.5 Decision Variables

The following is a non-exhaustive list of decisions that a wireless security optimization model might include.

2.3.5.1 Attacker

- **Select Channel Probabilities:** The jammer is successful in jamming a channel if and only if she chooses the channel on which data is transferred. Sweep jamming [83] is a jamming technique in which the jammer shifts its full power rapidly from one channel to another. This is effective because a jammer can jam multiple channels in quick succession but has a disadvantage of jamming only one channel at a time. It would be better for the jammer to choose a channel which has higher a chance of sending data rather than simply wasting its power on channels with low probability of transmission.

- **Jammer Location:** The location of the jammer is very important, because the magnitude of a jammer’s effect on a node depends on how close the jammer is to that node (see Eq. (4.1)). Commander et al. [31] study the problem of determining the optimal number and placement of jamming devices in order to neutralize communication on the network. This is known as the Wireless Network Jamming Problem (WNJP).

- **Jamming Power Level:** Jammers, like nodes in a wireless network, have restrictions on the amount of power they can use. Using the power wisely is also an important decision that jammers have to take [105]. In a warfare situation, the jammer might not have time to recharge the jamming device without losing critical information or even getting caught.

2.3.5.2 Defender

- **Select Channel Probabilities:** Changing channels to evade jamming attacks is effective [25]. If the channel access probability of the jammer is known the transmitter node can choose channels in such a way that it can minimize jamming. Without
knowing the channel access probability of the jammer, the node may choose channels with equal probability to reduce the maximum damage caused by the jammer [66].

- **Transmission Power Level:** The limitation on the power usage influences the decision of the node in the network [105]. Increasing the power increases the range of transmission (see Eq. (4.1), increasing the SINR (Eq. (4.2)). However, increasing the power reduces the lifetime of the node and also increases the attack probability because the transmitting node is easily detected. A regulated power usage is very important for nodes in wireless networks and is especially important for WSNs and AHNs [83].

- **Network Design:** [17] The network should be designed with the awareness of the fact that there is always going to be someone trying to attack. Metrics should be put in place to detect an attack even before deploying a network. Once the attack is detected, the nodes should be able to take counteractions to protect the data and the network. Cryptographic measures should also be taken to protect against intelligent attacks. While designing a wireless network topology the operator should make sure to locate network nodes in strategic locations where it might not be easy for the jammer to attack.

2.4 Modeling Examples

In this section we provide a few examples of models for each of the wireless networks discussed in Section 2.

2.4.1 WLAN

Sagduyu et al.[106] consider a single channel access point network with one transmitter and one jammer as shown in Figure 2.4. The transmitter is called Node 1 and the jammer is called Node 2. Let $\lambda$ be the arrival rate of packets in the queue at Node 1. Node 2 does not have any messages or queue of its own. Assume that each packet transmission from the transmitter or jammer consumes one unit of energy. The objective of Node 1 is to minimize the average energy cost. The probability of Node 1 transmitting is $p_1$ only if there is a packet in the queue. The transmission is successful if the jammer does not
transmit. If Node 2 transmits in the same time slot as Node 1 the packet is captured by the network (safely kept in memory) with a probability $q$. Assume that Node 2 transmits at a fixed probability $p_2 \in [0, 1]$. The service rate of Node 1’s queue is:

$$
\mu(p_1, p_2) = p_1((1 - p_2) + p_2q)
$$

(2.7)

The transmission of Node 1 is successful if and only if Node 1 transmits and Node 2 does not or the packet is captured with a probability $q$ if Node 2 transmits at the same time. A model for Node 1 is given as

$$
\max_{p_1 \in [0, 1]} \ u(p_1, p_2) = -\frac{\lambda}{\mu(p_1, p_2)} p_1
$$

(2.8)

s.t. $\mu(p_1, p_2) \geq r(\lambda, Q)$

(2.9)

The objective is to minimize the average cost of transmission, given the cost of one transmission is one unit of energy. Eq. (2.9) is the targeted minimum rate constraint and $Q$ is the quality of service parameter. The objective of Node 2, which is to maximize the average energy consumed by Node 1, is given by:

$$
\max_{p_2 \in [0, 1]} \ u(p_1, p_2) = \frac{\lambda}{\mu(p_1, p_2)} p_1
$$

(2.10)

s.t. $p_2 \leq E_2$

(2.11)

where Eq. (2.11) is the average energy constraint and $0 < E_2 < 1$. Sagduyu et al. [106] provide a Nash Equilibrium for the above model.
2.4.2 WSN

Li et al.[66] considered an undirected graph $G = (S, A)$ where $S$ is the set of sensor nodes and $A$ is the set of arcs. Every sensor transmits with a power level $P$ and has a range of transmission $R$. Let $N_i$ be the set of all neighbors of node $i$, and $n_i = |N_i|$. Also $E$ is the total amount of energy at each node. The parameter $\gamma$ is the channel access probability common for all nodes in the network. The transmission from node $i$ to node $j$ is successful only if node $i$ transmits and no other neighboring nodes transmit at the same time. The probability of collision at node $j$ is

$$\theta_0 = 1 - Pr\{\text{at most one neighbors transmit}\} = 1 - (1 - \gamma)^{n_j} - n_j \gamma (1 - \gamma)^{n_j - 1}$$

The jammer has energy level of $E_J$ and the transmission power $P_J$. The jammer also jams the area with a probability $q$ within its transmission range $R_J$. Collision occurs at node $i$ if the jammer jams and at least one neighbor transmits. The probability of a collision at node $i$ is:

$$\theta_1 = 1 - Pr\{\text{no neighbor transmits}\} - Pr\{\text{one neighbor transmits while adversary does not}\}$$

$$= 1 - (1 - \gamma)^{n_i} - (1 - q)^{n_i} \gamma (1 - \gamma)^{n_i - 1}$$
The average number of samples needed for detecting jamming is

\[ D(q, \gamma) = \frac{C}{\theta_1 \log \frac{\theta_1}{\theta_0} + (1 - \theta_1) \log \frac{1 - \theta_1}{1 - \theta_0}}. \quad (2.12) \]

A signal or a warning is sent out from the jammed area in the network to other neighboring nodes outside the jammed area once the jamming attack is detected. The average time needed for this signal to propagate in the network is

\[ W(q, \gamma) = \frac{H}{(1-q)\gamma(1-\gamma)^{\bar{n}-1}}, \quad (2.13) \]

where \( H \) is the number of hops needed for the signal to be delivered outside the area of a jamming attack, and \( \bar{n} \) is the average number of neighbors of a node along the path of the signal. The objective of the jammer is to maximize the total delay of the signal or warning to propagate outside the area under a jamming attack.

\[
\max_{0 < q \leq 1} \quad D(q, \gamma) + W(q, \gamma) \quad (2.14)
\]

s.t. \[ qP_m[D(q, \gamma) + W(q, \gamma)] \leq E_m, \quad (2.15) \]

\[ U_m C(q, \gamma) \geq U_m^0, \quad (2.16) \]

where Eq. (2.15) is the energy constraint and \( U_m C(q, \gamma) \) and \( U_m^0 \) are the cumulative and the minimum payoff for the jammer for corrupting the communication. The objective of the network is to minimize the total delay for the signal to propagate outside the jammed area, which is formulated as follows:
\[
\max_{0 \leq \gamma \leq 1} \quad D(q, \gamma) + W(q, \gamma) \\
\text{s.t.} \quad \gamma P[D(q, \gamma) + W(q, \gamma)] \leq E, \\
U_C(q, \gamma) \geq U^0,
\]

where Eq. (2.18) is the energy constraint and \( U_C(q, \gamma) \) and \( U^0 \) are the cumulative and the minimum payoff for the network for avoiding the attack. Li et al. [66] numerically evaluate the optimization model shown above. They also numerically evaluate the problem as a min – max problem, assuming that there is no information sharing between the jammer and the attacker about each other’s strategy.

### 2.4.3 Ad Hoc

Hanawal et al. [44] consider a mobile ad hoc network (MANET) model called the Poisson bipolar model. Each transmitter node in the network (Operator) has a particular receiver node and the transmitter node has an infinite amount of packets to send. Nodes in the network are scattered in a Euclidean space according to a homogeneous Poisson point process (HPPP) of intensity \( \lambda_1 \). A jammer also has jamming nodes scattered in a Euclidean space according to a homogeneous Poisson point process of intensity \( \lambda_2 \). The probability that a node transmits is \( q_1 \) and the transmitters of the nodes form a Poisson process process of intensity \( q_1 \lambda_1 \). Let \( P_1 \) and \( P_2 \) be the fixed power of transmission of the nodes and the jammer respectively. The transmitters of the jammer form a Poisson point process of intensity \( q_2 \lambda_2 \), where \( q_2 \) is the probability that the jammer transmits. Thus, a typical node is exposed to interference from the other nodes according to a Poisson point
process of intensity $q_1\lambda_1 + q_2\lambda_2$. The average density of power dissipated among the nodes of the Operator is $q_1\lambda_1 P_1$. Further, let the cost of transmission of an Operator node be $\rho_1$. Similarly, the average energy dissipated among the nodes of the jammer is $q_2\lambda_2 P_2$ and the cost of transmission is $\rho_2$. The strategy of the Operator nodes is to choose $q_1 \in [0,1]$ with which each of the nodes can access the channel. The strategy of the jammer is to choose $q_2 \in [0,1]$ such that the transmission of the jammer is turned ON at the same time slot as the nodes. The utility function of the nodes in the network is the density of successful transmission considering the average cost of transmission among the nodes:

$$U_1(q_1, q_2) = \delta(q_1, q_2) - \rho_1 q_1 \lambda_1 P_1$$  \hspace{1cm} (2.20)

The utility function of the jammer is to minimize the density of successful transmission of the Operator nodes considering the average cost of transmission:

$$U_2(q_1, q_2) = -\delta(q_1, q_2) - \rho_2 q_2 \lambda_2 P_2,$$  \hspace{1cm} (2.21)

where $\delta(q_1, q_2)$ is the density of successful transmission of the Operator nodes:

$$\delta(q_1, q_2) = \lambda_1 q_1 p_s(q_1, q_2)$$  \hspace{1cm} (2.22)

The objective of the Operator nodes in the network is to choose $q_1^*$, such that the density of successful transmission is maximized; thus

$$q_1^* \in \arg\max_{q_1 \in [0,1]} U_1(q_1, q_2)$$  \hspace{1cm} (2.23)
The objective of the jammer is to choose $q_2^*$, such that the density of successful transmission of the nodes is minimized; thus

$$q_2^* \in \arg\max_{q_2 \in [0,1]} U_2(q_1, q_2). \quad (2.24)$$

Hanawal and Altman [44] solve the above problem as a zero-sum game, finding a Nash Equilibrium solution.

2.5 Conclusion

The goal of this paper is to help the operations research community become acquainted with wireless network security, an important area of research. Toward this end, we described the basics of wireless networks as well as the most common attack and defense strategies. As an aid to the optimization modeler who is not familiar with wireless network security, we discussed the important components of an optimization model for wireless network security. Finally, we described a modeling example for each type of network.

For future research new global metrics should be developed to measure the performance of the network as a whole. Global metrics are measured at the network level. The performance metrics discussed in Section 2.2 with the exception of throughput which is a global metric, are local metrics, i.e., they are measured at the node level of the network. Another extension to this work could be a more comprehensive survey.
CHAPTER 3
JAMMING ATTACKS ON WIRELESS NETWORKS: A TAXONOMIC SURVEY

3.1 Introduction
3.1.1 Introduction to wireless networks

Wireless networks refers to computer networks where communication between two devices like laptops is done without the use of cables or wires. The most widely used wireless network is the wireless local area network (WLAN), more commonly known as Wi-Fi. WLAN is available in homes, schools, offices, coffee shops, etc., which allows for easy access to the Internet whenever needed, as long as the device can connect to the Wi-Fi signal. The computers connect to an access point (AP) through wireless means to connect to the Internet and allow the users to move freely within the range of the Wi-Fi signal. Figure 3.1 shows an example of a WLAN with one AP and six computers that communicate with the AP via a wireless medium. Another type of wireless network, used mostly in the military and disaster situations, is the wireless ad hoc network (AHN). The network is called ad hoc because it does not need any pre-existing infrastructure, like cables or access points. Here, each node, e.g. laptop, cellphones, participates in the networks routing of data by forwarding it from one node to another without any centralized management equipment like an AP. The nodes in an AHN dynamically decide which node to send the data to depending on network connectivity. Figure 3.2 shows a basic setup of
an AHN between laptops and phones that communicate among themselves without an AP.

Some of the most important application [103, 145] of AHNs are:

- Military units, such as soldiers, tanks, and ships can communicate even in the absence of well defined wireless infrastructure by forming an AHN.
- AHNs can also be used for emergency, law enforcement, and rescue missions.
- AHNs are also used in conferences, lectures, meetings, and other commercial areas where the network loads can be very high.

Another type of wireless network is the Wireless Sensor Network (WSN), which is a collection of a large number of individual autonomous nodes that share information among themselves. In a WSN the data collected is not directly sent to the user, rather, it is first aggregated and then sent [97]. A WSN consists of a gateway or base station, that connects the sensor nodes to other sensor networks, or to the end user (See Figure 3.3). The data at the sensor nodes is compressed and transmitted to the base station, which presents the results to the end user [119]. The data packets are sometimes sent to the destination via several intermediate nodes. This transmission by hopping from one node to another is called multi-hop. Figure 3.3 shows a WSN with a sensing area gathering information that is transmitted among the sensors, and the final result of all the data is sent to the base station to forward the data to the end user. One application of WSN is environment and habitat monitoring.

Even though wireless networks are easy to use, they have been exposed to security threats, because use of air as a medium to transmit data has made wireless networks susceptible to jamming attacks. A jamming attack is the transmission of radio signals that disrupt communications by decreasing the Signal-to-Inference-plus-Noise ratio (SINR) [15].
SINR is the ratio of the signal power to the sum of the interference power from other interfering signals and noise power. A ratio greater than 1 indicates the desirable state of more signal than noise. A jamming device, tuned to the same frequency as the opponent’s receiving equipment and with the same type of modulation, can, with enough power, override any signal at the receiver. Wireless signal jamming devices are most often used to interfere with wireless networks, a type of denial of service (DoS) attack. DoS attacks deny legitimate users sending data because of the illegitimate users presence. Advanced and more expensive jamming devices may jam satellite communications. A wireless signal jamming device can be used to stop transmission temporarily and short out or turn off the power of device or units like radios, televisions, microwaves, or any unit that receives electrical signals to operate.
The internal function of a wireless communication system is divided into the following abstract layers, each having a specific function. The abstract layers are:

1. **Physical Layer** [83, 125]: The transmission and reception of data via a physical connection like cables, fibers, wires, or air among devices on the network is managed by the physical layer; in wireless networks, the binary data among computers is translated into electrical signals and uses radio frequency to send and receive data. Radio jamming attacks can impact the physical layer.

2. **Data Link Layer** [83, 125]: Responsible for segmenting the data packets sent by the network layer to frames that can be sent by the physical layer and is responsible for communication between the network layer and the physical layer. The formatting of frames of data sent and error checking are the additional responsibilities of this layer. A sublayer which is a part of the data link layer and is responsible for moving data packets to and from one node to another across a shared channel is the Medium Access Control (MAC) layer. A channel in a wireless network is the frequency at which nodes send their data. Another, responsibility of the MAC sublayer is to ensure that the signal sent from different nodes across the same channel do not collide. This layer is susceptible to much more sophisticated jamming and energy efficient jamming than physical layer jamming attacks.
3. **Network Layer**: Links between the transportation layer and the data link layer and also responsible for figuring out the network topology, assigning address, and routing the data.

4. **Transportation Layer**: Responsible for reliable data transfer and recovers any lost data, retransmits data, and provides data encryption.

5. **Application Layer**: Defines the specifications of the data requested by the end user in the network.

Five abstract layers mentioned above are arranged in a hierarchy starting from the physical layer at the bottom to the application layer on top. Data packets are sometimes sent to the destination via several intermediate nodes. Mesh networking is a type of network topology where each node must not only capture and disseminate its own data, but also serve as a relay for other nodes and collaborate to propagate the data in the network. A wireless mesh network is a communications network made up of radio nodes in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh routers, and gateways. The mesh clients are often laptops, cellphones and other wireless devices, and the mesh routers forward traffic to and from the gateways which may, but do not need to, connect to the Internet.

### 3.1.2 Definition of game theory

Jamming attacks on wireless networks have been widely studied by researchers, and different solution approaches have been proposed for this attack. Of the methods proposed to solve the jamming problem, game theoretical approaches are increasingly being used by researchers. Game theory is a study of strategic decision making, or “the study of mathematical models of conflict and cooperation between intelligent rational decision-makers”
To be fully defined, a game must specify the following elements: the players of the game, the information and actions available to each player at each decision point, and the payoffs for each outcome. A game theorist typically uses these elements, along with a choice solution concept, to deduce a set of equilibrium strategies for each player such that, when these strategies are employed, no player can profit by unilaterally deviating from their strategy, the Nash equilibrium. Different varieties of games include the non-zero-sum game, zero-sum game, cooperative and non-cooperative games. Among these, researchers have widely applied zero-sum games to the jamming problem. A zero-sum game is a mathematical representation of a situation in which a participant’s gain, or loss, of utility is exactly balanced by the losses, or gains, of the utility of the other participant(s). If the total gains of the participants are added up and the total losses subtracted, the sum will be zero. In the literature there are many studies in finding the Nash equilibrium for a jamming game between the attacker and defender with each trying to increase and decrease the throughput.
respectively, but researchers have previously concentrated on single channel networks with only one communication frequency among network nodes.

### 3.1.3 Related literature and motivation

This section briefly discusses some of the survey papers available in the jamming attack literature. Pelechrinis et al. [92] survey different DoS jamming attacks papers. They discuss intelligent jamming attacks with different objectives, such as jamming gain, targeted jamming, and reduced probability of detection. They also discuss jamming efficiency metrics like packet delivery ratio, packet send ratio, and connectivity index. Young et al. [139] present the different papers that deal with different types of jammers like constant jammers, random jammers etc., and they compare the adversarial models presented. A survey on different game theoretic classification of the problems on network security as a whole is presented in[101]. They provide a taxonomy for classifying the different game theoretic approaches listed in the literature. [83] provide a survey on the different attack countermeasure strategies for WSNs in literature. Along with presenting the different papers in the literature, they also provide a taxonomy to distinguish the countermeasure schemes. The taxonomy divides the different countermeasures as (i) detection techniques, (ii) proactive countermeasures, (iii) reactive countermeasures, and (iv) mobile agent countermeasures. These survey papers are restricted to one type of wireless network or give a general overview of the all the types of attack and defense strategies, but they do not provide a clear picture of the types of attacks and the defense strategies employed.
To the best of our knowledge, [31] is the only study in the operations research (OR) literature that examines physically placing a jamming device in a strategic location to cause maximum damage. The authors solve for the jamming device placement but do not try to find the best \((X, Y)\) coordinates, rather, they choose from a set of available discrete locations of the jamming device and assume that a jamming device can jam all the channels between two nodes. Increased usage of wireless networks and their applications in military and critical time-sensitive environments has led researchers to find ways to make the wireless networks more reliable. Jamming attacks have gained more attention from researchers than other types of attacks.

Figure 3.4 shows an increase in the number of papers published in the literature in the years 2010-2014. However, there are only a few papers that survey the literature available on jamming attacks. For instance [139] and [92] each develop a survey on different types
of jamming attacks, methods to detect jamming attacks, and mechanisms to protect against attacks; also, [62] survey selective jamming along with detection and protection. This survey complements the previous surveys by categorizing different jamming attacks and solution methodologies based on the network type (WLAN, AHN, WSN).

3.1.4 Contribution

The major contribution of this work is to provide a classification scheme for the literature by identifying the different jamming attacks launched by the jammer, different defense, detection and prevention techniques against the jamming attacks and classifying them by the type of wireless networks they mainly affect and the defense against such attacks. After establishing the types of attacks classified by the type of network, the different attack strategies, defense strategies, detection and prevention strategies, and game theoretic strategies described in the literature are surveyed. An analysis of the gaps in the jamming attack literature is provided to better understand the importance of filling the gaps. A goal of this paper is to give the OR community a better understanding of the existing research in wireless network jamming and areas where it can contribute to finding better jamming attacks and ways to defend against jamming attacks. This survey also identifies new areas of research in jamming attacks for the OR community.

The rest of the paper is organized as follows: Section 3.2 provides the classification scheme for the survey, Section 3.3 provides a simple example of the jamming problem in wireless networks, Section 3.4.1 discusses the literature available for WLANs. Section 3.4.2 describes the literature available for WSNs. Section 3.4.3 describes the literature
available for AHNs. Finally, Section 3.5 discusses gaps in the literature and suggests areas for future research, and Section 3.6 concludes the paper.

3.2 Boundaries of study and classification scheme

3.2.1 Boundaries of study

The keywords used to search papers include ”jamming”, ”anti-jamming”, ”wireless networks”, and ”game theory”. These keywords were listed in the title, abstract, or body of text of journal articles or conference proceedings published in English. The data bases included in our search were Science Direct, Springer, IEEE libraries, and ACM libraries. We limited the time period of the search to 1980 forward because the first instance of jamming was explored in the literature in 1982.

3.2.2 Classification scheme

We provide a classification method for a one-stop easy reference for the jamming research available so far. Tables 3.1 - 3.3 show the classification schema provided in this paper. There are four major columns: Papers, Types of Network, Problem Perspective, and Methodology. Papers classifies and groups the papers published by year, with all the papers that fit the search criteria from 1980 to June 2014. Types of network further divides into the three wireless network types considered in this work, and each of these network types are further divided into single channel and multichannel networks. Problem Perspective further divides into Attacker, Defender, Both, and Game Theory. For example, a paper discussing a new set of jamming attacks would be classified as Attacker, and a new anti-jamming or defense mechanism would be Defender. Some authors solve both
the attacker and defender problem using game theory; these papers are classified as *Both*. The papers that propose a game theoretic approach are classified as *Game Theory*. *Game Theory* further divides into *Non-Cooperative, Bayesian, Stackelberg, and Other* depending on the type of game studied. The fourth major column in the classification is the *Methodology*, and this column further divides into *Protocol Design/Algorithm* and *Mathematical Programming Model*. The papers that provide a protocol design and/or an algorithmic approach are categorized under the column *Protocol Design/Algorithm*, and the papers providing a mathematical programming model come under the *Mathematical Programming Model* column. The x’s in the above described columns are the categories each of the papers on the left fall into.
<table>
<thead>
<tr>
<th>Papers</th>
<th>Types of network</th>
<th>Problem Perspective</th>
<th>Methodology</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>WLAN</td>
<td>WSN</td>
<td>AHN</td>
</tr>
<tr>
<td></td>
<td>Single Channel</td>
<td>Multi Channel</td>
<td>Single Channel</td>
</tr>
<tr>
<td>2010-2014</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[122]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[138]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[124]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[74]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[65]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[142]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[70]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[76]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[106]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[107]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[39]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[125]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[137]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[69]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[29]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[120]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[140]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[34]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[74]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[44]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[100]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[64]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[54]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>2007-2009</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[31]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[77]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[108]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[105]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>[109]</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
Table 3.2

Classification scheme

<table>
<thead>
<tr>
<th>Papers</th>
<th>Types of network</th>
<th>Problem Perspective</th>
<th>Methodology</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>WLAN</td>
<td>WSN</td>
<td>AHN</td>
</tr>
<tr>
<td></td>
<td>Single Channel</td>
<td>Multi Channel</td>
<td>Single Channel</td>
</tr>
<tr>
<td>[5]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[93]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[115]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[135]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[47]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[144]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[22]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[53]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[63]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[52]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[57]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[86]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[3]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[23]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[134]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[26]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[130]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[36]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[132]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[72]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[131]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[114]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>2004-2006</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[104]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[73]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[51]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[111]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[4]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[89]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[61]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
Table 3.3

Classification scheme

<table>
<thead>
<tr>
<th>Papers</th>
<th>Type of network</th>
<th>Problem Perspective</th>
<th>Methodology</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>WLAN</td>
<td>WSN</td>
<td>AHN</td>
</tr>
<tr>
<td></td>
<td>Single Channel</td>
<td>Single Channel</td>
<td>Multi Channel</td>
</tr>
<tr>
<td>[136]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[20]</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[133]</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[91]</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[118]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>[116]</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

2000-2003

| [2]   | x              | x                   | x           | x           |
| [128] |                | x                   | x           | x           |
| [85]  | x              | x                   | x           | x           |
| [79]  | x              | x                   | x           | x           |
| [129] |                | x                   | x           | x           |

1980-1999

| [95]  | x              | x                   | x           | x           |
| [81]  | x              | x                   | x           | x           |
| [140] | x              | x                   | x           | x           |
3.3 Example of wireless network jamming problem

Military strategists are always looking for better ways to improve their force’s effectiveness while reducing the number of causalities. In any adversarial situation, the attacker aims to neutralize the military’s communications. The military would like to make sure it can maintain communication by working around the adversaries’ attempts to neutralize communication. In a war situation, as it is not possible to have infrastructure for communication, the military needs to setup an AHN. In a wireless AHN, each node transmits data using one channel from a number of available channels. The jamming device seeks to choose a location such that, by choosing the same channel nodes are using, the data is not transmitted successfully. The main aim of the jamming device is to ensure that the nodes cannot use the network, and on the other hand nodes try to maximize the usage of the network. Both the jamming device and the node are playing a game. Think of it as a two player game, and the players are attacker/terrorist and defender/military. Figure 3.5 shows the network consisting of six nodes (n1-n6) and one jamming device (j1). Three communication channels of different frequencies, continuous, dotted, and dashed line, exist between each node. A channel is not a physical cable or connection, but a frequency at which the nodes communicate through air. Figure 3.5, assumes that nodes 5 and 6 are communicating using the 2.41 GHz (dotted) frequency channel.

The attacker chooses its location and chooses a frequency; in this case, it chooses 2.41 GHz (dotted), which is the same as the nodes. The communication channel between nodes 5 and 6 is in the radius of the jamming device’s power range. Since the jammer
chose a location with the available power and a frequency on which node 5 and 6 were communicating, the jamming is successful.

Figure 3.5
Example of jamming in a network

In the sections below we introduce the readers to some of most commonly used attack and defense strategies studied in literature. These lists of attack and defense strategies will help reader understand the 3.4 section better, as most of the papers discussed in this section use one more of these attack and defense strategies.

3.3.1 Types of jamming strategies

There are four types of jamming strategies most commonly studied in literature. In this section, we briefly discuss these different jamming strategies [83, 92, 125, 136]:

- **Constant Jammer**: Constant jammers continuously emit electromagnetic waves or radio signals or random sequence of bits that interfere with the legitimate transmission of the network. In the presence of a constant jammer the transmission channel of the legitimate network appears busy therefore disallowing legitimate transmission. The disadvantage of constant jammer is that, the continuous emission of signals drains the energy fast and require high amount of power.
Deceptive Jammer: Deceptive jammer like the constant jammer emits signals continuously, but unlike constant jammers does not emit random bit sequence, but emits a legitimate bit sequence which gives the network an impression of presence of a legitimate node. This impersonation makes deceptive jammers more effective than constant jammers.

Random Jammer: Unlike constant and deceptive jammers random jammer conserves energy by alternating between random jamming sleep states. Random jammers do not use energy in the sleep state therefore, reducing power consumption.

Reactive Jammer: Reactive jammers like the random jammers conserve power by not emitting signals continuously. Reactive jammers listen to the transmission channel and react by emitting signals in the presence of data transfer. The amount of power required to listen to a channel is much less compared to the power required for jamming.

3.3.2 Types of defense against jamming attacks

In this section we briefly describe some of the most common defense strategies against jamming attacks found in literature.

Transmission power: The use of low transmission power can be a defense strategy against jamming attacks in that, with the use of low transmission power makes it difficult for the jamming devices to detect legitimate transmission. However, use of low power can undesirably decrease SINR. It is important for the nodes in the network to vary their transmission power.

Frequency Hopping Spread Spectrum (FHSS): Spread Spectrum (SS) a modulation technique spreads data across the entire band of the transmission channel although the entire band of the transmission channel is not required. This spreading of data in the entire channel band ensures that the transmitted signal is resistant to interference. FHSS a spread spectrum technique evades jamming by rapidly switching between different transmission channel frequencies. The channel switching algorithm is shared between the sender and receiver prior to the actual data transmission. This technique works as long as the shared algorithm is kept secret from the attacker.

Directional Antennas: Jamming attacks can be evaded by using directional antennas. Directional antennas can transmit and receive data only in one direction unlike traditional omni directional antennas which can transmit and receive data from all directions, making omni directional antennas an easy target for the jammers. But, with directional antennas, the jammer has to be placed in the same direction of the directional antenna for it to successfully jam the signal.
• **Channel Surfing:** Channel surfing like FHSS evades jamming by quickly switching between channels. But, the difference between the two is that, FHSS, unlike, channel surfing requires specialized antennas for transmitting and receiving signals. The major difference between the two is that in channel surfing sharing of a secret algorithm between the sender and receiver is not required.

### 3.4 Discussion of literature

The first knowledge of jamming attack dates back to when it was used against military radios. The first countries to engage in jamming were Germany and Russia. The first time jamming attacks were used during a war situation was during World War II, when radio operators misled pilots by feeding them false instructions in their own language. The operators who started such an attack were known by the code name Raven, which was soon changed to Crow. During World War II radars were jammed, which was considered an invention at that time. Jamming attacks on foreign radio broadcasts stations were more common during tense international relations and wars, and they prevented listening to the radio transmission of enemy countries. The jamming of foreign radio signals could be avoided by changing the transmission frequency or by the power of transmission [83].

When jamming attacks were used for the first time, a new technology SS (discussed above) was invented by the military to cope.

SS received attention from early researchers after World War II. Although jamming attacks were popular during the war, the word “jamming” was used for the first time by [11] in 1982 in “Robust linear coding in continuous-time communication systems in the presence of jamming and with noisy side information at the decoder.” The authors in [95] study dynamic jamming in 1988. The authors study the throughput/delay performance of
the Slotted Aloha type network under dynamic jamming. They use Markovian decision model to find the optimal decision rules for the jamming device. The authors assume that the jamming is the ON-OFF type and has a finite amount of power. [141] provide uses and application of SS, and the authors in [1] analyze SS technology. [81] develops an information-theoretic approach. The authors in [140] study the multi-hop packet radio networks in the presence of active interference. They also consider power constraints for both the jamming device and the network nodes. The authors formulate the problem as a two player constant sum game.

The jamming problem has been studied widely in many wireless network settings, including wireless LAN networks [12, 41, 59], sensor networks [20, 66, 136], and multi-hop networks [115, 140]. Other general wireless networks have also received attention [6, 9, 21, 51, 79, 108]. Researchers assume the location of a jamming device and the effect of the locating a jamming device to solve the problem. But in [31] the authors solve the jamming device location problem, but they assume the effect a jamming device has on the wireless network to decide the location of the jamming device. The readers are recommended to read the tutorial by [120] to better understand jamming attacks and their defense mechanism available in literature.

3.4.1 Wireless Local Area Network (WLAN)

3.4.1.1 Single Channel

In this section, we further classify the literature as below:

A. Attack Strategies: Thuente et.al [117] show that normal jamming attacks, where the attacker constantly or periodically emits signals to jam the network, are inefficient in terms
of energy consumption, and introduce intelligent jamming attacks that enables the jamming attacker to corrupt the Clear To Send (CTS), Request To Send (RTS), and Acknowledge (ACK) packets. [116] extend their work in [117] to propose another intelligent attacking strategy called the fake RTS jamming attack. They also propose countermeasures to prevent such attacks as well as methods to overcome the proposed countermeasures. [126] develop a software-based reactive jamming attack and show that reactive jamming should be considered a real threat, and new defense mechanisms must be developed to cope with such attacks. The jamming attack as a DoS attack in wireless communication is discussed by [80]. The authors classify jamming attacks as client jamming or base station jamming. In client jamming, a mischievous client takes over and impersonates the legitimate client. The mischievous client can even jam the network so that the legitimate client cannot use the network. In base station jamming attacks the jamming device impersonates the legitimate base station or deprives the client of service. [95] study the throughput/delay performance of the Slotted Aloha type network under dynamic jamming using a Markovian decision model to find the optimal decision rules for the jamming device. The authors assume that the jamming is the ON-OFF type and has a finite amount of power. An information-theoretic approach is developed in [81]. Finally, jamming attack, is studied from the attackers and defenders point of view in [136] and provide four different models and show the problems associated with an effective attack. Then, they provide different measures that help the network to detect the attack. The authors find that signal strength and carrier sensing time are not enough to determine whether a poor connection is due to
jamming or because of the mobility of the nodes. They also determine which measures give a better understanding about the poor quality of network’s connection.

**B. Detection and Prevention Strategies:** [136] introduce two methods of detecting jamming attack: 1) Packet Send Ratio (PSR) and 2) Packet Delivery Ratio (PDR). PSR is the ratio of the number of packet sent to the number of packets intended to be sent. If the number of packet sent is less than the number of packets intended to send can indicate the presence of a jammer. PDR is the ratio of the number of received packets that pass the for completeness of data to the number of packets actually received. If only a few of the received packets pass the completeness check can indicate the presence of a jammer. These PSR and PDR methods of detecting jamming attacks opened new gates for research on jamming attacks. [125] combine some of the existing approaches such as PSR and PDR to detect jamming attacks and measure the PSR and PDR to evaluate the accuracy of their approach. The authors use a ns-2 simulation platform and the results obtained confirm that the approach of combining existing jamming detection approaches increases the accuracy of detecting jamming attacks.

**C. Defense Strategies:** [100] propose a local medium access control protocol called, JADE, that can protect a multi-hop wireless network with a single channel against an adaptive jamming device which can adapt its attack for its benefit. Here, the authors model the interference and transmission as a unit disk graph. The jamming strategies change from node to node and, hence, make it difficult to defend. The results of this work shows that JADE achieves an asymptotically optimal throughput. An anti-jamming strategy based on creating a timing channel: an extra channel overlaying the already existing physical and
link layer channel, between users of a network in the presence of jamming attack, is de-
veloped by [135], [95], [81], and [136] is discussed in 3.4.1.1. [27] discuss a binary key
tree and a dynamic tree-remerging method to evade broadcast jamming attacks. Finally,
[132] studies the issues associated with controlling the transmission power for improving
the successful transmission of data under a jamming attack.

D. Game Theoretic Strategies: [24] provide a game theoretic framework for the jam-
mimg attacks in wireless networks. The authors provide a defense strategy to fight the
jamming device actively by draining the jamming device of energy. The authors also show
that their strategy eliminates undesired equilibrium and increased the energy consumption
at the jamming device without negatively affecting the performance of the network. [69]
propose a dynamic jamming attack in which the attacker dynamically adjusts the jamming
period, to increase the attacker’s utility. The authors provide a method where the network
will change the re-transmission mechanism to defend against the jamming attacks. The
authors modeled the problem as a Stackelberg game and derive the Nash equilibrium.

[107] deal with jamming games in the MAC layer of the wireless network. They as-
sume that each of the nodes in that network knows only its type, i.e., a selfish user type or
a malicious user type that tries to jam the communication channel. The authors model the
jamming game as a multi-stage two-player Bayesian game. The action set of the node is a
set of transmission probabilities to choose from at random. The utility function of a selfish
user is the difference of its reward function, which is an increasing function of the SINR,
and the energy cost function, which is an increasing function of the node’s own power. The
utility function of a malicious node is the difference of its reward function and its energy
cost function. The reward function of the malicious user is the opposite of the function of the other user if that user is a selfish user, and zero if the other user is a malicious node.

The authors also consider the Bayesian Nash equilibrium as the expected strategies of the nodes. [105] present a game-theoretic model for the jamming problem at the MAC layer of the wireless network. They present different models based on power control and random access. They also derive the Nash equilibrium strategies depending on the degree of the type of uncertainty. Throughput rewards, transmission energy cost, and malicious attack incentives are used as performance measures. Random access games are studied in [108], and the jamming device and transmitter balance the throughput rewards and energy cost. [109] and [5] introduced different energy objectives based on power control with different utility functions, depending on throughput rewards and energy costs. [104] explore the effects of dynamic traffic on jamming attacks in a power controlled MAC, i.e., each transmitter chooses its power to transmit. MAC channels with two users in the presence of a jamming device is studied by [111].

The effects of random channels were studied in [8] for jamming games based on the throughput rewards and energy costs. [39] discuss the impacts of incomplete information related to fading channel gains on transmission parameters. For the purpose of solving this problem, the authors consider the Orthogonal Frequency Division Multiplexing (OFDM) network with transmitters and jamming devices. A Bayesian approach is presented by the authors and SINR is the metric used to optimize the problem. The authors show that incomplete information about the jamming device channel gains leads to utilization of same channels by different jamming devices under the equilibrium condition. The study also
shows that, under the equilibrium conditions, incomplete information about the transmitter leads to users sharing channels. The authors provide a closed form expression for the equilibrium. [7] studies how the increase in the number of jamming devices impacts the transmission game. The objective function of the node they consider is the SINR. The authors also analyze a zero-sum game scenario and an optimization scenario to show that the jamming device equalizes the quality of the best sub carrier.

[77] model jamming attacks as a gambler, and a new performance metric message invalidation ratio is introduced for time critical traffic networks. A two player game theoretic framework for an adaptive jamming attack and anti-jamming defense is modeled by [34],[140] study multi-hop packet radio networks in the presence of active interference. They also consider power constraints for both the jamming device and the network nodes, and the authors formulate the problem as a two player constant sum game. Multi-hop networks with packet forwarding are studied in [115]. From a game theoretic perspective of jamming in wireless networks, the transmission strategies may also include randomized power selection; see [79].

The jamming problem that [4] study is an intrusion detection problem. [106] discussed in Section 3.4.1.2 study both single channel and multichannel WLANs.

A total of 31 papers provided in this study classified as WLAN single channel are discussed in this section; including 7 papers classified as Attack Strategies, 2 papers as Detection and Prevention Strategies, 7 papers as Defense Strategies, and 19 papers as Game Theoretic Strategies.
3.4.1.2 Multichannel

In this section, we further classify the literature as below:

A. Attack Strategies: Among other papers in WLAN multichannel networks, to the best of our knowledge only [114] and [54] study jamming problem from an attackers perspective. [114] were the first to introduce the problem of flow-jamming attack and model flow-jamming attacks as a linear programming model. [54] provide stochastic search algorithms like iterative improvement, simulated annealing, and genetic algorithm and provide a stochastic optimization approach for flow-jamming attacks in multichannel wireless networks.

B. Detection and Prevention Strategies: To the best of our knowledge, there are no papers in literature within the scope of this survey that deal with detection and prevention strategies for multichannel WLAN.

C. Defense Strategies: [74] propose a two-slot cooperative relay scheme to maximize the secrecy rate in a one source, one destination, on eavesdropper, and multiple decode-and-forward relays wireless network. In the first slot the source and destination work together to jam the eavesdropper. In the second slot one optimally selected node transmits the signal from the source and cooperates with the source to jam the eavesdropper without causing interference at the destination. [37] consider cooperative jamming in a multiple antenna scenario as well as methods to maximize the system’s secrecy subject to a transmission power constraint. Reactive and proactive channel hopping techniques to evade jamming are studied in [52]. [86] study channel hopping in 802.11 networks. [23] discuss the jamming of broadcast control channels in the presence not only in external jamming
attacks, but also in relation to an internal traitor who has information about the channels in the network. [26] discuss a binary code tree technique which works with any SS communication technology. [53] introduce the problem of maximizing network goodput under jamming attacks through a combination of channel hopping and error correction coding. The gossip problem considered as jamming problems in wireless multichannel networks is presented by [36], and a deterministic algorithm based on Turan’s theorem is developed.

D. Game Theoretic Strategies: [106] explore a non-cooperative game between a jamming device and a transmitter in which both choose their transmission probabilities to access the collision channels with random packet capture. They consider random errors in the queue state for the jamming device and add a channel sensing capability to the jamming device. They provide the Nash Equilibrium with packet delay and energy constraints. The authors extend the game to multiple transmitters, jamming devices, sub-channels, and channel access points. A non-cooperative game theoretic game is proposed for Multiple Input Multiple Output (MIMO) fading channels in [51]. [93] explore a system with multiple channels, where the interactions of the transmitter and jamming device are formulated as game transmitting randomly over multiple channels. SPREAD, a multilayer mechanism hopping technique discussed in [72] based on using the frequency hopping technique for preventing jamming as a DoS attack. [72] formulate SPREAD as a non-cooperative game. Finally, a multi-path routing game-theoretic framework to evade jamming attack is proposed in [131].

A total of 14 papers provided in this study classified as WLAN multichannel are discussed in this section; including 1 paper classified as Attack Strategies, 0 papers as De-
tection and Prevention Strategies, 8 papers as Defense Strategies, and 6 papers as Game Theoretic Strategies.

3.4.2 Wireless Sensor Network (WSN)
3.4.2.1 Single Channel

In this section, we further classify the literature as below:

A. Attack Strategies: [124] propose an optimal relay and jammer selection scheme with power allocation to maximize the secrecy rate subject to a total transmission power constraint. [64] consider wireless relay networks under jamming attacks, and node geometry with received power constraints. The authors consider minimum square error and amplify forward relay strategy and the diagonal relay amplifying matrix is calculated to minimize the mean square error between the received signal and the transmitted signal. [61] develop jamming attacks that can work on encrypted packets. They expose the shortcomings of semantics of the data link layer and show that some of the MAC protocols are susceptible to a jamming attacks.

B. Detection and Prevention Strategies: The ideal way to stop a jamming attack is to detect the location of the jamming device, though this is may not be feasible. However, finding the device would be would be very cost effective as compared to other methods of designing protocols for escaping jamming attacks. [129] provide a mapping detection approach to provide feedback to the base station about further jamming areas and power management strategies for the nodes that are under jamming attack or within the range of the jamming device. The protocol consists of two parts: 1) the jamming detection module and 2) a mapping module. The jamming detection module monitors radio and MAC layers...
and then applies heuristics to determine whether the node is jammed or not. The mapping module groups the nodes that are jammed, based on the information received from the jamming detection module. [76] address the problem of locating a jamming device in a wireless network. They propose a least square (LSQ) based localization algorithm that estimates the location of the jamming device by using the changes in neighboring nodes caused by the device. The approach used by the authors does not depend on the signal strength in the jammed area, nor does it depend on delivering information out of the jammed area. They also study the LSQ based algorithm in the shadowing model. The authors show that the LSQ method significantly reduces the computational cost of locating the jamming device. [70] propose a method to find the location of multiple jamming devices in a network even when the jamming areas overlap. The method proposed by the authors, unlike other methods, does not depend on the signal strength to find the position, but uses distributed network communication instead. [47] study optimal DoS attack detection sensor placement problem to minimize the number of sensor required to detect the DoS attack and the cost for locating such sensors. Finally, in [22], two detection mechanisms distinguish between legitimate and adversary nodes under a DoS attack are discussed.

C. Defense Strategies: [128] study the DoS attack in wireless WSNs. The authors provide a classification of different type of DoS attacks and their known defense methods in the different abstract layers of the Internet. The authors study two different protocols that are used by WSNs that did not consider security initially. From the examples provided by the authors, they conclude that considering security during protocol design is essential. The authors describe jamming attacks as one of the major attacks on the physical layer,
and the jamming attack is very effective if the network is using a single frequency. A constant jamming attack will not allow the nodes to communicate if they are under attack, but it would not last long because the jamming device might use all its energy. SS is good for defending jamming attacks but it has high power and cost requirements; thus, the authors conclude that SS is not efficient in the case of sensors networks. The other defense strategy discussed is that the nodes should transmit data when the jamming device is not transmitting and using high power. But, this defense is possible only if the attack is intermittent. [91] discuss the holistic view of the security threats faced by the WSN and available defense strategies. Finally, the selection of relay nodes that increase the security of the WSN by protecting the destination node from eavesdropping and jamming attack is discussed in [57].

D. Game Theoretic Strategies: [29] study the proactive defense technique against jamming attacks in multi-hop relay networks. The network nodes send a deceptive flow along a routing path, so the attacker will use all its resources on the deceptive flow, which will reduce the impact of jamming on the real traffic. The authors provide a two stage Stackelberg equilibrium model for both the selfish and altruistic nodes. [146] provide a non-cooperative game theoretic model where network nodes try to maximize their utility by choosing a relay node, keeping in mind the interference from other nodes and the presence of a malicious node, while the malicious nodes try to maximize their capacity and choose either to be a jamming node or an eavesdropper.

A total of 13 papers provided in this study classified as WSN single channel are discussed in this section; including 3 papers classified as Attack Strategies, 5 papers as De-

56
tection and Prevention Strategies, 3 papers as Defense Strategies, and 2 papers as Game Theoretic Strategies.

3.4.2.2 Multichannel

In this section, we further classify the literature as below:

A. Attack Strategies: To the best of our knowledge, there are no papers in literature within the scope of this survey that deal with attack strategies for multichannel WSN.

B. Detection and Prevention Strategies: To the best of our knowledge, there are no papers in literature within the scope of this survey that deal with detection and prevention strategies for multichannel WSN.

C. Defense Strategies: Channel surfing is switching between between channels or frequencies to avoid jamming by the attacker. [133] propose two different versions of channel surfing methods: coordinated channel switching and spectral multiplexing, both of which combat jamming attacks in multichannel WSNs. [75] study a new method called BitTrickle, an anti-jamming scheme that allows communication in the presence of a reactive broadband high power jamming device. This wireless scheme exploits the reaction time of a reactive jamming device. The results show that the BitTrickle scheme works better than SS technology because it allows communication under a reactive jamming attack. [67] study adaptive anti-jamming techniques in wireless WSNs, in which the sensors can choose the best solution among the techniques available. The authors also propose a method where the strengths of several anti-jamming techniques are combined, and the choice of choosing a method depending on the jamming condition is left to the sensors.
to decide. MULtichannel Exfiltration PROtocol (MULEPRO), a protocol that rapidly exfiltrate data from a large distributed network, is explored by [3]. In [134] two different channel surfing methods are discussed: one where all the nodes in the networks change their channels and one in which the nodes in the jammed area change their channels to escape jamming. [130] propose DEEJAM, a novel protocol that has four layers of defense, hides the jamming communication and reduces the impact of damage. [142] study and propose a cooperative anti-jamming scheme designed to enhance the quality of the links degraded by jamming. In this scheme legitimate users cooperate among themselves to improve the quality of the links jammed in both WSN and AHNs. Finally, [65] investigate the connectivity of a multi-hop multichannel WSN and AHNs network subject to insider jamming attacks.

D. Game Theoretic Strategies: [137] provide power control methods in their study of a non-cooperative zero-sum game to detect and avoid energy efficient jamming attacks in wireless WSNs. They also model a one stage game between an intrusion detection system and an attacker, and provide a Nash equilibrium for both games.

A total of 9 papers provided in this study classified as WSN multichannel are discussed in this section; including 0 papers as Attack Strategies, 0 papers as Detection and Prevention Strategies, 8 papers classified as Defense Strategies, 1 papers as Game Theoretic Strategies.

3.4.3 Ad hoc Network (AHN)

3.4.3.1 Single Channel

In this section, we further classify the literature as below:
A. Attack Strategies: [31] study the problem of determining the optimal number and placement for a set of jamming devices in order to neutralize communication on the network. This is known as the Wireless Network Jamming Problem (WNJP). The jamming devices are assumed to have omni-directional antennas. The communication nodes are also assumed to be outfitted with omni-directional antennas and function as both receivers and transmitters. An undirected edge would connect two nodes if they are within a certain communication threshold. The study considers the transmitting nodes which emit radio signals and, correspondingly, the jamming devices which emit electromagnetic waves. The jamming effectiveness of a device depends on the power of its electromagnetic emission, which is assumed to be inversely proportional to the squared distance from the jamming device to the node being jammed. The authors provide an integer programming (IP) model for finding the minimum number of jamming devices needed to ensure a certain threshold is met. Further, they solve the Optimal Network Covering Problem (ONCP): The objective is to minimize the number of jamming devices used while achieving some minimum level of coverage at each node. They also solve the Connectivity Index Problem (CIP): The objective of this formulation of the WNJP is to minimize total jamming cost, subject to a constraint that the connectivity index of each node does not exceed some pre-described level. They consider a deterministic formulation. Instead of finding the connectivity as in the previous variant of the problem, the authors show that it is sufficient to jam some percentage of the total number of nodes in order to acquire effective control over the network. The Value-at-Risk (VaR) and Conditional Value-at-Risk (CVaR) are used to solve CIP. VaR is the measurement and control level of risk an individual/group can undertake, and it
is used mostly in financial risk analysis. CVaR is a percentile risk measure for estimating and controlling risks in stochastic and uncertain environments [31]. [31] to the best of our knowledge are the first to study and introduce jamming attacks to the OR community. [20] show that in a jamming attack, the jammer can jam a AHN even if the data is encrypted.

**B. Detection and Prevention Strategies:** To the best of our knowledge, there are no papers in literature within the scope of this survey that deal with detection and prevention strategies for single channel AHN.

**C. Defense Strategies:** [89] studies the problem of maintaining connectivity in a multi-hop AHN. The study introduces a connectivity index, which is the probability that a path exists between two nodes. From the results, the authors show that connectivity can be reduced even with a small number of jamming devices. And as a solution to the connectivity problem, the authors show that using sectored antennas improves the connectivity even in the presence of a high number of jamming devices. [2] propose methods to reduce the energy consumption of the low power batteries in wireless AHNs. The authors provide a power control loop similar to that found in cellular networks and use it in AHNs. The use group mobility, group communication, terrain blockage models are provided and the jamming attack problem is implicitly added into the terrain blockage model as a moving enemy jamming device in the battlefield and in inclement weather. The power consumption of the network under such blockages (jamming attack) is studied. The power control loop proposed by the authors reduced the energy consumption per transmitted byte by 10-20% and also increased the throughput of the network by 15%. [144] study a jamming acknowledgment (JACK) attack, and the work explores the weakness of many MAC schemes of
wireless networks to transmit an acknowledgment from the data receiver to the data sender to announce the successful arrival of a packet. The advantages of JACK attack are lower power consumption by the attacker, attack stealthiness, and damage the victim node. The Extended Network Allocation Vector scheme is proposed to combat such a JACK attack in [144].

D. Game Theoretic Strategies: [44] study the performance of a mobile AHN in presence of a jamming device. The objective of the jamming device is to degrade the performance of the network, while the objective of the operator is to optimize the network’s performance. The authors model this situation as a zero-sum game and define the Nash equilibrium under two cases. In one case, the distance between the receiver and transmitter is fixed, and, in the other, the distance is not fixed. [73] propose a Bayesian game formulation for intrusion detection in wireless AHNs and provide static and dynamic game models. In the static game the defender assumes the type of opponent with a fixed probability. In the dynamic game model developed by the authors, the defender updates his belief about the opponents’ type by keeping track of the history of the game. They find a mixed strategy and pure strategy Bayesian Nash equilibrium, and both players try to maximize their payoffs; the attackers’ payoff is to maximum damage without being detected, and the defender tries to maximize defending capability while constrained to energy usage. [138] present a Stackelberg game model to study defense against jamming attacks in both single channel and multichannel networks in the presence of a smart jammer, which learns the transmission power of the user and adaptively adjusts its transmission power to maximize the damage.
A total of 8 papers provided in this study classified as AHN single channel are discussed in this section; including 2 papers classified as Attack Strategies, 0 papers classified as Detection and Prevention Strategies, 3 papers as Defense Strategies, and 3 papers as Game Theoretic Strategies.

### 3.4.3.2 Multichannel

In this section, we classify the literature as defense and game theoretic strategies.

**A. Attack Strategies:** To the best of our knowledge, there are no papers in literature within the scope of this survey that deal with attack strategies for multichannel AHN.

**B. Detection and Prevention Strategies:** To the best of our knowledge, there are no papers in literature within the scope of this survey that deal with detection and prevention strategies for multichannel AHN.

**C. Defense Strategies:** [63] address the problem of control channel jamming attacks in multichannel AHNs. A frequency hopping technique, where the communicating nodes do not have a common frequency hopping scheme, is employed to combat such control channel jamming attacks. The papers [65, 142] have been discussed in Section 3.4.2.2.

**D. Game Theoretic Strategies:** Vadlamani et al.[122] solve a bi-level model jammer placement problem that accounts for the attacker defender, channel hopping, and Nash equilibrium strategies. In this paper, the authors model the jammer placement problem as $\min - \max$ problem. The jammer tries to minimize the number of jammers placed to minimize the throughput of the network. The defender tries to solve a max flow problem to maximize the throughput of the network. The attacker defender play a mixed strategy
channel hopping game. The authors show that, by increasing the number of channels in the network, the throughput of the network increases. If the number of jammers increases, the throughput of the network can be reduced considerably. [138] has been discussed before in Section 3.4.3.1.

A total of 5 papers provided in this study classified as AHN multichannel are discussed in this section; including 0 papers classified as Attack Strategies, 0 papers as Detection and Prevention Strategies, 3 papers as Defense Strategies, and 2 papers as Game Theoretic Strategies.

3.5 Next Steps
3.5.1 Gaps in Literature

As documented above, there is a dearth of papers in the area of wireless multichannel networks, so more research is needed. Figure 3.6 shows the number of jamming papers published for each wireless network type. Of the 28 papers that study multichannel wireless networks, 14 papers study with multichannel WLANs, 9 papers deal with multichannel WSNs, and 5 papers study with multichannel AHNs.

Only 13 papers found in the literature in this survey study with wireless AHNs, and out of them, only 5 papers that study with AHN multichannel networks. As seen in Figure 3.7, AHN contributes to only 16% of the total number of papers included in this literature review, and yet AHNs are expected to play an important role in the future civilian and military settings [45]. This absence of papers and increasing importance using AHN networks, highlights the clear need for more research in the areas of AHN as a whole and, more specifically about multichannel AHNs.
Figure 3.6
Number of papers by wireless network type

Figure 3.7
Percentage of the contribution of papers by wireless network type
Another observation apparent from the classification scheme presented above is the 13 papers from the year 2010-2014 that provide a game theoretic approach to solving the jamming problems. The number of game theoretic models provided in literature for years 1980-1999, 2000-2003, 2004-2006 and 2007-2009 are 1, 1, 5, and 9 respectively. An increasing number of studies are employing mathematical programming modeling and/or game theoretic models to solve complex jamming problems. This trend towards game theory suggests that OR, and specifically mathematical programming and game theory, has an important role to play in future research on jamming wireless networks.

3.5.2 Potential Research Problems

Below we discuss several new areas of research at the intersection of wireless network security and operations research.

3.5.2.1 A. Jammer Placement Problem

The jammer placement problem is an important areas of research for AHNs. The objective of the problem is to locate jamming devices in such a way that would either maximize or minimize the damage caused to the network. This problem is useful to the military; military strategists would like to find a way to locate the jamming devices and disrupt the communication of adversary networks. As discussed before, the jammer placement problem has studied by [31] and [122], but both these papers consider static jammer locations. An interesting problem might be to consider a moving jammer, i.e., what could be the impact of a jammer device that changes locations with time. This problem of moving jammers
is realistic in a war scenario or disaster aftermath situation where the jammer constantly moves to increase the impact of the attack.

3.5.2.2 B. Packet Routing Problem

The packet routing problem is to optimally route the data sent within the network even when the adversary is trying to jam the network. [56] develop a distributed path selection protocol tool that selects non-jammed paths in the network, but this paper studies wireless mesh networks. [35] introduce an intrusion-tolerant routing protocol for wireless sensor networks. The main objective of this protocol is to protect a WSN whose nodes have been compromised by an attacker and intends to launch a jamming attack among other attacks. This protocol effectively and securely constructs a tree-structured routing protocol that uses multiple paths to make the network more resilient to intrusion attacks. [96] introduce an adaptive decentralized routing protocol, called the least-resistance routing for radio networks. This method considers both interference and jamming in the network. The interference or jamming level determines the resistance of a particular path to transmit or receive data. The protocol chooses the path that has least resistance to transmit the data, thereby improving the throughput of the network. Since, these papers provide heuristic solution, it is necessary to develop a mathematical programming model to find optimal solutions for the packet routing problem for wireless networks under jamming attack. An interesting extension to the packet routing problem is the dynamic packet routing problem, in which every node can check to see if the link between it and the next node is jammed,
and route packets dynamically using other paths in the network as a defense against jamming attacks.

### 3.5.2.3 C. Transmission Scheduling Problem

Developing scheduling algorithms that use real time information about the network in the presence of a jamming attack is a very important area of research. The data to be transmitted should be scheduled in such a way that the impact of the jamming attack is minimized. There are many papers in literature that study transmission scheduling problem in wireless networks in general [10, 49, 71, 113], but not for wireless networks under jamming attacks. To the best of our knowledge there is only one paper that addresses the problem of transmission scheduling under jamming attacks. [3] as described above (see Defense Strategies in Section 3.4.2.2) provide a protocol that quickly moves that data from the attacked region to the region that is not under an attack. The scheduling problem they define is to find an assignment that maximizes the use of multiple channels to exfiltrate the data with interference and channel assignment constraints. But, the authors provide an algorithm to solve the problem and which heuristically solves the scheduling problem. Since one paper cannot capture all the issues in transmission scheduling and jamming there is necessity for further research in this area. Because [3] provide a heuristics solution there is a need for a mathematical programming model to find an optimal solution for the transmission scheduling problem under jamming attacks.
3.5.2.4  **D. Resource Allocation Problem**

In AHN's the nodes have very small amount of power available and efficient use of this power is very important. Many researchers such as [66] and [106] have used resource availability as a constraint to solve the jamming problem, but they do not try to optimize the allocation of the resource itself. During a jamming attack, the node in the network may have to reroute the packets or might use a higher signal strength to transmit data, which in turn would increase the power consumption. Hence, it is necessary to find optimization techniques that can improve the efficiency of the resource usage. Resource allocation problems under jamming attacks aim to minimizing the total amount of power consumption, cost, etc., used to evade jamming by employing routing techniques, or by efficient network node placement.

3.6  **Conclusions**

This paper, provides a comprehensive survey on the wireless network jamming problem. We provide a taxonomic classification of the different attack, defense, and detection and prevention techniques in literature by the type of wireless network they affect. Furthermore, different attack, defense, and detection techniques in literature are surveyed, in order to provide the interested researcher an understanding of the research done. This paper, offers a one-stop point for readers to get the complete picture of the research done in area of wireless jamming attacks, including the type of attack, the solution methodology to counteract the attack, and most importantly, the type of wireless network studied. This classification scheme and analysis on the number of papers available in literature shows
a potential gap in the dearth of research in wireless AHN and wireless multichannel networks. The papers shows that there is an increase in the usage of game theoretic strategies to address the problem of jamming attacks and hence points out areas where the OR community can contribute positively to the jamming literature. Areas and new research problems like jammer placement problem, scheduling, routing, and resource allocation under jamming attacks are identified where the OR community can contribute towards solving jamming problems in wireless network.
CHAPTER 4
A BI-LEVEL PROGRAMMING MODEL FOR THE WIRELESS NETWORK
JAMMING PLACEMENT PROBLEM

4.1 Introduction

Military strategists are always looking for better ways to protect a communication wireless network from attacks of terrorists. The use of air as a medium for data transfer makes wireless networks susceptible to various attacks. Of these attacks, jamming and denial of service attacks are most commonly occurring and hence are widely studied. The type of attack where the attacker transmit electromagnetic waves using a jamming device, so as to disrupt legitimate transmission is called jamming attack (see section 3 for details). In denial of service attacks, the attacker sends multiple data requests to the nodes in the network. This keeps the network busy continuously, preventing legitimate transmission from being sent through the network. Wireless networks, as the name suggests, are computer or mobile networks that send and receive data without the use of wires. The ease of installation and the added benefit of mobility (e.g., Laptops) within the area covered, make wireless networks very popular, especially in homes [40]. Wireless networks are also used in military applications and disaster situations. There are three main types of wireless networks: Wireless Local Area Network (WLAN), more commonly called Wi-Fi; Wireless Sensor Networks (WSN); and Wireless Ad-Hoc Networks (AHN). Wi-Fi networks
are mostly found in homes, coffee shops, malls etc., while WSNs are used for collecting data or information from places where it is difficult for the human to be physically present (e.g., hot deserts) [83]. AHNs are mostly used in military applications and disaster situations [103, 145] where it is not feasible to build an infrastructure for communications. Wireless networks can also be classified as single-hop and multi-hop networks. A network is called single-hop when the data from one node is sent directly to the other node without any intermediate nodes. In a multi-hop network the data is sent from the source node to the destination node via one or more intermediate nodes. This process of sending data from source to destination via intermediate nodes is called hopping. The data is sent through a shared channel between nodes. In wireless networks, data can often be sent on multiple channels, or bands of frequency. A wireless network can be a single-channel or a multi-channel network.

In this paper we study the wireless network jamming problem in multi-hop, multi-channel wireless networks. The problem is solved from the attacker’s point of view to place jamming devices in such a way that the throughput of the network is minimized. In addition to the jamming placement problem, our model also considers channel hopping, in which the attacker and operator (defender) switch channels randomly. We provide a min-max formulation where the attacker tries to minimize the throughput and the operator tries to maximize the throughput. We linearize the non-linear terms in min-max formulation and give an integer programming model for calculating the optimal throughput of the network. Numerical experiments of different problem instances are solved using CPLEX solver and
the results are reported. The results clearly show the damage jamming attacks can cause to mission critical wireless networks by reducing the throughput of the network.

The rest of the paper is organized as follows: in Section 4.2 a brief literature review is provided. In Section 4.3.1 we describe the problem and a mathematical model is provided in 4.3.2. Section 4.4 and Section 4.5 gives the solution and the numerical experiments. A conclusion is provided in Section 4.6 in the end.

4.2 Literature Review

The jamming problem has been studied widely in many wireless network settings, including wireless LAN networks [13, 42, 58], sensor networks [66, 136], and multihop networks [115, 140]. Other general wireless networks have also received their fair share of attention [6, 99, 51, 79, 109].

Commander et. al [31] studied the problem of determining the optimal number and placement of a set of jamming devices in order to neutralize communication of the network. This is known as the Wireless Network Jamming Problem (WNJP). The jamming devices were assumed to have omni-directional antennas. The communication nodes are also assumed to be outfitted with omni-directional antennas and function as both receivers and transmitters. An undirected edge connects two nodes if they are within a certain communication threshold. The jamming effectiveness of a device depends on the power of its electromagnetic emission, which is assumed to be inversely proportional to the squared distance from the jamming device to the node being jammed. The authors provide an in-
integer programming model for finding a minimum number of jamming devices needed to meet a certain threshold on the area that can be jammed.

For a system which has multiple channels, the interactions of the transmitter and jamming device is formulated as a game of transmitting randomly over multiple channels [93]. The jamming problem was studied by [4] as an intrusion detection problem. The problem of multi-hop networks with packet forwarding was studied in [115] and [140]. Zorzi et al [147] and [88] studied jamming problems and showed that a successful transmission by a transmitter depends on the probabilities of choosing the channel via probabilistic capture model.

To the best of our knowledge the WNJP has not been studied in wireless multi-hop, muti-channel networks. In this paper we formulate the WNJP as a network interdiction problem, using directional antennas instead of the omni-directional antennas used in Commander et. al [31]. We also model random channel selection for both the jammer and the operator.

4.3 Problem Description and Mathematical Model

Before we describe the problem, we will define some of the important terms needed to better understand the problem:

**Jamming Attacks**: The act of deliberately transmitting electromagnetic waves to a wireless network with the intention of disrupting or forestalling the legitimate transmission of the network is called a jamming attack. The word "jammer" is used to denote a device or an adversary with a device emitting electromagnetic waves to disrupt the network. In WSN and AHN the jammer disrupts the legitimate transmission by using the same radio frequency or the same channel that the legitimate nodes in the network use. Since WSN and AHN are mostly used in military applications and disaster situations where the data or information is critical, jamming attacks can
prove to be a serious threat. The higher the power of the jammer, the greater the damage to the network. However, there is a maximum limit on how much power the jammer can use.

- **Constant Jammer:** In this paper we study multi-hop wireless networks like AHN and WSN under the attack of a constant jammer. A constant jammer is a type of jammer which continuously emits electromagnetic waves or random sequences of bits through the channel. If the channel on which the jammer transmits is same as that of the nodes in the network, the channel is jammed, reducing the throughput on that channel.

- **Channel Hopping:** The attacker and operator choose channels with a particular probability to disrupt the network and to evade the jamming attack respectively. Once a channel is chosen all the power of the jammer is used on that channel to disallow the legitimate flow of data through that channel. The operator tries to change the channels to evade jamming and this technique has proved to be effective [25]. In this paper we assume that the jammer and operator do not have information about each other’s channel access probabilities as in [66]. In such a case, when there is no channel access information, the operator and jammer choose each channel with the same probability to reduce maximum damage and to cause maximum damage, respectively [66].

- **Directional Antennas:** Directional antennas used in wireless networks transmit and receive signal only from one direction. Noubir [89] proposed the use of directional antennas in AHN to reduce the effect of jamming attacks. The other more commonly used antennas in the literature are the omni-directional antennas. Unlike directional antennas, omni-directional antennas transmit and receive data from all directions. So, the use of directional antennas reduce interference from other concurrent transmission around it because it only transmits and receives in the direction of the other node. In this paper we assume that the nodes in the network use directional antennas. In other words, each node has as many directional antennas as the number of other nodes it is communicating with. This assumption of the operator using directional antennas is justifiable because in military applications, the position and direction of nodes (e.g. laptop, cell phone) is planned ahead of time. On the other hand, we assume that the jammer uses omni-directional antennas to maximize the range of damage it can cause. For a jammer to jam communication between two nodes using directional antennas, the jammer has to be located exactly in the direction of the receiving or transmitting directional antenna of the node.

- **Signal to Interference plus Noise Ratio (SINR):** Signal to interference plus noise ratio is defined as the ratio of the power of the signal of interest to the power of the interference from all other signals including the power from all the other nodes in the network transmitting, the power of the jammer transmitting and the white noise in the network. The higher the value of SINR the better the quality of the signal received and hence the operator would like to increase the, SINR. The jammer on
the other hand will try to increase the interference, thereby decreasing the SINR and hence disrupting the network.

- **Throughput:** In computer networks throughput is defined as the average rate of successfully transmitting data over a channel used in communication. The throughput is measured in bits/sec.

### 4.3.1 Problem Description

In wireless multi-hop networks, the data travels from the source node to the destination via multiple intermediate nodes. The jammer places the devices in locations such that the entire networks is rendered useless. Figure 4.1 shows a wireless multi-hop, multi-channel network with six nodes; with node 1 as the source, and 6 the destination, and all other nodes as intermediate nodes. The main purpose of the intermediate nodes is to relay data sent from the source to the destination without sending data of their own. The figure shows three channels denoted by solid, dotted and dashed lines each of different frequency $2.41 \ GHz$, $2.42 \ GHz$, and $2.40 \ GHz$ respectively. The triangles on arcs (1,2) and (1,4) represents the location of jamming devices. We assume that all nodes use directional antennas and hence the jamming devices have to be placed in the direction of transmission from node 1 to node 2. We assume that there is no concurrent transmission from the other nodes in the network, i.e., there is only one source node and one destination node. It can be seen that jamming the arcs going out of the source node or jamming the arcs going into the destination node will jam the entire network. The objective of the jammer is to place the jamming devices on the arcs such that throughput of the network is minimized. The objective of the operator is to maximize the throughput of the network. We assume that jammer can place the jamming device at midpoint of the arc between two nodes. There is also a limit on the
number of jamming devices that are available. The operator and jammer play a zero-sum simultaneous channel hopping game, and at equilibrium both select a channel with equal probability, i.e., in Figure 4.1 the probability of the operator selecting a channel is \( \frac{1}{k} = \frac{1}{3} \), where \( k \) is the number of channels. The channel hopping probability helps the operator to still use the network for transmitting data by choosing a channel different from the one used by the jammer. The operator uses channel hopping only for the arcs under jamming attack. The jammer and the operator can transmit data only on one channel at any given time. We assume that the attacker and the operator do not know each other’s channel hopping probabilities, thus, the channel hopping can be modeled as a simultaneous game in choosing channels. The mixed strategy Nash Equilibrium of the game is that both the jammer and the operator select channels with equal probabilities. So the probability for each player to choose a channel in Figure 4.1 is \( \frac{1}{3} \). A game theorist typically uses a set of elements, along with a solution to deduce a set of equilibrium strategies for each player such that, when these strategies are employed, no player can profit by unilaterally deviating from their strategy, this equilibrium is known as Nash equilibrium [84]. The probability of the operator and the jammer choosing a channel are independent, and hence the probability of a channel being jammed is \( \frac{1}{3^2} \) and the probability of a channel not being jammed is \( 1 - \frac{1}{3^2} = \frac{8}{9} \).

### 4.3.2 Mathematical Model

The objective of the operator is to maximize the throughput of the network and the objective of the jammer is to minimize the throughput of the network. Wood [127] proposed
a network interdiction problem for the flow of drugs in the South America. They provide a \( \min - \max \) formulation in which the enemy tries to maximize the flow and the drugs while the interdictor tries to minimize the flow by interdicting the drugs flow. In this paper the jammer tries to interdict and minimize the flow of the legitimate data by placing jamming devices in the network while the military or operator tries to maximize the flow by channel hopping. We present a \( \min - \max \) formulation. Given a directed graph \( G = (V, A) \), the data from the source node \( s \) flows to the sink node \( d \) via intermediate nodes. The data is sent using electromagnetic waves via air from one node to another. The binary data consisting of ones and zeros are converted to electromagnetic waves and transmitted using a directional antenna, in the direction of the next node. Electromagnetic waves attenuate in free space at a rate \( \frac{1}{t_{ij}} \), where \( t_{ij} \), is the distance between nodes \( i \) and \( j \) in the network. The electromagnetic waves from the jamming device \( \ell \) and node \( j \) also attenuates in free space with the rate \( \frac{1}{t_{\ell j}} \), where \( t_{\ell j} \), is the distance between jamming device \( \ell \) and node \( j \) in the network. The power \( p_{ij} \) is the power of node \( i \) received at node \( j \) and is given by:
\[ p_{ij} = \frac{\lambda}{t_{ij}^2} \] (4.1)

where \( \lambda \in \mathcal{R} \) is a proportionality constant; and without loss of generality, we set \( \lambda = 1 \).

The power \( p_{\ell j} \) between jamming device \( \ell \) and node \( j \) can be calculated using Equation (4.1) by replacing \( i \) with \( \ell \). The SINR for a given channel is given by:

\[ SINR_{ij} = \frac{p_{ij}}{I_j + v} \] (4.2)

where \( I_j \) is the total interference from all other concurrent transmissions from the jamming device \( \ell \) received at node \( j \) and is given by

\[ I_j = \sum_{\ell, j \in A} p_{\ell j} \] (4.3)

\( v \) is the white noise in the channel. The throughput of the channel used in communication is given by the Shannon’s rate [109]:

\[ C_{ij} = B \log(1 + SINR_{ij}) \] (4.4)

where \( C \) is the maximum theoretical throughput of the channel and \( B \) is the bandwidth of the channel measured in Hertz. In the presence of a jammer, the throughput decreases because jammer increases the noise. We assume that the bandwidth \( B = 1 \) Hertz. We fixed the power values for the signal and the interference from the jammer at 5 Watts each. The values of \( v \) is fixed to be a very small value close to zero. Let \( u_{ij} \) be the
throughput of a non-jammed channel \((i, j) \in A\) between nodes \(i\) and \(j\) as is calculated using Equation (4.4) with \(I_j=0\). Let \(w_{ij}\) be the throughput of the jammed the channel \((i, j)\), and is calculated using Equation (4.4) with \(I_j\) given by Equation (4.3). Here, \(i, j \in V\) and \(i, j = 1, 2, 3, \ldots, m\), \(m\) is the total number of nodes in the network. Let \(q_{ij}\) be the expected throughput of a channel between \((i, j)\), given arc \((i, j)\) is not jammed. There is no channel hopping when there the arc is not jammed and hence \(q_{ij}=u_{ij}\). Let \(v_{ij}\) be the expected throughput of an arc between \((i, j)\) given arc \((i, j)\) is jammed. Let \(s_{ij}=ku_{ij}\) be expected throughput of the arc between \((i, j)\). The expected throughput \(v_{ij}\) for a mixed strategy Nash Equilibrium channel hopping game between the operator and attacker is given by \(v_{ij} = (1 - \frac{1}{k^2})u_{ij} + \frac{1}{k^2}w_{ij}\), where \(k\) is the number of channels. The min – max mathematical model is shown in Model 1.

**Model 1:**

\[
\min_{\gamma} \max_x \quad x_{ds} \quad \text{(4.5)}
\]

subject to:

\[
\sum_j x_{sj} - \sum_j x_{js} - x_{ds} = 0 \quad \text{(4.6)}
\]

\[
\sum_j x_{ij} - \sum_j x_{ji} = 0 \quad \forall i \in V \setminus \{s, d\} \quad \text{(4.7)}
\]

\[
\sum_j x_{dj} - \sum_j x_{jd} + x_{ds} = 0 \quad \text{(4.8)}
\]

\[
x_{ij} - s_{ij}(1 - \gamma_{ij}) - v_{ij}\gamma_{ij} \leq 0 \quad \forall (i, j) \in A \quad \text{(4.9)}
\]

\[
\sum_{(i, j) \in A} \gamma_{ij} \leq n \quad \text{(4.10)}
\]

\[
x_{ij} \geq 0 \quad \forall (i, j) \in A \cup \{(d, s)\} \quad \text{(4.11)}
\]

\[
\gamma_{ij} \in \{0, 1\} \quad \forall (i, j) \in A \quad \text{(4.12)}
\]
where $x_{ij}$ is the flow on the arc $(i, j)$ and $\gamma_{ij}$ is 1 if a jammer is located on arc $(i, j)$ and 0 otherwise. The objective function is to minimize the expected throughput of the network from the attacker’s perspective, and maximize the throughput from the operator’s perspective. The internal max problem is the max flow problem objective. In the classic max flow problem, the objective is to maximize the flow possible through a capacitated graph. This can be thought of as the objective of the operator, to flow maximum data in the capacitated graph. Equations (6-8) are the flow balance constraints of the max flow problem. Let $\alpha_s, \alpha_d$ and $\alpha_j (j \neq s, d)$ be the dual variables associated with Equations (6-8), respectively. We assume that the attacker has a limited number of jamming devices denoted as $n$ in Equation (4.10). Let $\theta_{ij}$ be the dual variable associated with Equation (9), $(i, j) \in A$. We can write the dual of the internal max flow problem as shown in Model 2.

*Model 2:*

$$
\min_{\alpha, \beta} \sum_{(i, j) \in A} s_{ij}(1 - \gamma_{ij})\theta_{ij} - v_{ij}\gamma_{ij}\theta_{ij} \quad (4.13)
$$

s.t.

$$
\alpha_i - \alpha_j + \theta_{ij} \geq 0 \ \forall (i, j) \in A \quad (4.14)
$$

$$
-\alpha_s + \alpha_d \geq 1 \quad (4.15)
$$

$$
\sum_{(i, j) \in A} \gamma_{ij} \leq n \quad (4.16)
$$

$$
\alpha_i \in \{0, 1\} \ \forall i \in V \quad (4.17)
$$

$$
\theta_{ij} \in \{0, 1\} \ \forall (i, j) \in A \quad (4.18)
$$
Equation (4.13) in Model2 has a non linear term $\gamma_{ij}\theta_{ij}$, we linearize this equation by replacing $\beta_{ij} = \gamma_{ij}\theta_{ij}$ and adding related constraints to the model. Model3 shown below is the linearized form of Model2:

**Model 3:**

\[\begin{align*}
\min & \sum_{(i,j)\in A} s_{ij}\theta_{ij} - s_{ij}\beta_{ij} - v_{ij}\beta_{ij} \\
\text{s.t.} & \quad \alpha_i - \alpha_j + \theta_{ij} \geq 0 \quad \forall (i,j) \in A \\
& \quad -\alpha_s + \alpha_d \geq 1 \\
& \quad \beta_{ij} \leq \gamma_{ij} \\
& \quad \beta_{ij} \leq \theta_{ij} \\
& \quad \beta_{ij} \geq \theta_{ij} + \gamma_{ij} - 1 \\
& \quad \sum_{(i,j)\in A} \gamma_{ij} \leq n \\
& \quad \alpha_i \in \{0, 1\} \quad \forall i \in V \\
& \quad \theta_{ij}, \beta_{ij}, \gamma_{ij} \in \{0, 1\} \quad \forall (i,j) \in A
\end{align*}\] (4.19-4.27)

Equation (4.25) sets the upper limit on the number of jamming devices that can be placed in the network. Equations (21-23) are the linearization constraints.

### 4.4 Solution Approach

In this section we discuss the solution methodology. Consider a graph with one source node, one destination and nine other intermediate nodes as shown in Figure 4.2. This graph is the optimal solution obtained by solving Model3 using a commercial solver CPLEX.
for a graph with 9 intermediate nodes, 2 jammers, 3 arcs and 3 channels. The source node has three arcs \((0,1), (0,2), (0,3)\) connecting to nodes 1, 2, and 3. We assume that there are three channels between every node pair. The attacker can place a maximum of two jammers in the network to minimize the throughput. The operator and the attacker strategies are modeled as a mixed strategy Nash Equilibrium channel hopping sequential zero sum game. The operator and attacker both use their Nash equilibrium channel hopping probabilities of \(\frac{1}{k} = \frac{1}{3}\). We assume that the jammer and the nodes in the network transmit with a power of 5 Watts. The signal to interference noise ratio is given by Equation (4.2). The numerator is the signal strength (i.e., 5 Watts), while the denominator is the interference caused by the jammer placed in the direction of the signal being sent from one node to another is also 5 Watts. In the absence of jamming, the denominator value of the jammer power is zero. The value of the noise that exists in the channel in the presence and absence of a jammer is a very small close to zero. The throughput of a channel can be calculated by Equation (4.4). The operator’s objective is to maximize the throughput of the network and the jammer objective to minimize the throughput are considered by Model3. If there are multiple arcs going out of a node, even if the jammer is placed on one arc, the data is transferred through the other arc. Using multiple channels allow the operator to reduce the effect of jamming attack by choosing a different channel (see channel hopping above). The optimal solution for a jammer is to jam either the arcs going out of the source or the arcs going in to the destination node to cause maximum damage by reducing the throughput. From optimal solution shown in Figure 4.2, the jammer places the jamming devices on the arcs \((0,1)\) and \((0,2)\) and is denoted by dotted lines. But since the network
has a node degree of three, the throughput of the network is not reduced greatly as the operator can use the other arc \((0, 3)\) (denoted by a solid line to show non jammed arc) to send data.

![Figure 4.2](image)

**Figure 4.2**

Jamming in a network of 9 intermediate node

### 4.5 Numerical Experiments

In order to demonstrate the advantages of the proposed model \((Model3)\) to solve the network interdiction of wireless networks, we provide some case studies. The experiments were performed on a computer with a 2.5 GHz Intel i7 processor with 8 Gb RAM, Microsoft Windows 7 operating system. The problems are solved using a commercial solver CPLEX 12.5. We assume that the strategists can locate nodes randomly in a given area. We generate random graphs of 3, 4, and 9 intermediate nodes. Random graph topology can be
justified by the fact that in military applications, the military strategist (operators) do not have well established infrastructure to locate the wireless devices, for communication. The operator has to locate wireless devices in feasible areas. The source node and destination node have fixed locations and the other intermediate node locations are generated randomly. For example, in the case where there are 9 intermediate nodes in the network, the source node is located at coordinate (0, 0) and the destination node at coordinate (10, 10), the rest of intermediate nodes are randomly located at coordinates in the area divided into a grid of 10 x 10. Five replications for each of the problem instances were run and the average throughput of the five runs is reported. The running time of all the experiments are less than 1 sec and hence are not reported. Table 4.1, Table 4.2, and Table 4.3 show the optimal solution for 3, 5 and 9 intermediate nodes with different values of jammers, channels, and the node degree. The number of jammers are always strictly less than number of arcs from each node, this is to make sure that the jammers are not placed on all the nodes going out of the source node which otherwise would make the problem trivial.

Table 4.1

<table>
<thead>
<tr>
<th>No. Intermediate Nodes</th>
<th>No. Jammers</th>
<th>Arcs from each node</th>
<th>No. Channels</th>
<th>Average of 5 Replications</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>161.47</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>279.85</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>301.96</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>321.08</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>437.93</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>461.05</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>162.89</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>399.27</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>442.47</td>
</tr>
</tbody>
</table>
Table 4.2

5 Intermediate Nodes

<table>
<thead>
<tr>
<th>No. Intermediate Nodes</th>
<th>No. Jammers</th>
<th>Arcs from each node</th>
<th>No. Channels</th>
<th>Average of 5 Replications</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>162.92</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>279.37</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>300.47</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>317.67</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>437.07</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>459.59</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>461.21</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>498.41</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>441.33</td>
</tr>
</tbody>
</table>

From the experimental results shown above, it is clear that as the number of arc out of a node increase, the throughput of the network also increases and this is intuitive because more arcs provide alternate paths for the the maxflow problem. We can also see that as the number of channels increases the throughput also increases, this result is also intuitive because as the number of channels increase, the probability of jamming the channel which the nodes uses to transmit data is reduced. It is also observed that irrespective of the number of intermediate nodes (3, 5, 9) if the number of jammers increase the throughput of the network reduces. For example in the case of 9 intermediate nodes with no jamming attack, 3 arcs, and 3 channels the throughput of the network is 474.79 bits/sec. The throughput for the problem instance with 9 intermediate nodes, 1 jammer, 3 arcs, and 3 channels is 460.17 bits/sec, i.e., the reduction in throughput of the network is about 4%. The throughput for 9 intermediate nodes, 2 jammers, 3 arcs, and 3 channels (see Table 4.3), obtained by solving Model3, is 438.48 bits/sec. From this it is clear by having two jammer in place, the attacker can reduce the throughput of the network by 7%. In military and disaster situations where data transferred is very important reduction in throughput can be critical and prove to be dangerous.
Table 4.3

9 Intermediate Nodes

<table>
<thead>
<tr>
<th>No. Intermediate Nodes</th>
<th>No. Jammers</th>
<th>Arcs from each node</th>
<th>No. Channels</th>
<th>Average of 5 Replications</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>158.22</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>277.76</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>299.92</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>317.22</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>436.31</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>460.17</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>159.13</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>394.07</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>438.48</td>
</tr>
</tbody>
</table>

4.6 Conclusion

In this paper, we model a jamming problem as a network interdiction problem with the aim of locating jamming devices in a way such that the throughput of the network is minimized from the jammer perspective. The operator’s objective is to maximize the throughput of the network by changing the channels to send data. We model this as an attacker-operator mixed strategy Nash Equilibrium channel hopping game. We see that with the increase in the number of channels, the throughput of the network increases, but if the number of jamming devices increase the attacker can reduce the throughput considerably. In the future work, we will consider the effect of having different power levels of transmission by the attacker and the jammer rather than the constant values as considered in this work. We will also develop better techniques for the operator to evade jamming and increase the throughput of the network in the presence of jamming. We will also provide efficient heuristics to solve problems with larger networks.
CHAPTER 5
A MIXED-INTEGER PROGRAMMING APPROACH FOR LOCATING JAMMING DEVICES IN A FLOW-JAMMING ATTACK

5.1 Introduction

Wireless networks refer to communication networks in which devices, such as laptops, communicate among themselves without the use of cables or wires. A wireless local area network (WLAN), more commonly called Wi-Fi, allows for easy access to the Internet whenever needed as long as the device can connect to a Wi-Fi signal. Wi-Fi is available these days in schools, homes, and coffee shops [40]. Other wireless networks include wireless sensor networks (WSN) and wireless ad hoc networks (AHN). A WSN is a collection of a large number of autonomous nodes which collect information from the area in which they are deployed and share information among nodes or send information to the base station [83]. AHNs are used when building a well-established wireless network infrastructure is not possible, for example, in a disaster or a military situation [103].

With increased dependence on networked information systems, finding better ways to secure them is very important for the government and private sectors. Wireless networks do not need cables or wires to transmit data and allow easy movement as long as the nodes in the network are within a given range. However, this use of air as a medium for data transfer makes them susceptible to various attacks. Among the various attacks in wireless
networks such as Worm hole attacks [46], Sybil attacks [143], jamming attacks are the most critical security concern [112] because these attacks are easy to launch. Although not discussed within this paper, there are several other attacks and defensive strategies in wireless networks[121].

Wireless jamming attacks, a type of Denial of Service (DoS) attack [92], have been widely researched [60, 63, 77, 83, 106, 125] and may be employed by the military to deny terrorists the ability to transfer data through a network. In jamming attacks, the jamming device transmits radio signals that disrupt communication in the network by decreasing the Signal-to-Inference-plus-Noise ratio (SINR) [15], which is the ratio of the signal power to the sum of the interference power from other interfering signals and noise power. A desirable ratio greater than 1 indicates more signal than noise. With enough power, and by choosing the same frequency as the network’s frequency, coupled with the same type of modulation, the jamming device can override any signal in the network. A wireless signal jamming device can be used to temporarily stop transmission and short out or turn off the power of devices or units in use. Examples of such units or devices are radios, televisions, microwaves, or any unit that receives electrical signals for operation.

The data sent by a source node travels through different abstract layers before it reaches the destination node [17, 83]. A DoS attack on the physical layer is called a jamming attack [17]. However, [116] and [128] have studied jamming attacks on the link layer and not just on the physical layer. [114] introduced a more sophisticated jamming attack that uses higher layer information to jam the data flowing through the network. They studied the problem of intelligently assigning jamming devices to the flow of data in the
network and referred to the attack as a *flow-jamming attack*. An adversary planning to jam a network has a limit on the amount of power available in the jamming device. Hence, the adversary can choose to jam when minimal energy is required to jam. A single packet travels through multiple wireless links and hence the adversary can effectively jam the traffic flow in the network even with minimal amount of power as mentioned by [114]. So, a smart attacker can disrupt communication significantly by using higher layer information (e.g., the network layer), less power and by intelligently assigning jamming devices to the data flowing in the network.

Among the jamming literature there are a few papers that deal with location problems in jamming attacks. For example, finding the location of a jamming device as a defense against jamming attacks has been an area of research. [129] created a mapping detection approach to provide feedback to the base station about further jamming areas and power management strategies for the nodes that are under jamming attack or within the range of the jamming device. [76] addressed the problem of finding a jamming device located in a wireless network. They proposed a least square based localization algorithm that estimated the location of the jamming device by using the changes in neighboring nodes caused by the presence of a jamming device. [70] proposed a method to find the location of multiple jamming devices in a network even when the jamming areas overlap. Locating jamming device as an attack to increase the impact of jamming is another area of research. [31] studied how to optimally locate jamming devices for an attack by introducing the Wireless Network Jamming problem. The objective is to determine the optimal number and placement of a set of jamming devices to disrupt communication in a network. The
authors developed an integer programming model for finding the minimum number of jamming devices needed to meet certain jamming threshold. [123] solved a bi-level min-max jammer placement problem. The attacker places jamming devices to minimize the throughput of the network, and the defender’s objective is to maximize the throughput of the network by solving a max flow problem. However, the work by [31] and [123] cannot be directly applied to flow-jamming attacks because flow-jamming attacks use higher layer information, such as network layer information, when planning how to attack.

[114], who were the first to introduce flow-jamming attacks in wireless networks, defined various evaluation metrics to measure the impact of such attacks. They assumed that the jamming device locations were known, and solved a linear programming model to assign jamming devices to flows in order to optimize various jamming metrics. [55] proposed stochastic search algorithms like iterative improvement, simulated annealing, and genetic algorithm to provide a stochastic optimization approach for flow-jamming attacks in multichannel wireless networks.

[114] and [55] assumed known locations of jamming devices in their study of flow-jamming attacks. In this paper, we discuss flow-jamming attacks with location decisions. The adversary chooses where to locate the jamming devices and which traffic flows to jam in order to maximize the amount of jammed traffic. We studied the impact of jamming devices locations have on jamming effectiveness and provided a mixed integer programming model for our analysis. A Benders decomposition algorithm was provided to solve the problem. Since the computation time for the standard Benders decomposition algorithm was very high, we provided an accelerated Benders decomposition algorithm to solve large
problems. These acceleration approaches outperformed the commercial solver CPLEX in most cases.

The rest of the paper is organized as follows: Section 5.2 describes the problem at hand and provides a mixed integer programming model. Section 5.3 describes the Benders decomposition algorithm and the different acceleration techniques used. Section 5.4 provides the computational results and discussion of the results, and finally Section 5.5 concludes the paper.

5.2 Problem Description and Mathematical Model

The main objective of this paper is to develop a mixed integer programming (MIP) model for flow-jamming attacks which takes into account the impact of the location of jamming devices on the flow. The problem is approached from the attacker’s perceptive. The problem consists of locating a set of jamming devices by the adversary in a given set of locations in a way that maximizes the impact of the attacks. The adversary can choose to jam each packet sent by the network when minimal energy is required because a single packet traverses multiple wireless network links, effectively jamming the traffic flow. A flow in a network is a path on which the data or packets are sent from the source to the destination. The attacker, who has multiple jamming devices uses minimum power from the total available power to jam network flows over multiple jamming devices and to maximize the amount of disruption. Hence, the efficiency of the attack can be optimized by intelligently assigning jamming devices to flows. This can be thought of as a war scenario where military strategists try to jam flows or packets of information from one terrorist camp
to another. They ideally want to jam all the flow that is transmitted between the terrorist camps, but they have limited power levels. So, optimizing the jamming attack to get the maximum benefit is the goal of the military strategists.

The figures below demonstrate the effect of optimally locating jamming devices prior to a flow-jamming attack. Figure 5.1 shows a network with six nodes and two flows; Flow 1 and Flow 2. The flows are not under a jamming attack, and hence, they can each transmit 100% of their data. However, if the network is hit by a flow-jamming attack, some of the data may be lost. Suppose that an attacker launches a flow-jamming attack and places the devices as shown in Figure 5.2. In this case, 40% of Flow 1 and 30% of Flow 2 is jammed. If the jammer solves an optimization problem to find the optimal location of jamming devices, as shown in Figure 5.3, 50% of Flow 1 and 100% of Flow 2 is jammed. Therefore, it is important for the military to find the optimal location of jamming devices with an aim to maximize the impact of flow-jamming attacks.

In this paper, we consider a wireless network with node set $N$. The data or packet flows between the source and destination nodes in $N$ is considered to be a set of single path flows $F$. We assume that the location of the nodes and the number of flows does not change for the duration of flow-jamming attacks. It is a common problem in wireless networks that some of the packets or data sent by some of the nodes collide with concurrent transmission resulting in the loss of packets. As in [114] we assume that only one flow is scheduled at any given time, i.e., there will be no concurrent flows and hence any loss of packets is due to jamming. Let $I$ be the set of jamming devices and $J$ be the set of locations at which the jamming devices can be placed by the adversary. These jamming devices are placed by
Figure 5.1

Network without jamming

Figure 5.2

Flow jamming attack with arbitrary jamming device locations
Flow jamming attack with optimal jamming device locations

the adversary throughout the wireless network. We also assume that each jamming device has a limited amount of energy. The cost of placing a jamming device is considered to be a constant value and does not change with the location or jamming device and hence is ignored in this paper. The adversary tries to locate the jamming devices in a way that will reduce the energy consumption and yet increase the impact of the flow-jamming attacks.

Let $c_{jf}$ be the cost to jam flow $f$ by a jamming device at location $j$. The cost $c_{jf}$ is proportional to the squared distance from location $j$ to the closest non-source node on the flow $f$. If $r_f$ is the rate of flow in the network, i.e., the rate at which the packets are sent from the source to the destination in the network and is measured in bits/time, then $c_{jf}r_f$ is the total energy required for a jamming device $i$ to jam every packet in flow $f$ from location $j$. All the notations used in this paper are given in Table 5.1. Since, every jamming device
need not jam every packet in the flow $f$, we define a decision variable $0 \leq x_{ijf} \leq 1$ as the fraction of flow $f$ jamming device $i$ at location $j$ jams and $y_{ij}$ is a decision variable that is 1 if jamming device $i$ is placed at location $j$ and 0 otherwise.

We develop a mixed integer programming model for comparing the maximum impact of flow-jamming attacks as shown below:

\[\text{[MIFY]}\]

\[
\begin{align*}
\max & \quad \sum_i \sum_j \sum_f x_{ijf} \\
\sum_{j \in J} \sum_{f \in F} c_{ijf} r_f x_{ijf} & \leq c_i \quad \forall i \in I & (5.1) \\
\sum_{i \in I} \sum_{j \in J} x_{ijf} & \leq 1 \quad \forall f \in F & (5.2) \\
x_{ijf} - y_{ij} & \leq 0 \quad \forall i \in I, j \in J, f \in F & (5.3) \\
\sum_{j \in J} y_{ij} & \leq 1 \quad \forall i \in I & (5.4) \\
\sum_{i \in I} y_{ij} & \leq 1 \quad \forall j \in J & (5.5) \\
0 & \leq x_{ijf} \leq 1 \quad \forall i \in I, \forall j \in J, f \in F & (5.6)
\end{align*}
\]
The objective function of $[MIFJ]$ is to maximize the total fraction of jammed flows. Constraint (5.1) is the power constraint. The total resource or power expenditure on the left hand side should be less than or equal to the total available power $c_i$. Constraint (5.2) is the flow constraint. This constraint ensures that the amount flow jammed by the jamming devices assigned to a flow $f$ must not exceed the amount of flow sent. Constraint (5.3) ensures that a flow cannot be jammed by device $i$ at location $j$ unless a device $i$ is located at location $j$. Constraint (5.4) forces each jamming device to be deployed at at most one location. Constraint (5.5) forces each location can have at most one jamming device. Constraint (5.6) enforces non-negativity and upper bound on the fraction of flow jammed, and constraint (5.7) is the binary constraint.

5.3 Algorithmic Strategy

The structure of $[MIFJ]$ is such that we can separate the problem into two smaller problems: one with only binary variables and another with continuous variables. Taking advantage of this problem structure, we apply a Benders decomposition method ([14]), a well-known decomposition method to solve mixed integer linear programs. The basic idea behind this method is to decompose the original problem into: an integer master problem and a linear programming subproblem. In this section, we first provide a basic Benders decomposition formulation to solve $[MIFJ]$. Then, we utilize several valid inequalities to speed up the algorithm.
5.3.1 Benders Decomposition

The underlying Benders reformulation for model \([MIFJ]\) is given below:

\[
\max [MIFJ-SUB](x | y) \text{ subject to constraints (5.1), (5.2), (5.3), (5.4), (5.5), (5.6), and (5.7),}
\]

where \([MIFJ-SUB]\) is the Benders decomposition subproblem. For given values of \(\{y_{ij}\}_{i \in I, j \in J}\) variables that satisfy the integrality constraint (5.7), the model reduces to the following primal subproblem involving only the continuous variables \(\{x_{ijf}\}_{i \in I, j \in J, f \in F}\).

\[\text{[MIFJ-SUB]:}\]

\[
\hat{y} \max \sum_i \sum_j \sum_f x_{ijf} \quad (5.8)
\]

\[
c_i^{-1} \sum_{j \in J} \sum_{f \in F} c_{jff} x_{ijf} \leq 1 \ \forall i \in I \quad (5.9)
\]

\[
\sum_{i \in I} \sum_{j \in J} x_{ijf} \leq 1 \ \forall f \in F \quad (5.10)
\]

\[
x_{ijf} - \hat{y}_{ij} \leq 0 \ \forall i \in I, j \in J, f \in F \quad (5.11)
\]

\[
0 \leq x_{ijf} \leq 1 \ \forall i \in I, \forall j \in J, f \in F \quad (5.12)
\]

Let \(\gamma = \{\gamma_i \geq 0 \mid i \in I\}\), \(\mu = \{\mu_f \geq 0 \mid f \in F\}\), \(\delta = \{\delta_{ijf} \geq 0 \mid i \in I, j \in J, f \in F\}\), and \(\pi = \{\pi_{ijf} \geq 0 \mid i \in I, j \in J, f \in F\}\) be the dual variables for the constraints (5.9), (5.10), (5.11), (5.12) respectively. The dual of the primal subproblem, which we call the dual subproblem \([MIFJ-SUB(D)]\) is given below:

\[\text{[MIFJ-SUB(D)]}\]

\[
\min \sum_i \gamma_i + \sum_f \mu_f + \sum_i \sum_j \sum_f \hat{y}_{ij} \delta_{ijf} + \sum_i \sum_j \sum_f \pi_{ijf} \quad (5.13)
\]

\[
c_i^{-1} c_{jff} \gamma_i + \mu_f + \delta_{ijf} + 
\pi_{ijf} \geq 1 \ \forall i \in I, \forall j \in J, f \in F \quad (5.14)
\]

97
\[ \gamma_i, \mu_f, \delta_{ijf}, \pi_{ijf} \geq 0 \]  

(5.15)

Let \( \nabla \) be the polyhedron defined by the constraints (5.14) and (5.15), and let \( P_\nabla \) be the set of extreme points in the feasible region of \([MIFJ-SUB(D)]\). Now, let us introduce an extra variable \( \theta \). We can formulate the underlying Benders master problem \([MIFJ-MP]\) as below \([MIFJ-MP]\):

\[
\max \quad \theta \\
\sum_j y_{ij} \quad \leq \quad 1 \quad \forall i \in I \\
\sum_i y_{ij} \quad \leq \quad 1 \quad \forall j \in J \\
\theta \quad \leq \quad \sum_i \gamma_i + \sum_f \mu_f + \sum_i \sum_j \sum_f y_{ij} \delta_{ijf} \\
\quad + \sum_i \sum_j \sum_f \pi_{ijf} \forall (\gamma, \mu, \delta, \pi) \in P_\nabla \\
y_{ij} \quad \text{binary} \quad \forall i \in I, \forall j \in J
\]

(5.16) \hspace{1cm} (5.17) \hspace{1cm} (5.18) \hspace{1cm} (5.19) \hspace{1cm} (5.20)

Constraint (5.19) is often referred to as the Benders optimality cut. \( \theta \) is bound by the objective value of the dual subproblem \([MIFJ-SUB(D)]\). The model \([MIFJ-MP]\), although equivalent to the \([MIFJ]\), has a large number of optimality constraints (5.19) and exhaustively finding them is not efficient. Instead, we iteratively generate a subset of cuts that are sufficient to identify an optimal solution. In each iteration, we solve \([MIFJ-MP]\) by replacing the set \( P_\nabla \) with the subset \( P_\nabla^n \subseteq P_\nabla \) of extreme points available at each iteration \( n = 0, 1, 2, \ldots \). By solving the relaxed \([MIFJ-MP]\) problem with only a subset of all the constraints, we get an upper bound for the original master problem. The idea behind the standard Benders decomposition is described below.
The algorithm starts by solving the relaxed master problem [MIFJ-MP] which provides a valid upper bound to the original problem. We represent this upper bound as $UB$. The optimal solution of the relaxed [MIFJ-MP], given by $[z_{MP}^u]$, is used to set up the dual sub problem [MIFJ-SUB(D)]. The value of $\hat{y}_{ij}^D$ in each iteration is the optimal solution obtained from the $LP$ relaxation [MIFJ-MP]. The optimal solution of the variables of [MIFJ-SUB(D)], provides the optimality cut for the relaxed master [MIFJ-MP]. The optimal objective function value, given by $[z_D^u]$ provides a lower bound ($LB$) to the original problem at each iteration. If the gap between the upper bound and lower bound falls below a predefined threshold value, $\epsilon$, the algorithm terminates; otherwise $P^u_{\nabla}$ is updated by adding an optimality cut constraint (5.19). Pseudo-code of the standard Benders decomposition algorithm is as shown in Algorithm 1. It is to be noted that we do not add any feasibility cuts to the master problem because for any value of $i$ and $j$, $x_{ij}$ is always feasible.
Algorithm 1 Standard Benders Decomposition

Initialize, $UB = \infty$, $LB = 0$, $n = 1$, $\epsilon$, $P_\nabla = \emptyset$

while true do

Solve $[\text{MIFJ-MP}]$ for $y_{ij}$ and $[z^n_{\text{MP}}]$ 

if $[z^n_{\text{MP}}] < UB$ then

$UB = [z^n_{\text{MP}}]$ 

end if

For fixed values $y_{ij}$, solve $[\text{MIFJ-SUB(D)}]$ to obtain values of $(\gamma_i, \mu_f, \delta_{ijf}, \pi_{ijf}) \in P_\nabla$ 

and $[z^n_{\text{D}}]$ 

if $[z^n_{\text{D}}] > LB$ then

$LB = [z^n_{\text{D}}]$ 

end if

if $(UB - LB)/UB < \epsilon$ then

break

else

$P_{\nabla}^{n+1} = P_{\nabla}^n \cup \{(\gamma_i, \mu_f, \delta_{ijf}, \pi_{ijf})\}$

end if

$n = n + 1$

end while

5.3.2 Accelerating Standard Benders Decomposition

Computational efficiency of the standard Benders decomposition depends mainly on (i) computational effort needed to solve the $[\text{MIFJ-MP}]$, (ii) computational effort needed to
solve the \([\text{MIFJ-SUB}(D)]\), and (iii) the number of iterations required to solve the problem optimally \([33]\). In our initial experimentation, standard Benders decomposition could not solve the problems in reasonable amount of time. Hence, we provided acceleration techniques to solve the \([\text{MIFJ-MP}]\) problem faster and speed up convergence of Benders decomposition. The following subsections describe the acceleration techniques employed.

5.3.2.1 Pareto Optimality Cut

[78] showed that if the dual subproblem \([\text{MIFJ-SUB}(D)]\) has multiple optimal solutions, there could be a number of alternatives for the optimality cut constraint (5.19). They proved that, for the purpose of generating stronger cuts, adding cutting planes that are not dominated by other optimality cuts could improve convergence of the Benders decomposition. We say that a cut generated from an extreme point \((\gamma^1, \mu^1, \delta^1, \pi^1)\) dominates a cut generated from another extreme point \((\gamma^2, \mu^2, \delta^2, \pi^2)\) if and only if

\[
\sum_i \gamma^i_i + \sum_f \mu^f_f + \sum_i \sum_j \sum_f y_{ij} \delta^1_{ijf} + \sum_i \sum_j \sum_f \pi^1_{ijf} \leq \sum_i \gamma^2_i + \sum_f \mu^2_f + \sum_i \sum_j \sum_f y_{ij} \delta^2_{ijf} + \sum_i \sum_j \sum_f \pi^2_{ijf}
\]

with a strict inequality for at least one point \(y_{ij} \in Y\). Using the concept of core points [78] formulated a problem that generates Pareto-optimality cuts. A core point is defined as a point in the relative interior of the convex hull of the feasible region, and can be used as a proxy for the optimal solution. Let \(Y^{LP}\) be the polyhedron defined by (5.17), (5.18), and \(0 \leq y_{ij} \leq 1 \forall i \in \mathcal{I}, \forall j \in \mathcal{J}\). Let \(y^0\) be the candidate core point in the \(Y^{LP}\) found by solving the LP relaxation of the \([\text{MIFJ-MP}]\). Even though such a LP relaxation
solution is not guaranteed to be an efficient core point, it is often in the neighborhood of the integer optima ([110]). Furthermore, after some cuts are added to the master problem, the LP relaxation solution will typically be in the interior of the convex hull of \( Y \), and hence satisfy the requirement of being a core point ([110]). We solved the subproblem shown below to obtain the Pareto-optimal cuts. \([\textit{MIFJ-SUB(PO)}]\):

\[
\begin{align*}
\min & \quad \sum_{i} \gamma_{i} + \sum_{f} \mu_{f} + \sum_{i} \sum_{j} \sum_{f} y_{ij}^{0} \delta_{ijf} + \sum_{i} \sum_{j} \sum_{f} \pi_{ijf} \\
\text{subject to} & \quad \sum_{i} \gamma_{i} + \sum_{f} \mu_{f} + \sum_{i} \sum_{j} \sum_{f} y_{ij}^{0} \delta_{ijf} + \sum_{i} \sum_{j} \sum_{f} \pi_{ijf} = z(\bar{\gamma}_{i}, \bar{\mu}_{f}, \hat{\delta}_{ijf}, \hat{\pi}_{ijf}) \quad (5.24) \\
& \quad \gamma_{i}, \mu_{f}, \delta_{ijf}, \pi_{ijf} \geq 0 \quad (5.25)
\end{align*}
\]

where, \( z(\bar{\gamma}_{i}, \bar{\mu}_{f}, \hat{\delta}_{ijf}, \hat{\pi}_{ijf}) \) is the optimal solution of the dual problem. Constraints (5.23) and (5.25) enforce the dual feasible region, and constraint (5.24) restricts feasible dual solutions to the set of alternative dual optima. The objective function (5.22) corresponds to minimizing the value of the cut at \( y_{ij}^{0} \).

### 5.3.2.2 Trust Region

In cutting plane algorithms, such as Benders decomposition, the solutions oscillate in the initial iterations within the feasible region, thereby slowing down convergence ([110]). In order to overcome such an undesirable feature, [68] and [110] proposed a trust region (TR) method. In this paper, we use the following method that bounds the Hamming distance [43] of the next master problem solution from the previous solution. Let \( \hat{y}_{ij}^{n} \) be the solution obtained in the \( n^{th} \) iteration and let \( \mathcal{N} = \{(i, j) | \hat{y}_{ij}^{n} = 1\} \). The constraint below is imposed to the master problem in iteration \( n + 1 \):

\[
\sum_{(i, j) \in \mathcal{N}} (1 - y_{ij}) + \sum_{(i, j) \notin \mathcal{N}} y_{ij} \leq \Delta^{n} \quad (5.26)
\]

where \( \Delta^{n} < |\mathcal{J} \times \mathcal{L}| \) represents the trust region size for iteration \( n \). The drawback with this cut is that, if a non-redundant trust region is retained throughout the Benders decomposition algorithm, then the algorithm
takes longer to converge. Hence, constraint (5.26) is added to the restricted master problem \([\textit{MIFJ-MP}]\) only during the initial iterations, when the algorithm displays oscillations in the solution and then dropped after the algorithm stabilizes.

**5.3.2.3 Knapsack Inequality**

Initial experimentation showed, with an available good lower bound from the Benders decomposition algorithm, adding a knapsack inequality (KI) to the Benders master problem along with the optimality cut Constraint (5.19) has a significant impact on the solution quality. In this paper, the primal subproblem is a maximization problem and hence we get a lower bound in each iteration. So, we add the knapsack cut as shown below to the master problem. A variety of valid inequalities from the knapsack inequality can be derived by modern commercial solvers such as CPLEX which would speed up convergence of the Benders algorithm [110]. Let \(LB\) was the best known lower bound obtained so far from the Benders algorithm. Since the Benders decomposition algorithm ensures that the \(LB \leq \theta\), we can derive the following knapsack inequality which is added in iteration \(n + 1\):

\[
LB^n - \sum_i \gamma_i - \sum_f \mu_f - \sum_i \sum_j \sum_f \pi_{ijf} \leq \sum_i \sum_j \sum_f y_{ij} \delta_{ijf} \tag{5.27}
\]

**5.3.2.4 Solution Elimination Constraint**

[19] introduce the idea of adding solution elimination constraints (SECs) to the master problem. [18] use SECs to ensure convergence of decomposition algorithms. On the other hand [48] referred to SEC as “supervalid inequalities” and showed that adding these constraints speeds up convergence. The following SEC prohibits the jamming device location plan \(Y^n\) from being repeated:

\[
\sum_{(i,j) | Y^n = 1} (1 - y_{ij}) + \sum_{(i,j) | Y^n = 0} y_{ij} \geq 1 \tag{5.28}
\]

This cut is added for every \(n\), where, \(n\) is the current iteration number. The \(UB\) provided by solving the master problem \([\textit{MIFJ-MP}]\) with constraint (5.28) may not be valid if \(Y^n\) is optimal, and the bound may
even drop below \( [z^*] \). This happens only if an optimal solution is at hand, and at this point the validity of the bound is irrelevant. Here \( [z^*] \) is the optimal solution of the algorithm. If \([MIFJ-MP]\) is infeasible we set \( UB = LB \). The master problem \([MIFJ-MP]\) is infeasible because all the solutions have been eliminated by SECs, and, thus, the solution \( Y^n \) obtained must be optimal.

### 5.4 Computational Results and Analysis

To test our approaches, we solved the flow-jamming attack problem on two realistic networks CMU [30], MIT [82], and on one set of randomly generated networks. The number of nodes was obtained from the realistic network’s dataset. We studied two different cases; the first was for each of the realistic networks CMU and MIT and the second case for random networks. Figure 5.4 and Figure 5.5 show the topology of the CMU and MIT networks. The random generated networks were created by randomly generating node coordinates in a unit square. The set of flows \( \mathcal{F} \) in the network were chosen by selecting a pair of origin destinations at random from the network. The origin nodes were selected at random without replacement. In other words, we have a different origin node for each flow. The number of flows in the network was also predefined, but the specific flows were determined using the aforementioned strategy for both the realistic and the random networks. All the experiments were implemented using Python 2.7 and run on a desktop computer with an Intel Core i7 3.50 GHz processor and 32.0 GB RAM. The optimization solver used was CPLEX 12.6. Below we describe each of the cases and provide the results.

#### 5.4.1 Experimental Results

##### 5.4.1.1 Case 1:

In this case, we used the networks CMU and MIT, with 54 and 92 nodes, respectively. We assumed discrete locations for placing jamming devices. These discrete locations were constructed using 8 x 8 and 10 x 10 subgrids overlaid on a unit square, resulting in two levels of granularity. Figure 5.6 gives an example of a randomly-generated network with six nodes (1-6), two flows and 25 possible locations (shown as red stars) of the jamming devices overlaid on a network. It is apparent from the Figure 5.6 that locations of the nodes and the location of jamming devices were different. We had two types of jamming devices \( T1 \) and \( T2 \). The
Figure 5.4

Network Topology of CMU

Figure 5.5

Network Topology of MIT
$T_1$ jamming devices have a fixed power level of 1 mW and $T_2$ jamming devices have a fixed power level of 10 mW as shown in Table 5.2. The number of flows was fixed and the flows were decided using the random strategy discussed above. Table 5.3 shows 12 different experimental problem instances for both CMU and MIT.

![Image of jamming device locations](image)

**Figure 5.6**

Example of jamming device locations

**Table 5.2**

<table>
<thead>
<tr>
<th>T1</th>
<th>T2</th>
<th># jamming devices</th>
<th>Total Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5</td>
<td>10</td>
<td>55</td>
</tr>
<tr>
<td>0</td>
<td>5</td>
<td>5</td>
<td>50</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

The computational results for both networks are shown in Table 5.4 and Table 5.5. Column *Problem Instance* shows the type of experimental run. The major column *CPLEX* gives the details of the objective value, the optimality gap, and the time in seconds CPLEX took to solve each of the 12 problems. The major column *Standard Benders* gives the details of the objective value, optimality gap, time in seconds, and
Table 5.3

<table>
<thead>
<tr>
<th>Problem Instances</th>
<th># Locations</th>
<th>T1</th>
<th>T2</th>
<th># jamming devices</th>
<th># Flows</th>
<th>Total Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem 1</td>
<td>64</td>
<td>5</td>
<td>5</td>
<td>10</td>
<td>20</td>
<td>55</td>
</tr>
<tr>
<td>Problem 2</td>
<td>64</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>20</td>
<td>50</td>
</tr>
<tr>
<td>Problem 3</td>
<td>64</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>20</td>
<td>5</td>
</tr>
<tr>
<td>Problem 4</td>
<td>64</td>
<td>5</td>
<td>5</td>
<td>10</td>
<td>50</td>
<td>55</td>
</tr>
<tr>
<td>Problem 5</td>
<td>64</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>20</td>
<td>50</td>
</tr>
<tr>
<td>Problem 6</td>
<td>64</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>50</td>
<td>5</td>
</tr>
<tr>
<td>Problem 7</td>
<td>100</td>
<td>5</td>
<td>5</td>
<td>10</td>
<td>20</td>
<td>55</td>
</tr>
<tr>
<td>Problem 8</td>
<td>100</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>20</td>
<td>50</td>
</tr>
<tr>
<td>Problem 9</td>
<td>100</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>20</td>
<td>5</td>
</tr>
<tr>
<td>Problem 10</td>
<td>100</td>
<td>5</td>
<td>5</td>
<td>10</td>
<td>50</td>
<td>55</td>
</tr>
<tr>
<td>Problem 11</td>
<td>100</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Problem 12</td>
<td>100</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>50</td>
<td>5</td>
</tr>
</tbody>
</table>

the number of iterations the standard Benders decomposition algorithm without any acceleration techniques took to solve the same 12 problem instances. The third major column $KI + SEC + TR$ gives the details of the objective value, optimality gap, time in seconds, and the number of iterations for the Benders decomposition algorithm with the three acceleration techniques KI, SEC, and TR to solve each of the 12 problem instances. The last major column $Benders$-$all$-$cuts$ gives the details of the objective value, optimality gap, time in seconds, and the number of iterations for the Benders decomposition algorithm with all the acceleration discussed in this paper to solve the same 12 problem instances. It is very apparent from the results that the Benders decomposition with all the acceleration techniques is faster than CPLEX for most of the problem instances for the networks CMU and MIT.
<table>
<thead>
<tr>
<th>Problem Instance</th>
<th>CPLEX</th>
<th>Standard Benders</th>
<th>KI+SEC+TR</th>
<th>Benders-all-cuts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Obj Val</td>
<td>Gap (%)</td>
<td>CPU (sec)</td>
<td>Obj Val</td>
</tr>
<tr>
<td>Problem 1</td>
<td>20.00</td>
<td>0.00</td>
<td>6.76</td>
<td>20.00</td>
</tr>
<tr>
<td>Problem 2</td>
<td>16.23</td>
<td>0.31</td>
<td>15.71</td>
<td>16.23</td>
</tr>
<tr>
<td>Problem 3</td>
<td>7.07</td>
<td>0.00</td>
<td>82.57</td>
<td>7.07</td>
</tr>
<tr>
<td>Problem 4</td>
<td>33.39</td>
<td>0.20</td>
<td>1800</td>
<td>33.39</td>
</tr>
<tr>
<td>Problem 5</td>
<td>24.92</td>
<td>0.00</td>
<td>22.61</td>
<td>24.92</td>
</tr>
<tr>
<td>Problem 6</td>
<td>11.58</td>
<td>0.00</td>
<td>198.85</td>
<td>11.58</td>
</tr>
<tr>
<td>Problem 7</td>
<td>20.00</td>
<td>0.00</td>
<td>14.78</td>
<td>20.00</td>
</tr>
<tr>
<td>Problem 8</td>
<td>17.61</td>
<td>0.00</td>
<td>603.22</td>
<td>17.61</td>
</tr>
<tr>
<td>Problem 9</td>
<td>7.54</td>
<td>0.08</td>
<td>472.72</td>
<td>7.54</td>
</tr>
<tr>
<td>Problem 10</td>
<td>36.42</td>
<td>0.41</td>
<td>1800</td>
<td>36.42</td>
</tr>
<tr>
<td>Problem 11</td>
<td>25.27</td>
<td>0.14</td>
<td>1046.5</td>
<td>25.27</td>
</tr>
<tr>
<td>Problem 12</td>
<td>16.35</td>
<td>0.00</td>
<td>119.97</td>
<td>16.35</td>
</tr>
<tr>
<td>Problem Instance</td>
<td>CPLEX</td>
<td>Standard Benders</td>
<td>KI+SEC+TR</td>
<td>Benders-all-cuts</td>
</tr>
<tr>
<td>------------------</td>
<td>-------</td>
<td>-----------------</td>
<td>----------</td>
<td>-----------------</td>
</tr>
<tr>
<td></td>
<td>Obj</td>
<td>Gap (%)</td>
<td>CPU (sec)</td>
<td>Obj</td>
</tr>
<tr>
<td>Problem 1</td>
<td>20.00</td>
<td>0.00</td>
<td>4.67</td>
<td>20.00</td>
</tr>
<tr>
<td>Problem 2</td>
<td>20.00</td>
<td>0.00</td>
<td>2.56</td>
<td>20.00</td>
</tr>
<tr>
<td>Problem 3</td>
<td>13.25</td>
<td>0.04</td>
<td>12.78</td>
<td>13.25</td>
</tr>
<tr>
<td>Problem 4</td>
<td>42.13</td>
<td>0.00</td>
<td>30.78</td>
<td>42.13</td>
</tr>
<tr>
<td>Problem 5</td>
<td>37.46</td>
<td>0.00</td>
<td>693.25</td>
<td>37.46</td>
</tr>
<tr>
<td>Problem 6</td>
<td>18.15</td>
<td>0.00</td>
<td>221.76</td>
<td>18.15</td>
</tr>
<tr>
<td>Problem 7</td>
<td>20.00</td>
<td>0.00</td>
<td>6.93</td>
<td>20.00</td>
</tr>
<tr>
<td>Problem 8</td>
<td>20.00</td>
<td>0.00</td>
<td>4.43</td>
<td>20.00</td>
</tr>
<tr>
<td>Problem 9</td>
<td>15.65</td>
<td>0.26</td>
<td>48.98</td>
<td>15.65</td>
</tr>
<tr>
<td>Problem 10</td>
<td>43.91</td>
<td>0.24</td>
<td>1800</td>
<td>43.91</td>
</tr>
<tr>
<td>Problem 11</td>
<td>41.00</td>
<td>0.00</td>
<td>51.50</td>
<td>41.00</td>
</tr>
<tr>
<td>Problem 12</td>
<td>19.20</td>
<td>0.00</td>
<td>1493.9</td>
<td>19.20</td>
</tr>
</tbody>
</table>
5.4.1.2 Case 2:

In Case 2, we solved a randomly generated 150 node network in a unit square. The links between these nodes was restricted by a predefined communication range. We also had 10 x 10 possible discrete locations for the jamming devices. The number of jamming devices is given as shown in Table 5.2, the number of flows is 100. The flows, were chosen using the random strategy mentioned before. The total power is also as shown in Table 5.2. Computations were run on four random networks of each combination, i.e., 12 random networks in total, and the computational results are shown in Table 5.6.

5.4.2 Discussion

The computational results for Case 1 as shown in Table 5.4 and Table 5.5, shows that, as the number of flows increases the total impact of jamming also increases. This is due to the fact that as the number of flows increases, there are more flows in the network that can be jammed. Another observation is that as the number of locations to locate the jamming devices increases, the jamming devices have more options to locate a jamming device, thereby increasing the jamming impact. The number of jamming devices available to jam the flows also has a significant impact on the flow-jamming attacks. As the number of jamming devices increases, the impact of a flow-jamming attack also increases. This is because the adversary has more jamming devices to place, which collectively increases the impact. Notice also that, with the increase in the power level by using both $T_1$ and $T_2$, or $T_2$ alone, the impact of jamming on the flows in the network is more than using $T_1$ alone. With higher amount of power available the jamming device can jam more flows, thereby increasing the impact of flow-jamming attacks.

From Table 5.4 and Table 5.5, by grouping all the experimental runs where all the parameters are the same except for the location, one observation is that with the increase in the number of locations the computation time also increases for both the CMU and MIT networks, except for experimental runs 6 and 12 in CMU and experimental runs 5 and 11 in MIT, where the 100 location problem was solved faster than the 64 location problem. This anomaly can be attributed to the fact that the source and destination were randomly chosen. The computation time for CMU on the whole is higher than the MIT network. This is likely because of the differences in topology between the two networks.
Figure 5.7 shows the comparison of both CMU and MIT networks for each of the problem instances in terms of the total fraction of flows jammed to the number of locations. The MIT topology makes it more vulnerable to jamming attacks as compared to CMU, a point that is clear from the higher objective values of MIT as compared to CMU.
<table>
<thead>
<tr>
<th>Run</th>
<th>#Locations</th>
<th>T1</th>
<th>T2</th>
<th># Flows</th>
<th>Total Power</th>
<th>Obj Val</th>
<th>Gap (%)</th>
<th>CPU (sec)</th>
<th>Obj Val</th>
<th>Gap (%)</th>
<th>CPU (sec)</th>
<th>Iter</th>
<th>Obj Val</th>
<th>Gap (%)</th>
<th>CPU (sec)</th>
<th>Iter</th>
<th>Obj Val</th>
<th>Gap (%)</th>
<th>CPU (sec)</th>
<th>Iter</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100</td>
<td>5</td>
<td>5</td>
<td>100</td>
<td>55</td>
<td>67.00</td>
<td>0.90</td>
<td>7200</td>
<td>63.00</td>
<td>0.20</td>
<td>1800</td>
<td>909</td>
<td>66.00</td>
<td>0.08</td>
<td>1800</td>
<td>325</td>
<td>67.00</td>
<td>0.00</td>
<td>183.98</td>
<td>28</td>
</tr>
<tr>
<td>2</td>
<td>100</td>
<td>5</td>
<td>5</td>
<td>100</td>
<td>55</td>
<td>66.00</td>
<td>0.92</td>
<td>7200</td>
<td>64.00</td>
<td>0.18</td>
<td>1800</td>
<td>904</td>
<td>64.00</td>
<td>0.00</td>
<td>1800</td>
<td>330</td>
<td>66.00</td>
<td>0.00</td>
<td>134.25</td>
<td>20</td>
</tr>
<tr>
<td>3</td>
<td>100</td>
<td>5</td>
<td>5</td>
<td>100</td>
<td>55</td>
<td>66.00</td>
<td>0.00</td>
<td>131.45</td>
<td>66.00</td>
<td>0.00</td>
<td>191.54</td>
<td>89</td>
<td>66.00</td>
<td>0.00</td>
<td>142.39</td>
<td>35</td>
<td>66.00</td>
<td>0.00</td>
<td>122.60</td>
<td>19</td>
</tr>
<tr>
<td>4</td>
<td>100</td>
<td>5</td>
<td>5</td>
<td>100</td>
<td>55</td>
<td>68.00</td>
<td>0.00</td>
<td>3631.7</td>
<td>68.00</td>
<td>0.00</td>
<td>1785.3</td>
<td>105</td>
<td>68.00</td>
<td>0.00</td>
<td>345.10</td>
<td>105</td>
<td>68.00</td>
<td>0.00</td>
<td>291.02</td>
<td>42</td>
</tr>
<tr>
<td>5</td>
<td>100</td>
<td>0</td>
<td>5</td>
<td>100</td>
<td>50</td>
<td>46.00</td>
<td>0.00</td>
<td>130.69</td>
<td>46.00</td>
<td>0.00</td>
<td>762.65</td>
<td>532</td>
<td>46.00</td>
<td>0.00</td>
<td>608.45</td>
<td>202</td>
<td>46.00</td>
<td>0.00</td>
<td>13.45</td>
<td>38</td>
</tr>
<tr>
<td>6</td>
<td>100</td>
<td>0</td>
<td>5</td>
<td>100</td>
<td>50</td>
<td>48.00</td>
<td>0.00</td>
<td>60.23</td>
<td>48.00</td>
<td>0.00</td>
<td>98.78</td>
<td>56</td>
<td>48.00</td>
<td>0.00</td>
<td>101.21</td>
<td>31</td>
<td>48.00</td>
<td>0.00</td>
<td>53.22</td>
<td>14</td>
</tr>
<tr>
<td>7</td>
<td>100</td>
<td>0</td>
<td>5</td>
<td>100</td>
<td>50</td>
<td>48.00</td>
<td>0.00</td>
<td>199.04</td>
<td>48.00</td>
<td>0.12</td>
<td>1800</td>
<td>891</td>
<td>48.00</td>
<td>0.00</td>
<td>301.11</td>
<td>139</td>
<td>48.00</td>
<td>0.00</td>
<td>39.52</td>
<td>49</td>
</tr>
<tr>
<td>8</td>
<td>100</td>
<td>0</td>
<td>5</td>
<td>100</td>
<td>50</td>
<td>43.00</td>
<td>0.00</td>
<td>226.57</td>
<td>43.00</td>
<td>0.00</td>
<td>344.67</td>
<td>218</td>
<td>43.00</td>
<td>0.00</td>
<td>278.75</td>
<td>142</td>
<td>43.00</td>
<td>0.00</td>
<td>48.36</td>
<td>67</td>
</tr>
<tr>
<td>9</td>
<td>100</td>
<td>5</td>
<td>0</td>
<td>100</td>
<td>5</td>
<td>40.00</td>
<td>0.00</td>
<td>174.43</td>
<td>40.00</td>
<td>0.00</td>
<td>326.75</td>
<td>215</td>
<td>40.00</td>
<td>0.00</td>
<td>897.33</td>
<td>102</td>
<td>40.00</td>
<td>0.00</td>
<td>43.39</td>
<td>51</td>
</tr>
<tr>
<td>10</td>
<td>100</td>
<td>5</td>
<td>0</td>
<td>100</td>
<td>5</td>
<td>38.00</td>
<td>0.00</td>
<td>88.66</td>
<td>38.00</td>
<td>0.00</td>
<td>49.37</td>
<td>73</td>
<td>38.00</td>
<td>0.00</td>
<td>53.19</td>
<td>56</td>
<td>38.00</td>
<td>0.00</td>
<td>29.45</td>
<td>28</td>
</tr>
<tr>
<td>11</td>
<td>100</td>
<td>5</td>
<td>0</td>
<td>100</td>
<td>5</td>
<td>30.00</td>
<td>0.00</td>
<td>63.56</td>
<td>30.00</td>
<td>0.00</td>
<td>602.19</td>
<td>69</td>
<td>30.00</td>
<td>0.00</td>
<td>59.55</td>
<td>19</td>
<td>30.00</td>
<td>0.00</td>
<td>34.28</td>
<td>11</td>
</tr>
<tr>
<td>12</td>
<td>100</td>
<td>5</td>
<td>0</td>
<td>100</td>
<td>5</td>
<td>36.00</td>
<td>0.00</td>
<td>79.92</td>
<td>36.00</td>
<td>0.00</td>
<td>112.88</td>
<td>88</td>
<td>36.00</td>
<td>0.00</td>
<td>53.77</td>
<td>51</td>
<td>36.00</td>
<td>0.00</td>
<td>33.89</td>
<td>25</td>
</tr>
</tbody>
</table>
Table 5.4 and Table 5.5 show that with an increase in power the average impact of jamming increases. This is true for both CMU and MIT. So, providing the jamming devices with more power can provide a significant increase in the impact of the jamming attacks.

Table 5.6 shows computational results for Case 2 with random networks containing 150 nodes, 100 locations, 100 flows, and jamming devices as shown in Table 5.2. It is apparent that the Benders decomposition with all the acceleration techniques provided in this paper is much faster than CPLEX in most of the cases. Since each of the problem instances presented were randomly generated and have different run times, it should be noted that the jamming impact in the flow-jamming attacks depends not only the number of locations, number of flows, number of jamming devices, and amount of power available, but, also on the topology of the network.

Figure 5.8 shows the effect of network topology on the computation time for the random networks. Combination 1 is experimental runs 1 through 4, which have the same parameters but with a random topology. Combinations 2 and 3 are experimental runs 5-8 and 9-12, respectively, which have random topology. It is observed that even with the same parameters each of the combinations show variation in their computational
times. Therefore, it can be concluded that the topology of the network likely plays a significant role in flow-jamming attacks.

Figure 5.8

Effect of network topology on computational time-Random

5.5 Conclusion

This paper studies the impact of jamming device placement problem for flow-jamming attacks on wireless networks. A MIP formulation for the flow-jamming attacks was developed to determine the optimal jamming device location in order to maximize the impact of flow-jamming attacks.

Since CPLEX could not solve the problem in a reasonable amount of time we used a standard Benders decomposition algorithm to solve the problem. Due to the slow convergence of standard Benders decomposition algorithm, acceleration techniques to speed up the convergence are provided. Computational results show that the accelerated Benders decomposition algorithm can be used to solve realistic instances of large problems in reasonable time. By using two realistic networks CMU and MIT and 12 random network instances through computational experiments were conducted to test the model and draw useful insights. Based
on the results, optimally locating jamming devices has a major effect on flow-jamming attacks as compared to the random jamming device locations studied previously in the literature.

From the experimental results, it is apparent that different parameters, such as the number of jamming device locations, number of jamming devices, number of flows, and the amount of power available at each jamming device, play a very important role in the flow-jamming attacks. Another inference is that network topology plays a very significant role on the impact of jamming and the computational time.

For future research, a detailed study on finding network topologies that are vulnerable to jamming attacks should be considered. Since this paper concentrates on the attacker’s perceptive a mathematical programming model that incorporates the defenders strategies along with the attacker’s strategies should also be developed for the flow-jamming attacks. The defender’s strategies objective could minimize the impact of flow-jamming attacks, and a strategy to achieve this goal could be re-routing the packets through the network. This problem could be formulated as a bi-level attacker-defender problem.
CHAPTER 6
CONCLUSION AND FUTURE WORK

6.1 Conclusion

Wireless network security is an important area of research and concern for military and disaster responders. In this dissertation, we study one such problem called jamming attacks in wireless network security. We start the dissertation with a tutorial aimed at helping interested researchers, specifically, the operations research community to better understand jamming attacks. In this tutorial, we provide basic definitions and mathematical programming models studied in literature.

We provide a taxonomic survey of papers in literature and classify the papers into various categories such as types of wireless networks, problem perspective from an attacker, defender or both point of view, and solution methodology. Further, we identify new areas of research, which might provide new areas of research for the operations research community.

In the next chapter we provide a bi-level, attacker-defender, mathematical programming model. In this chapter, we study the impact of jammer placement on the throughput of the network and the impact of increasing the number of communication channels on the throughput of the network. The attacker aims to minimize the throughput of the network and the defender tries to increase the throughput of the network by playing a mixed-strategy Nash equilibrium game. We show that for smaller networks even two jammers can have a significant impact on the throughput. We also show that increasing the the number of communication channels helps the defender by providing alternate routes for communication.

Finally, we provide a mixed integer programming model for a specific type of jamming attack called flow-jamming attacks. In this chapter, we study the impact of optimally placing jammers on the flow in wireless networks. Since, CPLEX could not solve the problem in reasonable amount of time we provide a
Benders decomposition technique with some acceleration techniques. We solve the problem on two realistic networks and 12 random networks topologies. We show that optimally locating jamming devices can increase the impact of the attack on the network. We also show that the computation time and the impact on the flow in the network also depends on the topology of the network itself.

6.2 Future Work

For the future research developing stochastic models for flow-jamming attacks with uncertainty of attacking effects, and the attacker’s knowledge about the topology of the network will be interesting. Incorporating defense strategies and developing attacker-defender models for flow-jamming attacks should be considered. An example of defense strategy could be dynamically rerouting the data in the network, if a particular link is jammed. A study of different network topologies and the impact of flow-jamming attacks on them might be considered.

Further, improving the solution time by adding more acceleration techniques to the Benders decomposition might be considered. Other solution methodologies like Lagrangian relaxation and L-shape should be implemented to find quicker solutions. For larger networks finding efficient heuristic solutions should also be considered.
REFERENCES


[105] Y. E. Sagduyu, R. Berry, and A. Ephremides, “MAC games for distributed wireless network security with incomplete information of selfish and malicious user types,” International Conference on Game Theory for Networks (GameNets). 2009, pp. 130–139, IEEE.


125


