

**SECURITY IN WIRELESS SENSOR NETWORKS EMPLOYING MACGSP6**

by

**Yuttasart Nitipaichit**

B.E. in Electrical Engineering, Chiang Mai University, Thailand, 1996

M.S. in Electrical Engineering, University of Colorado at Boulder, 1999

Submitted to the Graduate Faculty of  
The School of Information Sciences in partial fulfillment  
of the requirements for the degree of  
Doctor of Philosophy

University of Pittsburgh

2010

UNIVERSITY OF PITTSBURGH  
SCHOOL OF INFORMATION SCIENCES

This dissertation was presented

by

Yuttasart Nitipaichit

It was defended on

December 9th, 2010

and approved by

Dr. Richard Thompson, Professor, Telecommunications, SIS

Dr. Prashant Krishnamurthy, Associate Professor, Telecommunications, SIS

Dr. Vladimir Zadorozhny, Associate Professor, Information Science, SIS

Dr. Piervincenzo Rizzo, Assistant Professor, ENGR

Dissertation Advisor: Dr. Joseph Kabara, Assistant Professor, SIS

Copyright © by Yuttasart Nitipaichit

2010

## **SECURITY IN WIRELESS SENSOR NETWORKS EMPLOYING MACGSP6**

Yuttasart Nitipaichit, MSEE

University of Pittsburgh, 2010

Wireless Sensor Networks (WSNs) have unique characteristics which constrain them; including small energy stores, limited computation, and short range communication capability. Most traditional security algorithms use cryptographic primitives such as Public-key cryptography and are not optimized for energy usage. Employing these algorithms for the security of WSNs is often not practical. At the same time, the need for security in WSNs is unavoidable. Applications such as military, medical care, structural monitoring, and surveillance systems require information security in the network. As current security mechanisms for WSNs are not sufficient, development of new security schemes for WSNs is necessary. New security schemes may be able to take advantage of the unique properties of WSNs, such as the large numbers of nodes typical in these networks to mitigate the need for cryptographic algorithms and key distribution and management. However, taking advantage of these properties must be done in an energy efficient manner. The research examines how the redundancy in WSNs can provide some security elements. The research shows how multiple random delivery paths (MRDPs) can provide data integrity for WSNs. Second, the research employs multiple sinks to increase the total number of duplicate packets received by sinks, allowing sink voting to mitigate the packet discard rate issue of a WSN with a single sink. Third, the research examines the effectiveness of using multiple random paths in maintaining data confidentiality in WSNs. Last, the research examines the use of a rate limit to cope with packet flooding attacks in WSNs.

## TABLE OF CONTENTS

<b>PREFACE.....</b>	<b>XIX</b>
<b>1.0 INTRODUCTION.....</b>	<b>1</b>
<b>1.1 MOTIVATION .....</b>	<b>2</b>
<b>1.2 PROBLEM STATEMENT .....</b>	<b>6</b>
<b>2.0 BACKGROUND: OVERVIEW OF WSNS.....</b>	<b>10</b>
<b>2.1 WSN MAC PROTOCOLS.....</b>	<b>12</b>
<b>2.1.1 Contention-based MAC protocols.....</b>	<b>12</b>
<b>2.1.2 Schedule-based MAC protocols .....</b>	<b>14</b>
<b>2.2 WSN ROUTING PROTOCOLS.....</b>	<b>15</b>
<b>2.2.1 Routing protocols based on network structure.....</b>	<b>16</b>
<b>2.2.2 Routing protocols based on protocol operations .....</b>	<b>17</b>
<b>2.3 ENHANCED MAC PROTOCOL FOR GSP.....</b>	<b>20</b>
<b>2.3.1 Former MAC protocols for GSP .....</b>	<b>20</b>
<b>2.3.2 MACGSP version 6 .....</b>	<b>20</b>
<b>2.3.2.1 Quiescent periods .....</b>	<b>21</b>
<b>2.3.2.2 Duty cycle.....</b>	<b>21</b>
<b>2.3.2.3 MACGSP version 6 algorithm.....</b>	<b>22</b>
<b>2.3.3 Summary .....</b>	<b>23</b>

<b>3.0</b>	<b>BACKGROUND: WIRELESS SENSOR NETWORK SECURITY .....</b>	<b>24</b>
<b>3.1</b>	<b>WIRELESS SECURITY ISSUES .....</b>	<b>25</b>
<b>3.1.1</b>	<b>Authentication.....</b>	<b>25</b>
<b>3.1.2</b>	<b>Confidentiality .....</b>	<b>26</b>
<b>3.1.3</b>	<b>Data integrity .....</b>	<b>28</b>
<b>3.1.4</b>	<b>Availability .....</b>	<b>29</b>
<b>3.1.5</b>	<b>Key establishment and distribution .....</b>	<b>29</b>
<b>3.2</b>	<b>SECURITY THREATS AND ATTACKS IN WSN.....</b>	<b>30</b>
<b>3.2.1</b>	<b>Eavesdropping .....</b>	<b>30</b>
<b>3.2.2</b>	<b>Node subversion / node identity impersonation.....</b>	<b>31</b>
<b>3.2.3</b>	<b>Malicious code injection and message modification.....</b>	<b>32</b>
<b>3.2.4</b>	<b>Denial of service attacks.....</b>	<b>32</b>
<b>3.2.5</b>	<b>Sybil attacks .....</b>	<b>34</b>
	<b>3.2.5.1 MACGSP with Sybil attacks.....</b>	<b>34</b>
<b>3.2.6</b>	<b>Sinkhole and wormhole attacks.....</b>	<b>35</b>
	<b>3.2.6.1 MACGSP with Sinkhole attacks.....</b>	<b>36</b>
<b>3.3</b>	<b>WSN SECURITY REQUIREMENTS.....</b>	<b>37</b>
<b>3.3.1</b>	<b>Confidentiality .....</b>	<b>37</b>
<b>3.3.2</b>	<b>Authentication.....</b>	<b>38</b>
<b>3.3.3</b>	<b>Data integrity .....</b>	<b>39</b>
<b>3.3.4</b>	<b>Availability .....</b>	<b>39</b>
<b>3.4</b>	<b>PREVIOUS RESEARCH OF SECURITY TECHNIQUES EMPLOYING MULTIPLE PATHS .....</b>	<b>39</b>

<b>4.0</b>	<b>RESULTS FOR WSNS EMPLOYING MRDPS .....</b>	<b>42</b>
<b>4.1</b>	<b>VERIFICATION OF MULTIPLE RANDOM DELIVERY PATHS.....</b>	<b>42</b>
<b>4.1.1</b>	<b>Average number of successful delivery paths and disjoint ratio.....</b>	<b>44</b>
<b>4.1.1.1</b>	<b>Packet walkthrough analysis.....</b>	<b>45</b>
<b>4.1.2</b>	<b>Packet delivery time .....</b>	<b>55</b>
<b>4.1.2.1</b>	<b>Graph theory analysis.....</b>	<b>56</b>
<b>4.1.2.2</b>	<b>Probability distribution function of first packet delivery time.....</b>	<b>59</b>
<b>4.1.3</b>	<b>Network throughput.....</b>	<b>61</b>
<b>4.1.4</b>	<b>Data exposure.....</b>	<b>64</b>
<b>4.1.5</b>	<b>Packet reception probability as a function of source and sink locations..</b>	<b>65</b>
<b>4.2</b>	<b>INTRINSIC SECURITY OF A WSN EMPLOYING MRDPS.....</b>	<b>72</b>
<b>4.2.1</b>	<b>SECURITY THREATS AND ATTACK MODELS .....</b>	<b>73</b>
<b>4.2.1.1</b>	<b>Integrity threats.....</b>	<b>73</b>
<b>(a)</b>	<b>Message modification attacks.....</b>	<b>73</b>
<b>(b)</b>	<b>Fault data injection attacks .....</b>	<b>74</b>
<b>4.2.1.2</b>	<b>Availability threats.....</b>	<b>74</b>
<b>(a)</b>	<b>Jamming attacks.....</b>	<b>75</b>
<b>(b)</b>	<b>Packet flooding attacks.....</b>	<b>75</b>
<b>4.2.1.3</b>	<b>Confidentiality threats.....</b>	<b>76</b>
<b>(a)</b>	<b>Eavesdropping attacks .....</b>	<b>76</b>
<b>4.2.2</b>	<b>Message modification attacks .....</b>	<b>76</b>
<b>4.2.2.1</b>	<b>Increasing numbers of attacking nodes generating message modification attacks.....</b>	<b>80</b>

4.2.2.2	Impact of attacker location on attack effectiveness .....	83
4.2.3	Fault data injection attacks .....	86
4.2.3.1	Increasing numbers of attacking nodes generating fault data injection attacks .....	89
4.2.3.2	Impact of attacker location on attack effectiveness .....	92
4.2.4	Node failure and jamming attacks .....	95
4.2.5	Packet flooding attacks .....	100
4.2.6	Eavesdropping attacks .....	104
4.2.7	Security and energy trade off .....	106
4.2.8	Conclusion .....	107
5.0	<b>RESULTS FOR WSNS EMPLOYING MRDPS WITH MULTIPLE SINKS...</b>	<b>108</b>
5.1	<b>MULTIPLE SINKS .....</b>	<b>108</b>
5.1.1	Packet reception probability for a WSN with three sinks .....	109
5.1.1.1	Packet reception probability at various sink locations.....	111
5.1.2	Integrity threats .....	113
5.1.2.1	Message modification attacks .....	113
5.1.2.2	Impact of attacker location on attack effectiveness .....	115
5.1.2.3	Increasing the number of nodes generating message modification attacks	119
5.1.3	Fault data injection attacks .....	122
5.1.3.1	Impact of attacker location on attack effectiveness .....	125
5.1.3.2	Increasing number of nodes generating a fault data injection attacks	129



5.1.4	Availability threats .....	132
5.1.4.1	Jamming attacks .....	132
5.2	QUIESCENT PERIODS AND RATE LIMITING AGAINST DENIAL OF SERVICE ATTACKS .....	134
5.3	DATA SEGMENTATION .....	137
6.0	CONCLUSION AND FUTURE WORK .....	139
6.1	CONCLUSION .....	139
6.2	FUTURE WORK.....	145
	BIBLIOGRAPHY .....	148

## LIST OF TABLES

Table 1. DoS attacks and their countermeasures classified at different network layers.....	33
Table 2. Probability table of all possible routes of a 4-node-square-grid WSN.....	47
Table 3. Probability table of all possible routes of a 9-node-square-grid WSN.....	50

## LIST OF FIGURES

Figure 1. Smart dust mote.....	1
Figure 2. Wireless sensor network architecture.....	10
Figure 3. a. An example of a random topology wireless sensor network,.....	11
Figure 4. a. An example of a star topology, b. An example of a peer-to-peer topology in LR-WPAN.....	13
Figure 5. The operation of GSP nodes and their states over time.....	19
Figure 6. Duty Cycle of MACGSP.....	21
Figure 7. MACGSP version 6's node operation sequence diagram. ....	22
Figure 8. Challenge-Response basic operation.....	25
Figure 9. Data authentication using Message Authentication Codes .....	26
Figure 10. Message Integrity Codes and Message Authentication Codes for data integrity .....	28
Figure 11. a. An example of a sinkhole attack, b. An example of a wormhole attack. ....	36
Figure 12. Examples of multiple delivery paths for a 100 square grid sensor network. ....	43
Figure 13. The average number of successful delivery paths vs. disjoint ratio of a 100-node-square grid WSN with 90% C.I .....	45
Figure 14. A 4-node-square-grid WSN.....	46

Figure 15. Packet reception probability of a 4-node-square-grid WSN compared between analytical and simulation approaches. ....	47
Figure 16. 9-node-square-grid network with source at the bottom left corner and sink at the top right corner.....	48
Figure 17. An example of a detour route in 9-node-square-grid network .....	48
Figure 18. 16-node-square-grid network with source in the middle and sink at the top right corner. ....	54
Figure 19. A simple finite square-grid graph representation of a square-grid network.....	57
Figure 20. Probability distribution function of packet delivery time of 900-node-square-grid network with source at coordinate (10, 10), sink at coordinates (20, 20), and $p_{gsp} = 0.1$ . ....	60
Figure 21. Probability distribution function of first packet delivery time of 16-node-square-grid network with source in the middle, sink at the top right corner, and $p_{gsp} = 0.1$ .....	61
Figure 22. Examples of blackout spreading with perfect capture effect and $p_{gsp} = 0$ .....	62
Figure 23. Average transmit time. ....	63
Figure 24. Data penetration of nodes in WSNs employing MACGSP6 when the source node is located in the middle of a 121- node-square-grid WSN. ....	65
Figure 25. 100-node-square-grid network with the source at (2,2) and sink at (6,6). ....	66
Figure 26. The packet reception probability of 100-node-square-grid network with alternative locations of source and sink.....	67
Figure 27 The average number of successful delivery paths of 100-node-square-grid network with alternative locations of source and sink.....	67
Figure 28. The disjoint ratio of 100-node-square-grid network with alternative locations of source and sink .....	68

Figure 29. The node acquisition of successful routing paths.....	69
Figure 30. 900-node-square grid topology.....	70
Figure 31. Packet reception probability of the sink as a function of distances between the source and the sink. ....	71
Figure 32. Packet reception probability of the sink compared between the location in the middle and near edge. ....	72
Figure 33. Legitimate packet acceptance rate of WSNs under a message modification attack....	78
Figure 34. Packet discard rate of a 900-node-square-grid WSN under a message modification attack.....	79
Figure 35. Probability of the sink accepting packets in a 900-node-square-grid WSN under a message modification attack. ....	79
Figure 36. Probability of the sink accepting modified packets in a 900-node-square-grid WSN under a message modification attack. ....	80
Figure 37. Legitimate packet acceptance rate of a 900-node-square-grid WSN under a message modification attack compared with 1%, 10% and 20% compromised nodes.....	81
Figure 38. Packet discard rate of a 900-node-square-grid WSN under a message modification attack compared with 1%, 10% and 20% compromised nodes. ....	82
Figure 39. Probability of the sink accepting packets in a 900-node-square-grid WSN under a message modification attack compared with 1%, 10% and 20% compromised nodes. ....	82
Figure 40. Probability of the sink accepting modified packets in a 900-node-square-grid WSN under a message modification attack compared with 1%, 10% and 20% compromised nodes. ..	83
Figure 41. Legitimate packet acceptance rate of a 900-node-square-grid WSN under a message modification attack as a function of attacker location. ....	84

Figure 42. Packet discard rate of a 900-node-square-grid WSN under a message modification attack as a function of attacker location.....	85
Figure 43. Probability of the sink accepting packets in a 900-node-square-grid WSN under a message modification attack as a function of attacker location.....	85
Figure 44. Probability of the sink accepting modified packets in a 900-node-square-grid WSN under a message modification attack as a function of attacker location.....	86
Figure 45. Legitimate packet acceptance rate of WSNs under a fault data injection attack.....	87
Figure 46. Packet discard rate of a 900-node-square-grid WSN under a fault data injection attack. ....	88
Figure 47. Probability of the sink accepting packets in a 900-node-square-grid WSN under a fault data injection attack.....	88
Figure 48. Probability of the sink accepting fault-data packets in a 900-node-square-grid WSN under a fault data injection attack. ....	89
Figure 49. Packet discard rate of a 900-node-square-grid WSN under a fault data injection attack compared with 1%, 10% and 20% compromised nodes.....	90
Figure 50. Probability of the sink accepting packets in a 900-node-square-grid WSN under a fault data injection attack compared with 1%, 10% and 20% compromised nodes. ....	91
Figure 51. Probability of the sink accepting fault-data packets in a 900-node-square-grid WSN under a fault data injection attack compared with 1%, 10% and 20% compromised nodes. ....	91
Figure 52. Legitimate packet acceptance rate of a 900-node-square-grid WSN under a fault data injection attack compared with 1%, 10% and 20% compromised nodes. ....	92
Figure 53. Legitimate packet acceptance rate of a 900-node-square-grid WSN under a fault data injection attack as a function of attacker location.....	93

Figure 54. Packet discard rate of a 900-node-square-grid WSN under a fault data injection attack as a function of attacker location. ....	94
Figure 55. Probability of the sink accepting packets in a 900-node-square-grid WSN under a fault data injection attack as a function of attacker location.....	94
Figure 56. Probability of the sink accepting fault-data packets in a 900-node-square-grid WSN under a fault data injection attack as a function of attacker location.....	95
Figure 57. Packet reception probability of a 100-node-square-grid WSN under 5 and 10 jamming attacks. ....	97
Figure 58. Packet reception probability of a 100-node-square-grid WSN under multiple jamming attacks. ....	97
Figure 59. Average number of routes of a 100-node-square-grid WSN under multiple jamming attacks. ....	98
Figure 60. Disjoint ratio of a 100-node-square-grid WSN under multiple jamming attacks. ....	99
Figure 61. Packet reception probability of a 900-node-square-grid network under multiple jamming attacks. ....	99
Figure 62. Energy usage per gossip period compared between normal operation and when a 100-square-grid network under packet flooding attack.....	101
Figure 63. Energy usage per gossip period compared between normal operation and when a 900-square-grid network under packet flooding attack.....	102
Figure 64. Probability of the sink accepting packets compared between normal operation and when network under packet flooding attack. ....	102
Figure 65. Energy usage vs. time compared between normal operation and when network under packet flooding attack. ....	103

Figure 66. Data exposure ratio of each node to a packet sent from the source node.....	106
Figure 67. A 900-node-square-grid WSN with three sinks. ....	110
Figure 68. Packet reception probability of a 900-node-square-grid WSN compared between a network with one sink and three sinks.....	111
Figure 69. Packet reception probability of a 900-node-square-grid WSN with three sinks compared between sinks far apart and sinks close together. ....	112
Figure 70. Legitimate packet acceptance rate of a 900-node-square-grid WSN under a message modification attack compared between a network with one sink and three sinks.....	113
Figure 71. Packet discard rate of a 900-node-square-grid WSN under a message modification attack compared between a network with one sink and three sinks. ....	114
Figure 72. Probability of Sink1 accepting packets in a 900-node-square-grid WSN under a message modification attack compared between a network with one sink and three sinks. ....	114
Figure 73. Probability of Sink1 accepting modified packets in a 900-node-square-grid WSNs under a message modification attack compared between a network with one sink and three sinks. ....	115
Figure 74. Legitimate packet acceptance rate of 900-node-square-grid WSNs under a message modification attack as a function of attacker locations from Sink1.....	116
Figure 75. Packet discard rate of 900-node-square-grid WSNs under a message modification attack as a function of attacker locations from Sink1.....	117
Figure 76. Probability of Sink1 accepting packets of 900-node-square-grid WSNs under a message modification attack as a function of attacker locations from Sink1.....	118
Figure 77. Probability of Sink1 accepting modified packets of 900-node-square-grid WSNs under a message modification attack as a function of attacker locations from Sink1.....	119



Figure 78. Legitimate packet acceptance rate of 900-node-square-grid WSNs under multiple message modification attacks compared between network with one sink and three sinks..... 120

Figure 79. Packet discard rate of 900-node-square-grid WSNs under multiple message modification attacks compared between network with one sink and three sinks. .... 120

Figure 80. Probability of Sink1 accepting packets of 900-node-square-grid WSNs under multiple message modification attacks compared between network with one sink and three sinks..... 121

Figure 81. Probability of Sink1 accepting modified packets of 900-node-square-grid WSNs under multiple message modification attacks compared between network with one sink and three sinks. .... 122

Figure 82. Legitimate packet acceptance rate of 900-node-square-grid WSNs under a fault data injection attack compared between network with one sink and three sinks. .... 123

Figure 83. Packet discard rate of 900-node-square-grid WSNs under a fault data injection attack compared between network with one sink and three sinks..... 123

Figure 84. Probability of Sink1 accepting packets of 900-node-square-grid WSNs under a fault data injection attack compared between network with one sink and three sinks..... 124

Figure 85. Probability of Sink1 accepting fault-data packets of 900-node-square-grid WSNs under a fault data injection attack compared between network with one sink and three sinks. . 125

Figure 86. Legitimate packet acceptance rate of 900-node-square-grid WSNs under a fault data injection attack as a function of attacker locations from Sink1..... 126

Figure 87. Packet discard rate of 900-node-square-grid WSNs under a fault data injection attack as a function of attacker locations from Sink1..... 127

Figure 88. Probability of Sink1 accepting packets of 900-node-square-grid WSNs under a fault data injection attack as a function of attacker locations from Sink1. .... 128

Figure 89. Probability of Sink1 accepting fault-data packets of 900-node-square-grid WSNs under a fault data injection attack as a function of attacker locations from Sink1. ....	129
Figure 90. Packet discard rate of 900-node-square-grid WSNs under fault data injection attacks compared between network with one sink and three sinks.....	130
Figure 91. Probability of Sink1 accepting packets of 900-node-square-grid WSNs under fault data injection attacks compared between network with one sink and three sinks. ....	130
Figure 92. Probability of Sink1 accepting fault-data packets of 900-node-square-grid WSNs under fault data injection attacks compared between network with one sink and three sinks....	131
Figure 93. Legitimate packet acceptance rate of 900-node-square-grid WSNs under fault data injection attacks compared between network with one sink and three sinks.....	132
Figure 94. Packet reception probability of 900-node-square-grid WSNs with one sink and three sinks under jamming attacks.....	133
Figure 95. Packet reception probability in a 900-node-square-grid WSN employing rate limiting as a function of thresholds. ....	135
Figure 96. Average energy per gossip period of a 900-node-square-grid WSN employing rate limiting as a function of thresholds.....	136
Figure 97. Average time until all packet leave the network of a 900-node-square-grid WSN employing rate limiting under packet flooding attacks as a function of thresholds. ....	137

## **PREFACE**

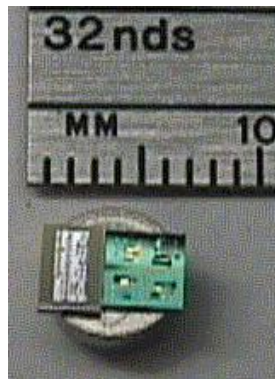
I would like to express my deepest gratitude to my advisor, Dr. Joseph Kabara, who constantly inspires, encourages, and guides me through the problems in my research. His wisdom and kindness have motivated me all these years. This dissertation would not be successful without his inspiration, encouragement, and support. I would also like to express my gratitude to the members of my PhD Dissertation Committee, Dr. Richard Thompson, Dr. Prashant Krishnamurthy, Dr. Vladimir Zadorozhny, and Dr. Piervincenzo Rizzo for their valuable suggestions and guidance that help improve the quality of this research.

I would like to thank CAT Telecom Public Co., Ltd for sponsoring me during my study at the University of Pittsburgh. And I would also like to give my special thanks to Dr. Maria Calle for her valuable ideas for me to start this research and for her moral support encouraging me to get through all obstacles in this research.

Most importantly, I would like to dedicate this dissertation to my parents, Suparut and Thongchai, who always gave me their unconditional love and support that made me who I am today. And, I am most grateful to my sisters, Numpetch and Rodchared, my aunts, Sukarnda and Supraneer, and the rest of my family members for their invaluable love and support. Lastly, I would like to thank my wife, Supaluck, for her continual love, support, and understanding. With all the love and support from my family and friends, I can make it through today. You all are parts of my success.

## 1.0 INTRODUCTION

A Wireless Sensor Network (WSN) has unique characteristics because it is constructed from low cost devices with limited computational power, communication capability and energy stores. Applications of WSNs include wildlife monitoring [1], structural monitoring [2], medical care [3], surveillance [4, 5], as well as military applications [6]. WSNs must operate autonomously and be easy to deploy. Recent technology in electronic devices has enabled the development of advanced wireless sensor nodes that have smaller size, lower power usage, and even higher computational capability. However, these increased capabilities will lead to increased demands by users. Figure 1 shows an example of a wireless sensor node: a smart dust mote [7]. However, even with advanced sensor nodes, the unique characteristics limit the design of WSNs.



**Figure 1.** Smart dust mote.

Most wireless systems are more sensitive to security issues than their wired counterparts, due to the broadcast nature of wireless communications channels. Security protocols have been proposed and implemented for wireless networks, including the Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) for Wireless LAN (WLAN). However, lack of appropriate security design will likely lead to security breaches similar to the ones already experienced in other wireless networks. As an example, in the early Analog Mobile Phone System (AMPS) there was no privacy or confidentiality service in the standard which lead to the problem of cellular phone clones and financial loss for wireless service providers [8]. The first version of the WEP protocol in WLANs is another example of a protocol with an improper security design which was broken easily by a simple script such as WEPCrack downloadable from the Internet [9].

## 1.1 MOTIVATION

WSNs have gained the attention of the research community because their diverse applications require solutions in which different variable(s) must be optimized. Security of WSNs includes data confidentiality, data integrity, and availability services. However, different applications require different security services. As an example, applications such as surveillance and environmental monitoring require data integrity and availability while applications such as medical care and military applications additionally require confidentiality. Security protocols for WSNs such as TinySec [10] and SPINS [11], provide data confidentiality and data integrity services. However, they do not address service availability and other WSN security threats, such as denial of service (DoS) threat. IEEE 802.15.4 has been proposed for some WSNs, however it

too has encountered problems such as initial vector (IV) management, key management, and integrity protection as described by Sastry and Wagner [12, 13].

A traditional way of building security is to employ cryptographic primitives. Cryptographic primitives are basic cryptographic algorithms used to build computer security systems [14, 15]. Examples include Message Authentication Codes (MAC) and encryption/decryption algorithms such as Advanced Encryption Standard (AES). However, execution of these algorithms requires drawing energy from a WSN node's limited energy store. Additionally, execution in a timely fashion also requires high computation capability of sensor nodes. Using these algorithms without modification is not always practical for nodes with limited CPU power and energy store. As an example, WSN security protocols such as TinySec and SPINS use lightweight versions of cryptographic primitives to reduce energy usage. However, these protocols still require sophisticated key management and distribution algorithms and protocols. Deploying key management and distribution may overly tax the resources of WSNs. As an example, a wireless sensor node has limited space for storing large or multiple keys. Keys that must be distributed over a wireless channel will need to use the nodes radio transmitter and receiver circuits, which require the most amount of energy to operate [16]. Additionally, wireless sensor nodes are usually autonomous and unattended, thus intruders can capture nodes to extract keys.

Cryptographic primitives are a necessary but not complete security solutions [17]. As current security mechanisms for WSNs are insufficient, development of new security mechanisms for WSNs continues. As new security mechanisms are developed they need to be compared against the intrinsic security provided by WSNs, so that the cost of the new mechanism can be weighed against the benefit of the increase in security. One unique feature of

WSNs is that they are assumed to be created from a very large number of tiny nodes. However, opportunities emerging from this may not be fully utilized by current WSN protocols. Defense against threats such as DoS require redundant nodes combined with nodes and protocol collaboration. New security mechanisms may take advantage of the large numbers of nodes in WSNs to strengthen security and at the same time comply with the energy and memory requirements of WSNs. A question emerges of how to make sensor nodes collaborate such that security can be strengthened apart from using cryptographic primitives alone.

Large number of sensor nodes with proper security design can reduce damage from threats like DoS. One method of exploiting redundancy from large number of sensor nodes is to use multiple paths to deliver a packet to a sink node. Multiple-path routing can be used for providing a secure communication [18, 19], providing a reliable communication [20-22], as well as load balancing [23]. Multiple paths together with data segmentation can also help provide confidentiality service [18]. Techniques such as a multipath approach for secure data delivery can be used to provide confidentiality service [18]. Protocols based on multiple paths such as INSENS (Intrusion-Tolerant Routing in Wireless Sensor Networks) are able to maintain service availability when a WSN is under DoS attacks. Since randomness can also be useful for building security, a WSN employing multiple random delivery paths (MRDPs) may be able to make WSNs even more robust to integrity threats such as message modification and fault-data injection attacks. Employing MRDPs may also help increase service availability when a WSN is under Denial of Service (DoS) attacks such as jamming attacks and packet flooding attacks.

WSNs may also need additional detection techniques to strengthen integrity as intruders can capture unattended sensor nodes, extract their secret keys, and use those nodes to launch security attacks such as message modification and fault data injection attacks. Additional

detection techniques can be useful but they must also be energy-efficient techniques. Since sensor nodes are energy constrained, adding detection mechanisms at sensor node may have limited benefit. However, the literature usually assumes a sink node to be less constrained. Implementing a sophisticated detection technique at the sinks is therefore possible.

A WSN employing MRDPs allows the sink to detect anomalies among packets received from a different path. However, the number of disjoint multiple paths can also be limited as they cannot be more than the node degree of the sink. As the number of attacks grows larger, the sink with limited disjoint multiple paths may not be able to detect the attacks. Moreover, even if the WSN can detect anomalies, a large number of attacks can reduce service availability as the sink discards all suspicious packets including legitimate packets. Using multiple sinks can increase the total number of multiple paths or the number of packets arriving at the sinks increasing detection capability of the sinks and allowing implementation of sink voting to reduce the number of discarded packets. Consequently, increasing number of sinks may be able to improve integrity and service availability of WSNs.

One problem in defending against attacks such as DoS attacks is that the security attacks may never cease. Dealing with these security attacks requires a combination of detection and containment mechanisms. Employing detection and containment mechanisms such as rate limiting can be effective against DoS attacks [24]. One can use packet receiving counters as a simple detection technique for packet flooding attacks. The counter increases by one every time a node receives a packet and decreases by one if the node is not receiving any packets. If the attacking node is repeatedly injecting a packet the counter increases indefinitely while normal traffic increases a counter to a certain threshold. The threshold differentiates illegitimate traffic from the traffic. Rate limit threshold is defined by the maximum number of consecutive packets



a sensor node can receive (similar to the size of a leaky bucket in the traffic shaping techniques that once the bucket is full the packet is discarded). Once the counter exceed rate limit threshold, the containment technique is applied by having the sensor node stops forwarding a packet for a quiescent period. Implementing a counter in wireless sensor nodes requires only a few additional instructions. Since the majority of energy used in wireless sensor nodes comes from transmitting and receiving packets, adding a few instructions can result in only a slight increase in energy usage of wireless sensor nodes.

## **1.2 PROBLEM STATEMENT**

Gossip-based protocols inherit a multiple random delivery path from its gossiping mechanism. WSNs uses gossip-based protocols then possess multiple random delivery path property. However, the number of MRDPs is unknown and the paths may consist of non-disjoint route sets. Thus, the security from this technique can be different from a WSN employing a multiple disjoint route set. Sink voting is useful for WSNs as it discerns between legitimate and illegitimate packets. However, false positives exist as sink voting is not always correct.

One can use MRDPs for another means to provide confidentiality service from data segmentation [18]. However, all segments must not be exposed to eavesdroppers allowing them to reconstruct original data. Additionally, despite receiving an incomplete set of data segments, intruders may gain knowledge of original data through semantic security techniques. Implementation of confidentiality service through data segmentation must then consider data exposure of a WSN and semantic security issues.

As rate limiting can be implemented in an energy-efficient method by using packet receiving counters, a question emerges of how to define rate limit threshold and how to make it effective against certain types of security attacks without harming WSN applications. Too large rate limit threshold results in an ineffective detection while too low causes performance drop in WSNs. Incorporating rate limit threshold with other detection techniques may improve the effectiveness of the detection. Once a WSN detects malicious activities, it requires a containment technique to suppress the attacks.

WSN can use node backoff as a simple containment technique for packet flooding attacks. The backoff node can still be awake to keep monitoring the activities but does not forward any packets received. If all sensor nodes adhere to this scheme, all the nodes surrounding the attacking node once detected the attack must be backoff isolating the attacking node completely from the network. However, the backoff nodes also stop forwarding all packets received from either legitimate nodes or the attacking node. Consequently, the backoff nodes and the attacking node become failed nodes and the performance of a WSN can also be affected.

**The following are the objectives of this research:**

- Investigate the intrinsic security issues of a protocol providing security via MRDPs.
- Develop mechanisms to enhance data integrity, confidentiality, and availability by employing redundancy in WSNs.
- Analyze the value of protocol overhead for additional security.
- Develop performance metrics to measure WSN performance regarding security issues.

**The following are the hypotheses of this research:**

H1: large blocks of data can be divided into smaller packets, each taking a random route along the WSN. Random routes can reduce the ability of intermediate nodes intercepting and receiving the entire message.

H2: random routes can reduce the ability of intermediate nodes modifying a message.

H3: in networks with multiple sinks data integrity can increase with an increasing number of sinks, provided that each sink can distinguish between normal data and anomalous data resultant from either node failure or message modification attack(s).

H4: rate limits and back off periods on each intermediate node can mitigate damage from packet flooding attacks.

**The following are the limitations of this research:**

- The most important constraint considered in the model is security and the second is energy usage. All other constraints are considered inferior to these two.
- The research considers only a WSN with stationary nodes.
- The physical topology of the studied networks is limited to square grids.
- The capture effect has little effect on the performance of networks employing MACGSP version 6 (not difference until the factor greater than 0.3 [25]), therefore to reduce complexity, this research assumes a perfect capture effect.
- The research assumes the attack models described in section 4.2.1.

**The dissertation is organized as follows:**

Chapter 2 reviews WSN topologies and architectures and their MAC and routing protocols.

Chapter 3 reviews security concepts and discusses general security issues. This chapter also discusses security threats and attacks and security issues of WSNs.

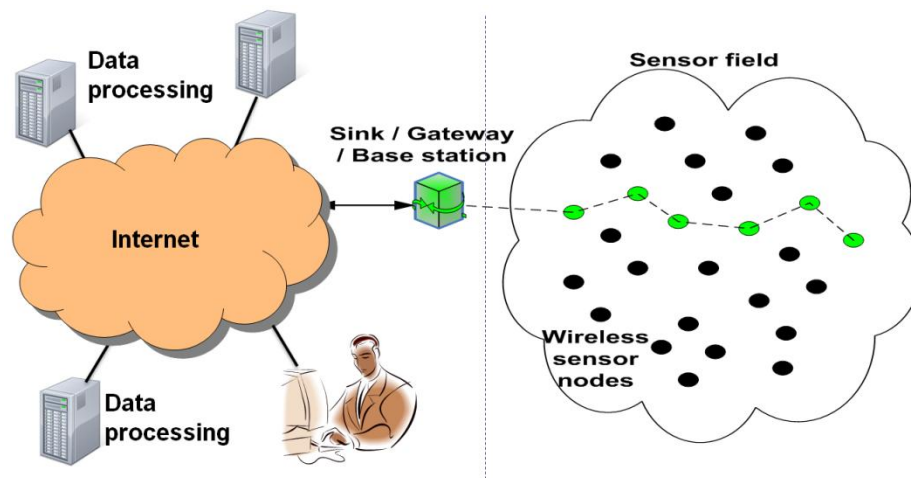
Chapter 4 analyzes security of a WSN employing MRDPs with a single sink.

Chapter 5 includes the results from WSNs with multiple sinks and rate limiting technique.

Chapter 6 contains conclusion and future works.

## 2.0 BACKGROUND: OVERVIEW OF WSNS

As shown in Figure 2, a WSN usually consists of hundreds or thousands of nodes scattered over a sensor field [6]. These nodes sometimes referred to as motes, collect their own sensed data and forward it in a multi-hop fashion to a sink, sometimes referred to as a base station or a gateway. The sink usually has high computation power, large storage, and unlimited energy store. WSNs use sink as a main data collector, a control and management, and even a key distribution center [26].

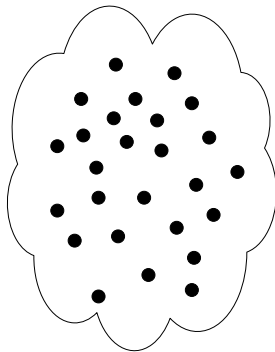


**Figure 2.** Wireless sensor network architecture.

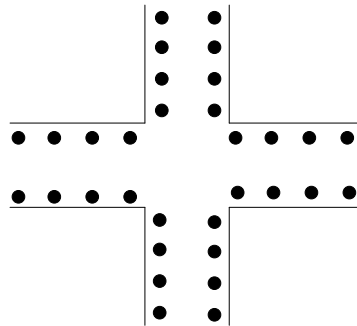
Wireless networks such as GSM and WLAN employ a wireless infrastructure network topology which allows for an infrastructure based security design [8, 27]. Unlike other wireless

networks, WSNs with random deployment may have hundreds or thousands nodes deployed throughout the sensor field. These nodes must also be capable of self-organizing where the topology may also change over the time e.g. when a sensor node dies or a new sensor node is added to the network [6].

The physical topology of WSNs includes a random topology (Figure 3A). However, WSN physical topologies can be very structured. As an example, a traffic monitoring application may deploy wireless sensor nodes along the roadside resulting in a structured physical topology as in Figure 3B.



(a) Random topology



(b) Topology for traffic monitoring application

**Figure 3. a.** An example of a random topology wireless sensor network,  
**b.** An example of a structured wireless sensor network.

Because of wide variety use of WSN applications, each different type of WSN applications requires different WSN protocol suites. As an example, applications such as temperature monitoring and chemical leak detecting have small data size and infrequent data

sending but require long lifetime and reliable sensor nodes [6]. Gossip-based WSN protocol such as MACGSP suits those characteristics as it is designed to be used in applications with small data size, low data rate, and limited resources for sensor nodes [25, 28]. Section 2.1 and 2.2 review medium access control and routing protocols for WSNs.

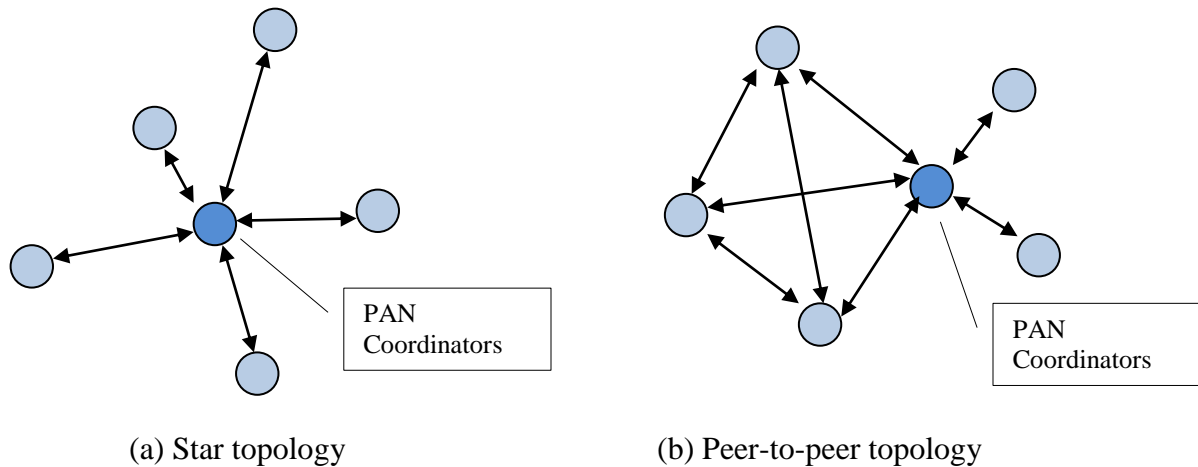
## **2.1 WSN MAC PROTOCOLS**

IEEE standard 802 defined the Medium Access Control (MAC) as a part of the Data Link Layer in the Open Systems Interconnection (OSI) reference model. MAC layer is responsible for error control, channel access control, and addressing [29]. This section explains a brief concept of MAC protocols implemented for WSNs. MAC protocols for WSNs can be classified as contention-based protocols and scheduled-based protocols.

### **2.1.1 Contention-based MAC protocols**

Contention-based MAC protocols work without schedule from central coordinator or node synchronization. One drawback of contention-based MAC protocols is that wireless sensor nodes waste their energy during idle listening if there are no transmissions [30]. Thus, contention-based MAC protocols require an efficient way to manage idle listening issues. Examples of schedule-based protocols include IEEE 802.15.4, Sensor-MAC (S-MAC) [31], WiseMAC [32, 33], etc. IEEE 802.15.4 is a standard for Wireless Medium Access Control and Physical Layer (PHY) specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs) [12]. A LR-WPAN is a simple, low-cost communication network that allows wireless connectivity in applications

with limited power and relaxed throughput requirements such as WSNs. The LR-WPAN operates in either a star topology or a peer-to-peer topology as shown in Figure 4. In the star topology, every sensor node communicates directly to a single central controller, called the PAN coordinator while sensor nodes in peer-to-peer topology can communicate directly with any other nodes in range with or without the PAN coordinator.



**Figure 4.** a. An example of a star topology, b. An example of a peer-to-peer topology in LR-WPAN

IEEE 802.15.4 [12] defines two services in the MAC sublayer: the MAC data service and the MAC management service. The MAC data service enables the transmission and reception of MAC protocol data units (MPDUs) across the PHY data service. The MAC sublayer is responsible for beacon management, channel access, guaranteed time slots (GTS) management, frame validation, acknowledged frame delivery, association, and disassociation. Additionally, the MAC sublayer provides functional description of secure mode. The MAC sublayer uses two mechanisms for channel access: contention based and contention free [12]. Contention-based access allows nodes to access the channel in a distributed fashion using a CSMA-CA backoff algorithm. Contention-free access is controlled entirely by the PAN coordinator through the use of GTSs.



Sensor-MAC (S-MAC) protocol operates in periodic sleep–listen schedules. Virtual cluster is formed among neighbors to set up a synchronized sleep-listen schedule. During listen period, a node sends data via RTS, CTS, and ACK exchanges similar to IEEE 802.11 scheme [29]. Virtual clustering maintains synchronization by periodically broadcasting SYNC packet. It is possible to have a node residing in two virtual clusters. Nodes residing in two virtual clusters wake up at the listen period of both clusters wasting their energy [34].

WiseMAC protocols decrease idle listening through non-persistent Carrier Sense Multiple Access (np-CSMA) with preamble sampling [33]. Idle listening is reduced by having all nodes in a network sleep most of the time but periodically wake up to sample the medium. The sampling period is set to be the same for every node but its relative schedule offset can be independent. Before sending each data packet, the transmitting node sends preamble sampling to inform the receiving nodes. The size of the preamble must be equal to or larger than the sampling period so the receiving nodes will not miss the preamble sampling when they wake up and sample the medium. If the receiving nodes detect the preamble sampling after they wake up, they continue to listen until they receive a data packet or the medium becomes idle again.

### **2.1.2 Schedule-based MAC protocols**

Schedule-based MAC protocols use schedules to allow nodes to receive or transmit in a shared medium without collisions similar to the techniques used in Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA). Unlike contention-based MAC protocols, schedule-based MAC protocols have no idle listening issue because sensor nodes know their schedules. However, schedule-based MAC protocols require schedule management adding overhead. Examples of schedule-based protocols include Power Efficient and Delay

Aware Medium Access Protocol (PEDAMACS) [35], Traffic-Adaptive Medium Access (TRAMA) [36], etc. PEDAMACS uses a control node or Access Point (AP) with transmission range covers all nodes similar to infrastructure mode of IEEE 802.11. PEDAMACS uses this AP for a topology learning scheduling phase. During topology learning, all nodes and APs use a MAC similar to IEEE 802.11. However, during the scheduling phase the AP broadcasts a schedule message to every node in the network so that every node can sleep, transmit, and receive according to its scheduled time slot.

TRAMA is a TDMA-based algorithm and therefore the time is slotted and all nodes are synchronized [36]. TRAMA eliminates the hidden node problem by using election algorithm for each time slot to choose one transmitter among node neighbors. To improve energy efficiency, TRAMA splits time into transmission slot and signaling slot. The signaling slot is contention-based and usually smaller than the transmission slot and is used to announce the slots a transmission node can employ to send a packet to the intended receivers. TRAMA has fewer collisions compared with contention-based protocols. However, the delay is higher than those of contention-based protocols because of its high percentage of sleep time. Moreover, the protocol requires node synchronization which can be difficult to achieve and cost more energy use.

## **2.2 WSN ROUTING PROTOCOLS**

Because of diversity in WSN applications several WSN routing protocols have been proposed. WSN routing protocols can be classified based on protocol operations or network structure [34].

### **2.2.1 Routing protocols based on network structure**

The routing based on network structure includes flat-based routing, hierarchical-based routing, and location-based routing depending on the network structure.

#### **a. Flat-based routings**

Flat-based routings usually treat each wireless sensor node equally and rely on data-centric routing requiring a query from the sink before sensor node can send the requested information to the sink. Examples of flat-based routing protocols include Sensor Protocol for Information via Negotiation (SPIN) [37], and Direct diffusion [38].

#### **b. Hierarchical-based routing**

Hierarchical-based routing are cluster-based routing methods consisting of at least two different types of wireless sensor nodes (e.g. high-energy nodes and low-energy nodes) used to form energy efficient routing in WSNs. In general, low-energy nodes collect raw data and send it to high-energy nodes while high-energy nodes or cluster heads process the collected data by performing data aggregation or compression in order to reduce the amount of information sending and then forward the processed data to the sink. Examples of hierarchical-based routing protocols include Low Energy Adaptive Clustering Hierarchy (LEACH) [39], and Power-Efficient Gathering in Sensor Information Systems (PEGASIS) [40].

#### **c. Location-based routing**

Location-based routing uses geographic information for its routing. Location based routing address sensor nodes from their locations obtained from either Receive Signal Strength Indicator (RSSI) estimation or an embedded low-power GPS. Examples of hierarchical-based routing protocols include Geographic Adaptive Fidelity (GAF) [41], Geographic and Energy Aware Routing (GEAR) [42], and SPAN [43].

### **2.2.2 Routing protocols based on protocol operations**

The routing based on protocol operations include multipath-based routing, query-based routing, negotiation-based routing, QoS-based routing, and gossip based routing protocols [34].

#### **a. Multipath-based routing**

Multipath-based routing uses multiple paths to provide reliable communication. Multiple paths increases network reliability at the expense of the increased overhead from additional paths. As an example, direct diffusion employs multiple paths to provide robustness of data delivery to the sink [38]. However, the multiple paths employed in direct diffusion are partially disjoint paths to reduce the cost of maintaining the multiple paths. An algorithm proposed by J. H. Chang and L. Tassiulas [44] uses multiple paths as a backup path and to increase the network life time by actively changing the routing path to the largest remaining energy path. The primary path remains in use until the total energy decreases below the energy of the backup path.

#### **b. Query-based routing**

Query-based routing sends information based on query request from the sink or base station. Example of routing protocols using query-based routing includes direct diffusion [38] and rumor routing protocol [45]. In directed diffusion, the base station sends interest query messages to sensor nodes. The gradients from the source to the base station are set up as the interest is propagated throughout the WSN. The node with data matching the interest sends the data back along the gradient paths. The rumor routing protocol uses a set of agents to create paths based on events they encounter, for example, when the agents find new shorter paths or more efficient paths, they adjust the paths in routing tables accordingly. A node synchronizes its events table with the agent every time it visits. Each node must maintain a list of its neighbors and an events table. Nodes can also generate an agent with a certain lifetime (as number of hops). The node

only generates a query if there is no route available. If the node does not receive a response, the node floods the network.

### **c. Negotiation-based routing**

Using flooding in routing causes unnecessary packet forwarding because nodes receive multiple copies of the same packet. Consequently, flooding often uses more energy. Negotiation-based routing protocols reduce these redundant data transmissions through negotiation. Examples of negotiation-based routing protocols include SPIN and its family protocols [37].

### **d. QoS-based routing**

QoS-based routing considers the balance between energy usage and QoS of data delivery in WSNs. Specifically the network must satisfy QoS parameters such as delay, energy, bandwidth, etc. As an example, the routing decision in Sequential Assignment Routing (SAR) depends on three parameters: packet priority, QoS on each path, and energy resources [46]. SAR also uses multiple paths and path restoration techniques for protection.

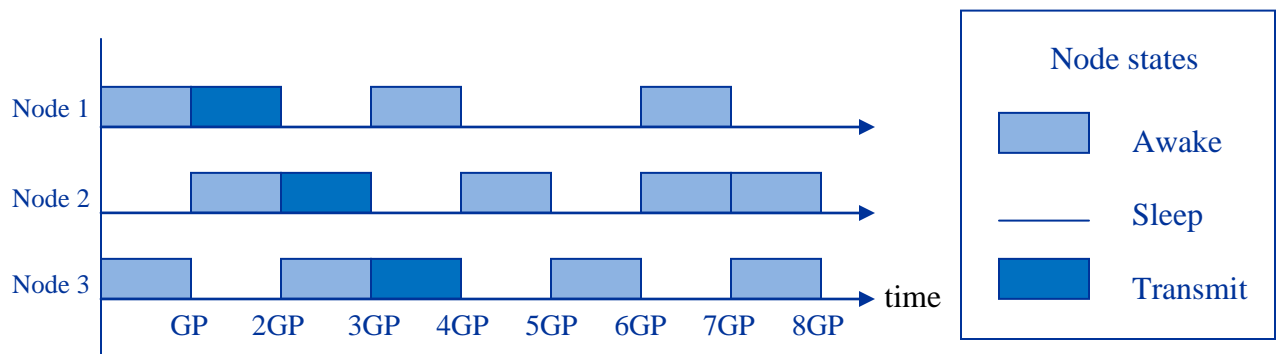
### **e. Gossip based routing protocol**

Routing protocols use flooding to send routing messages. Flooding causes unnecessary packet forwarding because a node with two or more neighbors receives multiple duplicates of the same packet. Gossip-based routing reduce unnecessarily packet forwarding by using gossiping mechanism, where each node decides to forward a packet with probability  $p$  called the gossip probability. Examples of gossip-based routing protocols include Gossip-based ad-hoc routing and Gossip-based Sleep Protocol (GSP). Gossip-based ad-hoc routing is an improved version of flooding-based routing [47]. Unlike flooding-based routing, Initial work hypothesized that given a sufficiently large network and a gossip probability  $p$  greater than a certain value, almost all the

nodes in the network can receive the message [48]. The original concept has been expanded into the Gossip Based Sleep Protocol.

Unlike Gossip-based ad-hoc routing, Gossip-based Sleep Protocol (GSP) decreases energy usage by having nodes sleep when not receiving a packet [49]. With GSP, each node decides to go in a sleep mode with gossip probability ( $p_{gsp}$ ) or to stay awake with probability ( $1 - p_{gsp}$ ). GSP operations are simple and scalable because GSP does not require routing information exchange among nodes and each individual node does not need to maintain the states of other nodes. Moreover, GSP does not require node addressing as nodes in GSP retransmit every packet received regardless of packet content, source, or destination. GSP protocol suits WSNs because of its simplicity and low overhead. However, its flooding like property limits WSN bandwidth resources shared among nodes in a WSN. Therefore, GSP is more suitable for WSN applications with low data rates for which it has been designed.

Figure 5 illustrates the operation of GSP, at the beginning of each gossip period, each node decides to go in a sleep mode by turning off its radio with probability  $p_{gsp}$  or stay awake with probability ( $1 - p_{gsp}$ ). All nodes in a sleep mode wake up at the beginning of next gossip period. All awake nodes, if receive a packet, transmit it at the beginning of the next gossip period. Nodes in GSP stay in one of three states: awake, sleep, or transmit.



**Figure 5.** The operation of GSP nodes and their states over time

## 2.3 ENHANCED MAC PROTOCOL FOR GSP

### 2.3.1 Former MAC protocols for GSP

MACGSP version 1 is the first protocol developed to enhance energy usage of GSP [25, 28]. With MACGSP version 1, the source node (a node with its own information) sleeps for two gossip periods after sending a packet. A relay node, once received a packet, retransmits the packet in the next gossip period and then sleeps for one gossip period. Nodes follow the same GSP mechanism deciding to sleep with the gossip probability  $p_{gsp}$  (or to wake up with probability  $1-p_{gsp}$ ) for all other circumstances. MACGSP version 2 operates in the same mechanism as MACGSP version 1 except that nodes wake up immediately after sleeping for their corresponding gossip periods (with MACGSP version 1, at this point, nodes must decide to sleep or wake up with  $p_{gsp}$ ) [28]. MACGSP version 2 reduces a great number of duplicates compare to both MACGSP version 1 and GSP. Consequently, it improves the total energy usage due to fewer duplicates [28]. However, despite the total energy usage improvement, the packet reception probability decreases.

### 2.3.2 MACGSP version 6

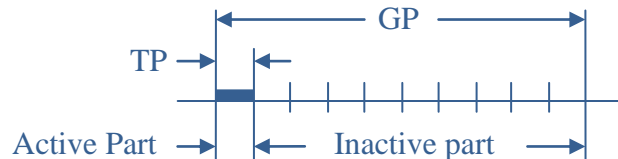
By employing quiescent periods and duty cycles, MACGSP version 6 improves total energy usage and packet reception probability of the protocol also improves up to 20% of GSP without adding overhead. Additionally, the protocol improves energy use per successfully received packet [25]. MACGSP version 3, 4, and 5 were internal development versions and never published.

### 2.3.2.1 Quiescent periods

MACGSP employs quiescent periods immediately after transmission to avoid receiving a duplicate packet [25, 28]. During quiescent periods, nodes turn off the radio, effectively discarding all incoming packets and at the same time saving more energy. MACGSP version 6 uses extended quiescent periods to improve energy efficiency. Extending the duration of the quiescent periods reduces the duplicates within the network. MACGSP version 6 uses quiescent periods of 10 gossip periods (GP) to eliminate all duplicates in the network with shorter delay. Higher values of quiescent periods do not improve much of the performance. In summary, quiescent periods improve energy usage, decrease the number of duplicates in the network, and allow for implementation of duty cycles to further reduce energy usage [25].

### 2.3.2.2 Duty cycle

In MACGSP version 6, the duration of the GP increases from 1 TP (Transmitting Period, the time it takes to transmit one packet) to 10 TPs or the length of a duty cycle. Each duty cycle is composed of active and inactive parts. As shown in Figure 6, awake nodes are active only during the first TP and sleep for all of the remaining TPs of a GP. Nodes in a sleep mode sleep for the whole GP.

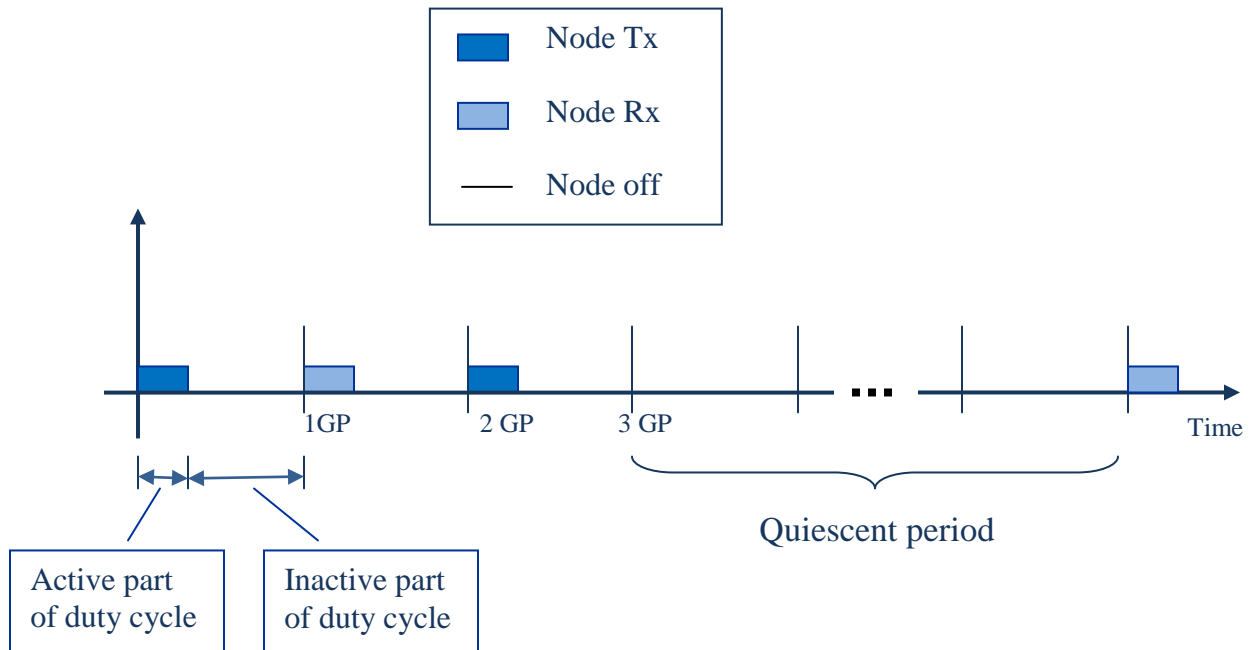


**Figure 6.** Duty Cycle of MACGSP



### 2.3.2.3 MACGSP version 6 algorithm

A Node employing MACGSP version 6 operates as depicted in the node operation sequence diagram in Figure 7. After each transmission, nodes remain on during the active part of the duty cycle and goes to sleep for the rest of their Gossip Period (GP). Then, at the beginning of next GP, the node transmitting in the previous GP checks the medium during the time it takes to receive the preamble of a packet. If the node hears the preamble, called an “Implicit ACK”, the node goes to sleep immediately for the period of time defined by the quiescent period. If the node hears nothing (no implicit ACK received), it retransmits the packet once in the next GP and sleeps for the quiescent period.



**Figure 7.** MACGSP version 6's node operation sequence diagram.

In MACGSP version 6, the waking nodes that do not receive a packet during the time it takes to receive the preamble of a packet go to sleep for the rest of the current GP and decide their state according to  $p_{gsp}$  at the beginning of the next GP. Nodes sleeping at the beginning of the previous GP as a result of  $p_{gsp}$  state (not because of a quiescent period) wake up in the next GP. In MACGSP version 6, every packet received is relayed in next GP.

### 2.3.3 Summary

Section 2.3 explains enhanced MAC protocol for GSP. MACGSP uses multiple nodes to deliver a packet to a sink node. Multiple nodes also work together as backup nodes making the protocol more robust to node failure. MACGSP mechanism also involves the gossip probability ( $p_{gsp}$ ) and there is no explicit route to the sink for each data packet sent which in turn makes the overall packet delivery appear random to an observer. In security, randomness plays an important role making it hard for intruders to use statistical analysis attacks [50]. MACGSP version 6 improves total energy usage and packet reception probability over its formers. These characteristics make MACGSP version 6 look promising as a candidate protocol for studying security. However, none research studies its intrinsic security properties. As discussed earlier, security is as important as other constraints of WSNs. Therefore, in order to use WSN in practice, one must consider its security issues.

### **3.0 BACKGROUND: WIRELESS SENSOR NETWORK SECURITY**

The concept of security often involves confidentiality, or keeping information secret [51]. However, security encompasses threats and services. Security concept is generally complex and cannot be adequately addressed in any one particular aspect [14]. A widely used perspective of security consists of four services: authentication, confidentiality, integrity, and availability.

Authentication is the verification of the claimed identity such that it is legitimate and belongs to a claimant [51]. Integrity is defined as the absence of improper alterations [51]. Confidentiality is the absence of unauthorized disclosure of information, and availability is the readiness for correct service [51]. Encryption algorithms such as DES [52] and AES [53, 54] offer confidentiality service. Message Authentication Codes (MAC) algorithms such as MD5, SHA-1, and HMAC provide authentication and data integrity service. These algorithms are cryptographic primitives.

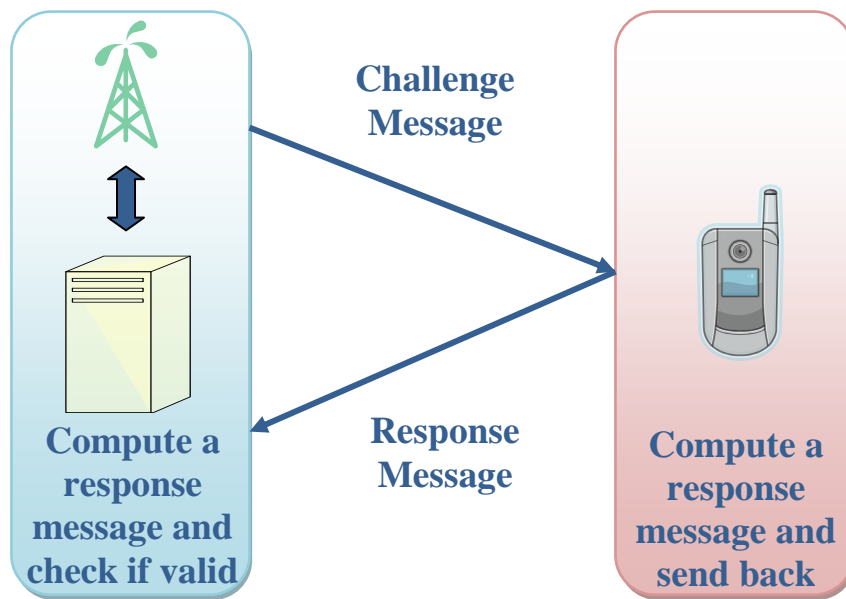
Cryptographic primitives are basic cryptographic algorithms that are widely used to build computer security systems. Cryptographic primitives involve a secret key for both encryption and decryption algorithm. Consequently, cryptographic primitives require key establishment and distribution. Key establishment and distribution remain important security issues for wireless systems. The following section discusses these security issues in the wireless environment.

### 3.1 WIRELESS SECURITY ISSUES

#### 3.1.1 Authentication

Infrastructure-based wireless systems such as cellular networks usually establish authentication at the beginning or the registration process. Cellular networks use challenge and response identification (C-R) for authentication service [15].

Figure 8 illustrates C-R basic operation; however, implementation details of C-R differ from system to system.

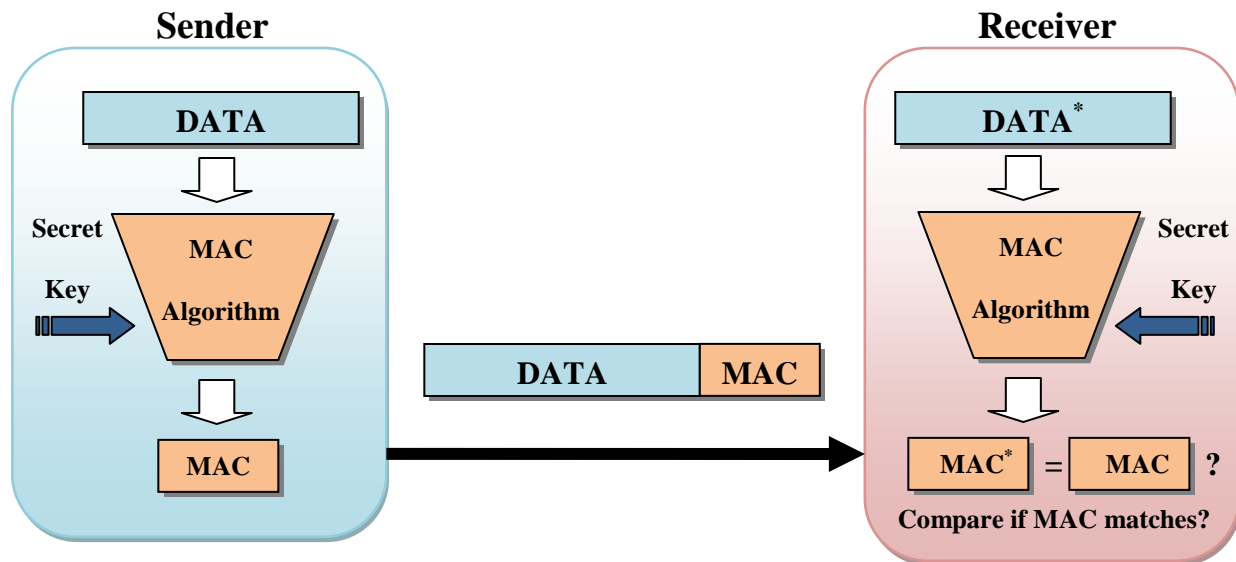


**Figure 8.** Challenge-Response basic operation.

A challenger first sends a challenge message to a responder, which then computes a response message based on the challenge message and the secret key presumably only known by both the responder and the challenger. Then, the responder sends the response message back to the challenger. The challenger then verifies the response message by using the secret key to

compute a response message in exactly the same way as the responder. If the computed message matches the one received from the responder, the challenger accepts the responder as legitimate.

Ad-hoc wireless systems use data authentication techniques such as Message Authentication Code (MAC) for authentication service. The sender and the receiver employ a shared a secret key used for computing a MAC for all messages communicated between them. The sender computes a MAC and sends it along with the original message/data as depicted in Figure 9. Both parties accept a message when a MAC is valid otherwise they reject the message.



**Figure 9.** Data authentication using Message Authentication Codes

### 3.1.2 Confidentiality

Confidentiality service helps keep information secret from unauthorized parties launching eavesdropping attacks. Encryption/decryption algorithms have been introduced to provide confidentiality service. Encryption/decryption algorithms include two different schemes: symmetric key cryptography and asymmetric key cryptography.

Symmetric key cryptography (or shared secret key cryptography) uses the same key in both encryption and decryption algorithms. Consequently, a sender and a receiver must share the same key in order to communicate securely through those algorithms. The method used for encryption and decryption is normally a block cipher. Examples of symmetric key cryptography include RC4, RC5, DES, 3DES, and AES.

Asymmetric key cryptography (or public-key cryptography) uses a key pair called a private key and public key in encryption and decryption algorithms. According to their names, private key is kept secret but public key is not. For each key pair, asymmetric key cryptography uses one key to encrypt and the other key to decrypt messages. Therefore, nodes setup a secure communication channel with other nodes by distributing a public key to the other nodes in the network. As an example, SSL (Secure socket layer) Protocol uses public-key cryptography to securely send a symmetric secret key to the SSL server to establish secure communication channel between a client and a server [55]. A node can generate a symmetric secret key, then encrypt it with a public key of destination node, and send it. The destination node can then decrypt the key by its own private key. This mechanism eliminates the complexity of key distribution scheme. However, it requires a powerful processor to encrypt, decrypt, and even generate a key pair in a timely manner. Moreover, its key size is typically large. As an example, an asymmetric key size of RSA 3072 bits is comparable to a symmetric key size of 128 bits [56].

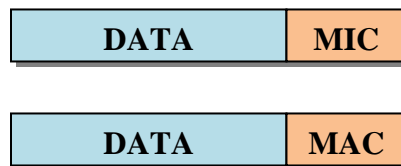
Given that an adversary does not know the secret key a priori, the security level, in terms of data confidentiality, depends upon the algorithm and the key size used to encrypt a message. For example, at present the minimum key size required for symmetric key cryptography is 112 bits and 2048 bits for asymmetric key cryptography [56]. Stronger data confidentiality requires a higher complexity encryption/decryption algorithm and longer key size. A higher complexity

encryption/decryption algorithm also requires more energy usage [57, 58]. Moreover, the longer the key size, the more memory required.

### 3.1.3 Data integrity

Data integrity is one of the most important security services for any networks. Not merely from a security aspect, is data integrity important in an intrinsic part of communication systems. Networks use a Message Integrity Code (MIC) such as Cyclic Redundancy Check (CRC) to provide non-secure data integrity service by attaching it along with data as shown in Figure 10. A MIC usually employs a non-secure hash function. The hash function produces a different output even when the input has a slight change. The function must minimize the probability of having the same output when the input message has been altered. However, hash functions are many-to-one functions, so it is possible for different data to have the same MICs.

In securing information a Message Authentication Code (MAC) can be used to provide secure data integrity service by replacing a MIC with a MAC as shown in Figure 10. Unlike a MIC, a MAC uses a cryptographic hash function requiring a secret key in its algorithm. The concept of integrity is sometimes mixed with that of authentication because a MAC can guarantee the integrity of the message while at the same time confirm authenticity of the original message.



**Figure 10.** Message Integrity Codes and Message Authentication Codes for data integrity

### **3.1.4 Availability**

Availability is another important security service for every network because it measures the readiness for correct service. Availability is usually measured in terms of a ratio of the total time a network is functioning (during a given interval) to the length of the interval. Typically, the objective of providing availability is to make a network function most of its lifetime [14]. The possible causes of losing service availability can be either from software/ hardware malfunction or a malicious intention. However, in terms of security, service availability focuses on a reduction of availability due to malicious actions.

### **3.1.5 Key establishment and distribution**

One traditional way of building security services in wireless systems is to use cryptographic primitives such as MAC and encryption/decryption. They also require secret keys for their operations. Consequently, key establishment and distribution become an important security issue for wireless systems.

Key establishment and distribution are one of the most challenging issues for WSNs, since WSNs have highly limited resources. The resource constraints impact in designing of key establishment and distribution mechanisms [59, 60]. As an example, a wireless sensor node has limited space for storing large or multiple keys. Although the simplest way is to use a global shared key, this is not suitable because sensor nodes are usually left unattended and a single compromised node can lead to a compromised network.



## **3.2 SECURITY THREATS AND ATTACKS IN WSN**

The unique topology, architecture, and characteristics of WSNs introduce security threats different from those in traditional wireless networks. However, common threats such as eavesdropping and message modification also pose a unique challenge. This section discusses security threats over WSNs and their countermeasures.

### **3.2.1 Eavesdropping**

Like other wireless systems, a WSN is prone to eavesdropping due to its broadcast nature in which intruders can easily capture frames or packets without having to directly connect a physical link to the target node. Intruders use eavesdropping as a basic element in a strategy to compromise the security and as the first step to attack a WSN. Without appropriate security mechanisms, a WSN suffers from lost crucial information. Moreover, intruder use this information to further exploit the network. Eavesdropping appears in two forms: passive eavesdropping and active eavesdropping [61]. In passive eavesdropping, the attacker passively monitors the wireless session and payload. In contrast, the attacker actively injects data into the communication to help decipher the payload in active eavesdropping.

As discussed in section 3.1.2, conventional methods to provide confidentiality service employ a strong encryption algorithm together with a large secret key. The encryption usually occurs at Media Access Control (MAC) layer. As an example, the MAC layer of WLANs employ WEP and WPA with a recommend key size for is no less than 128 bits [62]. However, in WSNs with limited resources, employing a strong algorithm with large key size is not practical.

To cope with this limitation in WSNs, WSN security protocols such as TinySec and SPINS use a lightweight version for their encryption algorithms [10, 11].

### **3.2.2 Node subversion / node identity impersonation**

Applications such as environmental or structural monitoring require sensor nodes to be left unattended, leaving nodes open to node subversion or node identity impersonation attack. In these attacks, intruders capture sensor nodes and gather control of management information such as node ID, secret keys, etc. Exposing this information causes a potential threat to the whole network especially in the case where WSNs use the same global secret key [14].

In general, deploying a tamper-proof device can protect against this attack. However, tamper-proof devices usually are expensive and impractical for WSNs with limited resources. Additionally, intruders still can extract secret keys out of both SRAM (Static Random Access Memory) and DRAM (Dynamic Random Access Memory) at room temperature within several seconds after the system is powered off [63, 64]. Effective key management and distribution help alleviate the impact of key exposing from node subversion [14].

Even with the best node subversion defense technique, there is no guarantee that nodes can never be compromised. Therefore, to prevent an adversary from using those nodes to further exploit the network, there must be a way to detect and exclude those nodes from the network if the nodes have been compromised. Adding this mechanism also requires more energy usage. Thus, this mechanism must also be designed in an energy-efficient way. This issue is still largely open to research.

### **3.2.3 Malicious code injection and message modification**

In the general Internet, malicious code such as viruses, worms, and Trojan horses cause damage to computers and networks. Similarly, malicious code injection and message modification can cause damage to WSNs. The defense against malicious code injection includes not only preventing nodes from infection but also containing malicious codes from spreading across the entire network.

The conventional method to prevent malicious code attacks is to use detection software which can be centralized or distributed across the network [65]. The software requires a large and constantly updated database to cope with a newly constructed malicious code. As a resource-constraint system, this method is not practical for WSNs.

Authentication is another possible technique that can be used to prevent malicious code injection and message modification. An adequate authentication technique can prevent an intruder from injecting malicious code or modifying a message as sensor nodes reject all unauthenticated packets. However, if nodes have been compromised, an intruder may use those nodes to inject malicious code or modify a message. Therefore, a proper authentication service or other effective mechanisms must be used to prevent malicious code injection and message modification.

### **3.2.4 Denial of service attacks**

A Denial of Service (DoS) attack is an attack that is hard to prevent not only for WSNs but also for other networks [24]. In WSNs, DoS attack can be in several forms and occur in any network layers, for example a jamming attack in the physical layer, collision attack in the link layer, and

misdirection and routing disruption attacks in the network and routing layer. Table 1 shows possible DoS attacks and their countermeasures classified at different network layers. In addition, other types of attacks such as node subversion and malicious code/fault data injection can be incorporated to form a DoS attack.

**Table 1.** DoS attacks and their countermeasures classified at different network layers

Network Layer	DoS attacks	Countermeasure
Physical layer	jamming	Spread-spectrum, frequency hopping, lower duty cycle, region mapping, mode change
MAC layer	Collision	Error-correcting code
	Energy depletion	Rate-limit
	Unfairness	Small frames
Network and routing layer	Misdirection	Egress filtering, authorization, monitoring
	Routing disruption	Secure routing
	Black holes	Authorization, monitoring, redundancy

Certain types of security attacks such as DoS attacks may never cease. Thus, WSNs require a combination of detection and containment mechanisms to cope with this attack [65]. Intrusion detection is one of the most challenging issues in WSNs because of its energy requirements and lack of reliable detection techniques [19]. Since intruders can always adapt their techniques to avoid being detected, detection poses a tough challenge. As an example, if a detection technique allows the number of packets received from neighbors to be no more than three consecutive packets, intruders can avoid detection by injecting a cycle of three consecutive

packets with one gap between them. The detection technique becomes useless in this case but intruders also have no choice but to comply with the rules. WSNs with limited resources make implementation of detection and containment techniques even more challenging. Detection techniques for WSNs must be simple and energy efficient.

### **3.2.5 Sybil attacks**

A Sybil attack is described as a situation where a malicious node illegitimately claims multiple identities [66]. Sybil attacks in WSNs can occur in both link and routing layers. At the link layer, multiple identities of a malicious node can dominate the shared radio resource ratio, preventing legitimate nodes from communicating. The Sybil attack can also cause damage to geographic routing protocols as they require nodes to exchange coordinate information with their neighbors in order to form efficient routes geographically.

To prevent Sybil attacks, authentication and confidentiality can be used. In addition, key establishment and distribution is also important to the Sybil defense mechanism. J. Newsome et al. have proposed the Sybil defense mechanism by leveraging the key pre-distribution process [67]. The key pre-distribution mechanism assigns to each node a unique secret key used for authentication. An intruder cannot claim a node identity without having a valid secret key.

#### **3.2.5.1 MACGSP with Sybil attacks**

Since MACGSP do not necessarily need node identities, in this case Sybil attacks cannot be applied against WSNs with MACGSP. However, if a WSN requires node identities, then we need to consider Sybil attacks as well. Generally, authentication and confidentiality can be used to prevent against Sybil attacks. Therefore, the packets may be equipped with data encryption

and authentication algorithms. However, using these algorithm one must carefully consider an overhead issue and key establishment and distribution issues. Moreover, since WSNs are based on multiple-hop forwarding, adding overheads for a packet can result in multiplicative increase of network overheads.

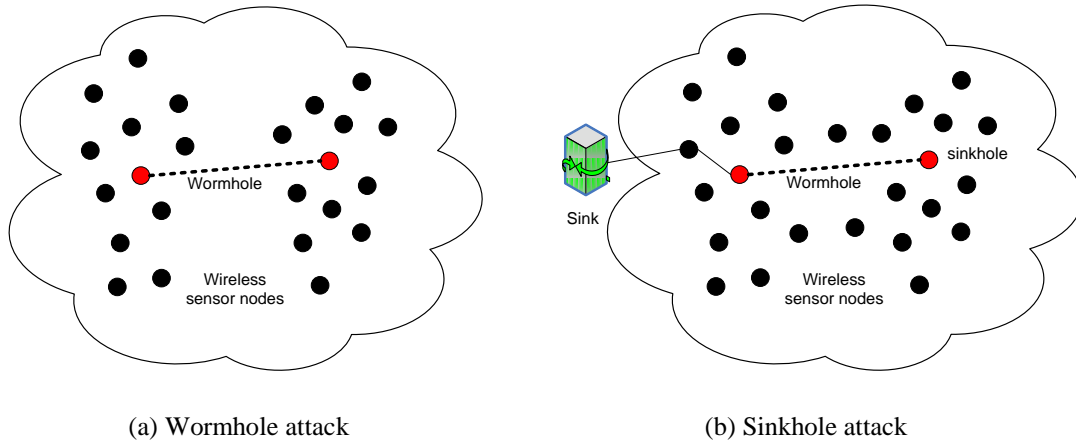
### **3.2.6 Sinkhole and wormhole attacks**

WSNs usually implement a many-to-one architecture where nodes send information to a sink in a multi-hop fashion. However, the many-to-one architecture causes WSNs to be vulnerable to a sinkhole attack. In a sinkhole attack, an intruder attempts to attract nodes in a particular area by employing invalid routing information, thus tricking the nodes into forwarding all packets to a specific node controlled by an intruder [68]. A sinkhole attack prevents the sink from obtaining a complete set of sensing data, and therefore causes a serious threat to WSNs' applications.

Depending on which routing algorithms are used by WSNs, there are techniques that can be used by an intruder to create a sinkhole. An intruder may spoof or replay a routing advertisement with a low cost route to a sink making a sinkhole node look more attractive than other surrounding nodes. Every targeted node then forwards its data packets to the sinkhole. As a matter of implementation, a Sybil attack and a wormhole attack can be used to create a sinkhole [69].

A wormhole attack involves two distant malicious nodes which cooperatively shorten the advertised distance between them by relaying packets through an exclusive tunnel (Figure 11 (a)) [70]. A wormhole attack can be used to disrupt a routing protocol, create a sinkhole, and help an intruder capture more data packets. Figure 11 (b) illustrates a sinkhole attack created by a wormhole. To create a sinkhole, an intruder can replays a routing advertisement of node A at

node B making node B the most attractive node among its neighbors as its distance is seemingly the closest to the sink.



**Figure 11. a. An example of a sinkhole attack, b. An example of a wormhole attack.**

Authentication can be used as a sinkhole and wormhole countermeasure. With authentication, replay messages cannot be used and consequently a sinkhole cannot be created. Authentication also prevents unauthorized nodes from joining the network and thus a wormhole cannot be formed. However, there must also be a technique to prevent a node from being compromised and then used to form a wormhole. There is also a technique for detecting wormhole attack proposed by Y. C. Hu et al. [69] and for detecting sinkhole attack proposed by E. Ngai et al. [68].

### 3.2.6.1 MACGSP with Sinkhole attacks

MACGSP can tolerate sinkhole attacks since MACGSP employs a probabilistic approach for forwarding decision making it more difficult for an intruder to lure nodes to forward the packet to the designated sinkhole node. In order to make nodes forward packets to the sinkhole node, intruders must capture all nodes and modify  $p_{gsp}$  of each node such that it forwards the packet to

the sinkhole node and partitions the sink from the source and the sinkhole node. However, once an intruder captured all nodes, doing sinkhole attack become trivial since an intruder can do more things than just to do sinkhole attack.

### **3.3 WSN SECURITY REQUIREMENTS**

The usual approach for security design is to use cryptographic primitives to provide security requirements such as confidentiality, authentication, and integrity. However, the unique characteristics of WSNs pose unique challenges for security design in WSNs. This section discusses these security requirements.

#### **3.3.1 Confidentiality**

Applications of WSNs such as military may require confidentiality of sensed data. To protect data from eavesdroppers, a confidentiality service must be provided for WSNs. Cryptographic primitives such as encryption algorithms provide confidentiality, however, these require sophisticated key management and distribution, adding more overhead to the network and requiring larger storage space on sensor nodes [71, 72].

Also, employing encryption alone is not sufficient as an eavesdropper can perform traffic analysis on encrypted data. WSNs with very short messages can suffer even more from traffic analysis as the sample space is small [50].

Data exposure is another important factor that needs a careful consideration when designing confidentiality service. WSNs usually have lower data exposure for an individual node



because of its short transmission range. However, when considering WSNs as a whole, multiple-hop forwarding causes higher data exposure as an intruder can intercept a packet from several locations. Protocols such as GBR and GSP have even higher data exposure because the packets are scattered all over the network. If such protocols were to be used for applications requiring confidentiality, a new security mechanism for confidentiality service is necessary.

### **3.3.2 Authentication**

For WSNs, Message Authentication Code (MAC) can be used to provide data authentication. However, data authentication alone does not solve the problem of compromised nodes because wireless sensor nodes are usually left unattended and adversaries, who capture the compromised nodes, can know the secret keys of legitimate nodes, which can be used by adversaries to authenticate themselves to other nodes [14]. An analogy is the case where a cell phone has been stolen. The cell phone thief can use that cell phone to call out as long as it has not been blocked by the cell phone service providers.

Protocols such as TinySec and SPINS use a lightweight version of MAC to provide data authentication because of resource constraints of WSNs [10, 11]. Using a MAC that is too short causes a WSN to be more susceptible to a birthday attack [73]. Conversely, using a large MAC adds overhead to the transmissions and receptions, consequently using energy more quickly. Also, WSNs can employ very short messages (e.g. 16 bits of data). Generating a random message can sometimes produce a legitimate pair of packet and MAC as a MAC is computed based on a many-to-one function.

### **3.3.3 Data integrity**

Data integrity is one of the most important requirements for WSNs. Without data integrity, WSN applications may fail to meet their objectives and cause untrustworthiness to the users. In applications of WSNs that rely on data aggregation, a MAC alone cannot be used to confirm the integrity of data because the data is altered as it travels through the network. To achieve integrity in this scenario, there must be other mechanisms used together with a MAC. This is a major challenge in the design of security for these applications.

### **3.3.4 Availability**

Loss of service availability can cause serious problems for WSN applications. As an example, in a disaster surveillance system with a WSN, if the network loses its service availability when the system needs to send a warning message about an incoming disaster, this system would be unacceptable. Also, in structural monitoring applications loss of service availability can result in a failure to detect a potential structure collapse. Therefore, a proper protection for service availability is necessary if WSNs were to be used in such applications.

## **3.4 PREVIOUS RESEARCH OF SECURITY TECHNIQUES EMPLOYING MULTIPLE PATHS**

Much research uses multiple paths to improve reliability and enhance security. As an example, multiple path routing enhances confidentiality by dividing a packet into small blocks based on

secret sharing principle and distributing them along multiple paths [18]. Multiple paths also work as backup paths and make WSNs more robust to node failures. As an example, highly-resilient, energy-efficient multipath routing in wireless sensor networks, proposed by Ganesan et al., uses non-disjoint routing paths to provide resilience to node failures [74]. The Reliable Information Forwarding using Multiple Paths (ReInForM), proposed by Deb et al., uses dynamic packet state to control the number of paths required for the desired reliability using only local knowledge of channel error rates. With ReInForM, data can be delivered at desired levels of reliability at proportional cost [75]. These techniques can be used to increase service availability of WSNs.

The multiple routing paths utilizes redundancy of routing paths to tolerate intrusions without the need for detecting malicious attempts [19]. However, sensor network routing and MAC protocols vary with different type of WSN applications. Therefore, one must develop security specifically for each particular protocol because each protocol has different properties and requirements. Protocols inherit security properties from their mechanisms making them more robust to a certain type of security threats. As an example, directed diffusion possesses robustness from flooding making it more difficult for an intruder to prevent data from reaching the sink [17], [38]. Conversely, each routing and MAC protocols also possess unique weaknesses.

Secure routing is important for WSNs as service can be interrupted if a routing disruption occurs [17]. Many routing algorithms in use today assume a stable path, i.e. the routing paths tend to be the same for a long period of time even though they can change [18]. INSENS employs multiple-path routing along with low-complexity security methods such as symmetric key cryptography and one-way hash function to provide intrusion-tolerant routing in WSNs [19]. Additionally, the multiple path algorithms provide better protection against packet flooding

attacks. The goal of this algorithm is to find the fewest common nodes in the paths as possible. Ideally, only source node and sink node can be shared among paths.

INSENS proposes routing discovery mechanism to build forwarding tables at sensor nodes. Routing discovery uses a flooding-based request message from the sink and a feedback message from each sensor node to the sink. To offload the computational burden, the sink computes the forwarding tables for each sensor node based on information received. Once the sink finished computing forwarding tables, it sends them to the respective nodes using a routing update message. Results showed that employing multiple paths can mitigate the damage from DoS threats such as packet flooding attacks when the number of compromised nodes are not too great [19]. However, the level of protection against DoS attacks varies with different topologies and different network densities as the percentage of blocking nodes for the low density network with grid topology is much less than those for high density network with either random or grid topology.

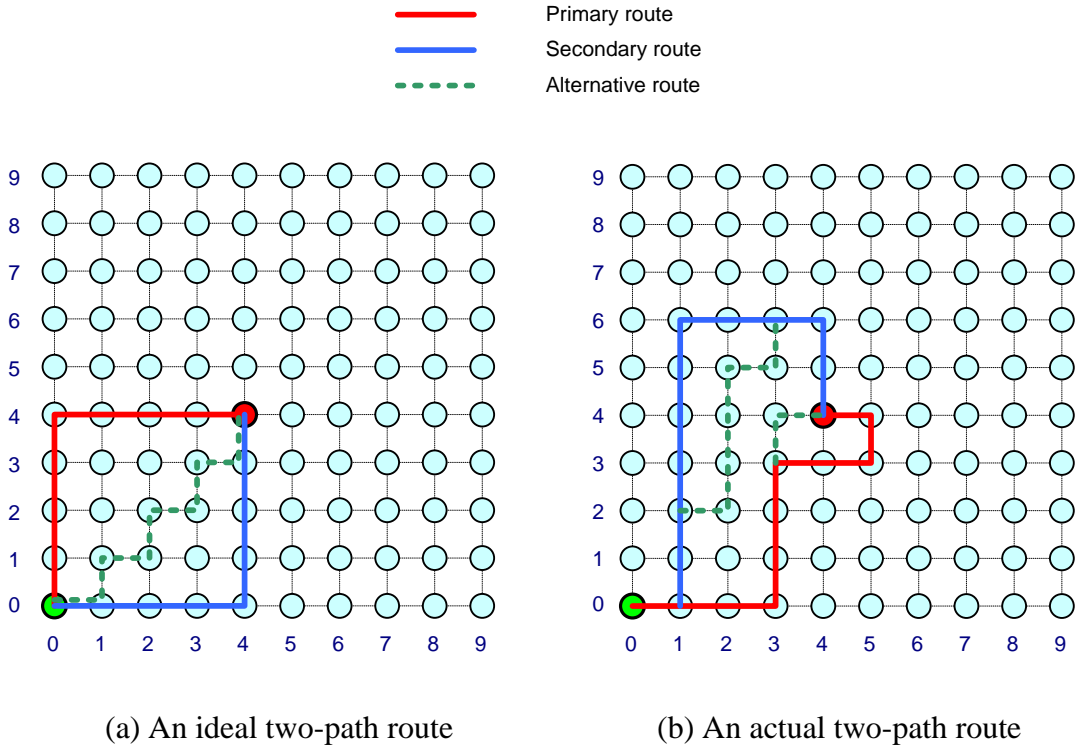
The multipath approach for secure data delivery employs multiple path routing and data segmentation using the secret sharing algorithm to provide secure data delivery [18]. The secret sharing algorithm divides data into  $N$  segments such that reconstructing the original data requires  $T$  out of  $N$  segments. Under the assumption that intercepting  $T$  segments are not possible or much difficult to achieve by an intruder, this technique can be used to enhance confidentiality service by sending each segment to a different path. The technique uses a distributed multiple path routing algorithm to find node disjoint paths in a network. The algorithm uses path independency, path quantity, and path cost to compute a set of disjoint paths.

## 4.0 RESULTS FOR WSNS EMPLOYING MRDPS

As multiple paths can be used to enhance security, the properties of multiple random delivery paths (MRDPs) and the intrinsic security issues of WSNs employing MRDPs with a single sink were studied. Unlike INSENS, MRDPs do not require route discovery and forwarding tables maintained at sensor nodes. Additionally, the routing paths are not statics making it harder for an intruder to learn where the packet will be routed. This study uses MACGSP version 6 to generate MRDPs to a single sink in a WSN. The MRDPs generated by the protocol are not always disjoint. However, reliability can be provided through non-disjoint routing paths [74, 75]. Moreover, the protocol does not create MRDPs for every packet sent because of the randomness. This following section investigates the properties of the MRDPs created by MACGSP version 6.

### 4.1 VERIFICATION OF MULTIPLE RANDOM DELIVERY PATHS

A gossiping protocol creates MRDPs by randomly forwarding packets through a WSN. In GSP, sensor nodes sleep randomly according to  $p_{gsp}$ , which implicitly creates a random number of random paths. The average number of paths depends on network physical topology, node density, and  $p_{gsp}$ . Figure 12 depicts examples of two delivery paths for a 100 square grid sensor network.



**Figure 12.** Examples of multiple delivery paths for a 100 square grid sensor network.

This study uses simulation to verify the properties of MRDPs and find the performance of WSN employing MRDPs with respect to security. Simulations were implemented using the C programming language to create objects such as sensor nodes, source, sink, etc. Each sensor node employs the MACGSP version 6 protocol subroutines. The exact same subroutine code can also be implemented on a physical sensor node such as a MICA2. These objects are replicated and placed on a location in a square grid coordinates. The simulation code employs a model of an ideal communication channel between a node and each of its neighbors. In these simulations the ideal communication channel was error free with transmission range is exactly 1 hop apart from the sensor node i.e. in a square grid WSN a sensor node has at most 4 neighbors. The simulations did however include collisions, which occur when two packets with different contents arrives at a sensor node at the same time. The simulation is time-based with one

transmission period (TP) increment. The simulation parameters such as the total number of nodes, source and sink location, attack types, location of attacking nodes, etc., are used to define simulation scenario. Simulations were run so that performance metrics at the 90% C.I. could be generated. To validate the results from the simulations the study uses packet walkthrough analysis to find the results of a 4-node-square-grid and 9-node-square-grid WSNs and compare with the results from the simulation of the same network.

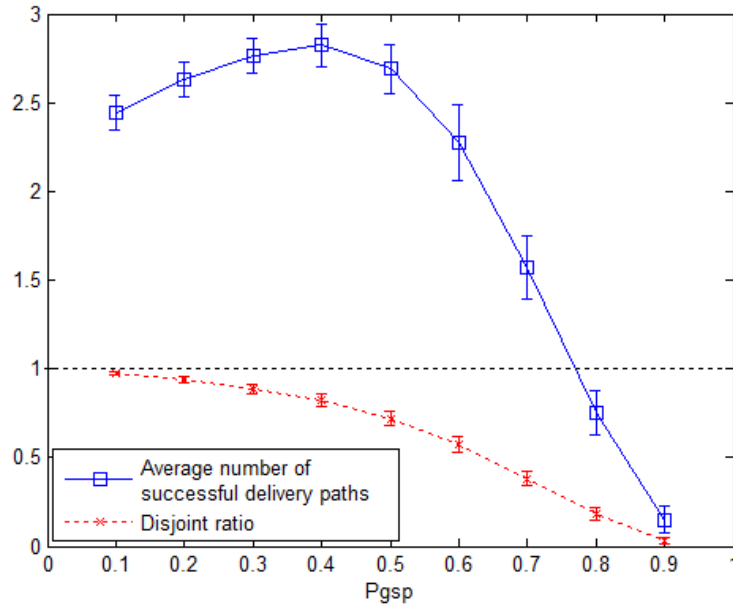
#### **4.1.1 Average number of successful delivery paths and disjoint ratio**

The number of successful delivery paths can be found by counting the number of packets from different paths received at the sink. Since the successful delivery paths share a number of common nodes, the *disjoint ratio* is defined as the number of nodes that are not common between paths to the total number of nodes in the paths. The analysis uses simulation to find the average number of route and disjoint ration. The simulation was run according to the following steps:

1. Source node sends 200 packets for each run.
2. For each packet send, the simulation runs until the last packet exits the network.
3. The simulation computes the average number of successful delivery paths and disjoint ratio for each run.
4. The simulation repeats 40 times to find the performance metrics at 90% C.I.

Figure 13 shows simulation results from a 100-node-square grid WSN where the source is at the (0, 0) coordinate and the sink is at the (4, 4) coordinate (Figure 12a). The results show that as  $p_{gsp}$  increases, the average number of successful delivery paths increases up to  $p_{gsp} = 0.4$  and then decreases afterward but the disjoint ratio decreases. Moreover, the average number of

delivery paths is more than 2 with the disjoint ratio greater than 50% given that  $p_{gsp}$  is less than 0.6. With this property, one can design a suitable average number of successful delivery paths and disjoint ratio by adjusting  $p_{gsp}$ . However, adjusting the  $p_{gsp}$  changes packet reception probability and the energy used by the network [25].

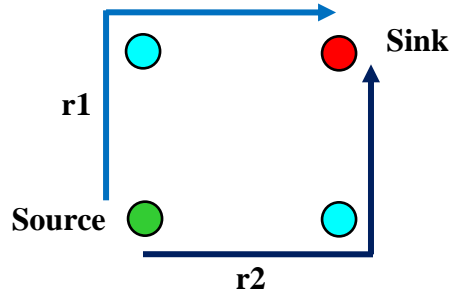


**Figure 13.** The average number of successful delivery paths vs. disjoint ratio of a 100-node-square grid WSN with 90% C.I

#### 4.1.1.1 Packet walkthrough analysis

Consider the 4-node-square-grid network illustrated in Figure 14. There exist two different routes from the source to the sink, each takes two hops or  $2GP$  seconds which is also the minimum transit time to deliver a packet in this network. From equation (1),  $S$  is equal to two for this network. The packet delivery time is therefore equal to  $2GP$  when either one or both of the intermediate nodes are awake. The packet retransmission uses two additional GPs for each retransmission. Thus, the packet delivery time is always an even multiple of GPs.

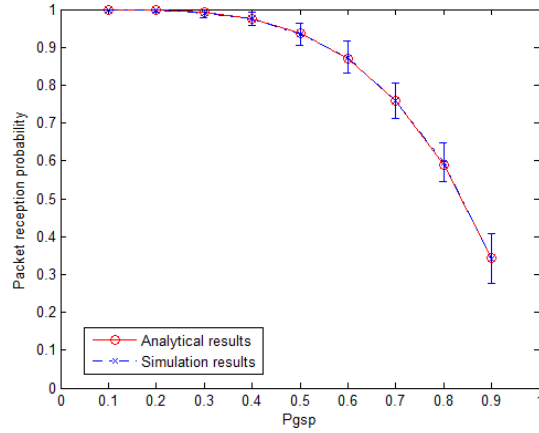




**Figure 14.** A 4-node-square-grid WSN

The sink node receives a packet if either or both of the intermediate nodes are awake when the source transmits a packet. If both of the intermediate nodes sleep during the source transmission, the sink can receive the packet if either or both of the intermediate nodes are awake during the source retransmission. The sink node does not receive a packet when both of the intermediate nodes sleep in two consecutive cycles (sleep, awake, and then sleep again).

Since the probability of a node being in a sleep mode is  $p_{gsp}$ , then the probability of a node being in a sleep mode for two consecutive cycles is  $p_{gsp}^2$  and the probability of two intermediate nodes being in a sleep mode for two consecutive cycles is  $p_{gsp}^4$ . Thus, in this 4-node square-grid WSN the probability that the sink does not receive a packet is  $p_{gsp}^4$ . Under this condition together with retransmission, packets reach the sink with the probabilities  $1 - p_{gsp}^4$  as shown in Figure 15. The analysis also computes probability of each different route and their combinations. The probability of each different route and their combinations can also be derived. Table 2 shows the probability of each different route and their combinations.

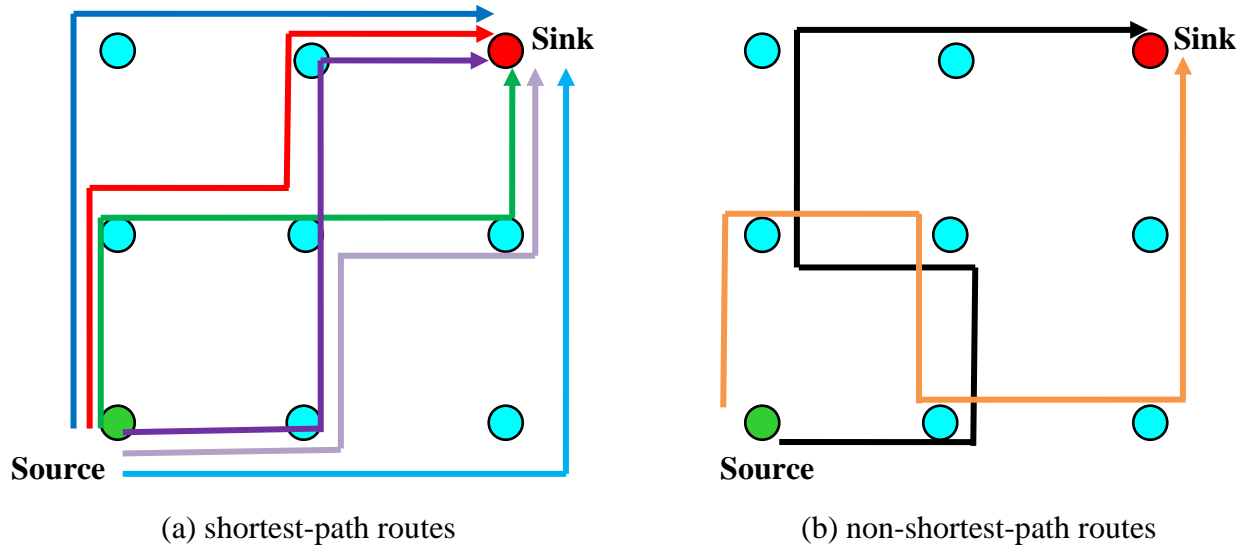


**Figure 15.** Packet reception probability of a 4-node-square-grid WSN compared between analytical and simulation approaches.

**Table 2.** Probability table of all possible routes of a 4-node-square-grid WSN

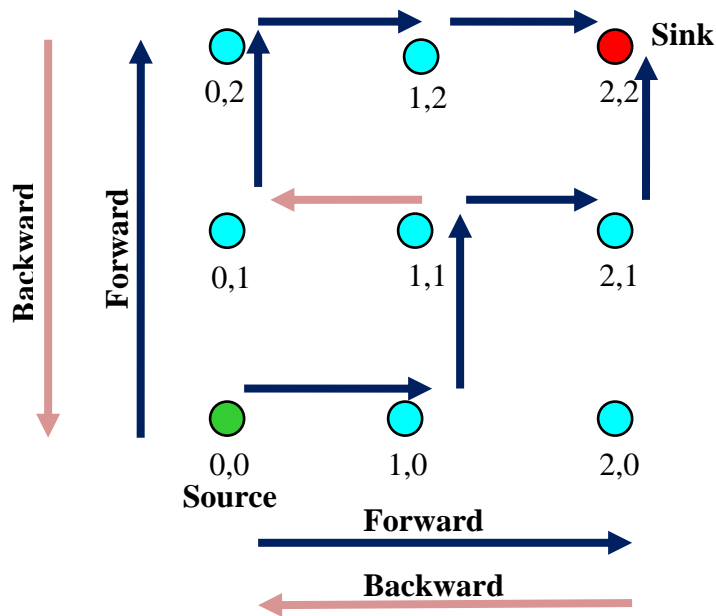
Routes	The probability of each route ( $p_r$ )
r1	$p_{gsp}(1 - p_{gsp})(1 + p_{gsp}^2)$
r2	$p_{gsp}(1 - p_{gsp})(1 + p_{gsp}^2)$
r1+r2	$(1 - p_{gsp})^2(1 + p_{gsp}^2)$

Now consider a 9-node-square-grid network with the source at the bottom left corner and the sink at the top right corner as shown in Figure 16. The minimum transit time is four hops or  $4*GP$  in this network. There exist eight different possible routes from the source to the sink. The eight different routes to the sink may be divided into two subsets (4-hop routes and 6-hop routes). The routes taken by packets consist of a combination of these routes. 6 of the 8 routes are the shortest-path routes (4-hop routes) and 2 of the 8 routes are non-shortest-path routes (6-hop routes).



**Figure 16.** 9-node-square-grid network with source at the bottom left corner and sink at the top right corner

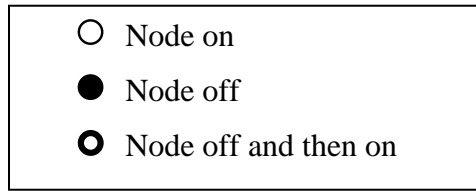
Figure 17 illustrates that the shortest-path routes occur when the packet only traverses forward while the non-shortest path routes occur when the packet traverses backward at some point in the path. Each step backward costs 2 additional hops, however in this case there is only 1 step backward because of the limited network size.



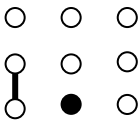
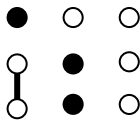
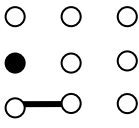
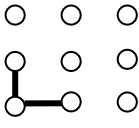
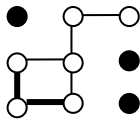
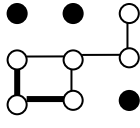
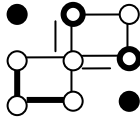
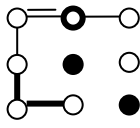
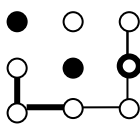
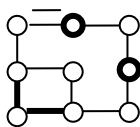
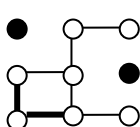
**Figure 17.** An example of a detour route in 9-node-square-grid network

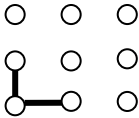
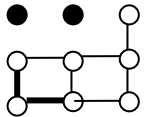
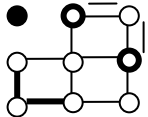
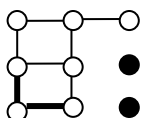
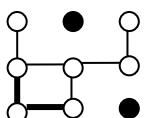
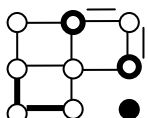
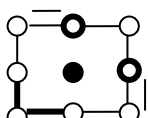
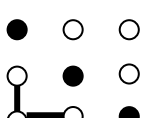
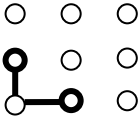
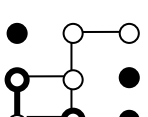
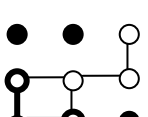
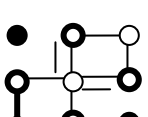
The analysis uses a packet walkthrough starting from the source node to find the probability of each individual route occurring. First, the source has only three nodes to forward a packet to, that is node 10, 01, and both in which each case has probability of occurring equal to  $p_{gsp}(1-p_{gsp})+p_{gsp}^3(1-p_{gsp})$ ,  $p_{gsp}(1-p_{gsp})+p_{gsp}^3(1-p_{gsp})$ , and  $(1-p_{gsp})^2+p_{gsp}^2(1-p_{gsp})^2$  respectively. A packet is lost when node 10 and 01 are both asleep in two consecutive rounds, with a probability equal to  $p_{gsp}^4$ . A packet can be forwarded to node 01 when node 01 is on and node 10 is off and when both nodes are off and then the next 2 GPs node 01 is on and node 10 is off and vice versa. Since both nodes sleep with probability  $p_{gsp}$  and since nodes are independent, the probability of the first event of the first option occurring is then equal to the product of the probability of both events i.e.  $p_{gsp}(1-p_{gsp})$ . The probability of the second event of the first option occurring is equal to  $p_{gsp}^3(1-p_{gsp})$ . The probability of the second option is derived in the same manner. The last option, where the packet is being forwarded to both node 01 and 10, occurs when the nodes are either both awake or both asleep during the first transmission in which they must both be awake the next GP and then follow GSP rules to be awake or sleep. Therefore, the probability of the node 01 and 10 sleep is equal to  $(1-p_{gsp})^2+p_{gsp}^2(1-p_{gsp})^2$ . The time it takes to transmit a packet to the next hop is one GP in all those events except the case when both node 01 and 10 are sleeping which takes two additional GPs to transmit a packet. The summary of all possible events and probabilities are shown in Table 3 below. The probability that the packet does not reach sink is equal to one minus probability that the packet reach sink (derived from the table). Note that  $p_{gsp}$  is written as  $P$  for short and the probability of each delivery time shown in the table must be multiplied by the probability in the first column (1<sup>st</sup> round).

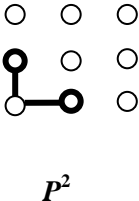
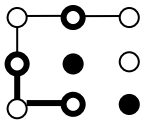
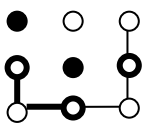
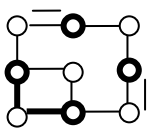
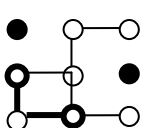
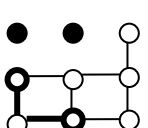
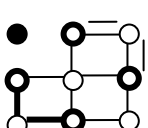
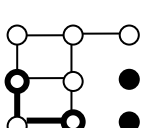
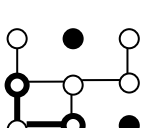
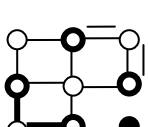
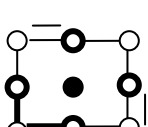
**Table 3.** Probability table of all possible routes of a 9-node-square-grid WSN



1 <sup>st</sup> round (GP)	2 <sup>nd</sup> round and so on.	4 GPs	6 GPs	8 GPs	10 GPs	12 GPs	
<p><math>P(1-P)</math></p>		$P(1-P)^*$ $(1-P)$	$P(1-P)^*$ $P(1-P)$				
		$P(1-P)^*$ $P^2(1-P)$					
		$P(1-P)^*$ $P^2(1-P)$					
		$P(1-P)^*$ $P^2(1-P)$					
		$P(1-P)^*$ $P^2(1-P)$		$P(1-P)^*$ $P^2(1-P)^*$ $(1-P)^2$	$P(1-P)^*$ $P^2(1-P)^*$ $2P(1-P)^2$	$P(1-P)^*$ $P^2(1-P)^*$ $P^2(1-P)^2$	
		$P(1-P)^*$ $P(1-P)^2$					
		$P(1-P)^*$ $P(1-P)^2$					
		$P(1-P)^*$ $P(1-P)^2$					
	$P(1-P)^*$ $(1-P)^3$		$P(1-P)^*$ $P^3(1-P^2)$				

 <p><math>P(1-P)</math></p>	 <p><math>(1-P)^2</math></p>	<p>All neighbors off but a packet was retransmitted</p>	<p>Shift above table to the right and multiply with <math>(1-P)^2</math></p>			
 <p><math>P(1-P)</math></p>	<p>Similar to above (symmetry property)</p>	<p>Similar to above</p>	<p>Similar to above</p>	<p>Similar to above</p>	<p>Similar to above</p>	<p>Similar to above</p>
 <p><math>(1-P)^2</math></p>	 <p><math>(1-P)P^2*</math> <math>P(1-P)</math></p>					
	 <p><math>(1-P)P^2*</math> <math>P(1-P)</math></p>					
	 <p><math>(1-P)P^2*</math> <math>(1-P)^2</math></p>		<p><math>(1-P)P^2*</math> <math>P^2(1-P^2)</math></p>			
	 <p><math>(1-P)P^2*</math> <math>(1-P)</math></p>		<p><math>(1-P)P^2*</math> <math>P(1-P)</math></p>			
	 <p><math>(1-P)P^2*</math> <math>(1-P)</math></p>		<p><math>(1-P)P^2*</math> <math>P(1-P)</math></p>			
	 <p><math>(1-P)^3*</math> <math>[2P(1-P) + (1-P)^2]</math></p>		<p><math>(1-P)^3*</math> <math>P^2(1-P^2)</math></p>			
	 <p><math>(1-P)^2P*</math> <math>P(1-P)</math></p>					

 <p><math>(1-P)^2</math></p>	 <p><math>(1-P)^2P^*</math> <math>P(1-P)</math></p>						
	 <p><math>(1-P)^2P^*</math> <math>(1-P)^2</math></p>	$(1-P)^2P^*$ $P^2(1-P^2)$					
	 <p><math>(1-P)^2P^*</math> <math>P(1-P)</math></p>						
	 <p><math>(1-P)^2P^*</math> <math>P(1-P)</math></p>						
	 <p><math>(1-P)^2P^*</math> <math>(1-P)^2</math></p>	$(1-P)^2P^*$ $P^2(1-P^2)$					
	 <p><math>P(1-P)^2*</math> <math>[2P(1-P) + (1-P)^2]</math></p>	$P(1-P)^2*$ $P^2(1-P^2)$					
	 <p><math>P^3</math></p>	<p>All neighbors off but the packet was retransmitted</p>	<p>Shift above table to the right and multiply with <math>P^3</math></p>				
 <p><math>P^2</math></p>	 <p>Shift All above table to the right and multiply with <math>P^2</math></p>	$(1-P)P^2*$ $P(1-P)$					
			$(1-P)P^2*$ $P(1-P)$				
			$(1-P)P^2*$ $(1-P)^2$	$(1-P)P^2*$ $P^2(1-P^2)$			

 $P^2$			$(1-P)P^{2*}$ $(1-P)$	$(1-P)P^{2*}$ $P(1-P)$		
			$(1-P)P^{2*}$ $(1-P)$	$(1-P)P^{2*}$ $P(1-P)$		
			$(1-P)^3*$ $[2P(1-P)$ $+ (1-P)^2]$	$(1-P)^3*$ $P^2(1-P^2)$		
			$(1-P)^2P^*$ $P(1-P)$			
			$(1-P)^2P^*$ $P(1-P)$			
			$(1-P)^2P^*$ $(1-P)^2$	$(1-P)^2P^*$ $P^2(1-P^2)$		
			$(1-P)^2P^*$ $P(1-P)$			
			$(1-P)^2P^*$ $P(1-P)$			
			$(1-P)^2P^*$ $(1-P)^2$	$(1-P)^2P^*$ $P^2(1-P^2)$		
			$P(1-P)^{2*}$ $[2P(1-P)$ $+ (1-P)^2]$	$P(1-P)^{2*}$ $P^2(1-P^2)$		



		All neighbors off but a packet was retransmitted	Shift above table to the right and multiply by $P^3$			
--	--	--	--	--	--	--

Figure 18 illustrates a network with a sink that has 4 neighbors. Consider only the nodes inside the square. This case is similar to the previous case where we have the shortest-path routes as a majority. The non-shortest-path routes take at least 2 additional hops to reach the sink. The shortest-path routes only contain inside the square or the direct plane. Again when a packet is moving one step outside the direct plane, it cost 2 additional hops to get back in. Two neighbors of the sink (1,2) and (2,1) reside within the direct plane while the other two (2,3) and (3,2) are outside. The routes of a packet received from those neighbors outside the direct plane must have at least 2 extra hops more than the shortest-path route.

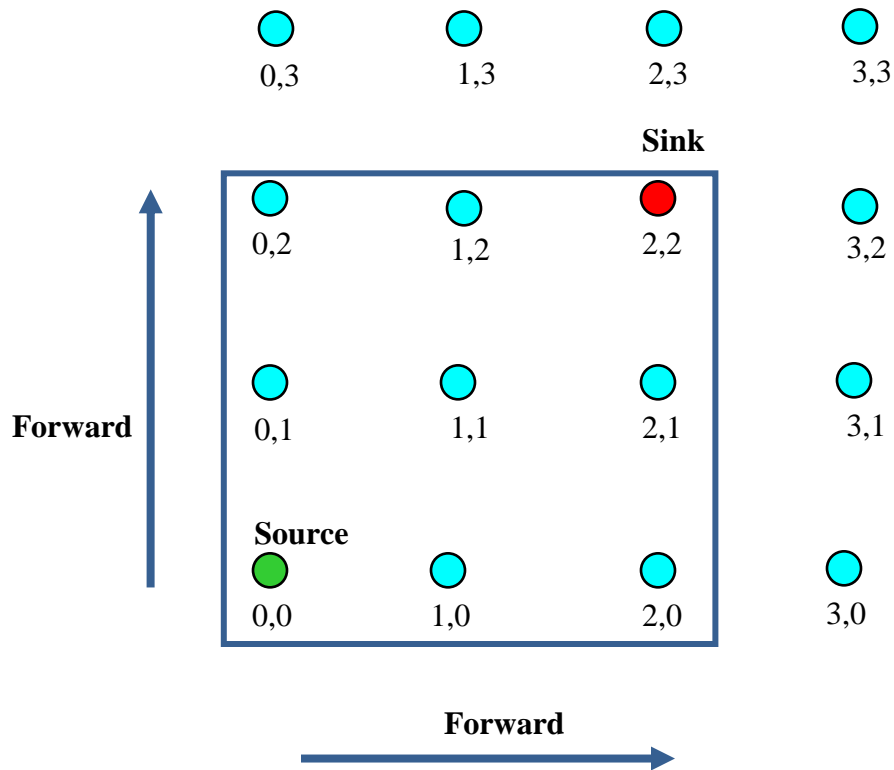


Figure 18. 16-node-square-grid network with source in the middle and sink at the top right corner.

Without packet retransmission, packet delivery time of this WSN now takes three different values 4, 6, and 8. Four-hop is the shortest-path routes, six-hop is for either one-step-backward or one-step-outside routes, and eight-hop is for the routes with one-step-backward and one-step-outside. As the network grows larger, packet delivery time remains in the form of the number of hops in the shortest path, plus multiples of two hops. The next section confirms this statement through graph theory analysis.

#### 4.1.2 Packet delivery time

Packet delivery time in WSNs with MRDPs is random and depends on factors such as routing paths, distance between source and sink, topology, gossip period,  $p_{gsp}$ , etc. Although packet delivery time is random, it can be useful in intrusion detection for WSNs. As an example, a packet delivery time out of normal range indicates suspicious activity in a WSN. The analysis model of packet delivery time is:

$T$  is the time it takes to deliver a packet via an individual route from the source to the sink

$S$  is the shortest distance (number of hops) between the source and the sink

$GP$  is gossip period (seconds)

Normally, packets taking the shorter path arrive before the packets taking longer paths. Packets taking the shortest paths traverse in a minimum transit time. As an example, if  $p_{gsp}$  is equal to zero meaning that all nodes are always awake and the packet reception probability of the sink is equal to one, by ignoring collisions and assuming a perfect channel a packet will arrive at the sink via the shortest path with the minimum transit time. As a packet requires one gossip period for transmitting in each hop, the minimum transit time is proportional to the number of

hops between the source and the sink multiplied by the gossip period assuming all nodes are synchronized. Therefore:

$$\text{The minimum transit time} = T_{min} = S \times GP \quad (1)$$

However, if  $p_{gsp}$  is not equal to zero, then packets may take longer routes to the sink and the packet delivery time becomes the minimum packet delivery time plus a number of extra hops. In other words:

Let E be a positive integer.

$$\text{The packet delivery time of longer path } (T_L) = T_{min} + E \times GP$$

$$T_L = S \times GP + E \times GP$$

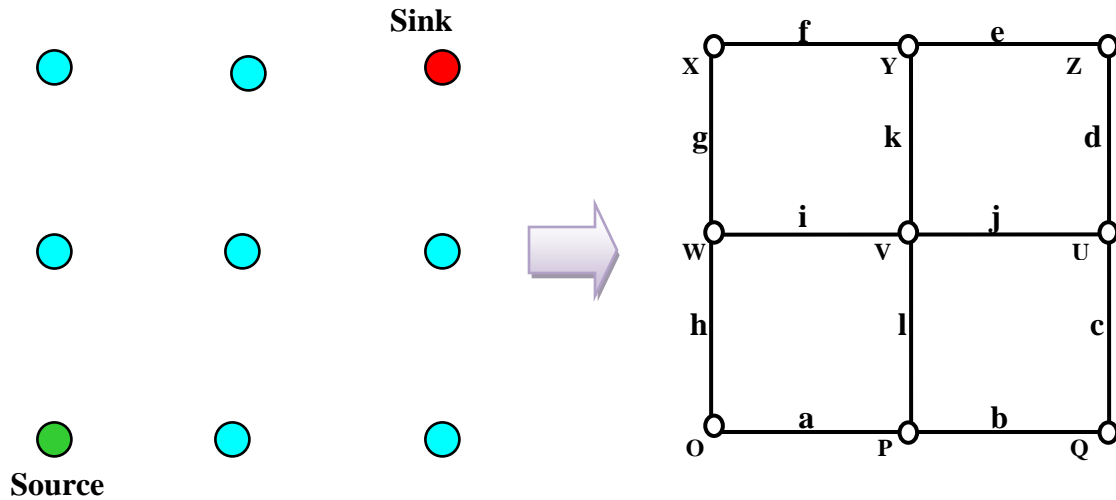
$$T_L = (S + E) \times GP \quad (2)$$

To find the form of packet delivery time the analysis considers two different approaches: Packet walkthrough is used because it illustrates how the packets travel through the network. Graph theory analysis confirms that the results generalize to larger networks.

#### 4.1.2.1 Graph theory analysis

The analysis uses a simple finite square-grid graph to represent a square-grid network as an example of 9-node-square-grid network shown in Figure 19. Since square-grid graph can be embedded in a plane, it is a planar or a plane graph [76, 77]. Additionally, every node is connected to each other because there exists a path between them, e.g. “OhWgXfYeZ” is one of the paths between node O and Z. In graph theory, a walk refers to a connected finite alternating sequence of nodes (or vertices) and links (or edges) while a path refers to a walk with distinct nodes and links [76, 77]. The analysis refers walks to the routing paths as the actual routing paths may contain loops and repetition nodes or links. As an example, “OhWgXfYkViWgXfYeZ” is one of the walks between node O and Z. Similarly, the retransmission packet in WSN with

MACGSP version 6 causes three repetition links in the walk “OaPaOaP” between the retransmitting node (O) and the receiving node (P) as shown in Figure 19. Given that the packets always leave the network, walks are finite.



**Figure 19.** A simple finite square-grid graph representation of a square-grid network

Consider the case of no edge repetition (no retransmission). Given a shortest path between a pair of vertices O and Z (a shortest route from the source to the sink) contains  $S$  edges and a detour walk (an alternative route) from O to Z contains  $D$  edges.  $S$  and  $D$  are integers in this case. Combining the shortest path and the detour walk together forms a loop containing the cycles and repeat edges (if any). Since the square-grid graph contains no odd cycles and the repeat edges have an even number of edges, the walks of the loop contain an even number of edges. If  $S$  is even,  $D$  must then be even. Similarly if  $S$  is odd,  $D$  must also be odd. Thus, the difference between the number of the shortest path edges and the detour walk edges is always an even number. In other words the loop has  $S+D$  edges where:

$$S + D \text{ mod } 2 = 0 \tag{3}$$

$$\text{Since} \quad -2 \times S \text{ mod } 2 = 0 \quad (4)$$

$$(3) + (4), \quad D - S \text{ mod } 2 = 0 \quad (5)$$

Similarly, if the detour walk contains a retransmission, the retransmission contains two extra edges (or hops) as the example shown in Figure 19. Consequently equation (5) remains valid.

$$T = D \times GP \quad ; \text{ where } D \text{ is positive integer} \quad (6)$$

From equation (2),

$$T_L = (S + E) \times GP = D \times GP$$

$$D = S + E$$

$$E = D - S$$

From equation (5),  $E$  is always an odd number and  $T$  can be expressed as:

$$T = (S + E) \times GP \quad ; \text{ where } E = 0, 2, 4, 6, \dots \quad (7)$$

Therefore, equation (6) confirms packet delivery time of each individual walk (or basis walk) from the source to the sink is in the form of the number of hops in the shortest path plus multiples of two hops. In WSNs employing MRDPs, the actual routes of each packet sent consist of a combination of the basis walks. Multiple copies of the same packet may arrive at the sink via different paths and at different times.

The first packet delivery time ( $T_1$ ) is the packet delivery time of the first copy of the packet arriving at the sink.  $T_1$  depends on  $p_{gsp}$ , network size, and source and sink locations. Considering only the case when a packet is not lost,  $T_1$  is a discrete random variable taking value of  $T_{min}$  plus  $E \times GP$  (multiples of 2 GPs). Consequently,  $E$  is also a discrete random variable. For each pair of source and sink locations of a square-grid-WSN, one can find  $T_1$ : A discrete random

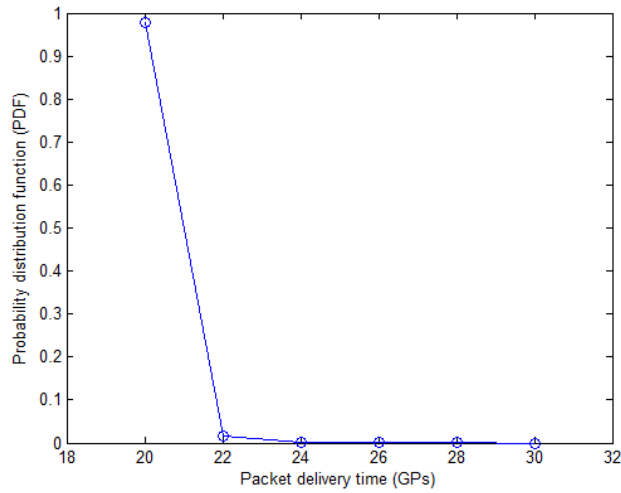
variable with mean  $E(T_1) = T_{min} + m(p_{gsp}) \times GP$  and variance  $(p_{gsp})$ . Therefore,  $E$  is a discrete random variable with mean  $E(E) = m(p_{gsp})$  and variance  $Var(E) = v(p_{gsp})$ .

#### 4.1.2.2 Probability distribution function of first packet delivery time

The analysis uses a simulation to find the probability distribution function of the first packet delivery time ( $T_1$ ). The simulation was run according to the following steps:

1. Source node sends 8000 packets.
2. For each packet send, the simulation runs until the first packet arrives at the sink.
3. The simulation finds  $T_1$  for each packet sent, counts its frequency, and constructs a histogram for  $T_1$ . The histogram is then normalized to represent the probability distribution function of  $T_1$ .

Figure 20 depicts the probability distribution of the first packet delivery time of a 900-node-square-grid WSN employing MACGSP version 6 source at coordinate (10, 10), sink at coordinates (20, 20) and  $p_{gsp} = 0.1$ . The shortest path routes between the source and the sink is 20 hops. The results show that  $T_1$  is in a form of minimum transit time (20 GPs) plus multiple of 2 GPs corresponding to equation (6). Moreover, the minimum transit time is the main dominance with more than 90% of the times. Note that different source and the sink locations result in a different distribution of  $T_1$ . As an example, the minimum transit time of the network with a straight line direct plane i.e. the source and the sink is in the same alignment is not necessarily the main dominance because there are only one shortest path but many for the longer paths between the source and the sink.

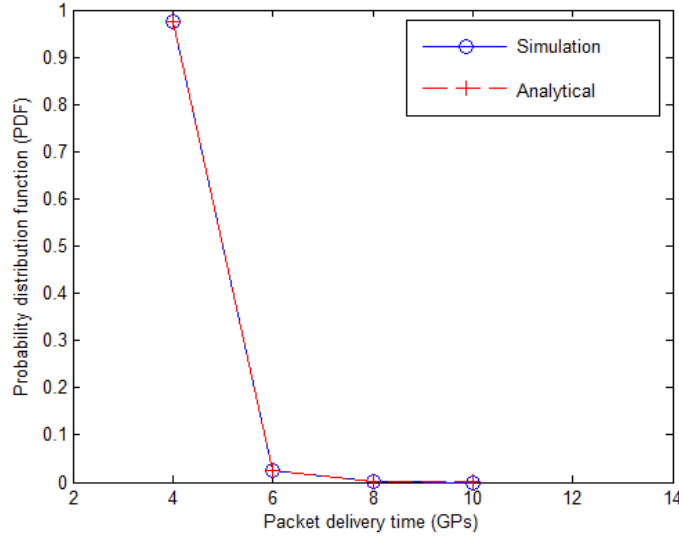


**Figure 20.** Probability distribution function of packet delivery time of 900-node-square-grid network with source at coordinate (10, 10), sink at coordinates (20, 20), and  $p_{gsp} = 0.1$ .

Analytical results are compared to the simulation results to cross-validate each other. The 9-node-square-grid network depicted in Figure 16 is analyzed. There exist six different 4-hop routes and two different 6-hop routes and their combinations. Observing that some routes are symmetric, the symmetric routes reduce the complexity to three different 4-hop routes and one 6-hop route. Additionally, there exists a possibility that a packet can be retransmitted, each retransmission adding two more GPs to the packet delivery time of the same route without retransmission.

The probabilities of each individual route in Table 2 can be combined to create a distribution function of the first packet delivery time for this network. The probability distribution function is “P(first packet delivery time (Number of hops) | a packet is sent from source)”. Figure 21 compares the probability distribution function of packet delivery time from both analytical and simulation approaches, for  $p_{gsp}$  equal to 0.1. The results are consistent and cross-validate each other. Moreover, the minimum transit time is also the majority of first packet delivery times in this case. The first packet delivery time from both analytical and simulation

approaches includes 4, 6, 8, and 10 GPs. The packet delivery time of the simulation and analytical results and in equation (7) from the graph theory analysis also cross-validate each other.



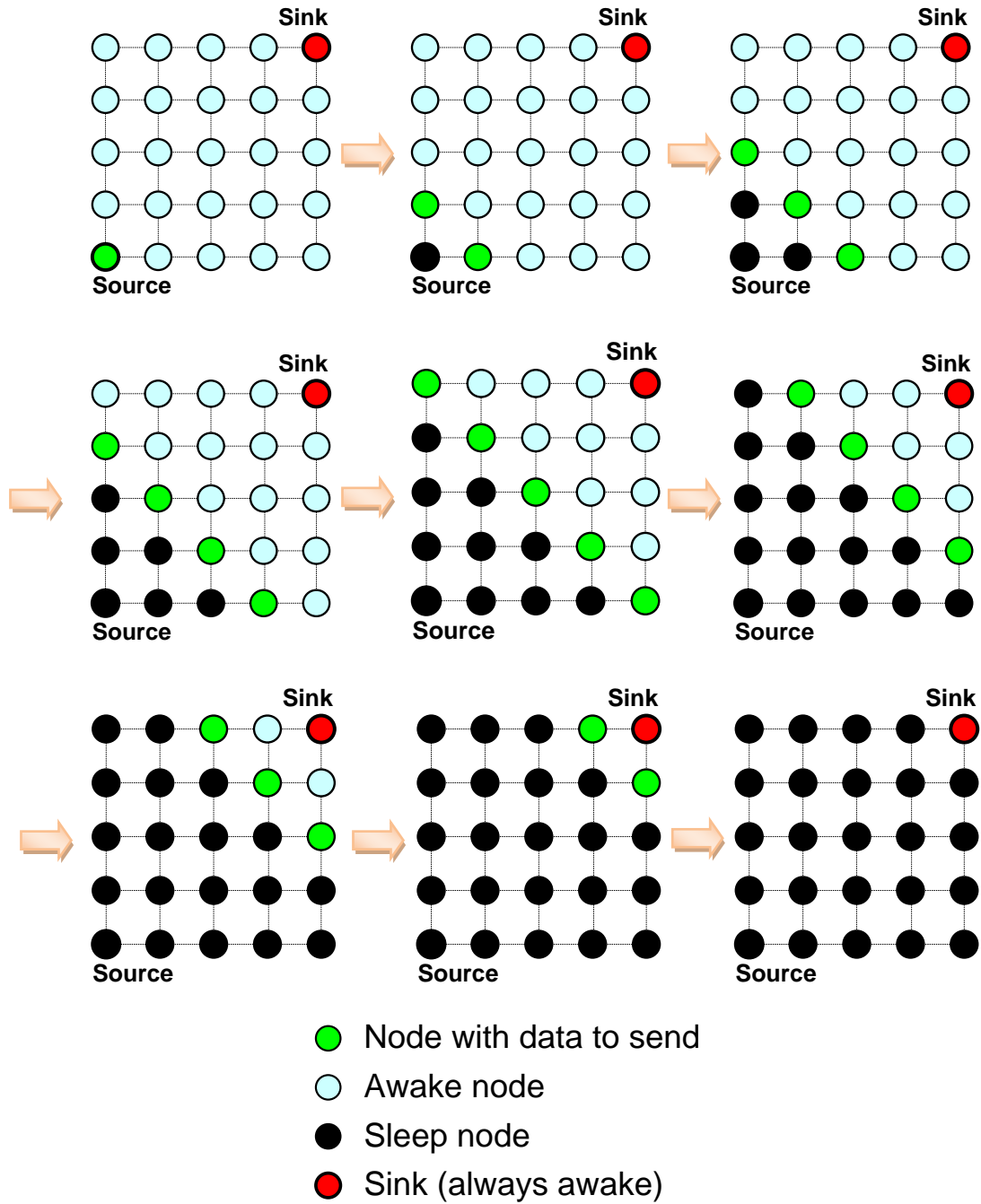
**Figure 21.** Probability distribution function of first packet delivery time of 16-node-square-grid network with source in the middle, sink at the top right corner, and  $p_{gsp} = 0.1$ .

### 4.1.3 Network throughput

The network throughput of WSNs employing GSP depends on factors such as data transfer rate of a sensor node, the total number of nodes, distance between source and sink,  $p_{gsp}$ , etc. In GSP, after a node successfully sends a packet to the nodes nearby, it sleeps for a quiescent period and the node is therefore unavailable for a period of time, defined to be the blackout period. Any new data packets sent during the blackout period cannot reach the sink as the sleeping nodes cascade throughout the network. Figure 22 shows an example of how blackout nodes spread out. The blackout period automatically limits the number of packets the source can send in a period of time, leading to an implicit rate limit of overall network throughput. Moreover, longer



quiescent periods increase blackout periods and decrease network throughput. However, the decrease in throughput is an implicit rate limit which can be useful against denial of service attacks such as energy depletion attack [24].

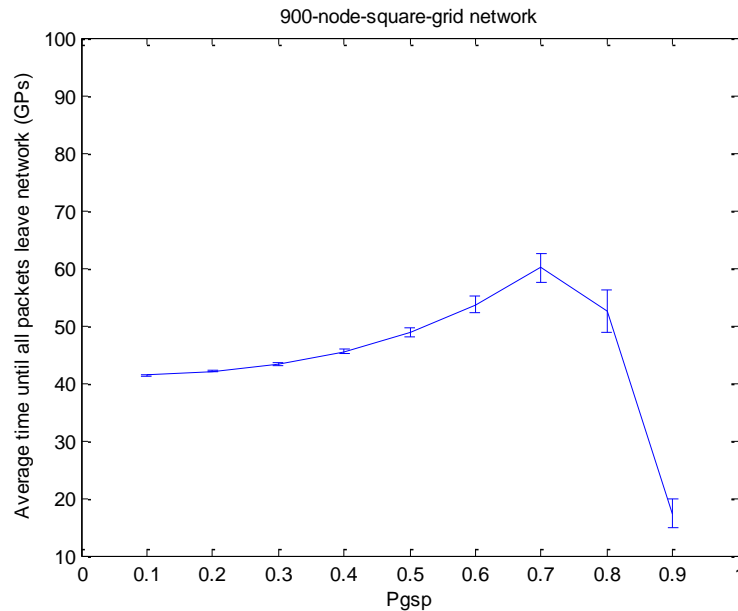


**Figure 22.** Examples of blackout spreading with perfect capture effect and  $p_{gsp} = 0$ .

Apart from the blackout period, the transmitting time, the active time until all packets leave the network, has an effect on network throughput. Longer transmit time reduces the network throughput because it increases GP and the blackout period. The analysis uses a simulation to find an average transmit time, the time it takes to eliminate all duplicate packets. The simulation was run according to the following steps:

1. Source node sends 200 packets for each run.
2. For each packet send, the simulation runs until the last packet exits the network.
3. The simulation computes an average transmit time for each run.
4. The simulation repeats 40 times to find the average transmit time at 90% C.I.

Figure 23 shows an average transmit time. Average transmit time varies according to  $p_{gsp}$ . Additionally, on average it is about twice as much (40 GPs) the minimum transit time (20 GPs in this case).



**Figure 23.** Average transmit time.

#### 4.1.4 Data exposure

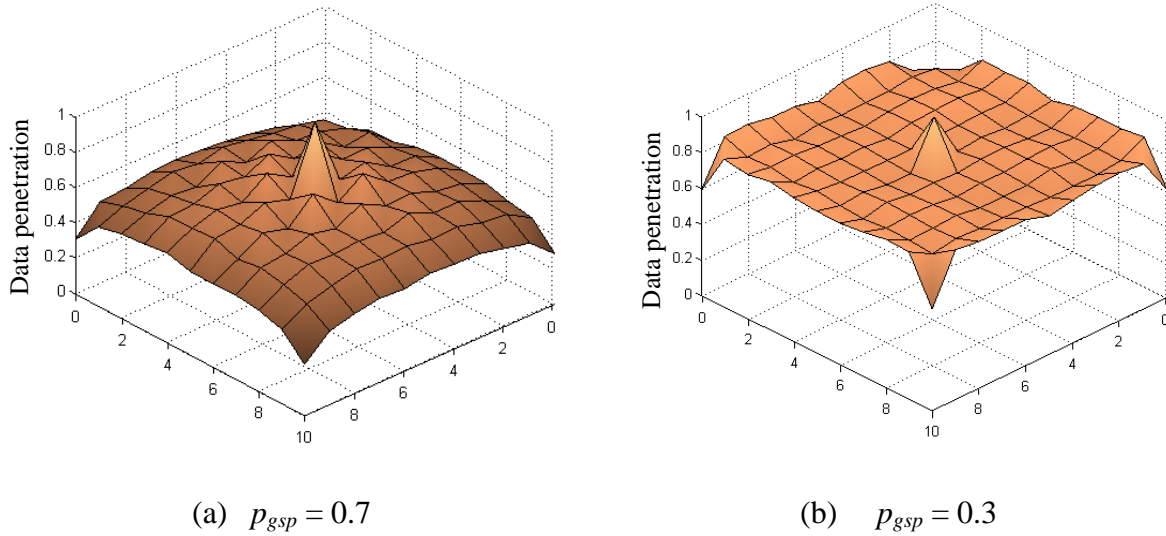
Gossiping belongs to the flooding family among WSN routing protocols. Consequently, each data packet traverses across the network, reaching almost every node in the network and causing high data exposure. High data exposure increases the flexibility of placing a sink node in a network. However, high data exposure also makes WSNs more susceptible to eavesdropping since an intruder has higher chance of intercepting a packet from any node.

One parameter indicating data exposure is data penetration defined as the percentage of packets received at each individual node given that a packet is sent from the source. Data penetration depends on factors such as  $p_{gsp}$ , node density, and physical topology of WSNs. The analysis uses a simulation to find data penetration. The simulation was run according to the following steps:

1. Source node, located at coordinate (5,5) in a 121-node-square-grid WSN, sends 200 packets for each run.
2. For each packet send, the simulation runs until the last packet exits the network.
3. The simulation computes data penetration at each individual node for each run.
4. The simulation repeats 40 times to find data penetration at 90% C.I.

Figure 24 illustrates data penetration of nodes in a WSN employing MACGSP6 when the source node is located in the middle of a 121-node-square-grid WSN. Figure 24 (a) shows that a large value of  $p_{gsp}$ , e.g.,  $p_{gsp} = 0.7$ , results in lower penetration to the distance nodes. Smaller values of  $p_{gsp}$  result in a higher data penetration as more nodes are awake. Figure 24 (b) shows that the penetration spreads evenly regardless of the distance to the source, with the exception of nodes at the four corners which have node degrees of 2. If  $p_{gsp}$  is equal to zero, data penetration

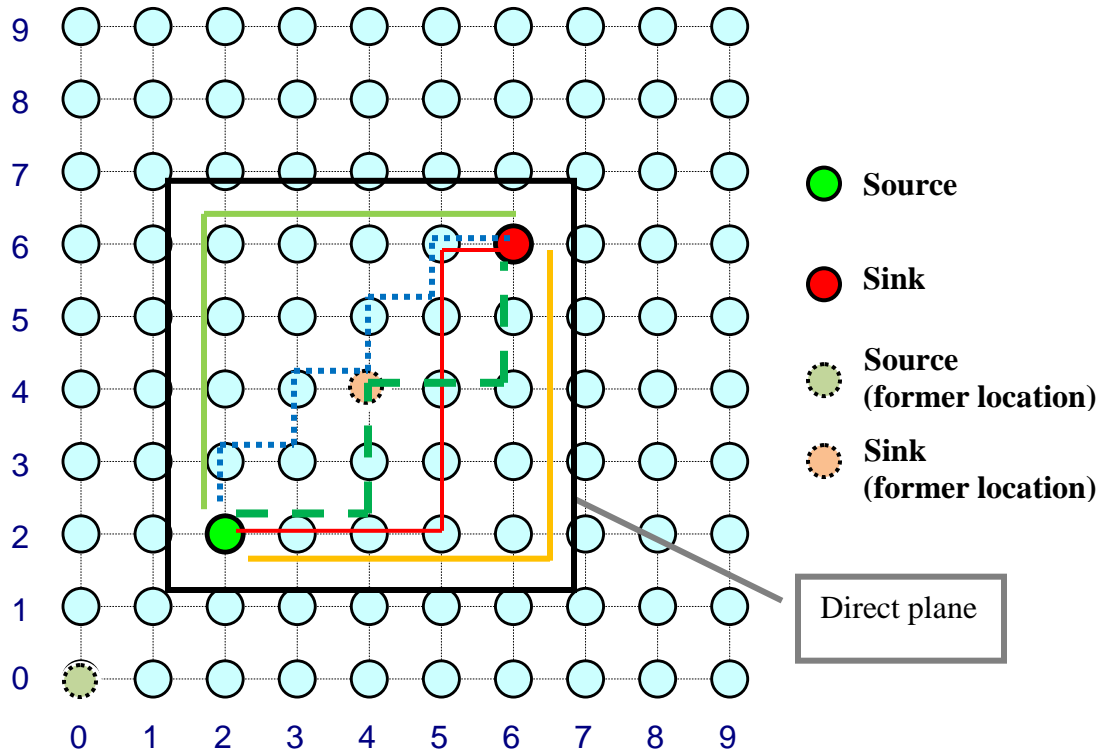
becomes 100% for every node in the network because every node is always awake receiving all packets sent from the source.



**Figure 24.** Data penetration of nodes in WSNs employing MACGSP6 when the source node is located in the middle of a 121- node-square-grid WSN.

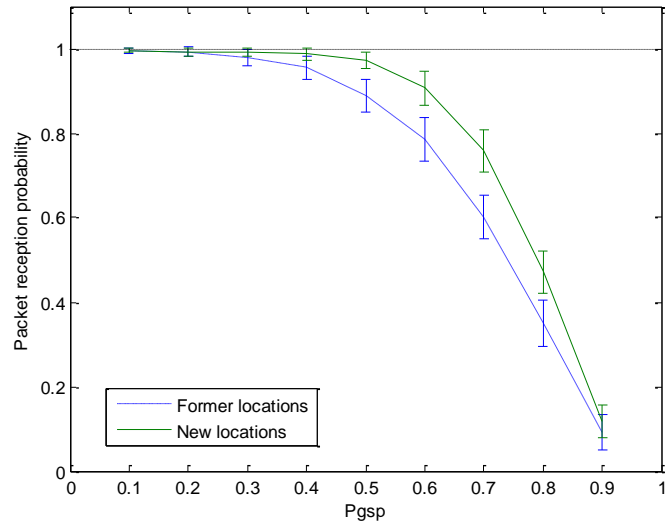
#### 4.1.5 Packet reception probability as a function of source and sink locations

Since the packet reception probability of WSNs varies with the locations of sources and sinks, this study investigates further by shifting the locations of the source and the sink to the middle of the square grid WSN to increase the node degree of the source. Keeping the same distance between source and sink, simulations were conducted with the source at coordinate (2,2) and the sink at (6,6) as shown in Figure 25.

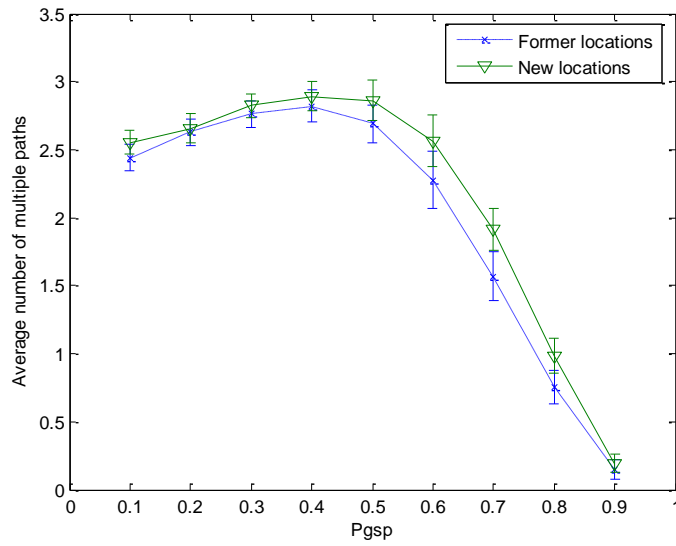


**Figure 25.** 100-node-square-grid network with the source at (2,2) and sink at (6,6).

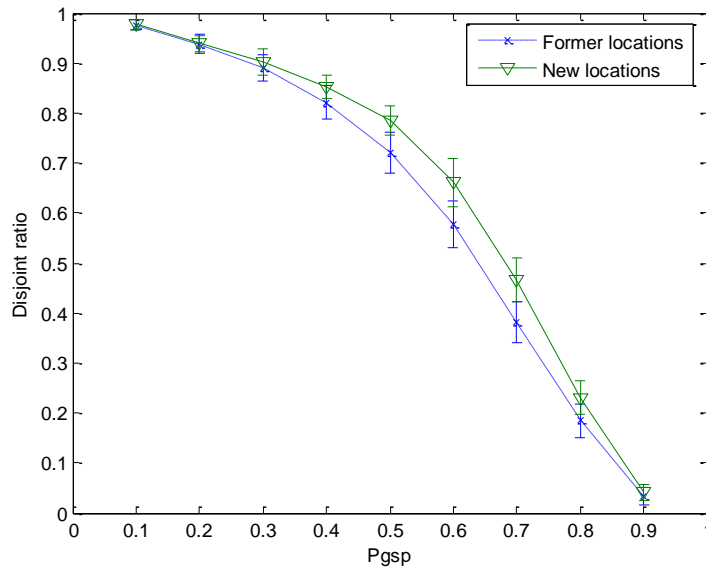
Figure 26, Figure 27, and Figure 28 illustrate the results compared with those of the sink in the corner. The packet reception probability increases without overlapping of the confident intervals for the middle range of  $p_{gsp}$ . However, while the average number of routes and disjoint ratio increased, the differences are not significant at the 90% confidence level.



**Figure 26.** The packet reception probability of 100-node-square-grid network with alternative locations of source and sink.

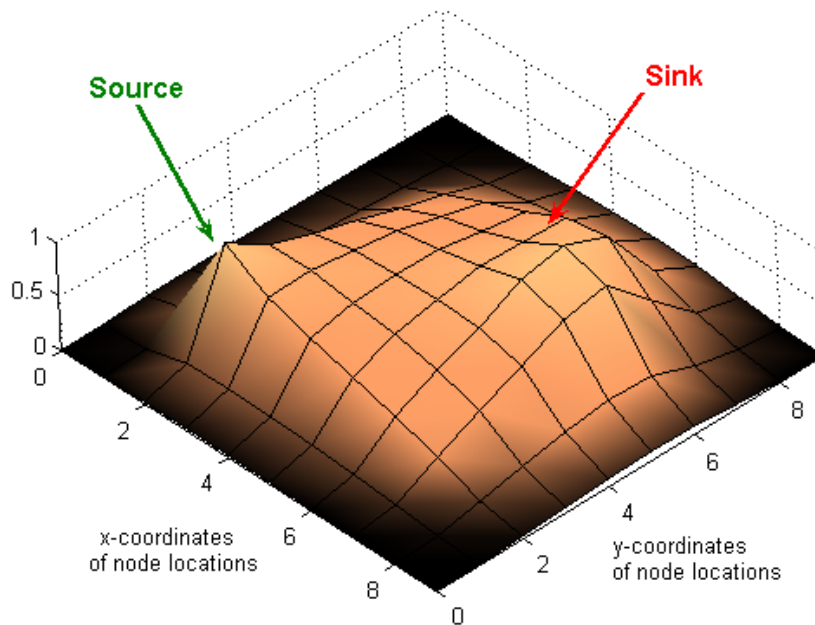


**Figure 27** The average number of successful delivery paths of 100-node-square-grid network with alternative locations of source and sink.



**Figure 28.** The disjoint ratio of 100-node-square-grid network with alternative locations of source and sink.

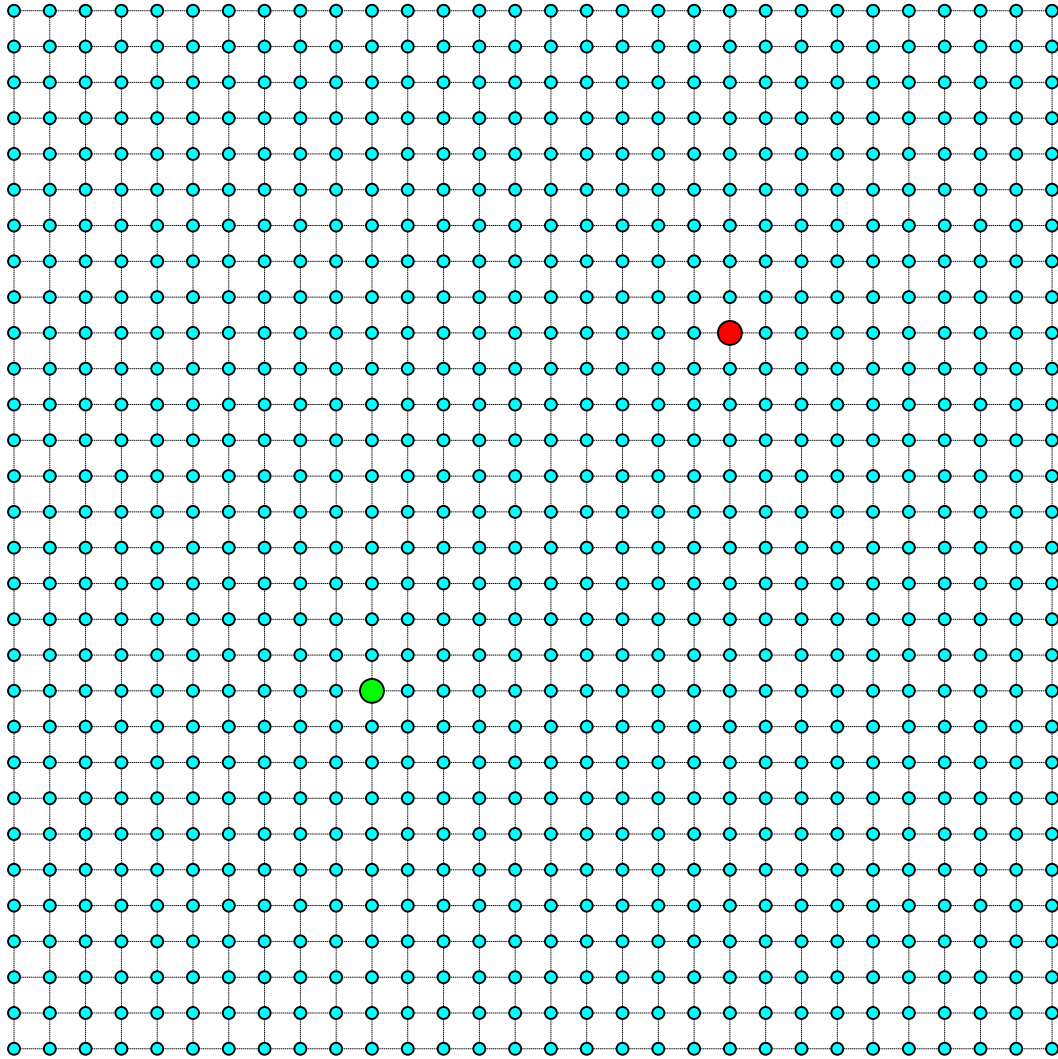
Additional simulations were conducted to determine the majority of nodes acquired by the successful routing paths. Figure 29 shows the node acquisition of successful routing paths. Figure 25 shows that the majority of high acquired nodes are inside the square area called a direct plane. The direct plane contains all the nodes belonging to the set of the shortest routing paths between the source and the sink. Figure 25 illustrated possible shortest routing paths inside a direct plane.



**Figure 29.** The node acquisition of successful routing paths.

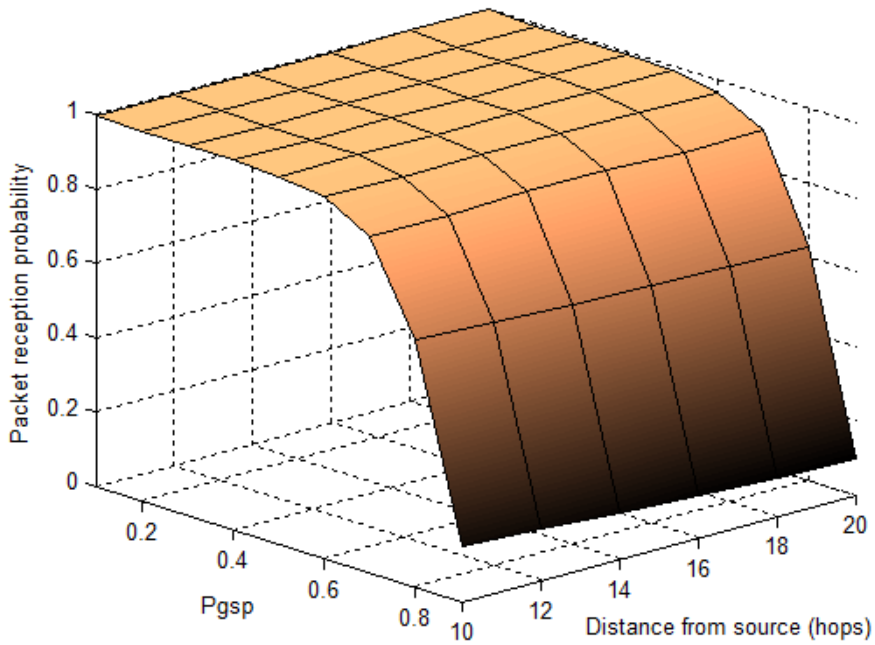
A different distance between source and sink nodes result in different packet reception probability of the network [25]. To study the interaction between packet reception probability and distances, a 900-node-square-grid network was simulated with a source at (10,10) and the sink for each case at 10,12,14,16,18, and 20 hops apart with the following coordinates: (15,15), (16,16), (17,17), (18,18), (19,19), and (20,20) respectively, as depicted in Figure 30.





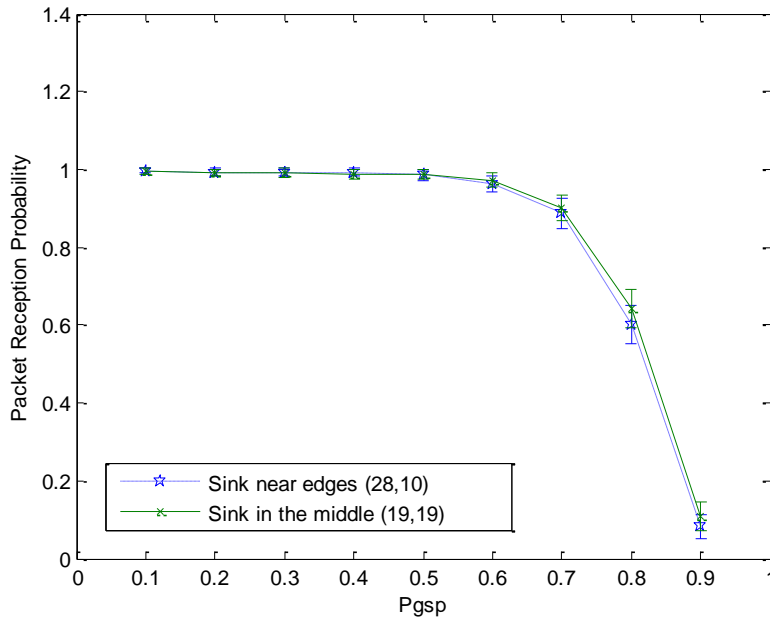
**Figure 30.** 900-node-square grid topology.

Figure 31 illustrates the packet reception probability of the sink as a function of distances between the source and the sink of 900-node-square-grid network. Intuitively, packet reception probability of the network of the closer distance between the source and the sink can be higher than that of the longer distance. However, the results show that closer distance has little impact to packet reception probability when using MACGSP version 6.



**Figure 31.** Packet reception probability of the sink as a function of distances between the source and the sink.

The impact of the sink location was studied by simulating the 900-node-square-grid WSN with the sink near network edge at coordinate (28,10). Figure 32 shows packet reception probability of the sink between the location in the middle and near edge. The result shows that the difference between the probability of reception of the network with sink near edge and the network with sink in the middle is not statistically significant at the 90% level.



**Figure 32.** Packet reception probability of the sink compared between the location in the middle and near edge.

## 4.2 INTRINSIC SECURITY OF A WSN EMPLOYING MRDPS

MRDPS pose both security benefits and problems. Intrinsic security of a WSN employing MRDPS with a single sink was investigated using simulations of a 100-node-square-grid topology as illustrated in Figure 25. This study places the source node at the coordinate (2,2) and the sink node at coordinate (6,6). The source sends two hundred packets for each simulation run. The simulation repeats for 40 runs to find the performance metrics and their 90% confident interval.

This study later extends the network to a larger scale using 900-node-square-grid topology as illustrated in Figure 30. Unless specifying otherwise, the study places the source node at coordinate (10,10) and the sink node at coordinate (20,20) or 20 hops apart from the

source node. Similarly, the source sends two hundred packets for each simulation run. The simulation repeats for 40 runs to find the performance metrics and 90 percent confidence intervals. The analysis considers the intrinsic security of a WSN employing MRDPs with three different types of security threats in WSNs including: integrity threats, availability threats, and confidentiality threats. The security threats and associated attack models used in this analysis are described in the following section.

## **4.2.1 SECURITY THREATS AND ATTACK MODELS**

### **4.2.1.1 Integrity threats**

WSN applications often require wireless sensor nodes to be left unattended, allowing intruders a chance to capture and compromise sensor nodes [1, 14]. If intruders successfully compromise sensor nodes, WSNs then can be vulnerable to security attacks such as fault data injection and message modification attacks. However, the number of compromised nodes may vary depending on how strong of security techniques implemented in sensor nodes. This study assumes the number of compromised nodes is limited and the more compromised nodes, the more difficult and expensive it is for an intruder to achieve its goal.

#### **(a) Message modification attacks**

In message modification attacks, intruders capture and compromise sensor nodes such that intruders can change the content of original message unnoticeable by any other nodes including the sink node. More specifically, these compromised nodes always transmit a modified packet whenever they receive a packet regardless of type or content of the packets. In WSNs with

multiple attacking nodes, the study assumes the worst case scenario where all attacking nodes send the same modified message as to deceive a WSN using majority voting.

#### **Attack model in this study**

- Intruders capture and compromise nodes allowing them to modify the received message and forward it to its neighbors.
- If the compromised node received a packet it always retransmits a modified packet

#### **(b) Fault data injection attacks**

In fault data injection attacks intruders capture and compromise sensor nodes which are used to send a fault-data packet resembling a legitimate packet. Intruders try to trick the sink into accepting a fault-data packet by injecting the fault-data packet into the network for every packet sent from a legitimate source. Assuming a worst case scenario, these compromised nodes always transmit the same fault-data packet regardless of type or contents of the packets originated from the source.

#### **Attack model in this study**

- Intruders capture and compromise nodes allowing them to send any message at will.
- Intruders use the compromised node to inject one fault-data packet into the network for every message sent from the source.
- If the compromised node receives a packet it always retransmits a fault-data packet.

#### **4.2.1.2 Availability threats**

Apart from integrity, an adversary can target WSN service availability such that WSNs cannot function properly. As an example, intruders can disable wireless communication of an individual or a group of sensor nodes by launching jamming attacks without having to capture any sensor

nodes. Moreover, if intruders successfully capture a sensor node, intruders can also launch packet flooding attacks, wasting network resources such as bandwidth and energy.

#### **(a) Jamming attacks**

A jamming attack is one type of DoS attack targeting on service availability. Jamming attacks performed at the physical layer by using a stronger signal to interfere the wireless signal used to communicate among sensor nodes. Thus, the target nodes cannot receive data from their neighbors due to stronger signal broadcasting from jammer source.

#### **Attack model in this study**

- Intruder approach the target node and broadcast a stronger signal.
- For a single attack only one targeted node cannot receive nor forward any packets sent from its neighbors.
- For multiple attacks, the analysis assumes an intruder launches a single attack on multiple locations with every location is equally likely to be attacked excluding the source and the sink.

#### **(b) Packet flooding attacks**

One possible method for an intruder to reduce service availability of WSNs is by taking over as much network resources as possible. If a sensor node is compromised, an intruder can use this sensor node to repeatedly inject bogus packets into the network, wasting the network resources (bandwidth and energy).

#### **Attack model in this study**

- Intruders capture nodes allowing them to send any messages at will.
- Intruders use the compromised node to repeatedly inject a packet into a network.

- The analysis assumes every location is equally likely to be attacked excluding the source and the sink.

#### **4.2.1.3 Confidentiality threats**

Confidentiality is the opposite of data exposure. High data exposure results in higher risk of packets being intercepted or monitored. If intruders are within the wireless range, they can launch eavesdropping attacks by monitoring the content sent along wireless sensor networks.

##### **(a) Eavesdropping attacks**

When node transmit packets in clear text intruders can launch a passive eavesdropping attack by capturing packets and read the content of the packet directly. This study assumes an eavesdropper can monitor transmitted data from any location in the network.

##### **Attack model in this study**

- Intruders approach an intermediate node allowing them to capture a packet from that particular node. Intruders capture a packet and read the content of the packet.

#### **4.2.2 Message modification attacks**

In message modification attacks, an intruder captures and compromises an intermediate wireless sensor node in a WSN and gains control over it. The intruder then uses the compromised node to attack a WSN by modifying every packet received and forwarding it to neighbors. Employing MRDPs allows the sink to detect anomalous received packets by comparing the multiple copies received via different paths. If the sink receives different contents among multiple copies of the same original packet, the sink assumes an anomaly occurred and discards all copies of the

packets received. Since the routing paths are random, the intruder has less chance of knowing the exact routing paths to the sink. Simulations were run according to the following steps:

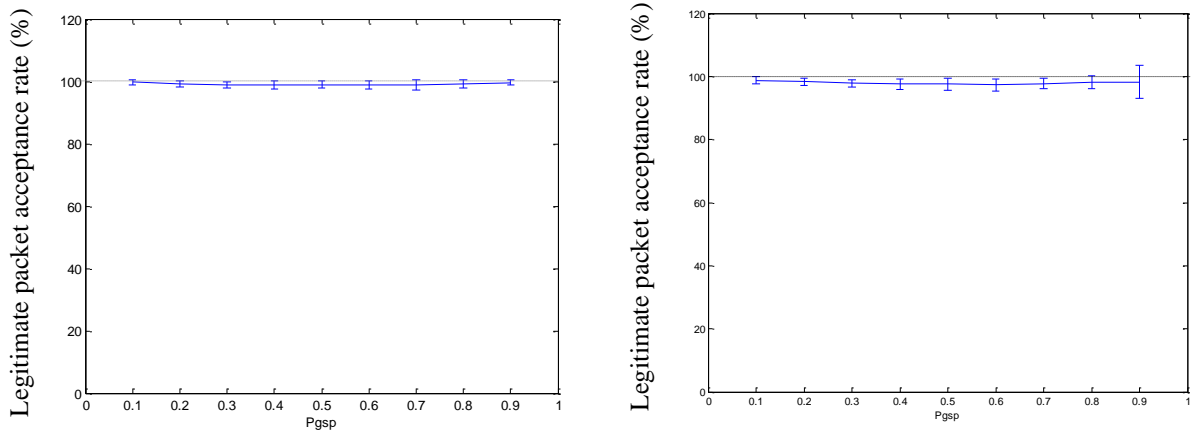
1. A compromised node is randomly selected. The compromised node turns every packet received into a modified packet and forwards it to its neighbors.
2. The source node sends 200 packets.
3. For each packet send, the simulation runs until the last packet exits the network.
4. The simulation repeats this process 40 times to find performance metrics at 90% C.I.

The simulation computes the following performance metrics:

- (a) Since the sink discards packets whenever it detects anomaly, the performance metrics includes packet discard rate.
- (b) Because of packet discarding, the probability of the sink accepting packets for a WSN changes, i.e., the effective packet reception probability during the attack. The simulation computes the probability of the sink accepting packets as the number of packets accepted divided by the total number of packets received at the sink.
- (c) As packets accepted by the sink include both legitimate and modified packets, the performance metrics also include the probability of the sink accepting modified packets as another performance metric defined by the number of modified packet accepted by the total number of packet received at the sink.
- (d) Finally, the simulations compute the legitimate packet acceptance rate of the sink as one of the performance metrics.



Figure 33 (a) shows the legitimate packet acceptance rate of a WSN with a single sink under a message modification attack for a 100-node-square-grid WSN with all nodes are equally likely to be compromised. In the case of one attacking node, the legitimate packet acceptance rate is very close to 100%. Figure 33 (b) illustrates the legitimate packet acceptance rate for a 900-node-square-grid WSN with a single sink in which the protocol responds in the same manner as the 100-node-square-grid WSN.

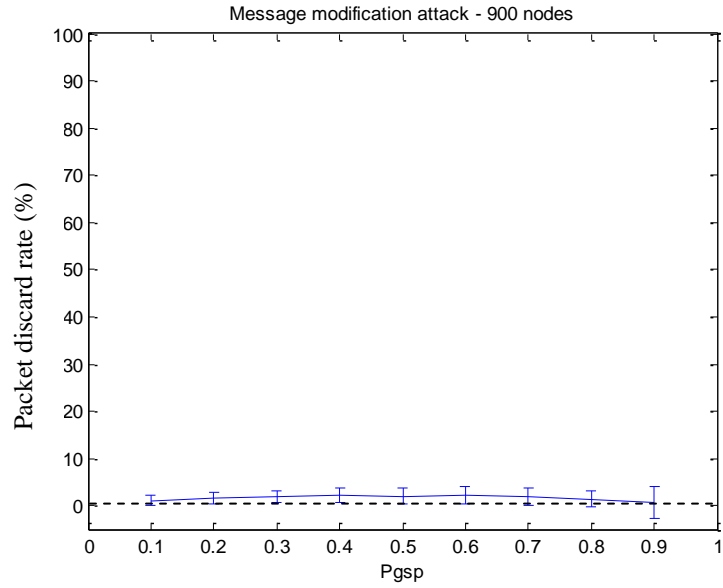


(a) A 100-node-square-grid WSN

(b) A 900-node-square-grid WSN

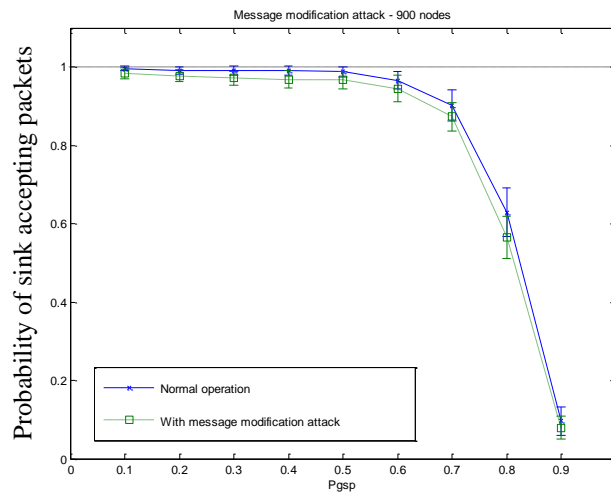
**Figure 33.** Legitimate packet acceptance rate of WSNs under a message modification attack.

The packet discard rate of a WSN with 900 nodes under a message modification attack is shown in Figure 34.



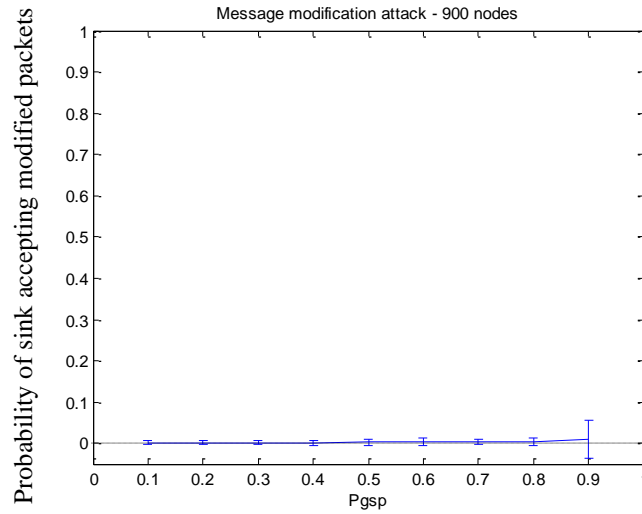
**Figure 34.** Packet discard rate of a 900-node-square-grid WSN under a message modification attack.

Figure 35 compares between the probability of the sink accepting packets in a WSN under the attack and that of a WSN without the attack. No difference is seen at the 90% confidence level.



**Figure 35.** Probability of the sink accepting packets in a 900-node-square-grid WSN under a message modification attack.

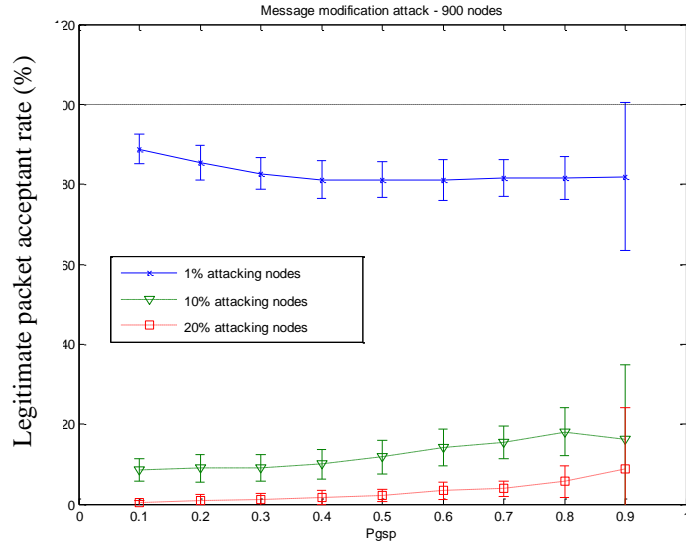
Figure 36 shows the probability of the sink accepting modified packets in a WSN with 900 nodes under a message modification attack which is very close to zero.



**Figure 36.** Probability of the sink accepting modified packets in a 900-node-square-grid WSN under a message modification attack.

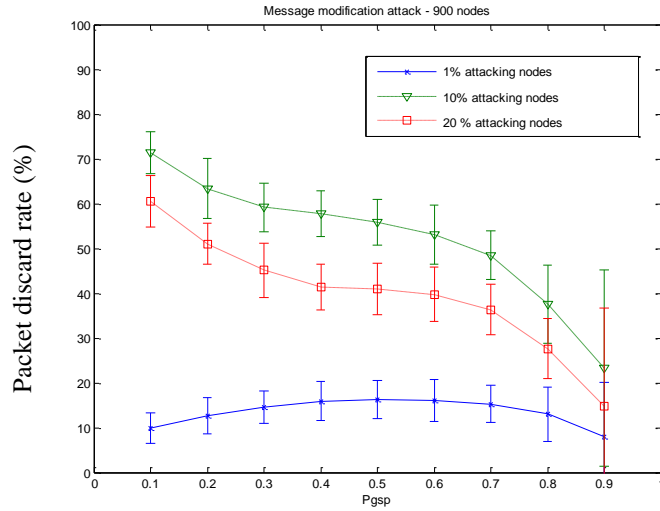
#### 4.2.2.1 Increasing numbers of attacking nodes generating message modification attacks

Simulations of 900 node WSN networks with increasing the numbers of attacking nodes were conducted. Results include 1% (9 nodes), 10% (90 nodes) and 20% (180 nodes) attacking the network. Figure 37 shows that the legitimate packet acceptance rate of WSNs with a single sink drops significantly as more nodes are compromised.



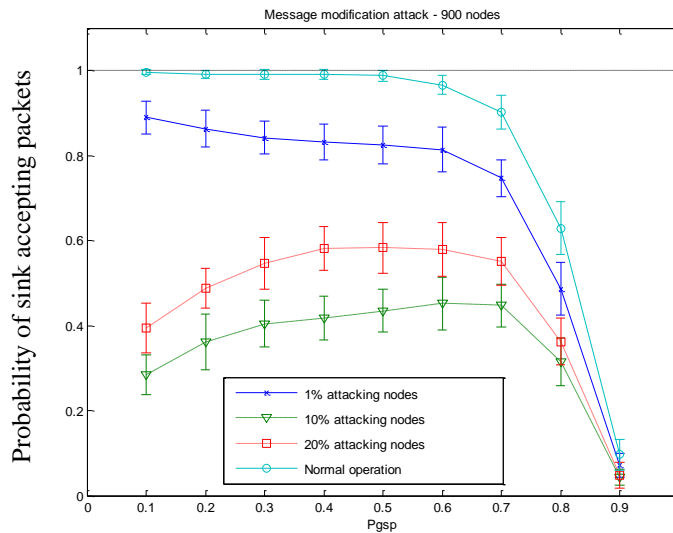
**Figure 37.** Legitimate packet acceptance rate of a 900-node-square-grid WSN under a message modification attack compared with 1%, 10% and 20% compromised nodes.

As depicted in Figure 38, the packet discard rate also increases but there is also an interesting behavior here. From the result, packet discard rate at 20% of compromised nodes lies in between packet discard rate at 1% and 10% of compromised nodes. One possible reason is that the packet discard rate goes beyond its peak and starts to drop down. Since the number of compromised nodes is too great such that the legitimate packets are almost unable to reach the sink, most of the time the sink receives only modified messages and accepts them as legitimate reducing the packet discard rate.

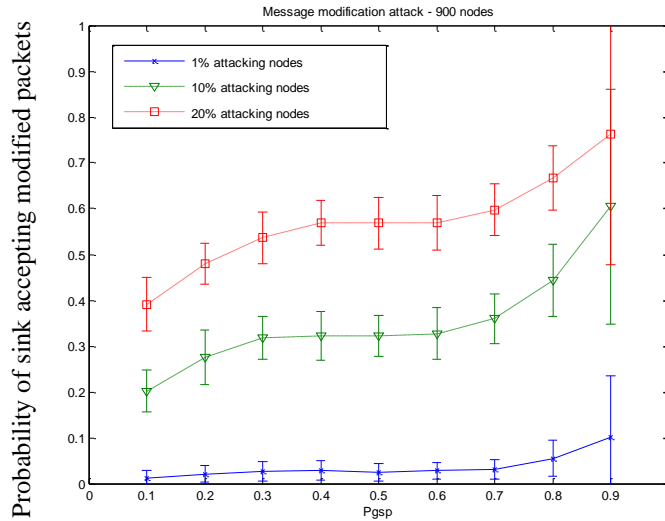


**Figure 38.** Packet discard rate of a 900-node-square-grid WSN under a message modification attack compared with 1%, 10% and 20% compromised nodes.

Figure 39 shows the probability of the sink accepting packets which responds in the same manner corresponding to the packet discard rate. Figure 40 confirms the explanation as the probability of the sink accepting packets increases more than 50% for the case of 20% compromised nodes.



**Figure 39.** Probability of the sink accepting packets in a 900-node-square-grid WSN under a message modification attack compared with 1%, 10% and 20% compromised nodes.



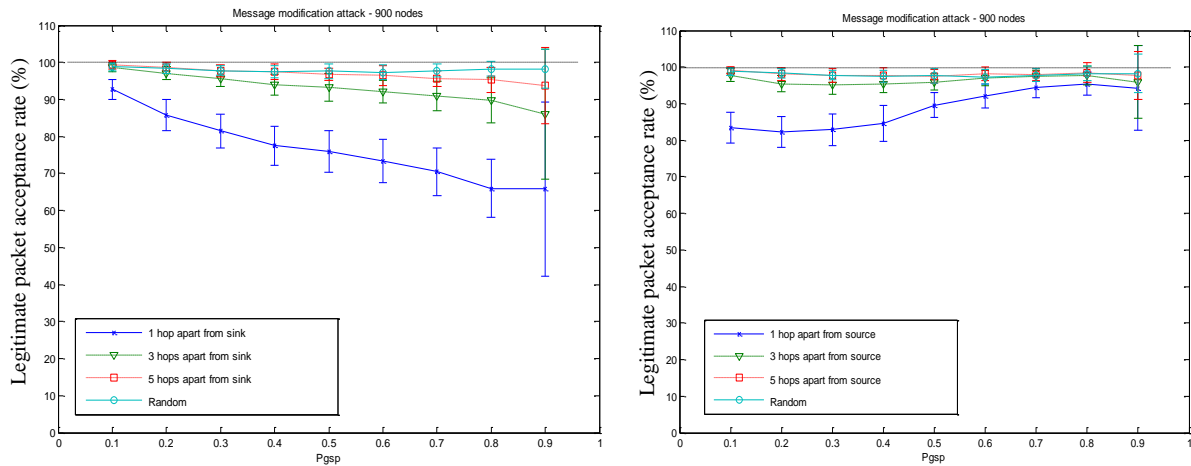
**Figure 40.** Probability of the sink accepting modified packets in a 900-node-square-grid WSN under a message modification attack compared with 1%, 10% and 20% compromised nodes.

#### 4.2.2.2 Impact of attacker location on attack effectiveness

Based on the result in section 4.2.2, when the number of attacking nodes is not too great, MACGSP version 6 is intrinsically robust to message modification attacks. However, the simulations consider only the case where all nodes are equally likely being compromised. In the real world, nodes may not always be equally likely being compromised because intruders can opt to compromise the nodes providing the best chance of success. For example, an intruder can choose to attack the nodes near the sink because the corrupted packets from these nodes are more likely to reach the sink than the legitimate packet. Similarly, if the attacker is close to the source the result can also be different because the attacker has higher chance of modifying packets before the packets reach the other nodes.

Figure 41 (a) depicts the legitimate packet acceptance rate when an attacker is closer to the sink. The results show that the attacker locations have little impact to the legitimate packet acceptance rate except for the case of an attacker next to the sink. When an attacker is next to the

sink, the attacking node becomes one of the sink's neighbors. Since every route to the sink contains at least one of the sink's neighbors, the chance of the attacking node becoming a part of the route increases. Figure 41 (b) shows the legitimate packet acceptance rate when attacker is closer to the source. Likewise, the results show that the attacker locations have little impact to the legitimate packet acceptance rate except for the case of an attacker next to the source.

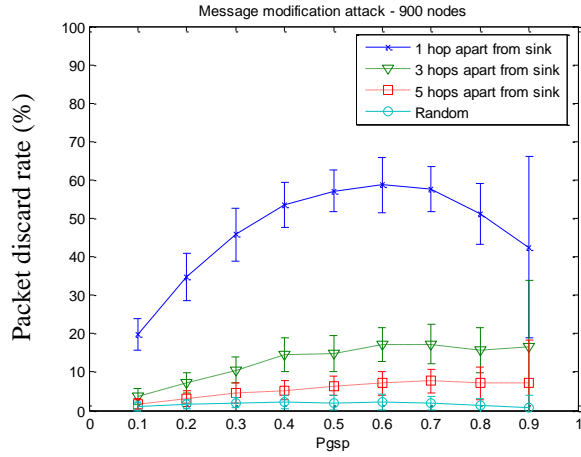


(a) an attacker close to the sink

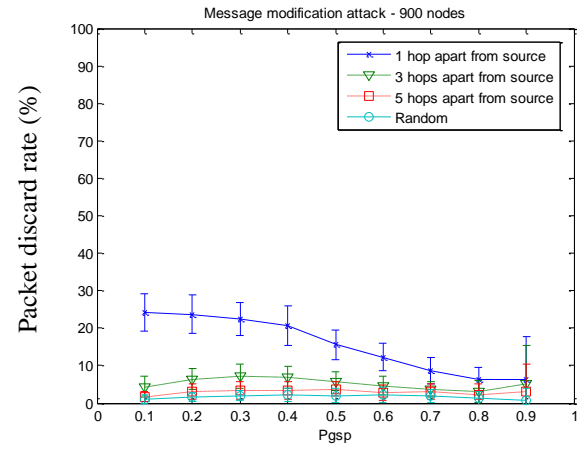
(b) an attacker close to the source

**Figure 41.** Legitimate packet acceptance rate of a 900-node-square-grid WSN under a message modification attack as a function of attacker location.

Figure 42 shows the packet discard rate when (a) an attacker is closer to the sink and (b) an attacker is closer to the source. The packet discard rate increases the most when an attacker is next to the sink.



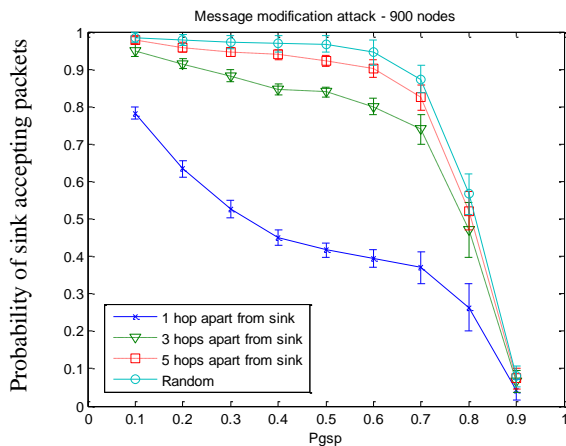
(a) an attacker close to the sink



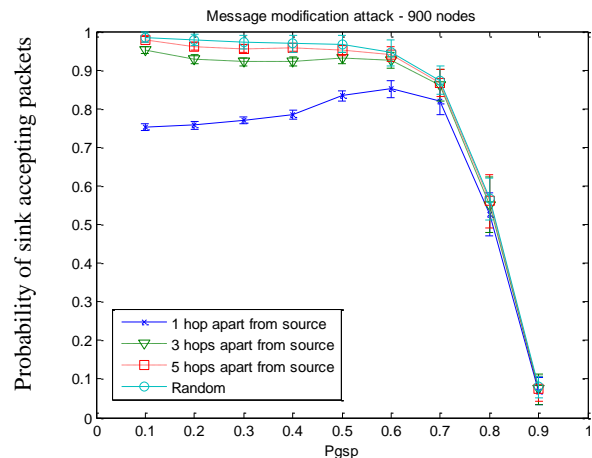
(b) an attacker close to the source

**Figure 42.** Packet discard rate of a 900-node-square-grid WSN under a message modification attack as a function of attacker location.

Figure 43 illustrates the probability of the sink accepting packets when (a) an attacker is closer to the sink and (b) an attacker is closer to the source. The results show that attackers closer to the sink are more effective at message modification attacks as the probability of the sink accepting packets decreases.



(a) An attacker close to the sink

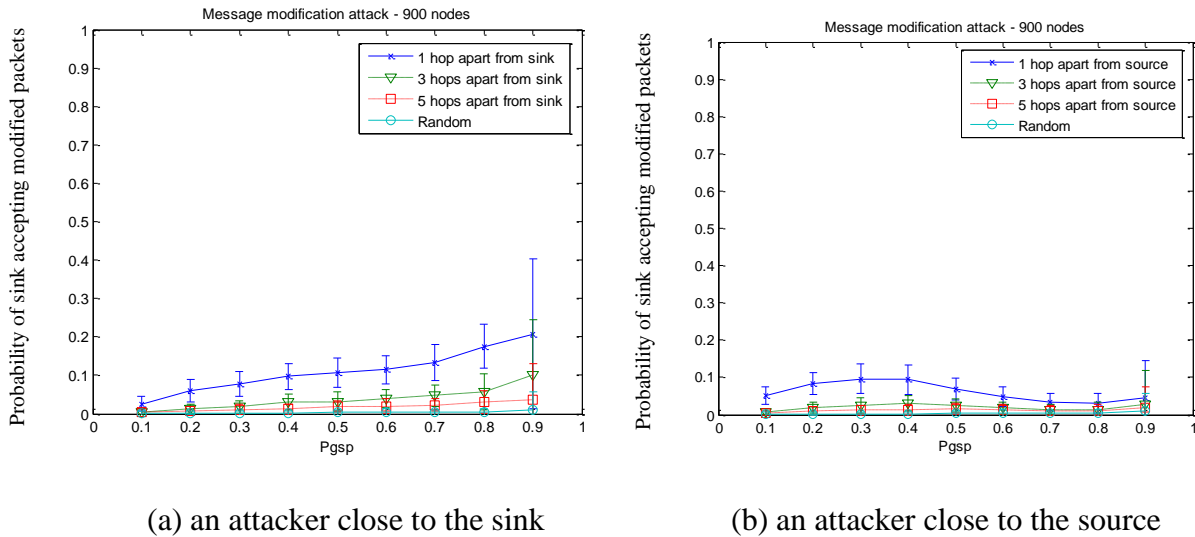


(b) An attacker close to the source

**Figure 43.** Probability of the sink accepting packets in a 900-node-square-grid WSN under a message modification attack as a function of attacker location.



Figure 44 depicts probability of the sink accepting a modified packet when (a) an attacker is close to the sink and (b) an attacker is close to the source. The probability of the sink accepting a modified packet increases when the attacker is next to the sink or the attacker is next to the source. In summary, during a message modification attack all security performance metrics of a WSN with an attacker near the sink are worse than they are with an attacker near the source.



**Figure 44.** Probability of the sink accepting modified packets in a 900-node-square-grid WSN under a message modification attack as a function of attacker location.

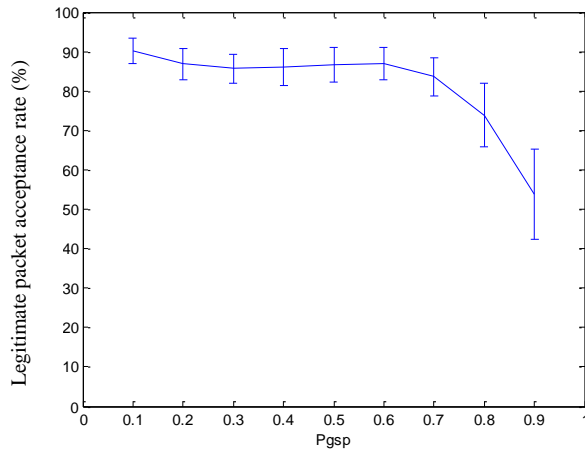
### 4.2.3 Fault data injection attacks

Similar to message modification attacks, MRDPs can also be useful against fault data injection attacks. Simulations were performed to find an average legitimate packet acceptance rate of a WSN with a single sink when an intruder performs a fault data injection attack. The study first considers the case when wireless sensor nodes are equally likely to be compromised and measures legitimate packet acceptance rate, packet discard rate, probability of the sink accepting

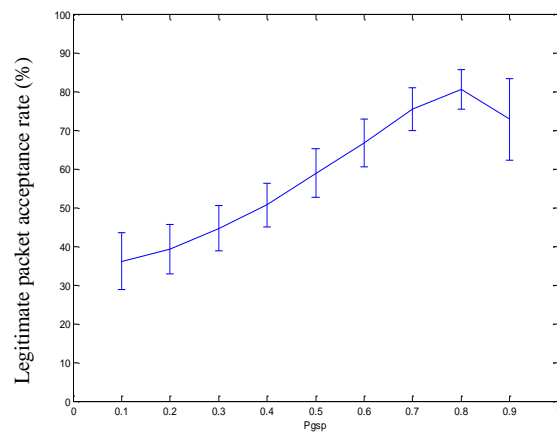
packets, and probability of the sink accepting fault-data packets. Simulations were run according to the following steps:

1. A compromised node is randomly selected. The compromised node turns every packet received into a fault-data packet and forwards it to its neighbors.
2. The Source node sends 200 packets
3. For each packet send, the simulation runs until the last packet exits the network.
4. The simulation repeats this process 40 times to compute security performance metrics at 90% C.I.

Figure 45 (a) shows the legitimate packet acceptance rate of a 100-node-square-grid WSN under a fault data injection attack when all nodes are equally likely to be compromised. Unlike the legitimate packet acceptance rate in the case of a message modification attack, the legitimate packet acceptance rate in this case decreases to be less than 90%. Figure 45 (b) illustrates the legitimate packet acceptance rate of a 900-node-square-grid WSN dropping greater than that of the 100-node-square-grid network.



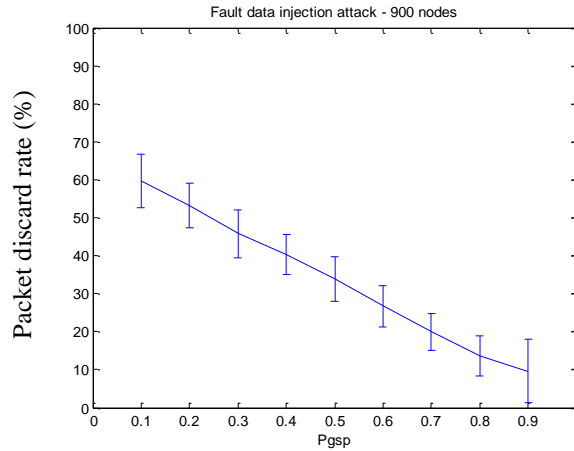
(a) A 100-node-square-grid WSN



(b) A 900-node-square-grid WSN

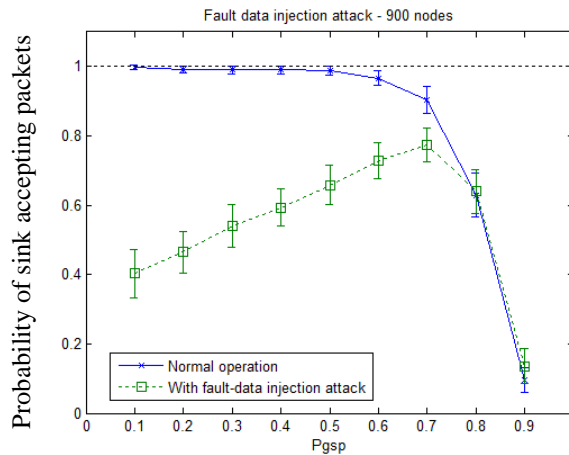
**Figure 45.** Legitimate packet acceptance rate of WSNs under a fault data injection attack.

Figure 46 illustrates packet discard rate of a 900-node-square-grid WSN under a fault data injection attack. The packet discard rate increases to be in between 10% to 60% (depending on  $p_{gsp}$ ).



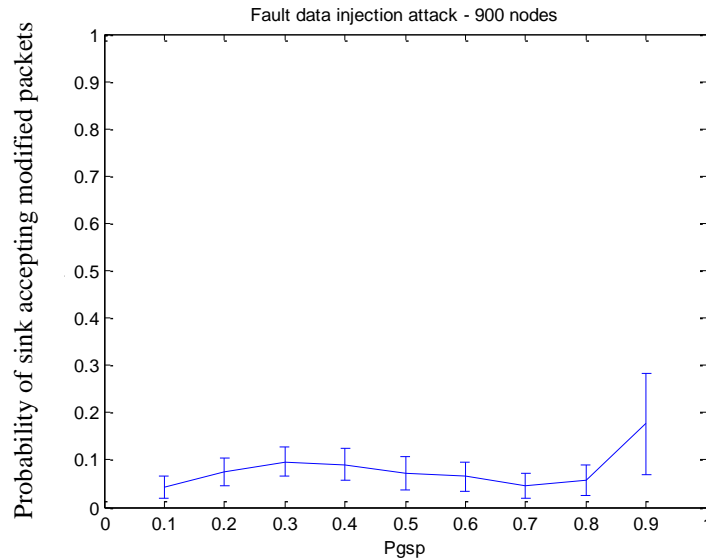
**Figure 46.** Packet discard rate of a 900-node-square-grid WSN under a fault data injection attack.

Figure 47 shows the probability of the sink accepting packets in a 900-node-square-grid WSN under a fault data injection attack. The probability of the sink accepting packets decreases considerably especially for  $p_{gsp}$  less than 0.6.



**Figure 47.** Probability of the sink accepting packets in a 900-node-square-grid WSN under a fault data injection attack.

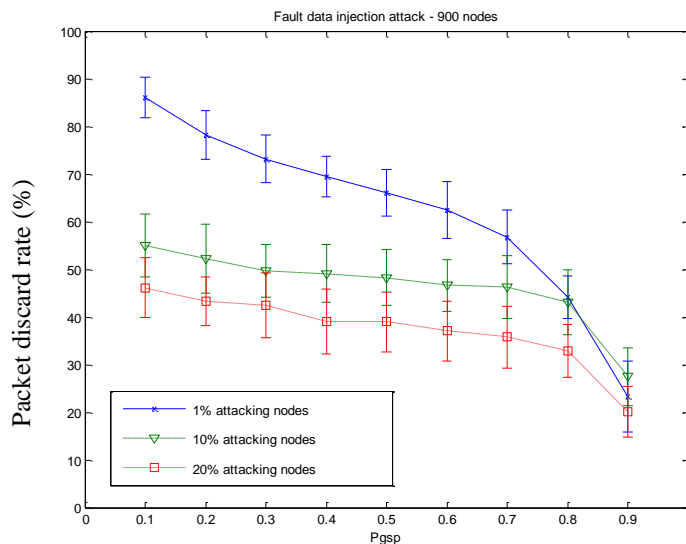
Figure 48 depicts the probability of the sink accepting fault-data packets in a 900-node-square-grid WSN under a fault data injection attack. The probability of the sink accepting fault-data packets also increases to be about 0.1.



**Figure 48.** Probability of the sink accepting fault-data packets in a 900-node-square-grid WSN under a fault data injection attack.

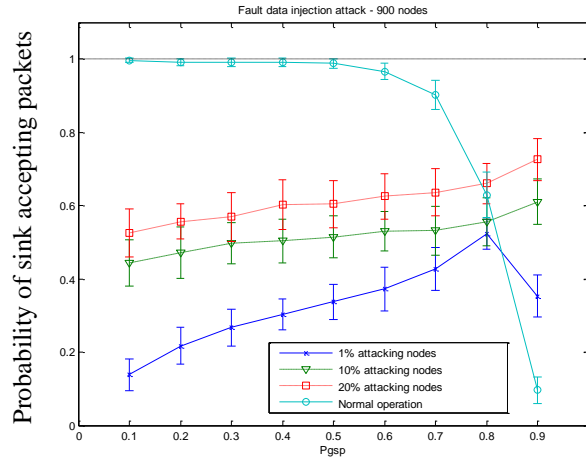
#### 4.2.3.1 Increasing numbers of attacking nodes generating fault data injection attacks

Likewise, the study increases the number of attacking nodes to 1% (9 nodes), 10% (90 nodes), and 20% (180 nodes). Figure 49 illustrates the packet discard rate of a 900-node-square-grid WSN under fault data injection attacks compared at a different number of attacking nodes. The result shows that increasing the number of attacking nodes reduces the packet discard rate.



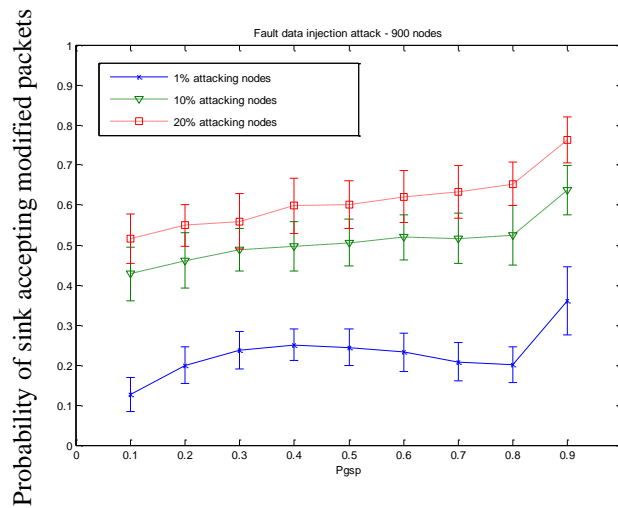
**Figure 49.** Packet discard rate of a 900-node-square-grid WSN under a fault data injection attack compared with 1%, 10% and 20% compromised nodes.

Figure 50 shows the probability of the sink accepting packets in a 900-node-square-grid WSN under fault data injection attacks compared at a different number of attacking nodes. Similarly, as the number of attacking nodes increases the probability of the sink accepting packets increases corresponding to the decreasing of packet discard rate. The results appears differently at higher value of  $p_{gsp}$  for both packet discarding rate and the probability of the sink accepting packets because they account only the case the sink receives a packet and packet reception probability is much less than one at higher value of  $p_{gsp}$ .



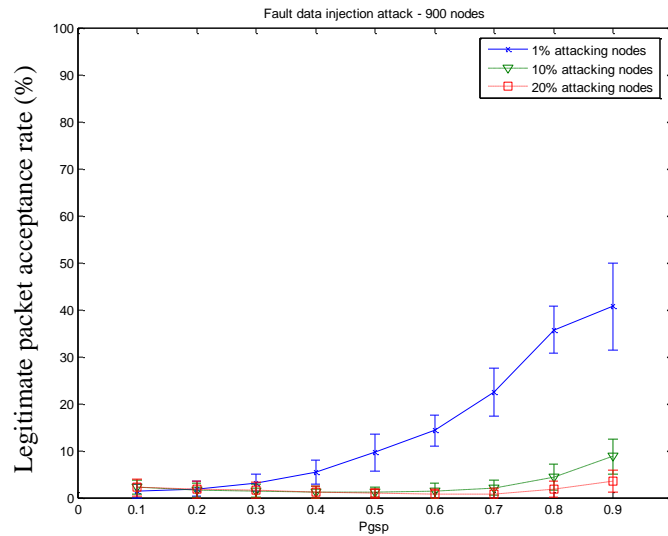
**Figure 50.** Probability of the sink accepting packets in a 900-node-square-grid WSN under a fault data injection attack compared with 1%, 10% and 20% compromised nodes.

Figure 51 shows the probability of the sink accepting fault-data packets in a 900-node-square-grid WSN under fault data injection attacks compared at a different number of attacking nodes. Increasing the number of attackers increases the probability of the sink accepting fault-data packets because the modified packets from the attacking nodes overwhelm the sink node reducing the chance of legitimate packets to arrive at the sink.



**Figure 51.** Probability of the sink accepting fault-data packets in a 900-node-square-grid WSN under a fault data injection attack compared with 1%, 10% and 20% compromised nodes.

Figure 52 depicts the legitimate packet acceptance rate of a 900-node-square-grid WSN under increased number of fault data injection attacking nodes. Similarly, more attacking nodes appear to reduce the legitimate packet acceptance rate because they increase the chance of fault packets arriving at the sink. However, with 1% attacking nodes (9 nodes) the legitimate packet acceptance rate decreases to almost zero for small value of  $p_{gsp}$ .

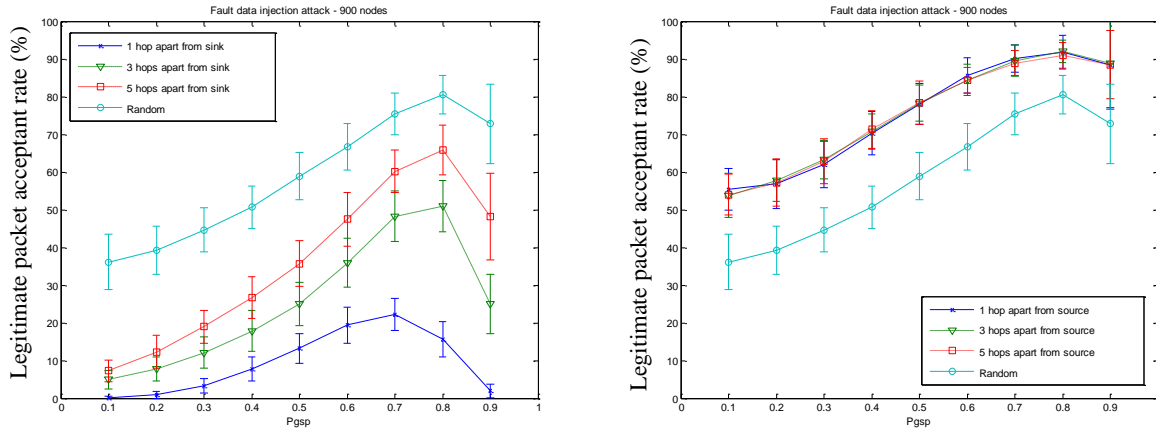


**Figure 52.** Legitimate packet acceptance rate of a 900-node-square-grid WSN under a fault data injection attack compared with 1%, 10% and 20% compromised nodes.

#### 4.2.3.2 Impact of attacker location on attack effectiveness

Figure 53 demonstrates legitimate packet acceptance rate of 900-node-square-grid WSNs under a fault data injection attack from two circumstances: (a) when an attacking node is close to the sink and (b) when it is close to the source. The result shows that legitimate packet acceptance rate decreases greatly when an attacker closes to the sink especially for the case of one hop apart from the sink. However, when an attacker is closer to the source the results are the same for all

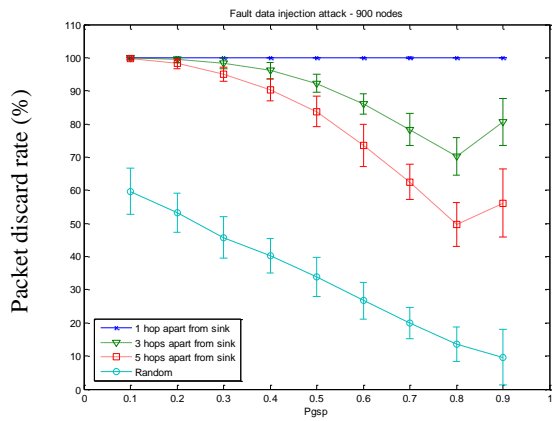
three different distances but they are better than those of random distances. The attacking nodes close to the source have almost the same chance as the source to reach the sink.



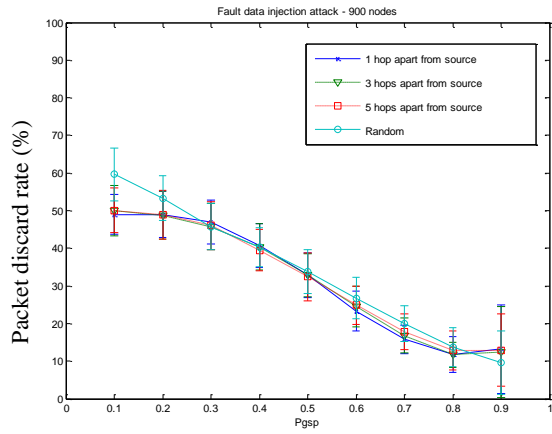
(a) an attacker close to the sink (b) an attacker close to the source  
**Figure 53.** Legitimate packet acceptance rate of a 900-node-square-grid WSN under a fault data injection attack as a function of attacker location.

Figure 54 (a) illustrates packet discard rate of a 900-node-square-grid WSN under a fault data injection attack when an attacker is close the sink. Packet discard rate increases to almost 100% when an attacker is next to the sink. Figure 53 (b) illustrates packet discard rate of 900-node-square-grid WSNs under a fault data injection attack when an attacker is close the source which is not much affected from various distances. Figure 55 depicts probability of the sink accepting packets in a 900-node-square-grid WSN under a fault data injection attack when (a) an attacker is close the sink and (b) an attacker is close the source. The probability of the sink accepting packets decreases to near zero when the attacker is next to the sink but remains unaffected regardless of the distances to the source.



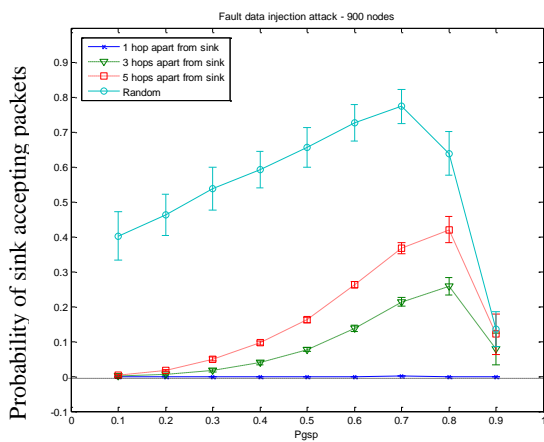


(a) an attacker close to the sink

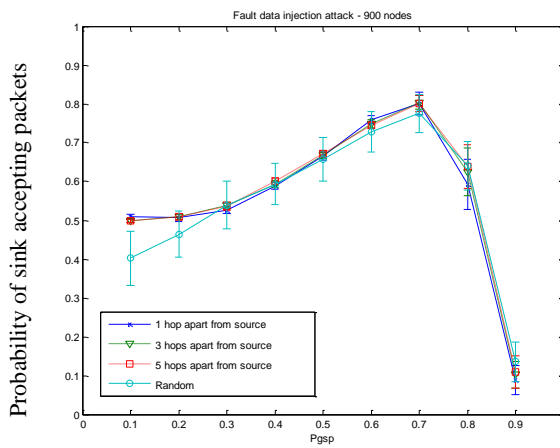


(b) an attacker close to the source

**Figure 54.** Packet discard rate of a 900-node-square-grid WSN under a fault data injection attack as a function of attacker location.



(a) An attacker close to the sink

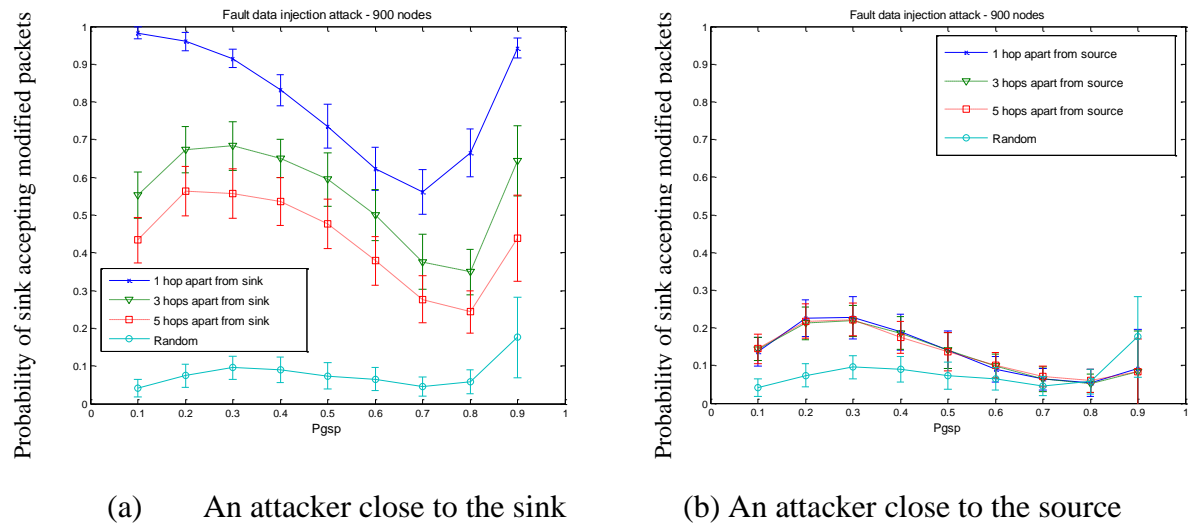


(b) An attacker close to the source

**Figure 55.** Probability of the sink accepting packets in a 900-node-square-grid WSN under a fault data injection attack as a function of attacker location.

Figure 56 depicts probability of the sink accepting fault-data packets in a 900-node-square-grid WSN under a fault data injection attack when (a) an attacker is close the sink and (b) an attacker is close the source. The probability of the sink accepting fault-data packets increases

as the attacker closer to the sink but remain unaffected regardless of the distances to the source. In summary, the security performance metrics indicates the fault data injection attack is more effective when an attacker is closer to the sink similar to message modification attacks. However, all security performance metrics of a 900-node-square-grid WSN under a fault data injection attack remain unaffected when an attacker closer to the source.



(a) An attacker close to the sink (b) An attacker close to the source

**Figure 56.** Probability of the sink accepting fault-data packets in a 900-node-square-grid WSN under a fault data injection attack as a function of attacker location.

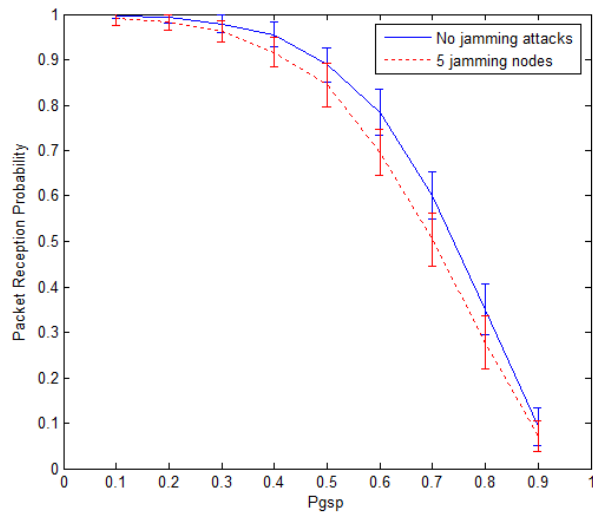
#### 4.2.4 Node failure and jamming attacks

MRDPs create implicit backup paths, making the network tolerant to a degree of node failure due to natural or adversarial causes. Examples of natural causes include, software malfunction, hardware malfunction, energy store depletion, or physical damaged. Examples of adversarial causes include DoS threats such as jamming attacks. Additional malicious examples include an adversary capturing a node, turning off nodes, removing batteries, or stealthily programming the

nodes to stop forwarding packets. Network behavior after a node failure depends on the protocols used to control the network. However, in networks employing MACGSP, a node failure results in a node that cannot receive or forward any packets.

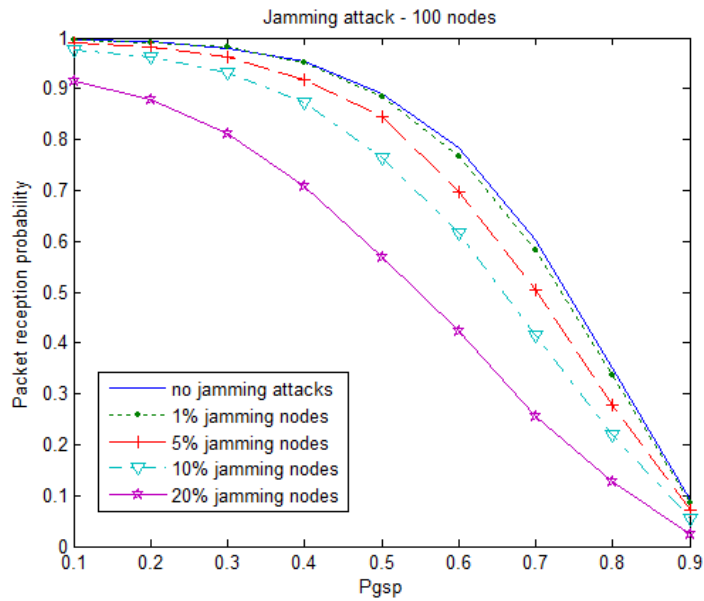
As MRDPs tend to provide fault tolerance to WSNs, if a node in a WSN fails either by nature or by DoS attacks such as jamming attacks, the network must be able to cope with this failure. The fault tolerance property of a WSN employing MRDPs when having a number of nodes fail (or die) was studied. The analysis uses simulation to randomly select the failed nodes for each packet sent. The analysis considers five different cases including the number of jamming attack causing nodes failed equal to 1%, 5%, 10%, 20% of total nodes (equivalent to 1, 5, 10, and 20 respectively for a WSN with 100 nodes). The simulation computes three performance metrics of a 100-node-square-grid WSN with a single sink at 90% C.I. including packet reception probability, average number of routes, and disjoint ratio.

Figure 57 depicts packet reception probability of a 100-node-square-grid WSN under jamming attacks causing 5 nodes failed. Compared with the normal operation, the packet reception probability decreases a little bit with overlapping C.I. However, with 10 failed nodes, C.I.'s of packet reception probability are clearly separated for the middle range of  $p_{gsp}$ .



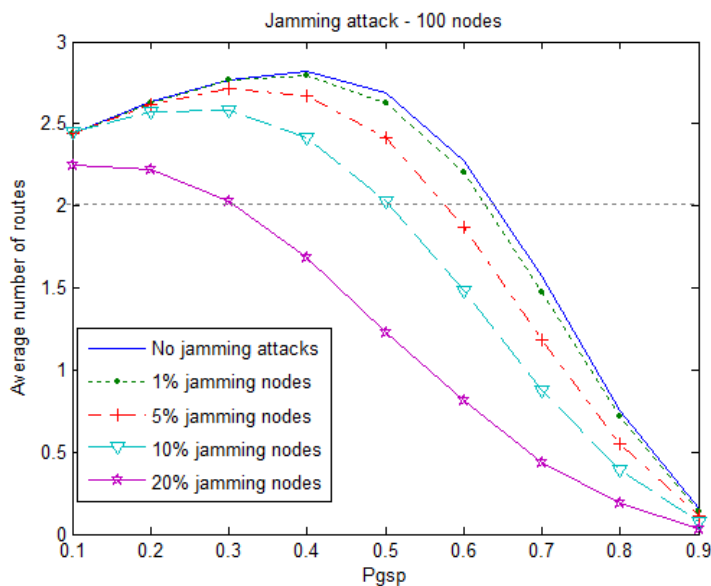
**Figure 57.** Packet reception probability of a 100-node-square-grid WSN under 5 and 10 jamming attacks.

Figure 58 illustrates packet reception probability of a 100-node-square-grid WSN under multiple jamming attacks (with 90% C.I. left off for a clear view). Increasing the number of jamming attacks decreases packet reception probability.



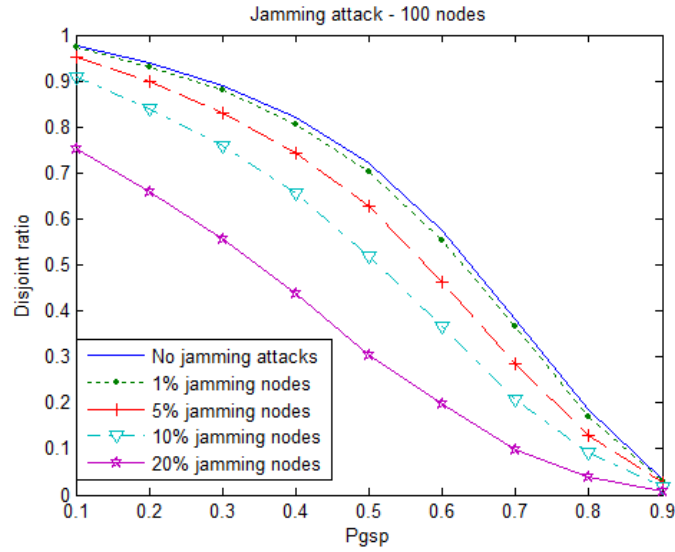
**Figure 58.** Packet reception probability of a 100-node-square-grid WSN under multiple jamming attacks.

Figure 59 illustrates the average number of routes of a 100-node-square-grid WNS under multiple jamming attacks. Similarly, the average number of routes decreases as the number of attack increases.



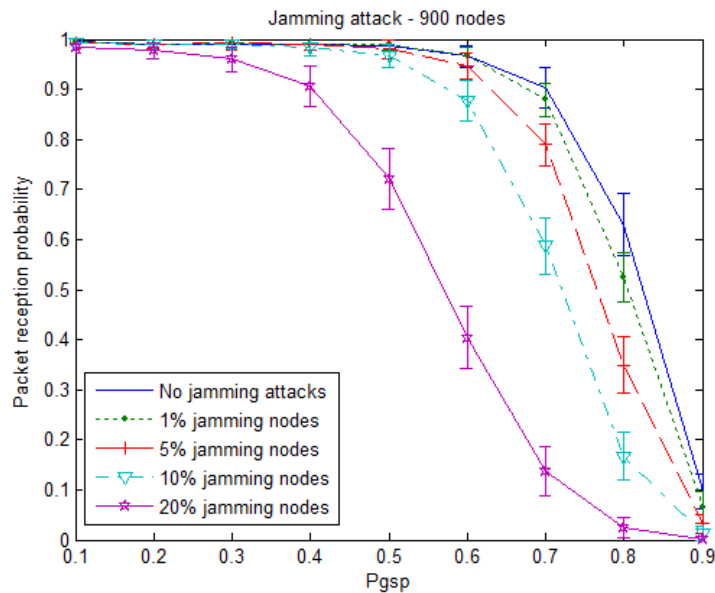
**Figure 59.** Average number of routes of a 100-node-square-grid WNS under multiple jamming attacks.

Figure 60 illustrates disjoint ratio of a 100-node-square-grid WNS with multiple jamming attacks. The disjoint ratio also decreases in the same manner. According to the results, all three performance metrics decrease significantly with 10% or more of failed nodes caused by jamming attacks.



**Figure 60.** Disjoint ratio of a 100-node-square-grid WSN under multiple jamming attacks.

The study increases the number of node in the network to 900 nodes and computes the packet reception probability. Figure 61 depicts the packet reception probability of a 900-square-grid WSN with a single sink under multiple jamming attacks. The results resemble the results of the 100-square-grid WSN.



**Figure 61.** Packet reception probability of a 900-node-square-grid network under multiple jamming attacks.

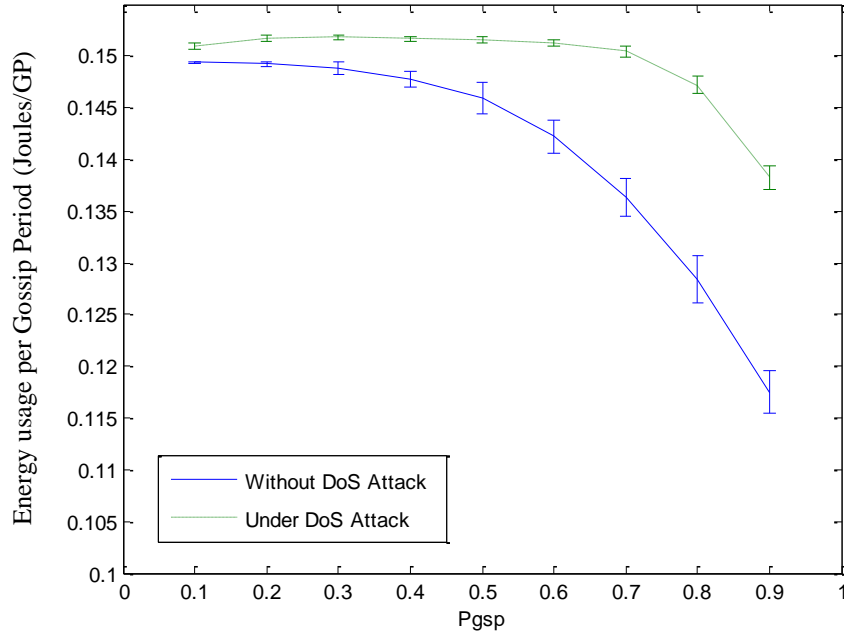
#### 4.2.5 Packet flooding attacks

Intruders use several methods to launch packet flooding attacks, one of DoS attacks. As an example, an intruder can simply use a rouge wireless sensor node to repeatedly inject a packet into the network in WNSs without authentication service. However, if WSNs have authentication service in sensor nodes, nodes can detect illegitimate packets and discard them. However, in some cases despite using authentication service, intruders can still compromise a sensor node if they capture sensor nodes and authentication service is weak. If an intruder successfully compromises a sensor node, the intruder can use the compromised node to launch a packet flooding attack. In this case, the other nodes do not know that the packet sent from the compromised node is in fact illegitimate. The nodes receiving the packet must then forward a packet wasting energy.

Packet flooding attacks cause a great damage to WSNs without protection. Not only do the nodes waste energy, packet discard rate at the sink also increases due to the illegitimate and legitimate packets arrive at sink. As a result, WSNs encounter a DoS and energy depletion attack at the same time. The study uses simulations to find an average of energy usage per gossip period and the probability of the sink accepting packets causing by packets discarded at the sink when a compromised node is repeatedly injecting a fault packet into a network. The study finds energy usage per gossip period of WSNs starting from the source sends a packet until all packet exits the network.

Figure 62 depicts energy usage per gossip period of a 100-node-square-grid WSN compared between normal operation and when the network is under packet flooding attack. The results shows that when the network is under a packet flooding attack, energy usage per gossip period for  $p_{gsp}$  less than 0.5 increases around 0.005 joules/GP or less than 5% of energy usage for

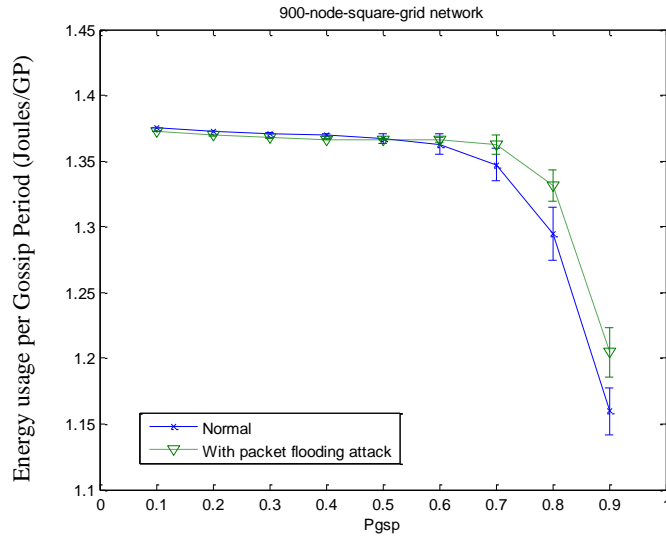
sending one packet. The energy usage per gossip period is less than 0.155 joules/GP in both cases.



**Figure 62.** Energy usage per gossip period compared between normal operation and when a 100-square-grid network under packet flooding attack.

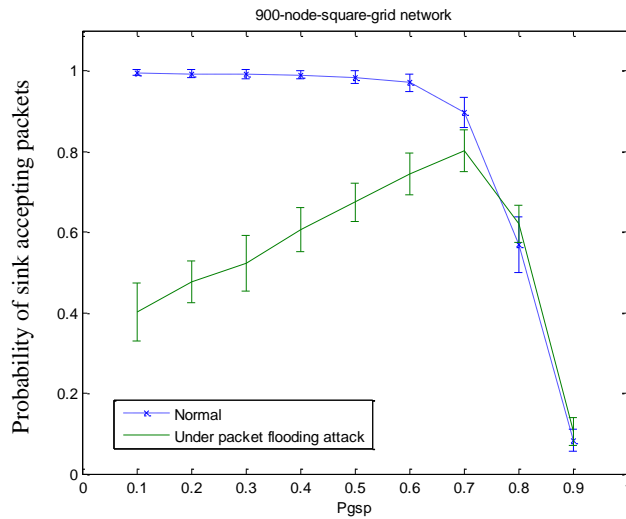
Figure 63 illustrates the energy usage per gossip period of the 900-node-square-grid network. At larger network scale, the energy usage per gossip period of the network with and without the attacks is almost the same for  $p_{gsp}$  less than 0.6. When  $p_{gsp}$  greater than 0.6, the energy usage per gossip period of the network with the attacks is higher than that of the network without the attacks.





**Figure 63.** Energy usage per gossip period compared between normal operation and when a 900-square-grid network under packet flooding attack.

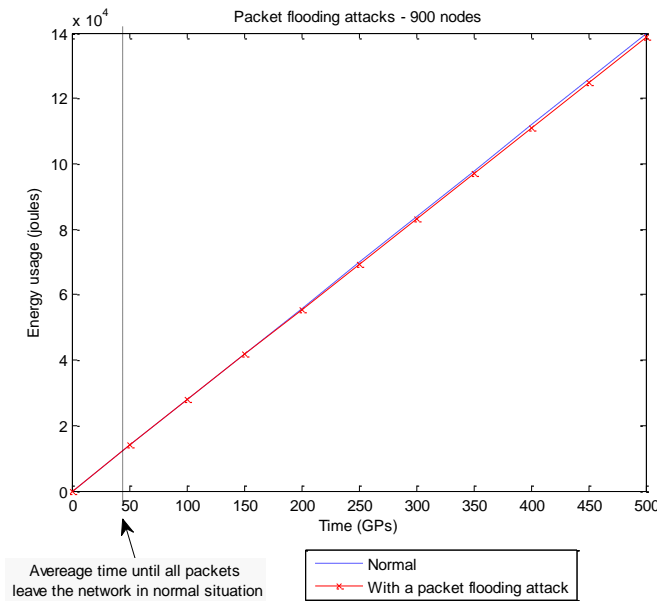
Figure 64 depicts probability of the sink accepting packets in a 900-node-square-grid network when under a packet flooding attack. When the network is under attacks, the probability of the sink accepting packets decreases significantly similar to the case of a fault data injection attack. Thus, if the attack persists, still WSNs cannot function properly.



**Figure 64.** Probability of the sink accepting packets compared between normal operation and when network under packet flooding attack.

Despite energy usage per gossip period is bound to certain amount when network is under attacks, it is also possible that the total energy usage of the network with packet flooding attacks is higher than the network without packet flooding attacks especially when operating at low data rate. Typically, a WSN without attacks loses its energy at peak draining rate only when sending a packet. However, a WSN with packet flooding attacks may be constantly losing energy at peak draining rate shortening its network lifetime.

Figure 65 illustrates the energy usage vs. time of a WSN with and without a packet flooding attack. The result shows that previous statement is not always true. In this case, the energy usage during the attacks is even slightly less than that without the attack. The possible reason is because while the attacking node is repeatedly injecting fault packets, the nodes received a packet also sleep more frequent (due to quiescent periods after transmitting) compensating the energy lost from forwarding a packet caused by the attack. Thus, quiescent period pay an important role for energy usage when WSNs under packet flooding attacks.



**Figure 65.** Energy usage vs. time compared between normal operation and when network under packet flooding attack.

According to section 4.1.3, the average time it takes until all packets exit the network of this 900-square-grid network is about 40 GPs. From Figure 65, the slope looks consistent even after all packets leave the network meaning that the network draining rate is always constant whether or not the network has nodes sending data. Consequently, WSNs employing MACGSP version 6 is robust against energy depletion threats caused by packet flooding attacks. Nevertheless, if the attack is persistent, nodes sleep more frequent and the blackouts also occur more frequent reducing the chance of any new arrivals of legitimate packets reaching the sink. With packet flooding attack, WSNs experience DoS threats rather than energy depletion threats.

#### **4.2.6 Eavesdropping attacks**

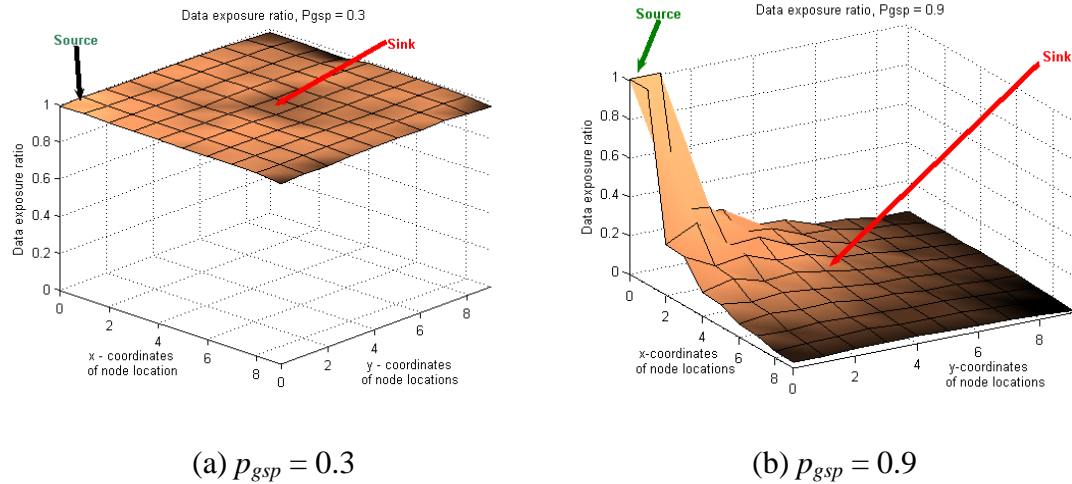
Wireless sensor nodes have a short range transmission. Intruders must be close to either a source node or a wireless sensor node carrying data in order to launch eavesdropping attack. However, a WSN consists of a large number of wireless sensor nodes covering large area allowing eavesdroppers to monitor the packets from any places along packet routing paths. Thus, routing paths play an important role to eavesdropping attack.

A WSN employing MRDPs uses gossiping to forward data to the sink. Consequently, data spreads out almost the entire network enabling an intruder to monitor traffic from almost every location in the network. How much information an eavesdropper receives depends on how much data a WSN exposes at eavesdropper locations. In chapter six, data penetration of a WSN employing MRDPs depends on  $p_{gsp}$ . Larger  $p_{gsp}$  results in less penetration at the distance nodes. Smaller  $p_{gsp}$  results in an almost constant data penetration on the entire WSN. However, data penetration does not tell exactly how much a WSN exposes data when an intruder monitors the network. The study uses data exposure ratio as a parameter to indicate data exposure of each

individual node location derived from the number of times an intruder receives a packet at one particular location by the total number of times the source sends a packet. This parameter tells us the chance that an intruder can intercept a packet of each node location. Alternatively, given that a sink is placed at one particular location data exposure ratio is similar to a packet reception probability of the sink at that location.

The analysis uses simulations to find data exposure ratio of every node location in a 100-node-square-grid WSN shown in Figure 12 (with the source node placed at coordinate 0,0 and the sink placed at coordinate 4,4). Figure 66 (a) shows data exposure ratio of each individual nodes in a WSN with  $p_{gsp} = 0.3$  when a packet sending from the source. In this case the data exposure ratio is almost 1 for every node location in the network.

Figure 66 (b) depicts data exposure ratio of each individual nodes in a WSN with  $p_{gsp} = 0.9$  when a packet sending from the source. The result show that data exposure ratio decreases over the distance from the source. Consequently, as  $p_{gsp}$  gets larger, data exposure ratio gradually decreases over the distance from the source. The result confirms that when  $p_{gsp}$  is not too large a WSN employing MRDPs in this example has a flooding like property in which the packet reception probability spreads evenly on every node location in the network. Therefore, WSNs employing MRDPs requires additional mechanisms to provide confidentiality service especially when WSNs' applications are sensitive to information leakage.



**Figure 66.** Data exposure ratio of each node to a packet sent from the source node.

#### 4.2.7 Security and energy trade off

One of the most important constraints of WSNs includes energy usage. However, building security requires additional energy usage [58, 78]. In general, stronger security mechanism requires more energy usage [58]. The first question is how much energy is available for building security. What would happen if the available energy is not enough to build a strong security mechanism? In some cases security cannot be trade off because if security fails the application may not be working properly. Security requirements depend on the applications of WSNs. Different applications require different security requirements. Next chapter discusses about additional mechanisms to improve security in WSNs employing MRDPs by considering techniques with minimum amount of additional energy requirements.

#### 4.2.8 Conclusion

According to section 4.1, a WSN employing MACGSP with a single sink has an average number of duplicates received at sink between 2-3 packets depending on  $p_{gsp}$ . MRDPs help a WSN with a single sink helps reduce the chance of intruders successfully modifying a message or injecting fault data. The average number of delivery paths and disjoint ratio play an important role against this attack. A higher disjoint ratio indicates a higher chance of packet being delivered without passing through a common compromised node. However, in a WSN employing MACGSP version 6 for  $p_{gsp}$  less than 0.4, increasing  $p_{gsp}$  decreases disjoint ratio but increases the average number of successful delivery paths compensating the reduction of disjoint ratio. Thus, the variation of  $p_{gsp}$  does not have an effect on the security performance metrics when a WSN is under message modification and fault data inject attacks as the security performance metrics are not statistically different over the different value of  $p_{gsp}$  in that range. However, as the number of attacking nodes increases e.g. at 20%, increasing  $p_{gsp}$  decreases the legitimate packet acceptance rate in accordance with the disjoint ratio. MRDPs also help protect against jamming attacks as the differences are not significant at 90% confidence level between packet reception probability of a WSN during normal operation and a WSN with 10% nodes under jamming attacks when  $p_{gsp}$  is less than 0.4.

## 5.0 RESULTS FOR WSNS EMPLOYING MRDPS WITH MULTIPLE SINKS

### 5.1 MULTIPLE SINKS

Chapter 4 showed that employing multiple random paths in a network with a single sink helps reduce the chance of intruders successfully modifying a message or injecting fault data. However, the sink does not always detect malicious packets. Additionally, the results from chapter 4 showed that the probability of the sink accepting packets greatly decreases due to the increasing of packet discard rate leading to a denial of service attack exploited by adversaries. This chapter studies security performance of WSNs employing multiple sinks. Adding more sinks may increase packet reception probability in both a normal operation and a situation when a WSN is under attacks provided that every sink must be connected such that all data can be collected and analyzed at the main sink.

In chapter 4, WSNs with one sink have an average number of multiple delivery paths of 2.8 routes (for  $p_{gsp} = 0.4$ ) which cause multiple copies of a packet to arrive at the sink, which the sink uses to detect anomalies. Upon detecting an anomaly the sink discards the packets, however this reduces the overall packet reception probability of the sink. Adding more sinks to the network increases the total number of packets received at sinks making sink voting possible assuming that all sinks are connected. A simple majority voting system is implemented and

studied. The sink accepts the most received packets as a legitimate packet and denies the least received packets. However, if the voting results are tie, the sink rejects all packets.

Sink voting may reduce the packet discard rate and improve the overall probability of the sink accepting packets. However, the false positives may still exist, as the voting results are not always correct. Additionally, packet discarding still occurs if the voting result is tie between two different packets received. Security performance of WSNs with multiple sinks was studied using four classes of metrics: legitimate packet acceptance rate, packet discard rate, probability of the sink accepting packets, and probability of the sink accepting modified packets. This study assumes the additional sinks send all received packets to the main sink via back channels and the decision is made at the main sink.

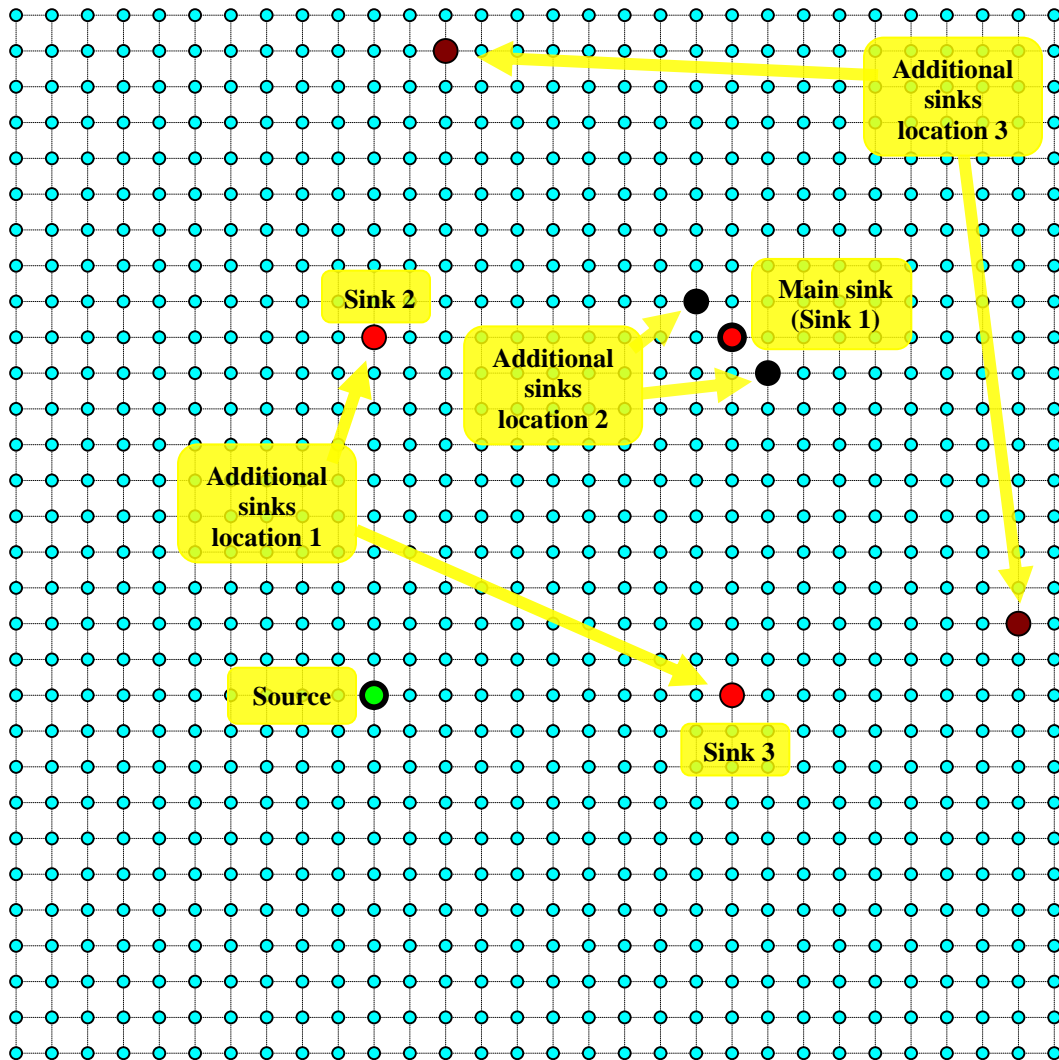
Adding more sinks does not increase energy usage on each sensor node, when MACGSP is used, because the node operations of sensor nodes remain the same. However, adding more sinks requires connections among the sinks in order to do sink voting. If those connections are implemented in band or using sensor nodes to deliver information between sinks, then one must consider additional energy usage. However, in this study the connections between multiple sinks made via backhaul links, thus, sensor nodes use the same amount of energy as those in WSNs with a single sink.

### **5.1.1 Packet reception probability for a WSN with three sinks**

To test the security performance of WSNs with multiple sinks, the study adds two more sinks into the network. The study uses simulations on a 900-node-square-grid WSN to find performance metrics. As shown in Figure 67, the first study places two additional sinks at location 1 with coordinates (10,20) and (20,10). The source node and the main sink (Sink 1)



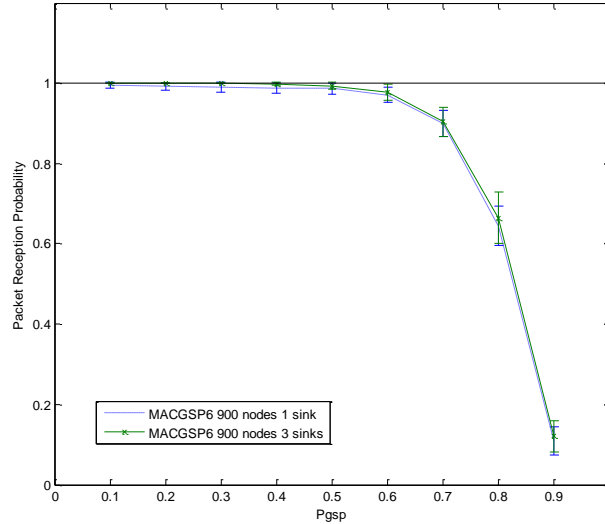
remain at coordinate (10,10) at coordinate (20,20) respectively similar to the chapter 4. The source sends two hundred packets for each simulation run and the simulation repeats for 40 rounds to find performance metrics and 90 percent confident interval.



**Figure 67.** A 900-node-square-grid WSN with three sinks.

Figure 68 shows the packet reception probability of WSNs with three sinks. Packet reception probability for a WSN with three sinks increases to 100% for  $p_{gsp}$  less than 0.4, for

larger values of  $p_{gsp}$  packet reception probability of WSNs with three sinks appears to increase slightly but overlapping confident intervals make the result unclear.



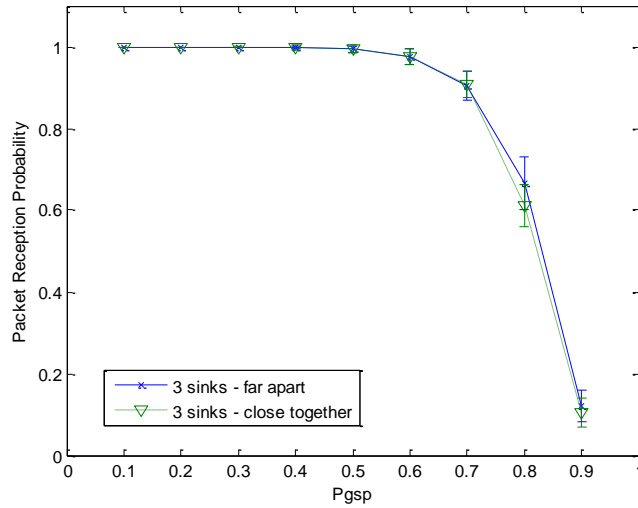
**Figure 68.** Packet reception probability of a 900-node-square-grid WSN compared between a network with one sink and three sinks.

### 5.1.1.1 Packet reception probability at various sink locations

Differing sink locations may result in different packet reception probability. Two sink configurations: sinks close together and sinks far apart were studied. As shown in Figure 67, the main sink (Sink1) location remains constant. The two additional sinks are at coordinates (21,19) and (19,21) in the case of close sinks as depicted in Figure 67 (with location 2). Figure 67 also illustrates the case of sinks far apart, the locations of the sinks are at coordinates (28,12) and (12,28) (with location 3).

Based on the results in chapter 4, packet reception probability of the sink in a WSN with a single sink is almost identical for all sink locations when  $p_{gsp}$  is not too large (except for the locations at the corners), therefore, intuitively packet reception probability of a WSN with three sinks should not be different among different locations of the sinks. Figure 69 compares packet

reception probabilities of the WSN with 3 sinks far apart and 3 sinks close together. The results from both cases overlap and appear almost identical.



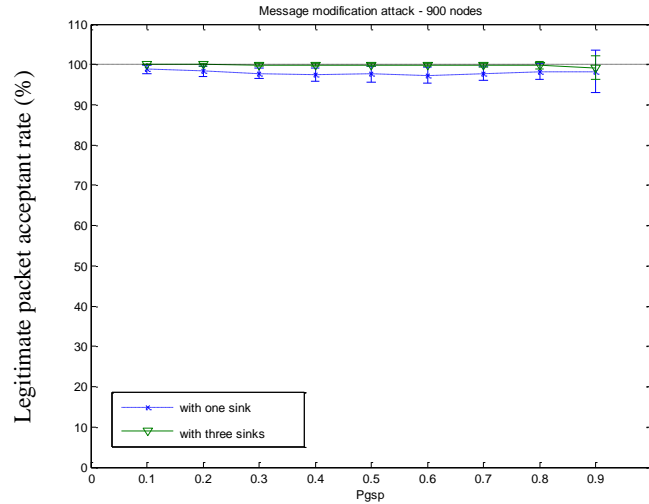
**Figure 69.** Packet reception probability of a 900-node-square-grid WSN with three sinks compared between sinks far apart and sinks close together.

Based on the result from section 4.2.6, with  $p_{gsp} = 0.3$ , the packet reception probability spreads evenly on every node location in the network except the node on the edge having fewer node degrees. If the three sinks are located on any locations apart from those on the edge, they must have the same packet reception probability. Consequently, one can expect similar packet reception probability of the network with three sinks for the other different sink locations except for the case of sinks on the edge of the network where they have fewer node degrees.

## 5.1.2 Integrity threats

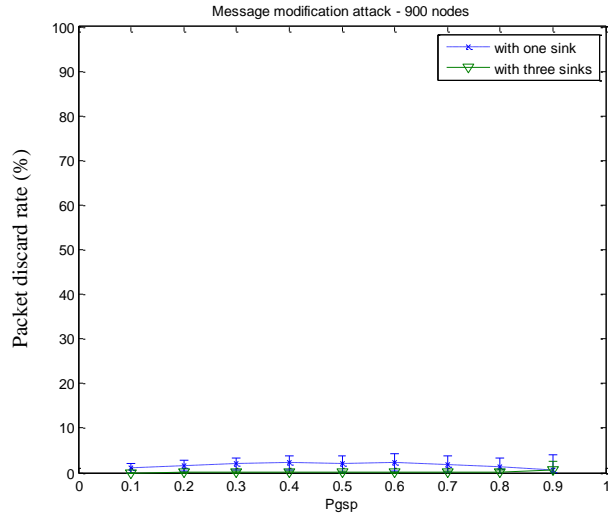
### 5.1.2.1 Message modification attacks

Figure 70 compares legitimate packet acceptance rate of a 900-node-square-grid WSN with one sink and three sinks under a message modification attack. Employing three sinks increases the legitimate packet acceptance rate from 98% to 100% for  $p_{gsp}$  less than 0.8. Although the confidence intervals overlap the increase is probably still significant because 100% is the upper bound.



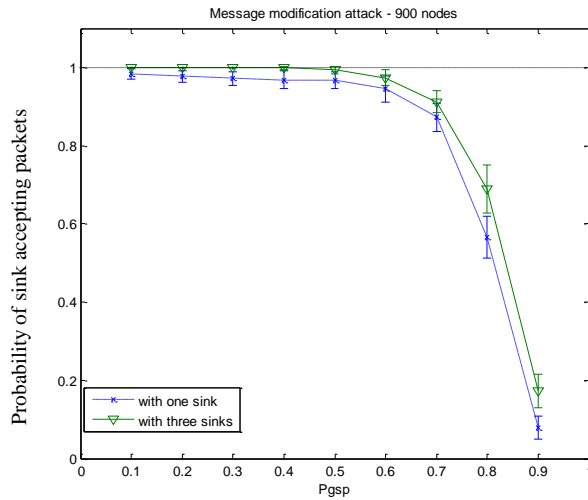
**Figure 70.** Legitimate packet acceptance rate of a 900-node-square-grid WSN under a message modification attack compared between a network with one sink and three sinks.

Figure 71 depicts packet discard rate of a 900-node-square-grid WSN with one sink and three sinks under a message modification attack. Packet discard rate decreases to almost zero when using three sinks.



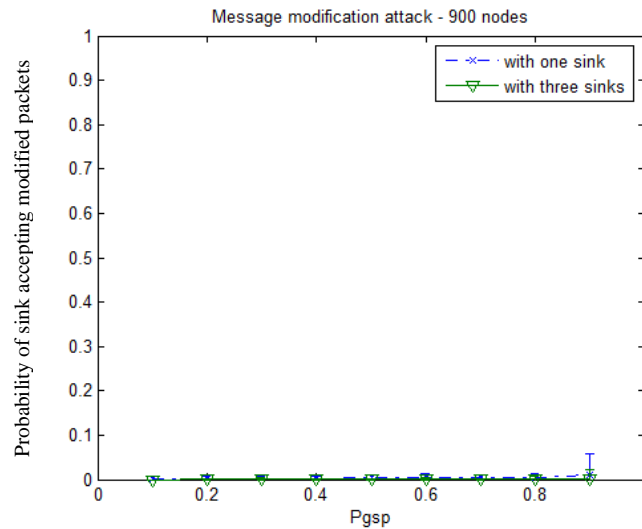
**Figure 71.** Packet discard rate of a 900-node-square-grid WSN under a message modification attack compared between a network with one sink and three sinks.

Figure 72 compares the probability of Sink1 accepting packets in a 900-node-square-grid WSN with one sink and three sinks under a message modification attack. Probability of Sink1 accepting packets increases to be almost the same as the packet reception probability during normal (no attack) operation.



**Figure 72.** Probability of Sink1 accepting packets in a 900-node-square-grid WSN under a message modification attack compared between a network with one sink and three sinks.

Figure 73 shows the probability of Sink1 accepting modified packets in a 900-node-square-grid WSN with one sink and three sinks under a message modification attack. The probability of Sink1 accepting modified packets becomes close to zero.

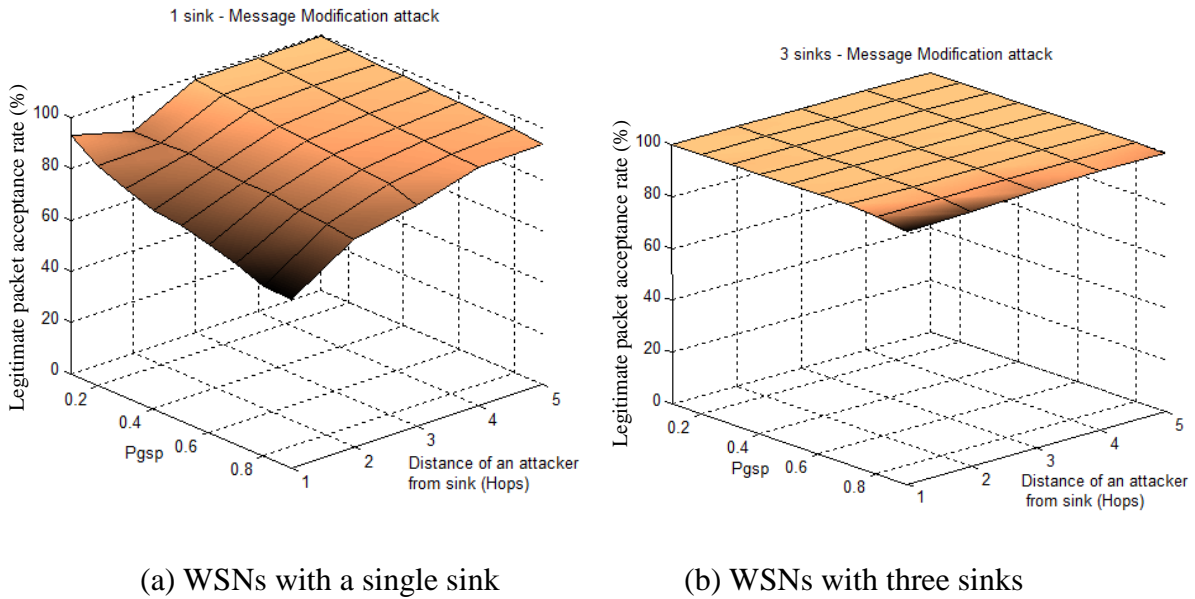


**Figure 73.** Probability of Sink1 accepting modified packets in a 900-node-square-grid WSNs under a message modification attack compared between a network with one sink and three sinks.

### 5.1.2.2 Impact of attacker location on attack effectiveness

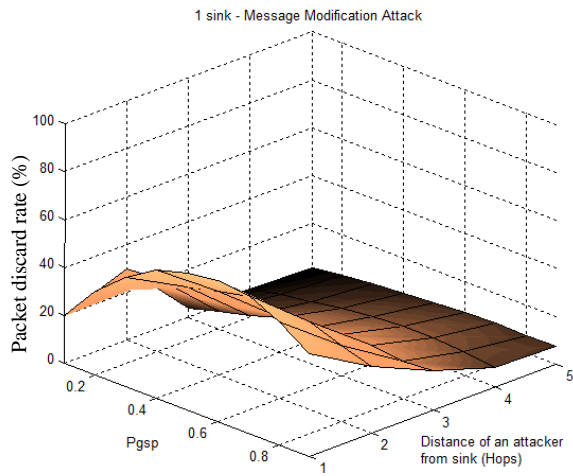
Chapter 4 shows that the locations message modification attacker next to the sink cause the most damage to WSNs with one sink among other locations. Although the legitimate packet acceptance rate is still above 95%, the packet discard rate increases considerably reducing the probability of the sink accepting packets of WSNs with a single sink. WSNs with three sinks increase performance to almost the same performances as the network without the attack. Figure 74 (a) illustrates legitimate packet acceptance rate of a 900-node-square-grid WSN with a single sink under a message modification attack at different attacker locations from the sink and (b) illustrates legitimate packet acceptance rate of a 900-node-square-grid WSN with three sinks.

Employing three sinks increases legitimate packet acceptance rate even when an attacker is next to Sink1.

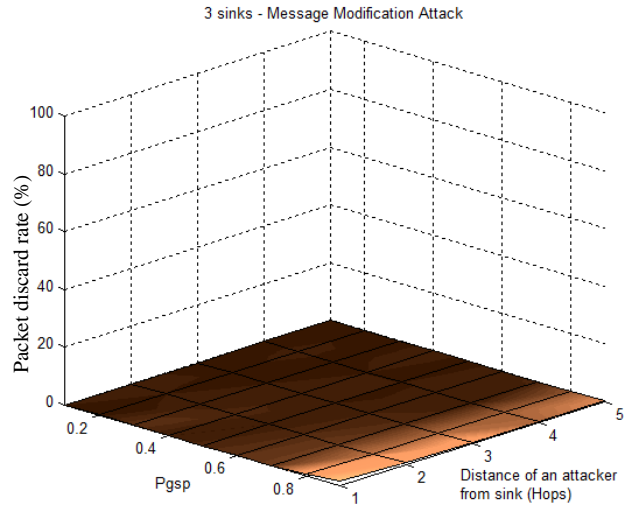


**Figure 74.** Legitimate packet acceptance rate of 900-node-square-grid WSNs under a message modification attack as a function of attacker locations from Sink1.

Figure 75 (a) compares the packet discard rate of a 900-node-square-grid WSN with a single sink and (b) illustrates packet discard rate of a WSN with three sinks under a message modification attack as a function of attacker distances to Sink1. WSNs with three sinks reduce discarding rate to be close to zero and even when an attacker is next to Sink1.



(a) WSNs with a single sink

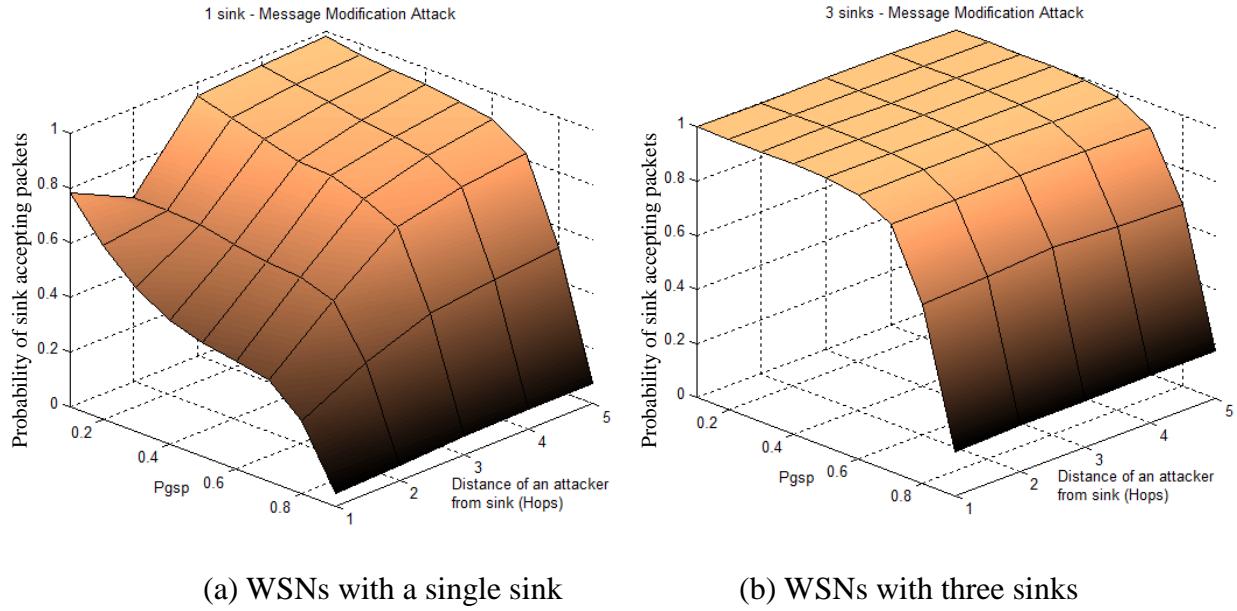


(b) WSNs with three sinks

**Figure 75.** Packet discard rate of 900-node-square-grid WSNs under a message modification attack as a function of attacker locations from Sink1.

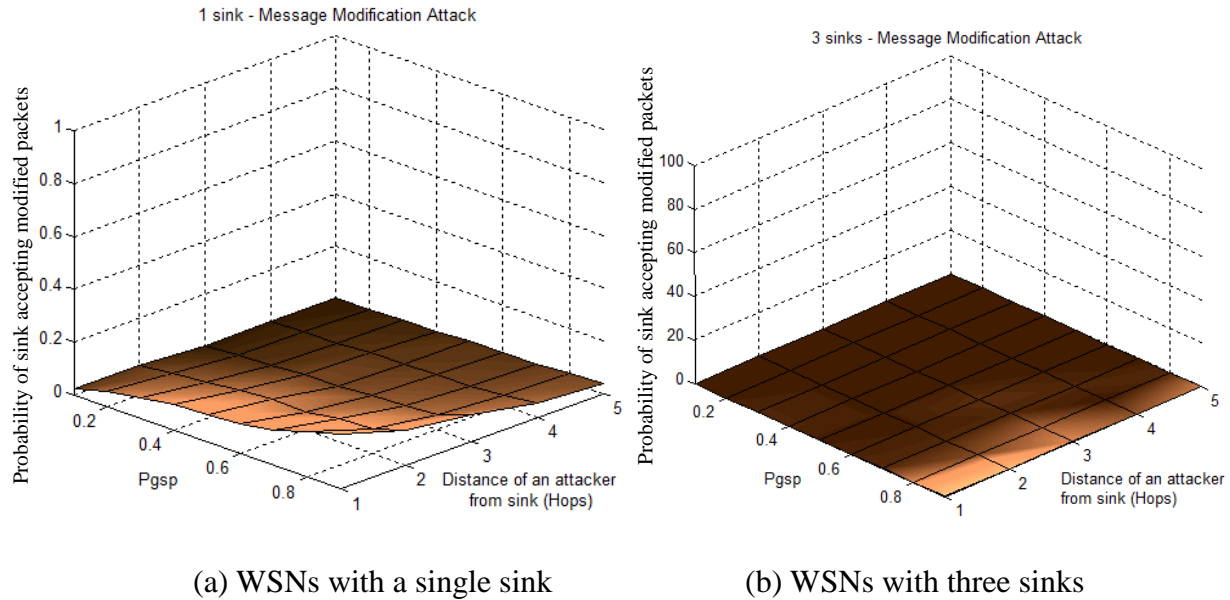
Figure 76 (a) shows the probability of the sink accepting packets in a 900-node-square-grid WSN with a single sink and (b) illustrates probability of Sink1 accepting packets in a packet in a WSN with three sinks under a message modification attack as a function of attacker locations from Sink1. Also, probability of Sink1 accepting packets in a WSN with three sinks increases to be the same as a WSN without the attack corresponding to the zero value of packet discard rate previously shown.





**Figure 76.** Probability of Sink1 accepting packets of 900-node-square-grid WSNs under a message modification attack as a function of attacker locations from Sink1.

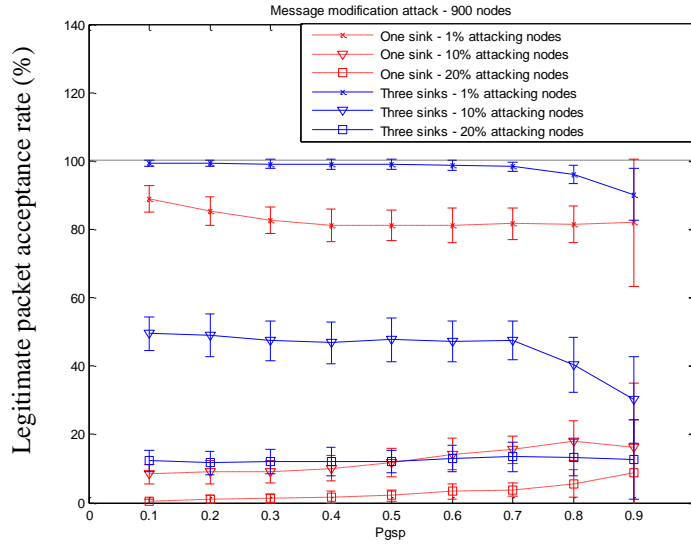
Figure 77 (a) illustrates the probability of Sink1 accepting modified packets in a 900-node-square-grid WSN with a single sink and (b) illustrates probability of Sink1 accepting modified packets in a WSN with three sinks under a message modification attack as a function of attacker location from Sink1. The probability of Sink1 accepting packets in a WSN with three sinks decreases to nearly zero.



**Figure 77.** Probability of Sink1 accepting modified packets of 900-node-square-grid WSNs under a message modification attack as a function of attacker locations from Sink1.

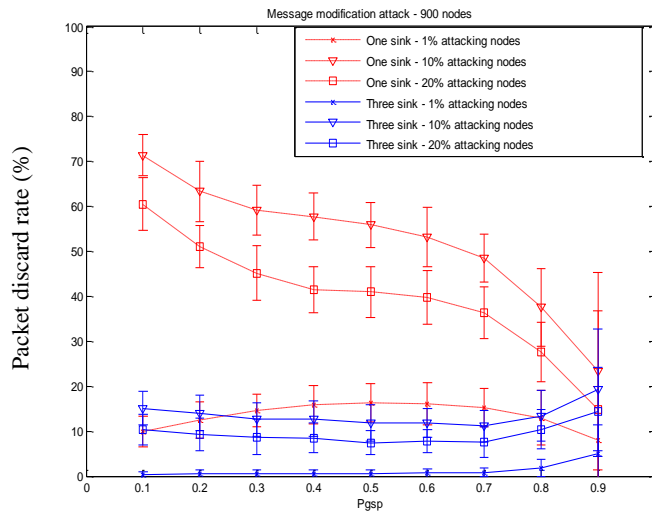
### 5.1.2.3 Increasing the number of nodes generating message modification attacks

To study the effect of multiple attackers simulations were conducted of networks where 1%, 10% and 20% of the nodes were attacking. Figure 78 shows the legitimate packet acceptance rate of a 900-node-square-grid WSN under multiple message modification attacks. The legitimate packet acceptance rate decreases significantly as the number of attacking nodes increase. More attacking nodes increase the number of modified messages in the network and the chance of modified messages arriving at Sink1 as well as increasing the intruders' chances of success. However, at 1% of attacking node the legitimate packet acceptance rate of WSNs with three sinks is close to 100%.



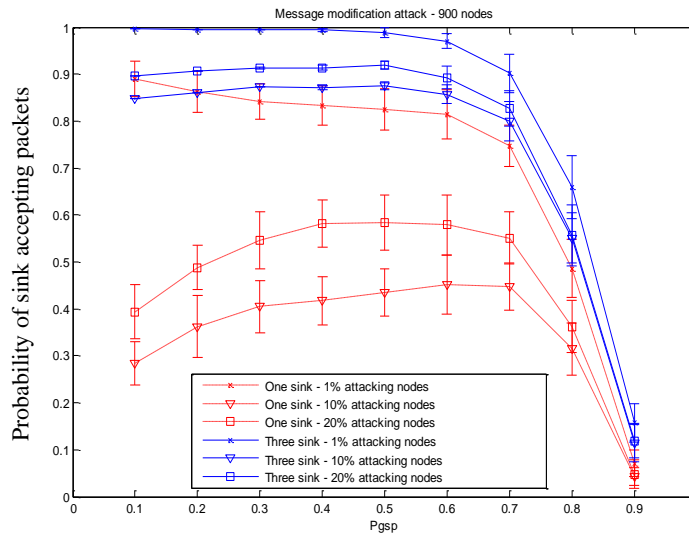
**Figure 78.** Legitimate packet acceptance rate of 900-node-square-grid WSNs under multiple message modification attacks compared between network with one sink and three sinks.

Figure 79 shows the packet discard rate for WSNs with three sinks. The packet discard rate is reduced to be less than 20% for all three cases. In the case of 1% compromised nodes the packet discard rate is nearly zero, the same as the single compromised node case.



**Figure 79.** Packet discard rate of 900-node-square-grid WSNs under multiple message modification attacks compared between network with one sink and three sinks.

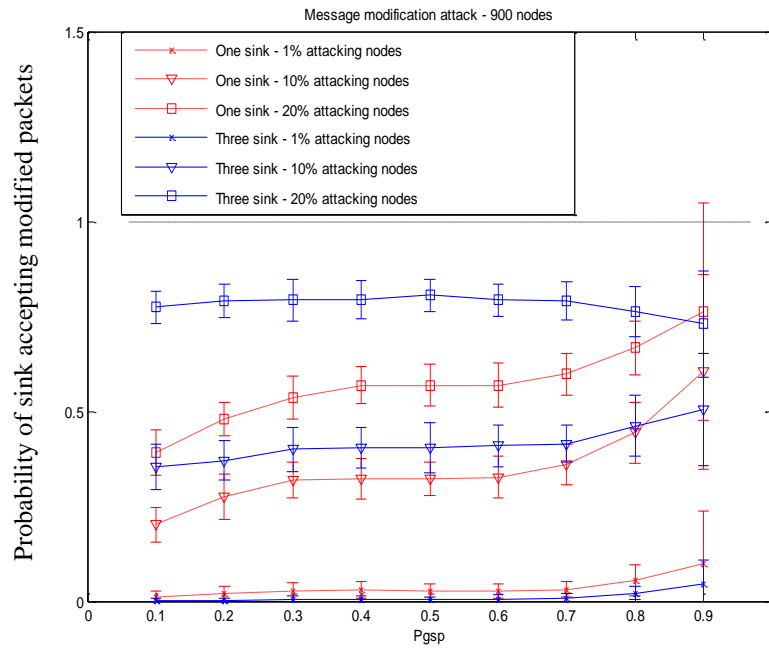
Figure 80 compares the probability of Sink1 accepting packets under a message modification attack for 900-node-square-grid network in networks with one sink and three sinks. Employing three sinks increases the probability of Sink1 accepting packets when the network is under message modification attack.



**Figure 80.** Probability of Sink1 accepting packets of 900-node-square-grid WSNs under multiple message modification attacks compared between network with one sink and three sinks.

Figure 81 compares the probability of Sink1 accepting modified packets under a message modification attack for 900-node-square-grid network compare in networks with one sink and three sinks. When the network is under multiple message modification attacks, the probability of sink1 accepting modified packets of the network with three sinks is higher than that of the network with only one sink except for the case of 1% of compromised nodes. The higher probability of sink1 accepting modified packets of the case of 10% and 20% compromised nodes results from the fact that the modified packets outnumber the legitimate packets and adding more sinks allows sinks to accept more illegitimate packets. Additionally, the network with three sinks has a higher probability of Sink1 accepting packets (including both legitimate and modified

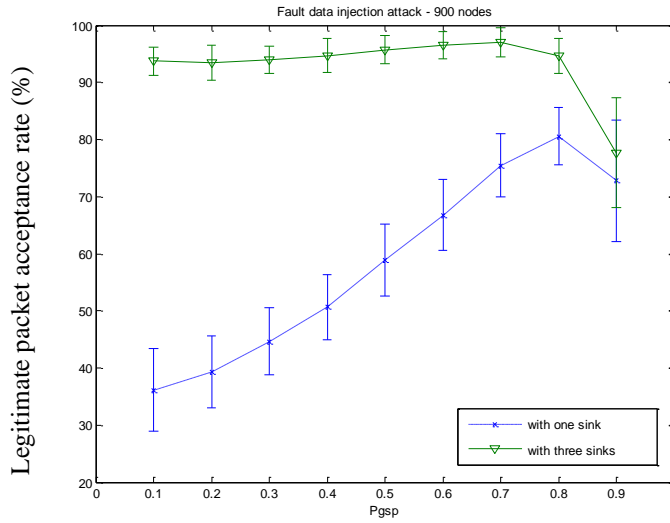
packets) than the network with one sink due to the voting mechanism. The only circumstance that it must reject a packet is when the voting result is a tie, while the network with one sink always rejects a packet if it receives both legitimate and illegitimate packets.



**Figure 81.** Probability of Sink1 accepting modified packets of 900-node-square-grid WSNs under multiple message modification attacks compared between network with one sink and three sinks.

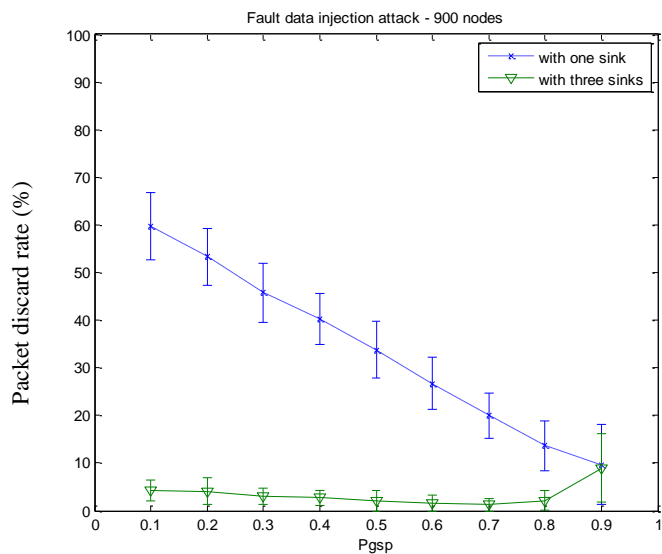
### 5.1.3 Fault data injection attacks

Figure 82 shows the legitimate packet acceptance rate of a 900-node-square-grid network under a fault data injection attack compared between network with one sink and three sinks. The network with three sinks outperforms the network with a single sink.



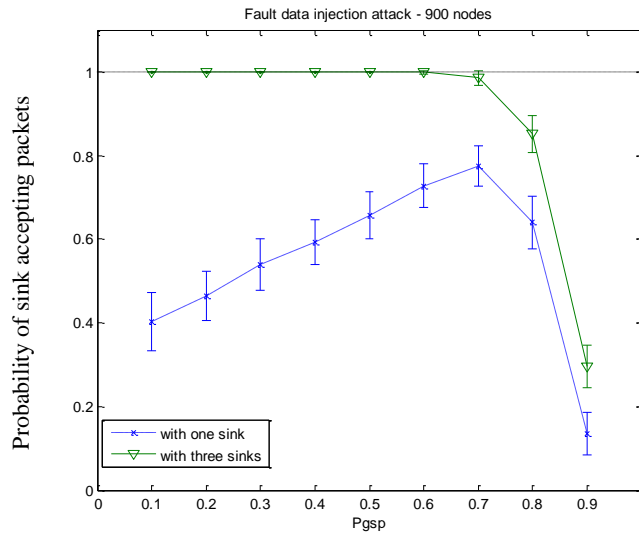
**Figure 82.** Legitimate packet acceptance rate of 900-node-square-grid WSNs under a fault data injection attack compared between network with one sink and three sinks.

Figure 83 compares the packet discard rate of a 900-node-square-grid network under a fault data injection attack in WSNs with one sink and three sinks. The packet discard rate of the network with three sinks decreases to be less than 5% for  $p_{gsp}$  less than 0.8.



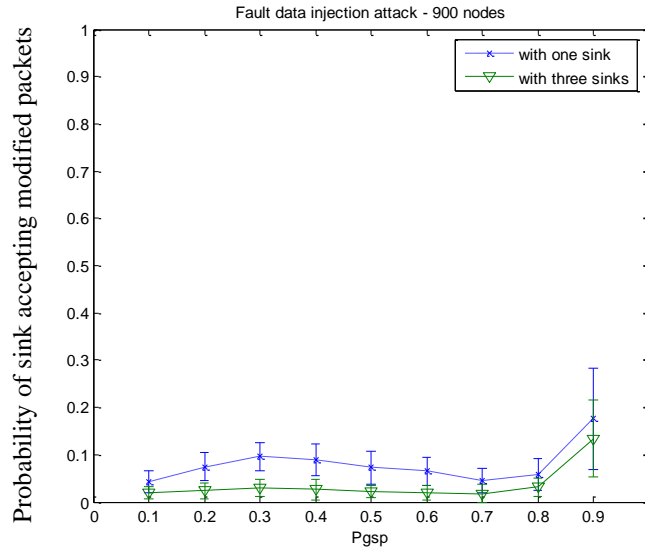
**Figure 83.** Packet discard rate of 900-node-square-grid WSNs under a fault data injection attack compared between network with one sink and three sinks.

Figure 84 compares the probability of Sink1 accepting packets in a 900-node-square-grid network under a fault data injection attack in WSNs with one sink and three sinks. The probability of Sink1 accepting packets of the network with three sinks increases significantly also corresponding to the decreasing of packet discard rate.



**Figure 84.** Probability of Sink1 accepting packets of 900-node-square-grid WSNs under a fault data injection attack compared between network with one sink and three sinks.

Figure 85 compares the probability of Sink1 accepting modified packets in a 900-node-square-grid network under a fault data injection attack in WSNs with one sink and three sinks. Employing three sinks also helps decrease the probability of Sink1 accepting fault-data packets down to be less than 3% for  $p_{gsp}$  less than 0.8.

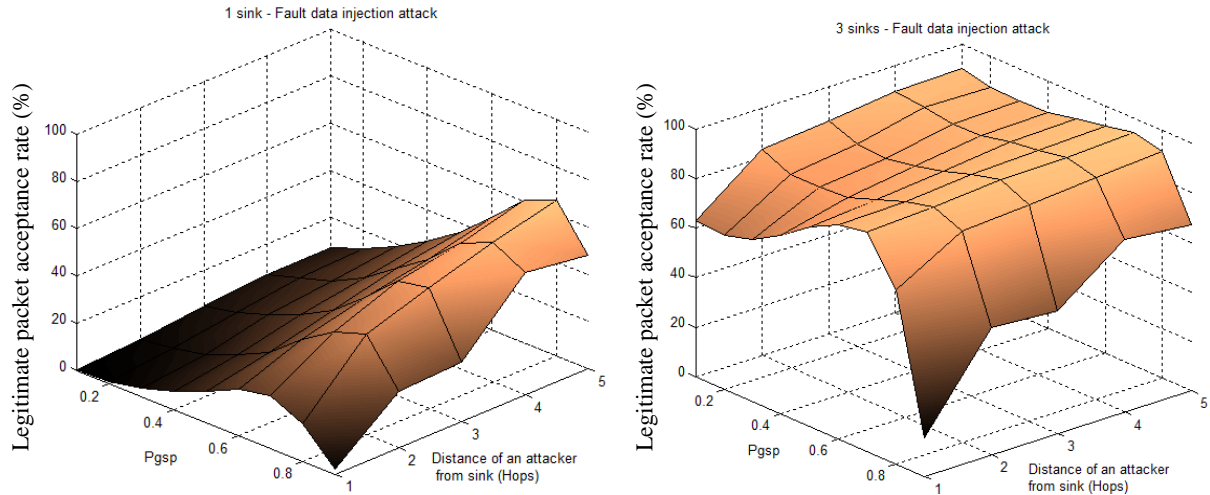


**Figure 85.** Probability of Sink1 accepting fault-data packets of 900-node-square-grid WSNs under a fault data injection attack compared between network with one sink and three sinks.

### 5.1.3.1 Impact of attacker location on attack effectiveness

The effect of attacker locations by having the location to be one, two, three, four, and five hops apart from Sink1 was studied using simulations of 900 node WSNs. Figure 86 (a) and (b) exhibit the legitimate packet acceptance rate of the network with one sink and three sinks respectively under a fault data injection attack as a function of attacker locations from Sink1. With one sink, the legitimate packet acceptance rate decreases greater as the attackers are closer to Sink1. However, employing three sinks helps increase legitimate packet acceptance rate and also reduce the effect of attacker locations as the legitimate packet acceptance rate is almost equal regardless of the distance of the attacker from Sink1.



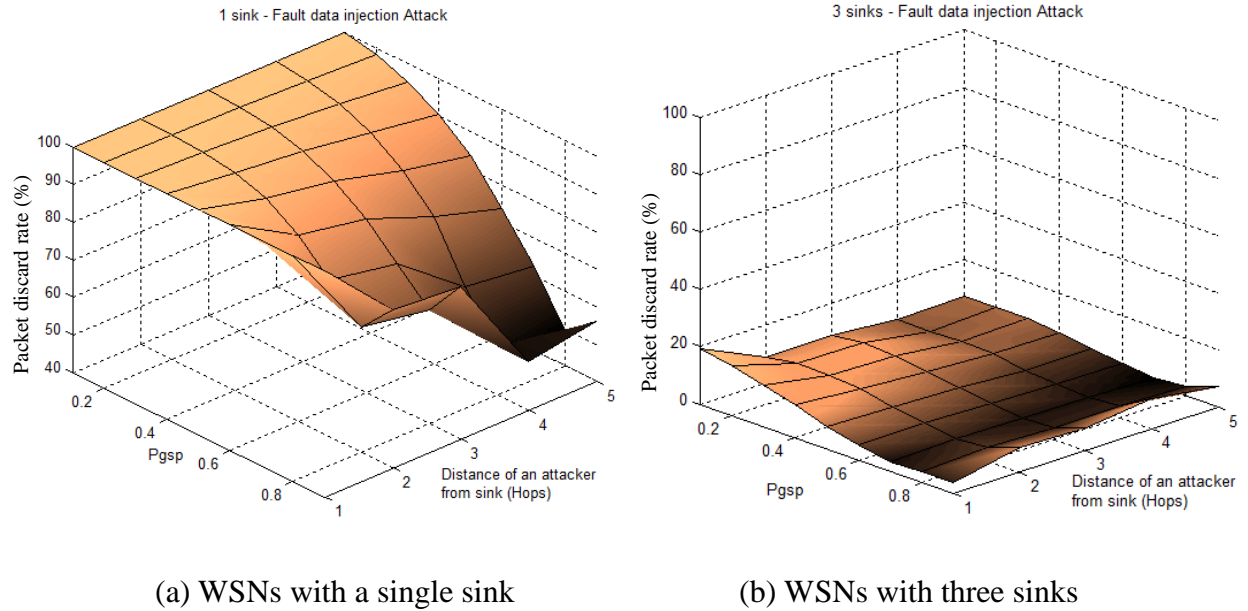


(a) WSNs with a single sink

(b) WSNs with three sinks

**Figure 86.** Legitimate packet acceptance rate of 900-node-square-grid WSNs under a fault data injection attack as a function of attacker locations from Sink1.

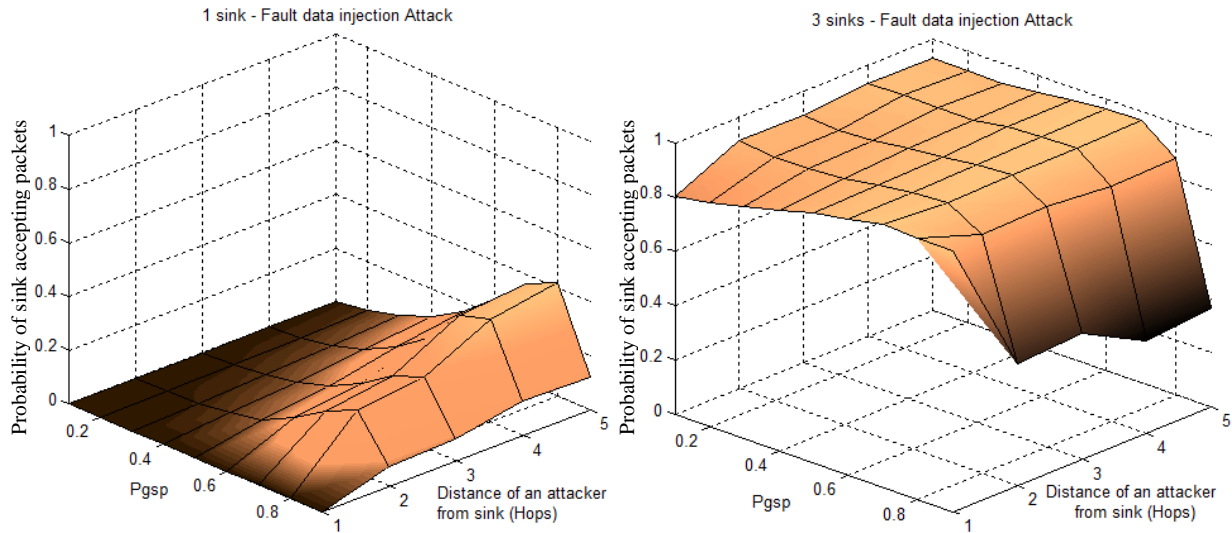
Figure 87 (a) and (b) illustrate the packet discard rate of a 900-node-square-grid WSN with one sink and three sinks respectively under a fault data injection attack as a function of attacker locations from Sink1. At smaller values of  $p_{gsp}$ , the location of an attacker has little effect on the packet discard rate, however at higher  $p_{gsp}$  it does have an effect. In WSNs using three sinks the packet discard rate is about the same for all the distances from Sink1.



(a) WSNs with a single sink (b) WSNs with three sinks

**Figure 87.** Packet discard rate of 900-node-square-grid WSNs under a fault data injection attack as a function of attacker locations from Sink1.

Figure 88 (a) illustrates the probability of the sink accepting packets in a 900-node-square-grid WSN with one sink under a fault data injection attack as a function of attacker locations from the sink. Figure 88 (b) illustrates the probability of Sink1 accepting packets in a 900-node-square-grid WSN with three sinks under a fault data injection attack as a function of attacker locations from Sink1. The probability of Sink1 accepting packets in a WSN with three sinks does not change with the distance of an attacker while that of a WSN with one sink vary considerably when  $p_{gsp}$  greater than 0.5.

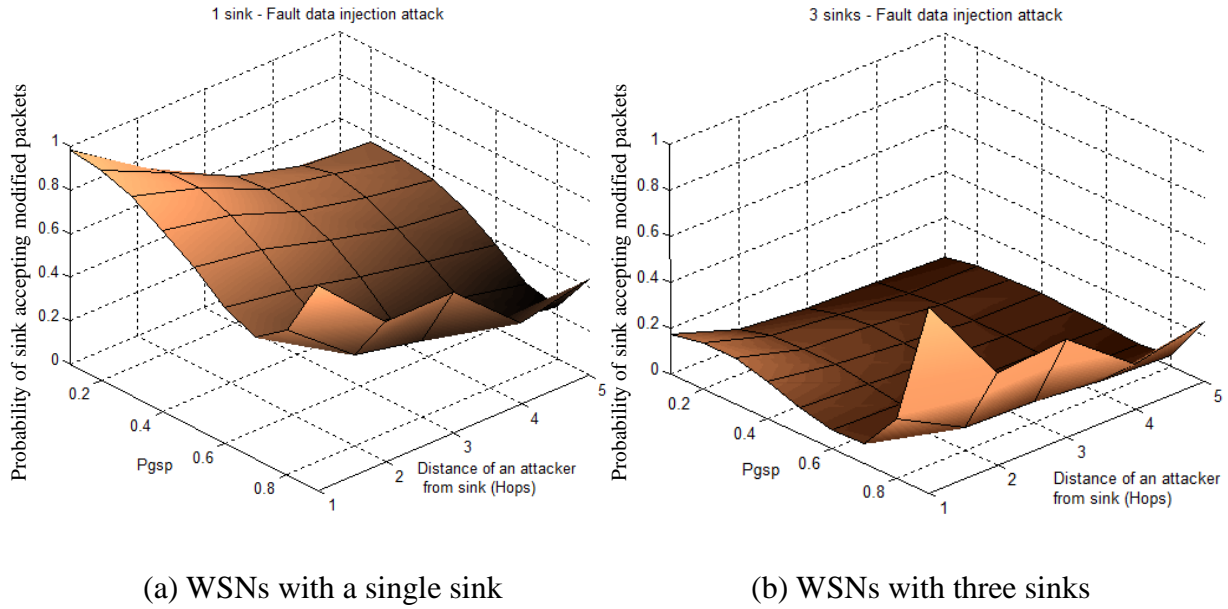


(a) WSNs with a single sink

(b) WSNs with three sinks

**Figure 88.** Probability of Sink1 accepting packets of 900-node-square-grid WSNs under a fault data injection attack as a function of attacker locations from Sink1.

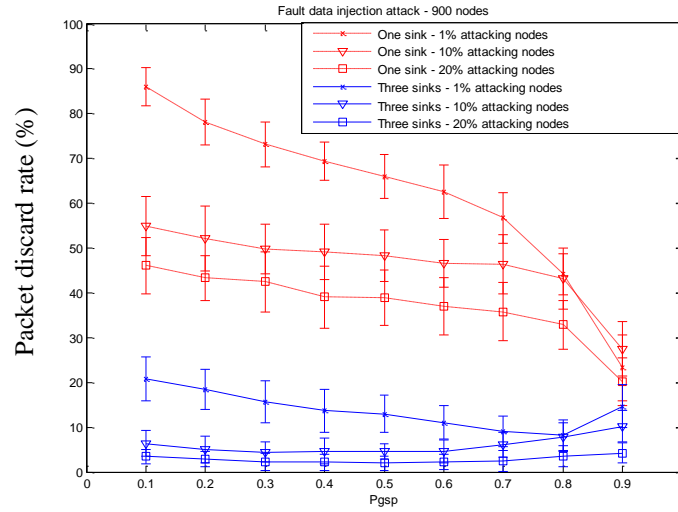
Figure 89 (a) shows the probability of the sink accepting fault-data packets in a 900-node-square-grid WSN with one sink under a fault data injection attack as a function of attacker locations from the sink. Figure 89 (b) shows the probability of Sink1 accepting fault-data packets in a 900-node-square-grid WSN with three sink under a fault data injection attack as a function of attacker locations from Sink1. The probability of the sink accepting fault-data packets in a WSN with a single sink increases greater when the attacker is closer to the sink. Figure 89 (b) shows that in WSNs employing three sinks the probability of Sink1 accepting fault-data packets reduces significantly and so does the effect of the distance of the attacker.



**Figure 89.** Probability of Sink1 accepting fault-data packets of 900-node-square-grid WSNs under a fault data injection attack as a function of attacker locations from Sink1.

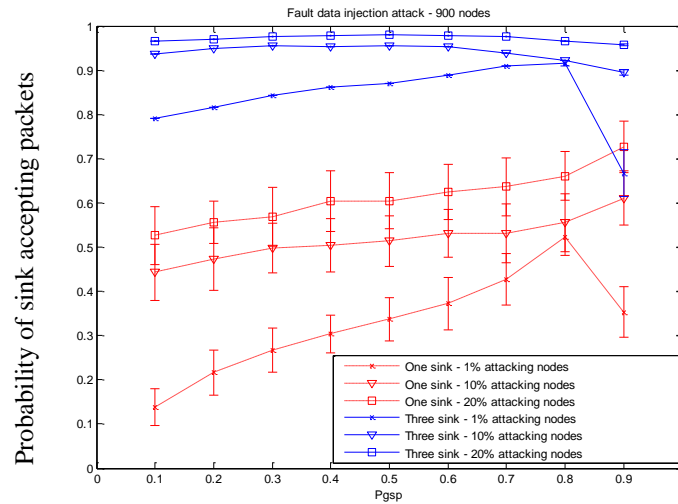
### 5.1.3.2 Increasing number of nodes generating a fault data injection attacks

To study the effect of multiple attackers simulations were conducted of networks where 1%, 10% and 20% of the nodes were attacking. Figure 90 depicts packet discard rate of a 900-node-square-grid WSN under fault data injection attacks as a function of number of attacks. As the number of attacking nodes increases to the point that fault packets outnumber the legitimate packets, the packet discard rate starts to decrease as Sink1 receives only fault packets and accepts them as legitimate, increasing the false positive rate. Employing three sinks also decreases the packet discard rate to be less than 20%, 10%, and 5% for the case of 20%, 10%, and 1% attacking nodes respectively.



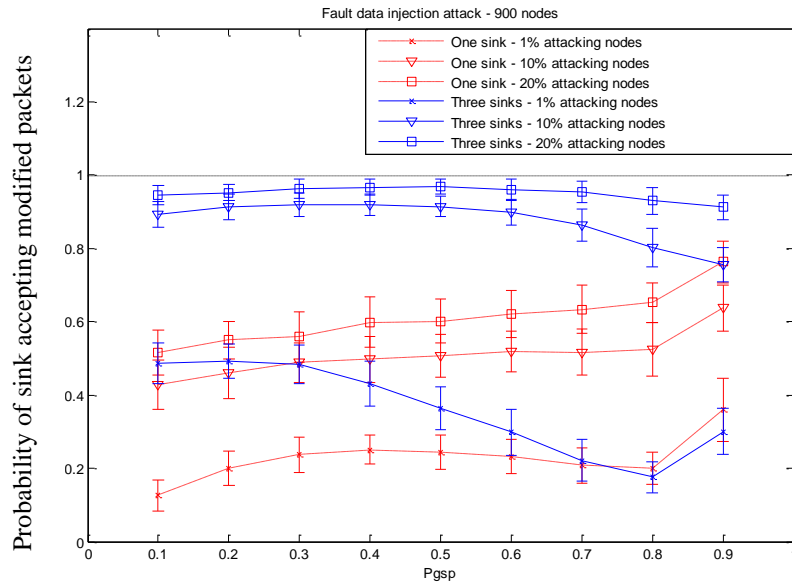
**Figure 90.** Packet discard rate of 900-node-square-grid WSNs under fault data injection attacks compared between network with one sink and three sinks.

Figure 91 shows the probability of Sink1 accepting packets in a 900-node-square-grid WSN under fault data injection attacks as a function of number of attacks. The probability of Sink1 accepting packets of WSNs employing three sinks also increases, corresponding to the packet discard rate.



**Figure 91.** Probability of Sink1 accepting packets of 900-node-square-grid WSNs under fault data injection attacks compared between network with one sink and three sinks.

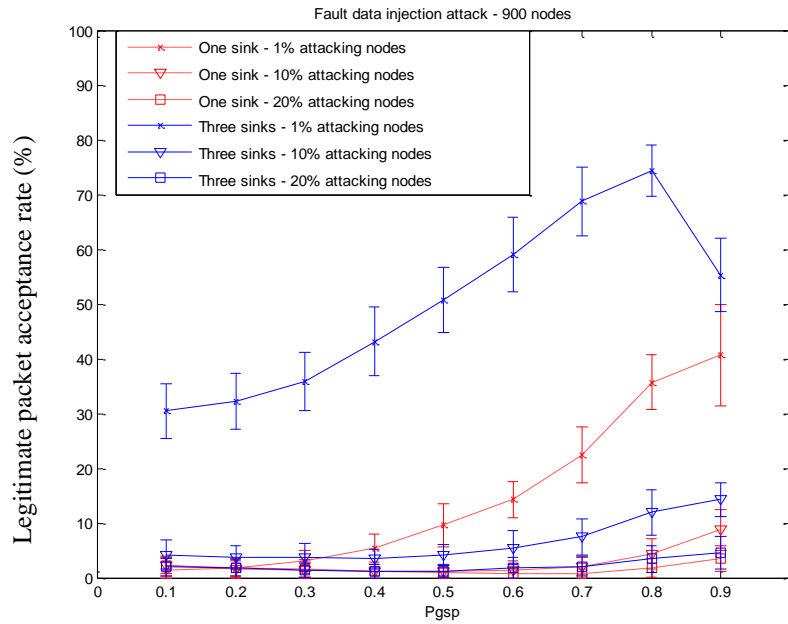
Figure 92 illustrates the probability of Sink1 accepting fault-data packets in a 900-node-square-grid WSN under fault data injection attacks as a function of the number of attackers. The probability of sink1 accepting fault-data packets increases to almost equal to one when the number of attacker increase to 20%. Increasing the number of attacking nodes increases the probability of sink1 accepting fault-data packets.



**Figure 92.** Probability of Sink1 accepting fault-data packets of 900-node-square-grid WSNs under fault data injection attacks compared between network with one sink and three sinks.

Figure 93 depicts the legitimate packet acceptance rate of 900-node-square-grid WSNs under fault data injection attacks for 900-node-square-grid network as a function of number of attackers. In WSNs with one sink, increasing the number of attacking nodes decreases the legitimate packet acceptance rate. Increased numbers of attacking nodes increase the chance of injected packets to arrive at the sink and increases intruders' chances of success as the legitimate packet acceptance rate decreases. Employing three sinks increases the legitimate packet

acceptance rate to be around 30% – 70% when having 1% attacking nodes but does not increase when having 10% and 20% attacking nodes.



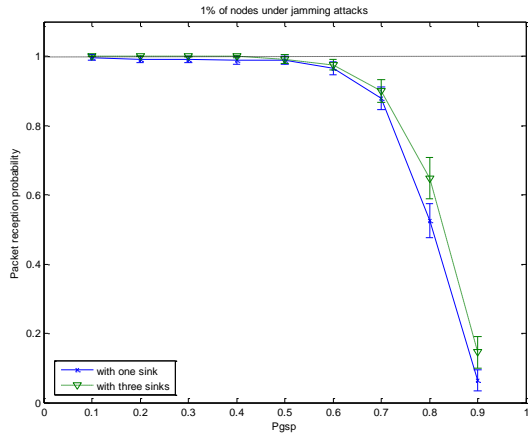
**Figure 93.** Legitimate packet acceptance rate of 900-node-square-grid WSNs under fault data injection attacks compared between network with one sink and three sinks.

## 5.1.4 Availability threats

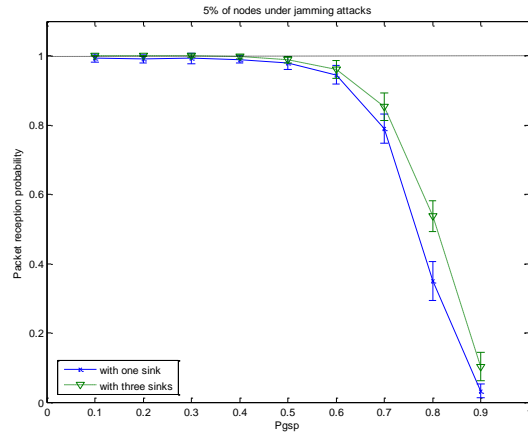
### 5.1.4.1 Jamming attacks

From chapter four, WSNs employing MRDPs with a single sink can tolerate some node failure and jamming attacks. Section 5.1.1 also showed that adding two more sinks helps increase packet reception probability regardless of locations of additional sinks. Adding more sinks may also increase overall packet reception probability when the network is under jamming attacks or experiencing node failures. Simulations were created for WSNs with 1%, 5%, 10% and 20% of

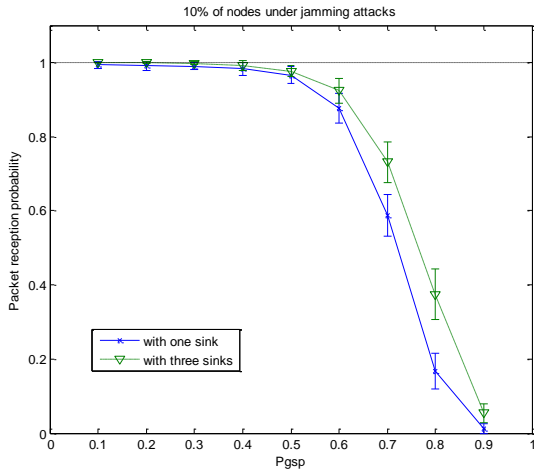
the node under jamming attacks. Figure 94 illustrates the results in comparison with the case of a single sink. Employing three sinks increases packet reception probability in all four cases.



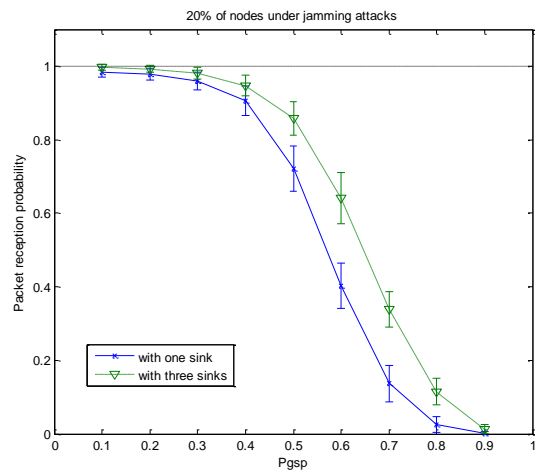
(a) 1% of nodes under jamming attacks



(b) 5% of nodes under jamming attacks



(c) 10% of nodes under jamming attacks



(d) 20% of nodes under jamming attacks

**Figure 94.** Packet reception probability of 900-node-square-grid WSNs with one sink and three sinks under jamming attacks.

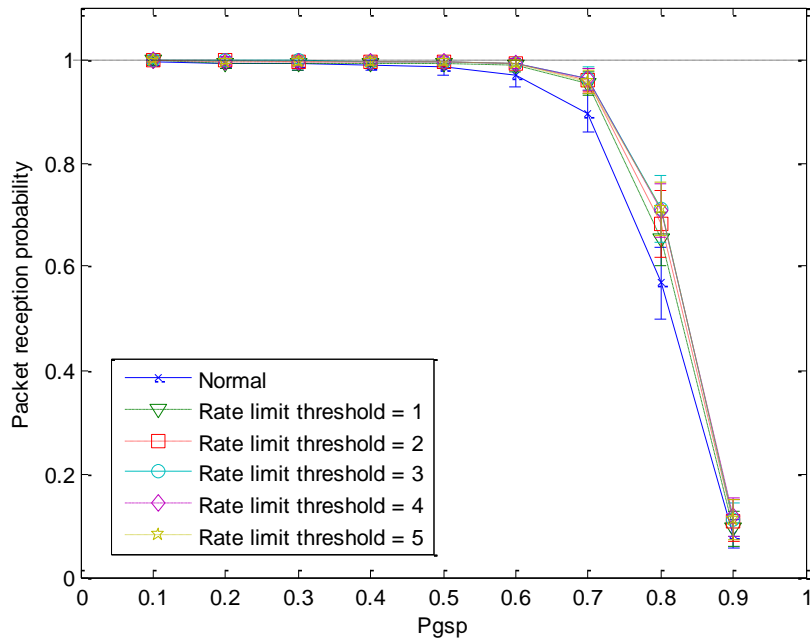


## 5.2 QUIESCENT PERIODS AND RATE LIMITING AGAINST DENIAL OF SERVICE ATTACKS

Chapter 4 showed that a WSN employing MRDPs through gossiping is not affected by an energy depletion threat such as a packet flooding attack. Instead, the network experiences a DoS threat as the probability of the sink accepting packets decreases under the present of packet flooding attack. If the attack continues, the network cannot function properly. Protection against packet flooding attacks requires a combination of detection and containment techniques. Rate limiting via packet receiving counters and quiescent periods is studied. The effectiveness of this technique was analyzed over different rate limit thresholds when applying to WSNs employing MRDPs with a single sink.

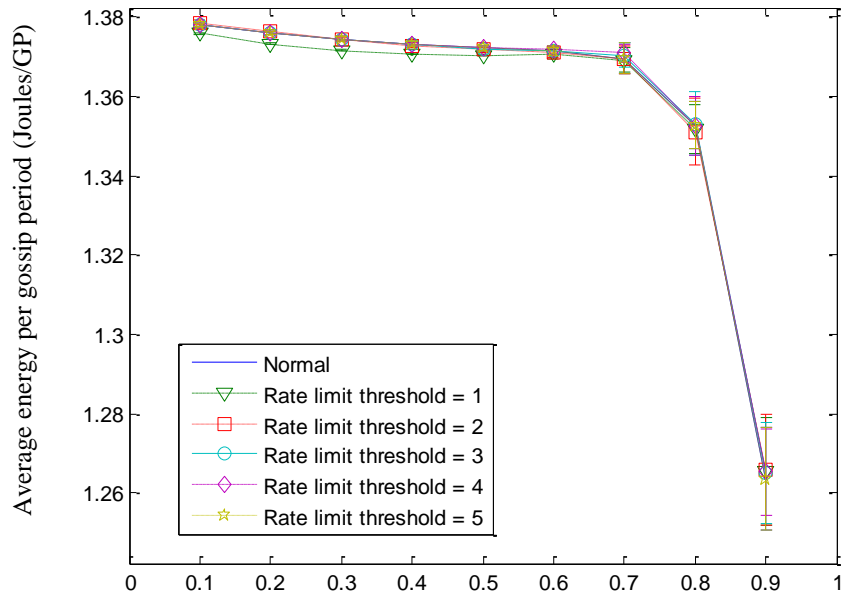
The analysis considers 900-node-square-grid WSNs as shown in Figure 30. Simulations were conducted to find how fast the network detect and contain the packet flooding attack. The last packet leaving the network indicates the network successfully contains the attack because when the attack persists packets never leave the network. The simulations compute average time until all packets leave the network. The results from chapter 4 showed that when a WSN is under a packet flooding attack, the probability of the sink accepting packets decreases because of the interference from injected traffic. The simulations compute the probability of the sink accepting packets in WSNs employing rate limiting at different thresholds. Therefore, the performance metrics include probability of the sink accepting packets and an average time until all packets leave the network.

Figure 95 presents the probability of the sink accepting packets in a 900-node-square-grid WSN employing rate limiting at different thresholds. The results show that rate limiting does not affect the packet reception probability of the network.



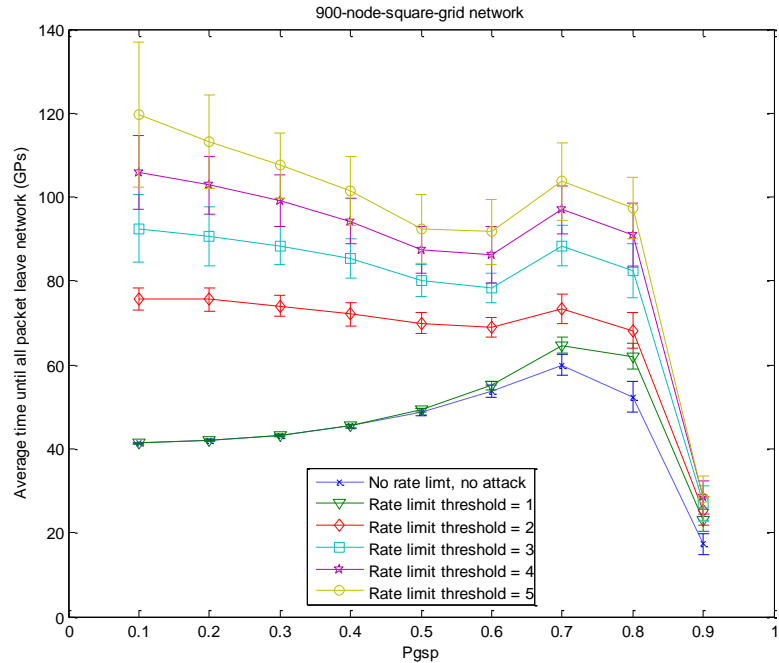
**Figure 95.** Packet reception probability in a 900-node-square-grid WSN employing rate limiting as a function of thresholds.

Figure 96 shows the average energy per gossip period of a 900-node-square-grid WSN when employing rate limiting at different thresholds. The results show that rate limiting does not affect the average energy per gossip period of the network.



**Figure 96.** Average energy per gossip period of a 900-node-square-grid WSN employing rate limiting as a function of thresholds.

Figure 97 depicts the average time until all packets leave the network (or transient period) of a 900-node-square-grid WSN employing rate limiting under a packet flooding attack as a function of rate limit thresholds. The transient period is very close to the normal operation for rate limit threshold equal to one. For the other rate limit thresholds, increasing the thresholds increases the transient period.



**Figure 97.** Average time until all packet leave the network of a 900-node-square-grid WSN employing rate limiting under packet flooding attacks as a function of thresholds.

### 5.3 DATA SEGMENTATION

A multipath routing approach for secure data delivery proposed by W.Lou et al. uses multiple paths with the secret sharing principle for secure data delivery [18]. Secret sharing divides data into  $N$  segments and passed it through an algorithm such that a receiver can reconstruct the original data from  $T$  out of  $N$  received segments. The technique assumes that intruders cannot intercept  $T$  segments. However, a WSN employing gossiping results in high data exposure allowing intruders to have the same chance of receiving the data as the sink. Therefore, data segmentation does not help a WSN using gossiping or any other flooding protocol, as all data segments are equally likely being exposed.

Another disadvantage of using data segmentation for a WSN employing gossiping is that to receive a message split into multiple packets, the sink node must receive all segments. An adversary can exploit this requirement by launching a DoS attack which prevents one of the segments from reaching the sink. Moreover, the packet reception probability ( $p_{rcpt}$ ) of gossip-based protocols becomes  $(p_{rcpt})^T$ , where T is the number of segments required to recover original data. Since  $p_{rcpt}$  is usually less than or equal to one, the factor of T reduces  $(p_{rcpt})^T$  greatly when T is large. Additionally, data segmentation is not effective if the eavesdroppers are closer to either source or the sink nodes because the chance of eavesdroppers intercepting all segments increases. Therefore, data segmentation does not help reduce high data exposure of a WSN using gossiping.

## 6.0 CONCLUSION AND FUTURE WORK

### 6.1 CONCLUSION

The primary research objective was to study the intrinsic security properties emergent from WSN MAC and routing protocols and develop simple mechanisms to enhance security for WSNs. Chapter 2 and 3 provided overviews of WSNs and their security threats and attacks. Chapter 4 discussed security in WSNs employing MRDPs with a single sink. Section 4.1 showed that a WSN employing MRDPs created by a gossiping protocol has an average number of successful delivery paths more than 2, when  $p_{gsp}$  is less than 0.6. The results also show that the disjoint ratio varies inversely with  $p_{gsp}$  and is greater than 50% for  $p_{gsp}$  less than 0.6. Additionally, large values of  $p_{gsp}$  result in fewer paths and smaller disjoint ratios.

The packet reception probability, average number of successful delivery paths, and disjoint ratio of the network with source node degree of 4 (at coordinate 2,2) is better than those of the network with source node degree of 2 (at the lower left corner). However, for the larger scale network such as 900-node-square-grid network, location of source and sink has less influence on the packet reception probability of the network. The study also shows that average packet delivery time can be determined in terms of minimum transit time plus random numbers for a given WSN with square-grid topology. The PDFs of the first packet delivery time for a square-grid WSN from both analysis and simulation cross validated each other.

Section 4.2 discussed the intrinsic security of a WSN employing MRDPs. The four security performance metrics are legitimate packet acceptance rate, packet discard rate, probability of the sink accepting packets, and probability of the sink accepting modified packets. The results in section 4.2.2 demonstrate the legitimate packet acceptance rate is still almost 100% when a WSN is under message modification attack. Additionally, the packet discard rate and probability of the sink accepting modified packets are still low while the probability of the sink accepting packets decreases compared to normal operation. However, increasing the number of attacking nodes causes greater damage to WSNs, degrading all performance metrics. Moreover, different attacker locations results in a different security performance. If an attacker is closer to the sink the performance metrics are worse than they are when attacker is closer to the source. Therefore, a WSN employing MRDPs with a single sink can benefit from additional security mechanisms to help increase its security performance against message modification attacks.

Section 4.2.3 illustrates the security performance metrics when WSN under a fault data injection attack. The legitimate packet acceptance rate is between 40-80% when a WSN is under a fault data injection attack. Moreover, the packet discard rate increases up to 60% corresponding to the decreased probability of the sink accepting packets. The probability of the sink accepting modified packets also increases to be about 0.1. Increasing the number of nodes creating the fault data injection attack greatly reduces the legitimate packet acceptance rate. The legitimate packet acceptance rate decreases to be almost zero with only 1% attacking nodes. However, increasing the number of attacking nodes decreases the packet discard rate and increase the probability of the sink accepting packets. Despite the increased number of packets accepted by the sink, WSNs actually suffer more due to the increased number of modified packets accepted by the sink. The

results indicate that the packets injected by attacking nodes overcome a legitimate packet sent from the source, increasing the probability of the sink accepting modified packets and reducing the legitimate packet acceptance rate. Attackers closer to the sink result in more attack effectiveness as the legitimate packet acceptance rate decreases. Conversely, attackers closer to the source result in less attack effectiveness as the legitimate packet acceptance rate is higher than the case of random location. The fault-data packets injected by an intruder from the location near the source have the same chance as the legitimate packet to reach the sink. Despite the vulnerability from attacker locations near the sink, the results in chapter 4 showed that the random routes can reduce the ability of intermediate nodes modifying a message as stated in the hypothesis H2.

Chapter 5 discusses using multiple sinks and applying rate limiting to WSNs to improve WSN security. Employing multiple sinks allows sink voting for WSNs and does not require additional energy for wireless sensor nodes. Section 5.1 showed that adding two more sinks increases packet reception probability regardless of the additional sink locations. The results from simulations indicate that under a message modification attack WSNs with three sinks outperform WSNs with a single sink. WSNs with three sinks improve the security performance metrics to be almost the same as networks without the attack. Moreover, WSNs with three sinks decrease the impact of attacker location close to the sink as the security performance metrics yield almost the same results for all attackers at any distance to the sink. The increased number of message modification attacks decreases the legitimate packet acceptance rate and the probability of the sink accepting packets and increases the packet discard rate and the probability of the sink accepting modified packets in a WSN with a single sink. With increasing numbers of attacking nodes, employing three sinks increases the probability of Sink1 accepting packets and



decreases the packet discard rate and the probability of Sink1 accepting modified packets in comparison to WSNs with a single sink. However, with 10% or more attacking nodes, the probability of Sink1 accepting modified packets increases to be more than 40%. When the number of attackers goes beyond 10% of total nodes, the malicious packets outnumber the copies of the legitimate packet, causing the WSN to accept the modified packet.

Under a fault data injection, the network employing three sinks outperforms the network employing only one sink in all security metrics. The legitimate packet acceptance rate increases up to 97%, packet discard rate decreases to be less than 5%, the probability of the sink accepting packets increases up to 1, and the probability of Sink1 accepting fault-data packets is smaller than 3% for  $p_{gsp}$  less than 0.8. When the attacker is closer to the sink, the performance metrics are not different except for the case of the attacker location next to the sink. When the attacker is next to the sink, the legitimate packet acceptance rate is still around 80% and the packet discard rate is about 20%, corresponding to the decreased probability of Sink1 accepting packets. The probability of Sink1 accepting fault-data packets also increases. Increasing the number of nodes generating fault data injection attacks degrades all security performance metrics but employing three sinks help increase the legitimate packet acceptance rate and the probability of Sink1 accepting packets and decrease packet discard rate and the probability of Sink1 accepting fault-data packets. However, with 1% attacking nodes the probability of Sink1 accepting modified packets increases to be more than 40%. In summary, employing multiple sinks with majority voting fails when the number of attacking nodes increases to 1%. Therefore, WSNs still need additional mechanisms when the number of nodes generating message modification and fault data injection attacks is more than 10% and 1% respectively. Despite the failure when the numbers of attacking nodes increase, the results confirm that the hypothesis H3 is valid as the

legitimate packet acceptance rates of a WSN with three sinks in all cases increase in comparison to WSNs with a single sink.

In WSNs, service availability threats include both DoS threats and energy depletion threats. Security attacks such as jamming attacks and packet flooding attacks cause service disruption to WSNs. The results in section 4.2.4 demonstrate that the packet reception probability is a function of the number of nodes under jamming attacks. WSNs employing MRDPs tolerate jamming attacks to the point where 5% of failed nodes or jammed nodes results in a slight drop of packet reception probability. Nevertheless, 20% of nodes under jamming attacks still cause the packet reception probability to drop considerably. A WSN with three sinks improves its packet reception probability during normal operation and during jamming attacks as the packet reception probability of WSNs with three sinks slightly decreases even when the number of nodes under jamming attacks increases up to 20%.

From the results in section 4.2.5., packet flooding attacks do not pose energy depletion threats. However, packet flooding attacks instead continuously pose DoS threats and integrity threats in the similar manner as a fault data injection attack. The probability of the sink accepting packets of WSNs with rate limiting remains the same for low and middle range value of  $p_{gsp}$ . Rate limit threshold value of one can stop the flooding packet within the same amount of transmitting time used for sending one packet. However, the interference from injecting packet remains during the transient period. As a result, rate limit and back off periods with rate limit threshold can limit the interference to only one transient period mitigating the damage from packet flooding attack, supporting hypothesis H4.

The results in section 4.2.6 show that WSNs employing MRDPs are vulnerable to eavesdropping attacks because the data exposure ratio is close to one, regardless of location of

the sensor nodes, for  $p_{gsp}$  is not too large. Larger  $p_{gsp}$  results in reduced data exposure ratio at locations distant from the source. However, larger values of  $p_{gsp}$  also cause lower packet reception probability at the sink node for sink locations farther away from the source. Even though WSNs employing MRDPs have a definite number of successful random delivery paths, there exist a number of unsuccessful delivery paths which cause a high data exposure ratio. Thus, dividing a large packet into smaller packets and send them via MRDPs through gossiping does not help improve data exposure ratio and does not benefit confidentiality service. Under these circumstances, the hypothesis H1 is invalid as the data segmentation is not helpful for a WSN with high data exposure ratio.

In testing these hypotheses, the following metrics have been implemented:

- Data exposure ratio
- Legitimate packet acceptance rate
- Packet discard rate
- Probability of the sink accepting packets
- Probability of the sink accepting modified packets
- Average time until the last packet leave the network

The results showed that these metrics can be used to assess protocol performance with respect to security. The results from these metrics also indicated that MRDPs with non-disjoint route sets can be used to increase integrity and availability service of WSNs. Moreover, the results are a function of  $p_{gsp}$  as large values of  $p_{gsp}$  result in fewer paths. Therefore, the metrics can also be used to tune protocol parameters to optimize security in WSNs.

## 6.2 FUTURE WORK

The high data exposure ratio of a WSN employing gossiping requires an alternative way to reduce high data exposure ratio. A possible method is to employ gossiping only during multiple random route discovery process. The WSN can later send segments of confidential data only to those specific multiple paths discovered by gossiping. Future work for improving confidentiality service may also include the physical layer encryption which takes the benefits from noise in communication channel to provide natural randomness for encryption algorithms [79-82]. Moreover, employing a modulation scheme such as frequency hopping or ultra-wide band (UWB) together with physical layer encryption may be helpful in hiding locations of sensor nodes.

The results in chapter 5 showed that the attacker located next to the sink increases the attack effectiveness. To eliminate this weakness, future research should consider maximum likelihood voting or other detection techniques providing more effective ways to detect malicious activities. Since multiple sinks with even simple majority voting improve security performance, especially when the attacker is next to the sink, additional studies should investigate the case of having sinks vote based on correlation of the time the packets arrive. The first packet delivery time can be determined in terms of  $T_{\min}$ ,  $E$ , and  $GP$  and its PDF exists according to the analysis in section 4.1.2. Because the first packet delivery time is different among different originating locations, one can use the first packet delivery time at each individual sink to form a correlation among them and use it to define maximum likelihood decision function for the detection of fault-data injection attacks. As an example, a sink can use time stamps to determine the differences of packets received time at each sink and to form a vector of the first packet delivery. The sinks can use this vector to represent an incident vector for each of the received packets of similar content. The dimension of the incident vector depends on the number of sinks. A probability distribution

function of the incident vector for each source location can be formed and the maximum likelihood decision function can be determined from the PDF of the incident vectors. The sink can then use this information to perform maximum likelihood voting. Moreover, using this technique does not require additional energy for wireless sensor nodes, similar to the majority voting technique used in this research.

The results also indicated that WSNs employing multiple delivery paths do not reliably deliver data when the number of nodes participating in a message modification attacks increases to more than 10%, even when using three sinks, because the modified packets outnumber the copies of the legitimate packet. To reduce the probability of Sink1 accepting modified packets, one can use the threshold voting e.g. accepting a packet if more than 75% of the packets of similar content received (denying if less than 75%). However, increasing the threshold can also increase in the packet discard rate. An alternative solution is to increase threshold only when a large number of attacking nodes are detected, which requires additional detection techniques. Future research may also consider detection techniques at intermediate nodes. However, detection at intermediate nodes will necessarily employ energy for detection, which may or may not be greater than the energy required to forward a modified packet.

In packet flooding attacks, employing rate limiting helps contain the attacks but the sink still receives the flooded packet reducing the probability of the sink accepting packets. Moreover, if the attacker injects a packet at the same rate as the legitimate traffic rate, the detection techniques using only rate limit cannot detect this malicious activity. Employing three sinks and rate limiting at the same time may help improve both data integrity and availability of the network under a packet flooding attack.

The techniques proposed in this study only focus on improving data integrity and availability, however, authentication was not studied because it does not readily emerge from the MAC and routing protocols studied. To improve security, future research should also consider authentication, which may possibly emerge from other MAC protocols. Moreover, this study considers only WSN with low utilization. The gossip based protocols may not be suitable for applications with high burst rates. Future research may also consider security for WSN applications which require MAC and routing protocols which support high burst data rates.

## BIBLIOGRAPHY

- [1] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks," *Communications of the ACM*, vol. 47, pp. 53-57, June 2004.
- [2] X. Ning, R. Sumit, C. Krishna Kant, G. Deepak, B. Alan, G. Ramesh, and E. Deborah, "A wireless sensor network For structural monitoring," in *Proceedings of the 2nd international conference on Embedded networked sensor systems* Baltimore, MD, USA: ACM, 2004.
- [3] V. Shnayder, B. Chen, K. Lorincz, T. R. F. Fulford-Jones, and M. Welsh, "Sensor Networks for Medical Care," Division of Engineering and Applied Sciences, Harvard University 2005.
- [4] L. Konrad, J. M. David, R. F. F.-J. Thaddeus, N. Alan, C. Antony, S. Victor, M. Geoffrey, W. Matt, and M. Steve, "Sensor Networks for Emergency Response: Challenges and Opportunities." vol. 03, 2004, pp. 16-23.
- [5] K. Lorincz, D. J. Malan, T. R. F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton, "Sensor networks for emergency response: challenges and opportunities," *Pervasive Computing, IEEE*, vol. 3, pp. 16-23, 2004.
- [6] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," in *IEEE Communications Magazine*, 2002, pp. 102-114.
- [7] W. Brett, L. Matt, L. Brian, and S. J. P. Kristofer, "Smart Dust: Communicating with a Cubic-Millimeter Computer." vol. 34, 2001, pp. 44-51.
- [8] J. E. Wilkes, "Privacy and authentication needs of PCS," *IEEE Personal Communications*, vol. 2, pp. 11-15, 1995.
- [9] M. Sutton, "Hacking the Invisible Network: Insecurities in 802.11x," July 2002.
- [10] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: a link layer security architecture for wireless sensor networks," in *the 2nd International Conference on Embedded Networked Sensor Systems*, 2004, pp. 162-175.
- [11] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security protocols for sensor networks," in *The Seventh Annual International Conference on Mobile Computing and Networking*, 2001.
- [12] IEEE, "IEEE 802.15.4-2003: Wireless MAC and PHY Spec. for Low Rate Wireless Personal Area Networks (LR-WPANs)," 2003.
- [13] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks," in *the 2004 ACM workshop on Wireless security*, Philadelphia PA, USA, 2004.
- [14] E. Shi and A. Perrig, "Designing secure sensor networks," *Wireless Communications, IEEE [see also IEEE Personal Communications]*, vol. 11, pp. 38-43, 2004.
- [15] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. Boca Raton: CRC Press, 1997.

- [16] D. W. Carman, P. S. Kruus, and B. J. Matt, "Constraints and approaches for distributed sensor network security.," NAI Labs, The Security Research Division Network Associates, Inc. September 2000.
- [17] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, pp. 293-315, September 2003.
- [18] W. Lou and Y. Fang, "A Multipath Routing Approach for Secure Data Delivery," *MILCOM 2001*, vol. 2, pp. 1467-1473, 2001.
- [19] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-tolerant routing for wireless sensor networks," *Computer Communications*, vol. 29, pp. 216-230, 2006.
- [20] A. Tsirigos and Z. J. Haas, "Analysis of multipath routing, Part 1: The effect on the packet delivery ratio," *IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS*, vol. 3, Jan 2004.
- [21] A. Tsirigos and Z. J. Haas, "Analysis of Multipath Routing, Part 2: Mitigation of the Effects of Frequently Changing Network Topologies," *IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS*, vol. 3, March 2004.
- [22] S. J. Lee and M. Gerla, "AODV-BR: Backup routing in ad hoc networks,," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, 2000, pp. 1311–1316.
- [23] Y. Ganjali and A. Keshavarzian, "Load Balancing in Ad Hoc Networks: Single-Path Routing versus Multi-path Routing," *IEEE INFOCOM*, vol. 2, pp. 1120-1125, 2004.
- [24] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, pp. 54-62, 2002.
- [25] M. Calle, "Complementing the GSP Routing Protocol in Wireless Sensor Networks." vol. Ph.D. Pittsburgh: University of Pittsburgh, 2009.
- [26] J. L. Hill, "System architecture for wireless sensor networks," Berkeley: University of California, 2003.
- [27] R. Flickenger, *Building Wireless Community Networks*: O'Reilly Media, 2002.
- [28] M. Calle and J. Kabara, "MAC Protocols for GSP in Wireless Sensor Networks," *Journal of Networks*, Academy Publisher, 2008.
- [29] IEEE, "IEEE standard for information technology- telecommunications and information exchange between systems- local and metropolitan area networks- specific requirements Part II: wireless LAN medium access control (MAC) and physical layer (PHY) specifications," 2003.
- [30] I. Demirkol, C. Ersoy, and F. Alagöz, "MAC Protocols for Wireless Sensor Networks: A Survey," *IEEE Communications Magazine*, vol. 44, pp. 115-121, April 2006.
- [31] W. Ye, J. Heidemann, and D. Estrin, "An energy-efficient MAC protocol for wireless sensor networks," in *INFOCOM*, 2002, pp. 1567-1576.
- [32] A. El-Hoiydi, "Spatial TDMA and CSMA with Preamble Sampling for Low Power Ad Hoc Wireless Sensor Networks," in *ISCC 2002*, 2002, pp. 685-692.
- [33] C. C. Enz, A. El-Hoiydi, J. D. Decotignie, and V. Peiris, "WiseNET: an ultralow-power wireless sensor network solution," *Computer*, vol. 37, pp. 62-70, 2004.
- [34] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *Wireless Communications*, vol. 11, pp. 6-28, 2004.
- [35] S. C. Ergen and P. Varaiya, "PEDAMACS: power efficient and delay aware medium access protocol for sensor networks," *Mobile Computing, IEEE Transactions on*, vol. 5, pp. 920-930, 2006.



- [36] V. Rajendran, K. Obraczka, and J. J. Garcia-Luna-Aceves, "Energy Efficient, Collision-Free Medium Access Control for Wireless Sensor Networks," *Wireless Networks*, vol. 12, February 2006.
- [37] W. R. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," in *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, Seattle, Washington, 1999, pp. 174-185.
- [38] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed Diffusion for Wireless Sensor Networking," *IEEE/ACM Transactions on Networking*, vol. 11, pp. 2-16, Feb 2003.
- [39] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *System Sciences, the 33rd Annual Hawaii International Conference on*, 2000.
- [40] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems," in *Aerospace Conference*, 2002.
- [41] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for Ad Hoc routing," in *the 7th annual international conference on Mobile computing and networking*, Rome, Italy, 2001.
- [42] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy aware routing: a recursive data dissemination protocol for wireless sensor networks," Computer Science Department, University of California at Los Angeles, May 2001.
- [43] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks," *Wireless Networks*, vol. 8, pp. 481-494, 2002.
- [44] J. H. Chang and L. Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks," in *Advanced Telecommunication and Information Distribution Research Program*, College Park, MD, 2000.
- [45] D. Braginsky and D. Estrin, "Rumor Routing Algorithm For Sensor Networks," in *The 30th International Conference on Distributed Computing Systems*, 2001.
- [46] K. Sohrabi and J. Pottie, "Protocols for Self-Organization of a Wireless Sensor Network," *IEEE Personal Communications*, vol. 7, pp. 16-27, 2000.
- [47] Z. J. Haas, J. Y. Halpern, and L. Li, "Gossip-based ad hoc routing," *IEEE/ACM Transactions on Networking (TON)*, vol. 14, pp. 479-491, 2006.
- [48] Z. Haas, L. Li, and J. Halpern, "Gossip-based ad hoc routing," 2002.
- [49] X. Hou, D. Tipper, D. Yupho, and J. Kabara, "GSP: gossip-based sleep protocol for energy efficient routing in wireless sensor networks," in *The 16th International Conference on Wireless Communications*, Calgary, 2004.
- [50] S. R. Fluhrer and D. A. McGrew, "Statistical analysis of the alleged RC4 keystream generator," *Lecture Notes in Computer Science*, pp. 19-30, 2001.
- [51] A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, pp. 11-33, Jan-March 2004.
- [52] M. Matsui, "Linear cryptanalysis method for DES cipher," *Lecture Notes in Computer Science*, vol. 765, pp. 386-397, 1994.
- [53] J. Daemen and V. Rijmen, *The design of Rijndael: AES--the Advanced Encryption Standard*: Springer Verlag, 2002.

- [54] J. Daemen and V. Rijmen, "AES Proposal: Rijndael, AES Algorithm Submission," September 1999.
- [55] C. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World*, 2nd ed.: Prentice Hall, 2002.
- [56] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for Key Management–Part 1: General," *NIST special publication*, pp. 800-57, 2005.
- [57] N. Ruangchaijatupon and P. Krishnamurthy, "Encryption and Power Consumption in Wireless LANs," in *The Third IEEE Workshop on Wireless LANs*, Newton, Massachusetts, 2001.
- [58] X. Luo, K. Zheng, Y. Pan, and Z. Wu, "Encryption algorithms comparisons for wireless networked sensors," 2004.
- [59] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Transactions on Information and System Security (TISSEC)*, vol. 8, pp. 41-77, 2005.
- [60] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Computer Communication*, vol. 30, pp. 2314-2341, 11-12 September 2007.
- [61] D. Welch and S. Lathrop, "Wireless security threat taxonomy," 2003, pp. 76-83.
- [62] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Computer Security: Recommendation for Key Management – Part 1," NIST March 2007.
- [63] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten, "Lest we remember: Cold boot attacks on encryption keys," in *the 17th USENIX Security Symposium*, 2008, pp. 45–60.
- [64] S. Skorobogatov, "Low temperature data remanence in static RAM," *University of Cambridge Computer Laboratory Technical Report*, vol. 536, 2002.
- [65] S. Northcutt and J. Novak, *Network Intrusion Detection*, 3rd ed. Indianapolis: New Riders Publishing, 2002.
- [66] J. R. Douceur, "The sybil attack," in *1st International Workshop on Peer-to-Peer Systems*, 2002, pp. 251–260.
- [67] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *the third international symposium on Information processing in sensor networks*, Berkeley, California, 2004, pp. 259-268.
- [68] E. C. H. Ngai, L. Jiangchuan, and M. R. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks," in *Communications, 2006. ICC '06. IEEE International Conference on*, 2006, pp. 3383-3389.
- [69] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, 2003, pp. 1976-1986 vol.3.
- [70] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L. W. Chang, "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," in *Wireless Communications and Networking Conference, 2005 IEEE*, 2005, pp. 1193-1199 Vol. 2.
- [71] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," 2003, pp. 197-215.
- [72] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," *IEEE Computer*, vol. 36, pp. 103-105, October 2003.

- [73] M. Bellare, J. Kilian, and P. Rogaway, "The security of the cipher block chaining message authentication code," *Journal of Computer and System Sciences*, vol. 61, pp. 362-399, December 2000.
- [74] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 5, pp. 11-25, 2001.
- [75] B. Deb, S. Bhatnagar, and B. Nath, "ReInForM: Reliable Information Forwarding Using Multiple Paths in Sensor Networks," *Local Computer Networks, Annual IEEE Conference on*, pp. 406-415, 2003.
- [76] M. Behzad and G. Chartrand, *Intro to the Theory of Graphs*: Allyn and Bacon, 1972.
- [77] J. A. Bondy and U. S. R. Murty, *Graph Theory with Applications*, 5th ed. New York: North-Holland, 1982.
- [78] D. A. Menasce, "Security performance," *IEEE Internet Computing*, vol. 7, pp. 84-87, 2003.
- [79] D. Reilly and G. S. Kanter, "Noise-Enhanced Encryption for Physical Layer Security in an OFDM Radio," in *Radio and Wireless Symposium, IEEE*, 2009, pp. 344-347.
- [80] A. e. Zúquete and J. a. Barros, "Physical-Layer Encryption with Stream Ciphers," in *IEEE International Symposium on Information Theory*, 2008, pp. 106-110.
- [81] G. S. Kanter, D. Reilly, and N. Smith, "Practical physical-layer encryption: The marriage of optical noise with traditional cryptography," *IEEE Communications Magazine*, vol. 47, pp. 74-81, November 2009.
- [82] A. Ahmad, A. Biri, and H. Afifi, "Study of a new physical layer encryption concept " in *5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, 2008, pp. 860-865.