

## LIST OF FIGURES

|                                                                                                              |    |
|--------------------------------------------------------------------------------------------------------------|----|
| Figure 2.1 Information Security components also known as CIA Triad.....                                      | 6  |
| Figure 2.2 Backpressure Collection Protocol routing topology.....                                            | 8  |
| Figure 2.3 Collection Tree Protocol routing topology.....                                                    | 9  |
| Figure 2.4 A tree-like DODAG topology and flow.....                                                          | 10 |
| Figure 2.5 Structure of a Standard ICMPv6 Control Message.....                                               | 11 |
| Figure 2.6 DIS Control Message.....                                                                          | 12 |
| Figure 2.7 DIO Control Message.....                                                                          | 12 |
| Figure 2.8 DAO Control Message.....                                                                          | 12 |
| Figure 2.9 DAO-ACK Control Message.....                                                                      | 13 |
| Figure 2.10 Type of RPL attacks that impact resource of sensor or network.....                               | 13 |
| Figure 2.11 Type of RPL attacks that impact the topology of network.....                                     | 15 |
| Figure 2.12 Type of RPL attacks that impact the traffic of network.....                                      | 16 |
| Figure 3.1 The procedure of simulation implementation and data collection.....                               | 19 |
| Figure 3.2 Construction process algorithm of RPL DODAG.....                                                  | 20 |
| Figure 3.3 Source code and related variables for implementing Flood Attack.....                              | 22 |
| Figure 3.4 Source code and related variables for implementing VNM Attack.....                                | 23 |
| Figure 3.5 Source code and related variables for implementing Blackhole Attack.....                          | 23 |
| Figure 4.1 Average Hop Count of nodes from Reference Network simulation.....                                 | 26 |
| Figure 4.2 Number of received and lost packets in Reference Network<br>observed from Cooja Simulator.....    | 26 |
| Figure 4.3 Average Hop Count of nodes from Flood Attack Network simulation.....                              | 27 |
| Figure 4.4 Number of received and lost packets in Flood Attack Network<br>observed from Cooja Simulator..... | 28 |
| Figure 4.5 Average Hop Count of nodes from VNM Attack Network simulation.....                                | 29 |
| Figure 4.6 Number of received and lost packets in VNM Attack Network<br>observed from Cooja Simulator.....   | 30 |
| Figure 4.7 Average Hop Count of nodes from Blackhole Attack Network<br>Simulation.....                       | 31 |
| Figure 4.8 Number of received and lost packets in Blackhole Attack Network                                   |    |

|                                                                                                    |    |
|----------------------------------------------------------------------------------------------------|----|
| observed from Cooja Simulator.....                                                                 | 34 |
| Figure 4.9 Differences of Simulated VNM Attack and Mitigated Network in<br>Power consumptions..... | 40 |
| Figure 4.10 Differences of Simulated VNM Attack and Mitigated Network in<br>Routing Overhead.....  | 40 |
| Figure 4.11 Differences of Simulated VNM Attack and Mitigated Network in<br>E2E Delay.....         | 40 |
| Figure 4.12 Differences of Simulated VNM Attack and Mitigated Network in<br>Routing Overhead.....  | 41 |
| Figure 4.13 Differences of Simulated Blackhole Attack and Mitigated Network<br>in PDR.....         | 41 |