Forensic Analysis Of Blackhole Attack in Wireless Sensor Networks

By

Ahmad Hasan

Fall 2017-MS(IT) - 00000203491

Supervisor

Dr. Muazzam Ali Khan Khattak

Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters of Science in Information Technology (MS IT)

In

School of Electrical Engineering and Computer Science,

National University of Sciences and Technology (NUST),

Islamabad, Pakistan.

(February 2020)

Approval

It is certified that the contents and form of the thesis entitled "**Forensic Analysis Of Blackhole Attack in Wireless Sensor Networks** " submitted by **Ahmad Hasan** have been found satisfactory for the requirement of the degree.

Advisor: **Dr. Muazzam Ali Khan Khattak**

Signature: _____

Date: _____

Committee Member 1: **Dr. Mehdi Hussain**

Signature: _____

Date: _____

Committee Member 2: **Dr. Safdar Abbas Khan**

Signature: _____

Date: _____

Committee Member 3: **Dr. Hasan Tahir**

Signature: _____

Date: _____

Abstract

In recent years, Wireless Sensor Networks (WSN) has been exponentially proliferated in almost every domain of life encompassing civil and military sectors. In fact, due to the flexible implementation nature, WSN has become one of the richest domains of Information technology echo-system.These sensor networks can be implemented in challenging and unusual terrains and environments, in which human reachability or sustainability is difficult or even impossible. The wireless broadcasting and resource-constrained environments along-with limited transmission range make WSN prone to various types of cyberattacks such as DDoS, Sybil, Sinkhole, blackhole, and wormhole attacks.An exertive research effort has been devoted to secure WSN, but security is never ultimate. Instead of the state of the art detection and preventing techniques, cyberattacks still occur. It is the need of the hour to forensically investigate and analyze the cybercrimes in sensor networks. The Critical Infrastructures which are heavily dependent upon WSN required to be analyzed after failure and the facts behind the failure need to be unraveled. Specifically, in case of mobility, it is challenging to sustain and maintain the availability, confidentiality and integrity of the network. We examined the performance of the network with the AODV routing protocol under the

Blackhole attack using the Friis propagation loss model on the network simulator (NS3). We briefly examined the traffic in the network and on the nodes by different tools to asses the damage of the attack on the network.

Dedication

I dedicate this Dissertation to the people who love me and the people whom I love.

Certificate of Originality

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics which has been acknowledged.

Author Name: **Ahmad Hasan**

Signature: _____

Acknowledgment

Thanks to Almighty Allah SWT for showering his blessings upon me. The ability to learn is one of the greatest blessings of Him. Thanks to Him for providing me the opportunities to follow my dreams, Alhamdulillah.

I do not have words to explain the efforts and prayers of my great mother as without her I'm nothing. She is the real value of my life. I am thankful to my father for his best formation for us, I have never a man like his courage. I have learned the things from my father which no institute can teach. I am thankful and indebted to my siblings. They are true friends and supporters. I am very thankful to my cousin brother M Saleem Siddiqi for his support and guidance. I am thankful to my maternal and paternal uncles and aunties in the family for their prayers and support. I am thankful to my friends M. Adnan, Imran F, M. Tayyab, S Ali, H Murtaza, Z Alizai, and my lovely group of class for their support and prayers.

I am grateful to my supervisor. He is a true gem and a wonderful leader. I will always be indebted to him. I am thankful to Dr. Shahzad Saleem, Dr. Safdar A Khan, Dr. Hasan Thir Batt, and Dr. Mehdi Hussain for their guidance and support.

Alhamdulillah for having you all in my life.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

A network contained a group of small battery-powered, specific purposes, autonomous wireless transducer devices that observe and record physical conditions in different environments called a wireless sensor network (WSN). The wireless sensor networks have a massive implication range covering civilian and military domains under its umbrella. These networks are usually deployed in exceptional environments and generally supervised parameters are pressure, vibration strength, chemical intensities, dampness, gale speed and directions, rain, temperature, pollution, biological and zoological interpretations for process control and real-time monitoring. There are numerous types of wireless sensor networks according to their specific nature and responsibilities. They are usually categorized as Ad-hoc and centralized networks, and certain eminent types of wireless sensor networks are Mobile Ad-hoc Networks (MANETs), Wireless Sensor Networks (WSNs), and on a broad note

the finest of all the Internet of Things (IoT).

WSN contain large numbers of inexpensive tiny sensor devices deployed in special areas observing the environment. The data observed by nodes is maintained and safely delivered to the central device or other fellow nodes [1]. These self organised wireless networks of geographically distributed nodes are dedicated to exceptional responsibilities specific to their deployment objectives. They monitor surroundings, perform surveillance of physical and logical environments and collect data to a principal locality.The data transmission is carried out via wireless medium so it is very cost effective and faster. The distinctiveness of these networks is that the nodes are autonomous, they are not subordinated to a central device. They are robust, self-responsible, self-maintained, executing multi-path routing, and not bound to any specific network topology. Generally, WSNs are installed in remote and problematic terrains, which are challenging to human reachability and sustainability [2]. In classic WSNs the sensor nodes are connected to gateway nodes which are further attached to wired infrastructure. A mobile ad-hoc network (MANET) is a decentralized type of WSN, which is comprised of multiple mobile wireless devices. Each device in MANET is independent in its nature. It can move freely and spontaneously in several directions and frequently alter and modify its connection with fellow devices [3]. Unlike WSNs, MANETs are peer-to-peer, infrastructure-less, self-forming, continuously self-healing networks, and usually deployed on a small scale in competitive tactics. In wireless mobile ad-hoc all nodes bear responsibilities of joining and leaving the network, and several nodes can have the capabilities to generate a new network. Every node in MANETs endures the obligation of discovering route and data

transfer within the Network [4]. The decentralized illustration of MANETs is attractive because it results in the possibility for several applications to operate in geographically diverse, dispersed and problematic regions. The mobility with a multi-hop fashion results in advances in network capacity and robustness. The Internet of things (IoT) is comparatively fresh embedded

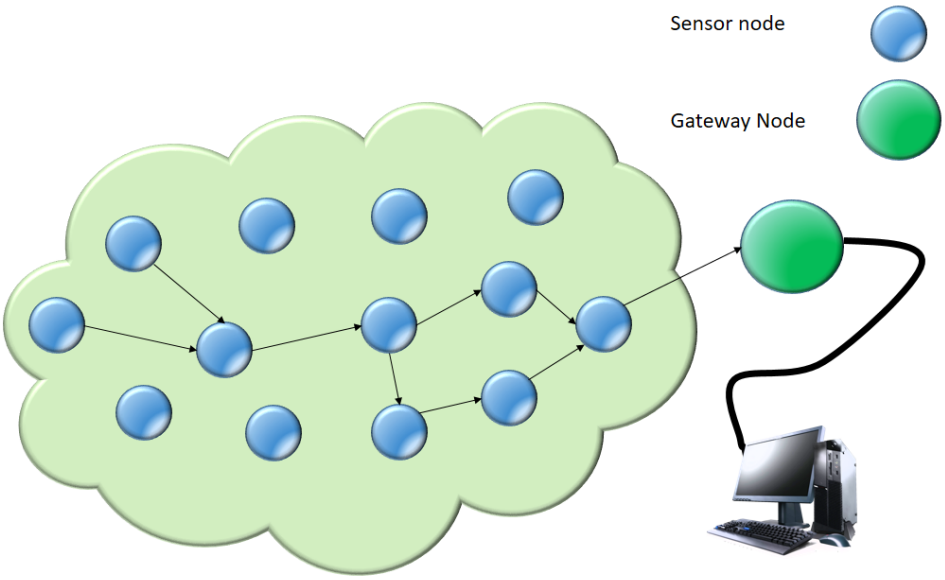

Figure 1.1: A simple Wireless Sensor Network

technology domain in Sensor Networks Empire, without uniform architecture and comprised of a network of common everyday objects and physical nodes [5]. Actually, the main idea behind the Internet of things (IoT) is the connection between everything which can be connected to the Internet i.e. household items, pets, industrial equipment. It is the extension of the Internet to objects, animals, people, digital and mechanical equipment, and computing devices by distributing unique identifiers (UID) to each entity. This

results in wiping out humans to the computer or human to human interaction for the conveyance of data over a network [6]. The inception of IoTs belongs to Kevin Ashton. He presented this idea in 1999 and its cost-effectiveness, Wireless communication technology, mobility incorporated influence make the internet of things (IoT) attractive in the modern era. Wireless Sensor Networks have very immense implementation domain encompassing civilian and armed environments and have appealing recognition in both domains because WSNs are usually installed in a difficult and challenging area where human accessibility and sustainability are problematic. These networks help users to attain efficiency and reliability in delay-sensitive and time-critical operations. So they are widely used in agriculture, ecology, medical, rescue, physiology, health care, and engineering industry in civil domains encompassing air, land, water. In the military domain, especially WSNs and MANETs have a huge acceptance base, including air, land and under-water operations i.e. weapons, robots, Army tactical MANETs, UAV, Naval Ad-hoc Networks. Especially, IoTs are forming a smart world by its magical features and shaping the rigorous execution of daily maneuvers in each domain. In the past few years, IoTs and WSN have taken massive prominence in the world, by connecting people and critical infrastructure and devices gained integral proliferation in every domain discussed above. The widespread use of sensor networks in every domain has some shortcomings such as likeability to security attacks. The mobile and broadcasting atmospheres of WSNs along with resource constrained infrastructure are vulnerable targets to diverse cyber-attacks [7]. Network availability, access control, confidentiality, anonymity and integrity is most crucial to sustaining in such fragile infrastructure es-

pecially in the networks of mobile devices. Security in these networks is a very critical issue because usually, the data which is being transferred may be intensely crucial. Content dissemination in sensor networks is susceptible to numerous complications such as mobility, snooping, espionage, and link breakage especially in IoT communique due to nodes diversity. The emerging technologies such as WSNs, MANET, and especially embedded infrastructure of the internet of things (IoT) have financial and societal benefits, but when these services are misused or impersonated by malicious entities may imply some severe threats [5,6]. These threats may increase from individuals to community-level contingent on the capacity of the malicious entity. There are numerous cyber threats to sensor networks (SN), in which one attack is a blackhole attack. Blackhole attack may be exceptionally detrimental to significant functionalities of Sensor Networks because it may lead to large scale DDoS(Distributed Denial of Services Attack) at a big canvas I.e. resource distributions, routing, data aggregations and misbehavior detection.

1.2 Blackhole Attack

Blackhole or packet-drop attack is an active and harmful attack among the extremely detrimental possible attacks in WSN. In this particular type of attack, an adversary node claims the shortest path till destination via RREP (Route Replay) message to the source node even it does not have any route or path towards the destination. As a result of this, the sender transmits all the data packet to this malicious node, and it drops the data packet instead of forwarding it to the destination [4, 7] affecting the collective throughput

and energy of the nodes. Due to this packet absorbing behaviour, we call malicious node a 'Blackhole Node' and this attack 'The Blackhole attack'. Usually, normal nodes broadcast the RREQ (Route Request) in the discovery for a route phase to know the shortest path towards the destination. Every node which receives the RREQ packet checks it's routing table as it has updated the shortest path to the destined node. Then each node compiles the RREP packet and replies to the specific node which broadcasted the RREQ packet. Normal node trusts the RREP of the malicious node due to the absence of identification of the legitimacy on nodes and the malicious node takes advantage of this. The source node starts to transmit data packets to the malicious node in a hope that it will deliver these packets to the destination. The malicious or Blackhole node drops or discard these packets. The nature of this packet dropping behavior may be absolute or selective and will be a gateway to other fatal and catastrophic attacks. The Blackhole node may drop the packet after transmitting x number of packets, or packet after some time t, or packets between a specific time period p, or packets from a specific source s, and the packets towards the specific destination d. If the Blackhole node starts to drop all of the incoming data packets all the time, then the normal nodes or the source node come to know that the specific node is an adversary, and the sources try to discover alternative paths discarding the malicious node. The selective behavior of the Blackhole node is the most harmful or lethal form of the attack because in this case, it is almost impossible to detect that if an attack is active or not, or the node is dropping packet on purpose or due to some normal behavior. In the selective behavior of blackhole nodes, some or most of the traffic still flows towards

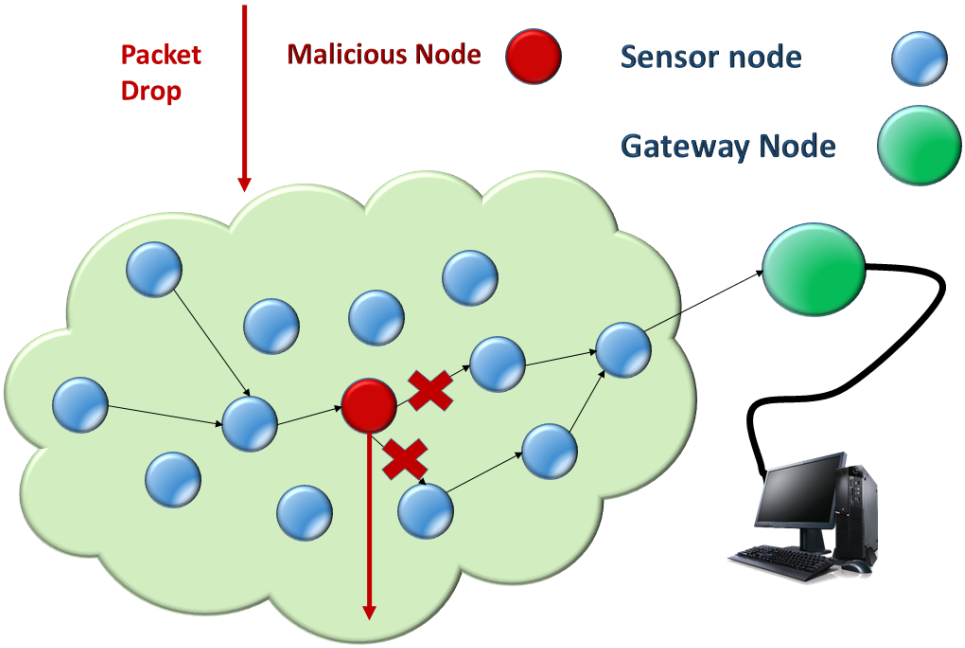

Figure 1.2: A Simple Blackhole Attack Scenario

the destination. There are two categories of blackhole attack depending on the number of malicious nodes in the network [8]. The classification of the attacks named as single Blackhole attack and a co-operative Blackhole attack. On the other side, in a single Blackhole attack, only a single node drops the data packets, while in cooperative Blackhole attack multiple nodes drop the data packets to degrade the network performance and reliability.

1.3 Digital Forensics

Forensics or criminalistics is the postmortem investigative branch of science aimed to unravel the hidden facts behind some unusual incidents. Forensic science is the implementation of scientific methodologies to criminal and

civil legislation. “Forensic Science” consists of two Latin words. The word forensic means public dialogue or inspection, investigation, and examination. Second-word ‘science’ is related to the term ‘systematic way to get knowledge’. This is a fine-grained procedure consists of operationally connected and naturally isolated processes. The forensic investigators follow the standard procedures and use authentic tools and techniques to collect, preserve, and analyze evidence during the entire investigation course. The forensic investigation usually comprised of multiple investigative roles such as evidence collector specialist, laboratory specialist, evidence analyst, and presentation specialist.

Digital Forensic Science is comparatively a fresh domain in the digital world, and it was first defined by G. Palmer in the Digital Forensic Research Workshop back in 2001. The exceptional growth of digital volume all over the world due to the extensive recognition and acceptance of modern digital technologies like WSN and IoT in the public and private sectors has raised serious complications. The penetration of digital technology in our world resulted in their use in malicious, unlawful, and criminal activities to gain several unauthorized benefits.The digital crime, malicious action, or unusual incident is the unauthorized and illegal actions performed to disrupt planned legal digital operations [9]. So it resulted in the creation of a new branch of Forensic Science named as digital forensics. It is a modern subdivision of forensic science, covering the retrieval and examination of criminal evidence extracted from digital media by using scientifically proven procedures and methodologies [9]. These methodologies are implemented for the identification, preservation, collection, validation, analysis, interpretation, documenta-

tion, and presentation of the digital evidence extracted from digital resources. Usually, the digital forensics investigation process recreates the incident that happened previously with the support of the electronically stored information (ESI) at hand, and thus assists the crime investigations and the legislative proceedings and processes [10]. The digital evidence or electronically stored information is bit by bit binary data which is stored or transmitted through digital media and can be presented at legal platforms [11]. The successful Digital investigation process results in [10]:

- Proving or disproving the integrity of the Digital evidence
- Proving the individuals or parties inculpatory
- Proving the individuals or parties exculpatory

The digital forensic investigator and examiners should be professionally and ethically trained and they should have good moral qualities with neutral nature. The result of their investigation will end in the inculpatory or exculpatory of someone. The non-professional, non-serious, and biased approach may result in fatal consequences. The integrity and professionalism of an investigator should be unquestionable and exemplary. The digital forensic investigation totally relies upon the preserved digital evidence. And the integrity of digital evidence is very important for a successful investigation [10].

A little outline of these sub-processes of the digital forensic investigation process is given below.

- Identification: This process is related to the identification of the unusual incident and the resources required for the incident
- Preservation: Data security, isolation, and preservation from the victim devices of traffic logs

• Forensic Triage: Prioritizing the digital evidence from preserved data

• Analysis: This part consists of identifying the tools and techniques for examining preserved data and digital evidence. Then processing that data through these tools. After that interpreting the result of the analysis. Our research is mainly related to this process.

• Documentation: The documentation process is the detailed paper presentation of the crime. The images, sketches and maps of the crime scene is part of the documentation.

• Presentation: Summarization and description of consequences.

Digital forensics is further divided into sub-branches in which we are concerned with mobile device forensics, network forensics, IoT forensics, Cloud forensic, DB forensics and forensic data analysis. The digital forensics investigation process aimed to answer these critical questions.

• What Happened?

• Where did it happen?

• What are the victim devices?

• When did it happen?

• Most critical question of all. How did it happen?

• What are the flaws in the security system?

• External or Internal attribution of crime?

• Who is behind this incident?

In device forensics, we examine a device to preserve, identify, extract and collect evidentiary data. Then we use that data to perform root cause analysis. In fact, we can use two investigation approaches. First, Device as a victim, and secondly the device as an attacker tool. It is essential to apply

robust, accurate, and distinct techniques and methodologies in the forensic investigation process. On the other side, Network forensics is an investigation of what ports have been used to access network for attack [12]. We identify, preserve, analyze and present digital evidence to expose illegitimate actions in a network. There are two main ways of collecting digital evidence in network forensics, the captured traffic of network and the data maintained by network devices. Forensic data analysis is the most crucial process of digital investigation and it is the backbone of the entire forensic investigation. Our objective of this research activity is to execute a postmortem analysis of the Blackhole attack in WSN and uncover the facts behind malicious activity performed.

1.4 Problem Statement

Security is never ultimate and perfect security is just an illusion. The wireless infrastructure and especially the mobile nature of wireless sensor networks (WSN), the terrains of their deployment, and the criticality of their objectives make them vulnerable to cyberattacks and appeals to the attackers to compromise or disturb the network for their malicious activities. The Blackhole Attack is one of the top detrimental attacks in the sensing domain. The Blackhole attack is a sort of DoS attack. Despite the efforts and security mechanisms, the attacks occur. It is very important to investigate what, when, how, and why that incident happened. The vulnerabilities and loopholes in the system should need to be revealed. The damage to the system due to the incident should be measured. The countermeasures should be

developed under the past observations. Digital Forensics is all about the postmortem analysis of the crimes observed in the cyber world.

1.5 Motivation

The rapid proliferation of wireless sensor realm in every domain of life has raised several security risks with harmful consequences regarding personal security, personal rights, privacy, and basic human rights. In the past decade, crimes in the digital world or crimes conducted by using digital devices have been boosted up all across the globe due to the massive digitalization of routine operations. The digital forensics investigators unlike conventional forensic scientists collects and analyze digital evidence (DE), bit patterns, data record transmitted and received, data stored instead of blood sample, DNA, finger prints and so on. The digital world always is an easy target of criminal minds because it is not always the necessary physical appearance of criminals at the crime scene. There were different kinds of crimes observed in the digital world. The list of some notable types of cybercrimes is given below.

- Fraud
- ID Theft
- Scamming
- Ransomware
- Child pornography
- Denial of Services
- Ransomware

- Injecting Malware
- Unauthorized access to critical infrastructure
- Cross-site Scripting
- Botnets

In the last one and half-decade, the immense research efforts have been dedicated to secure the sensor networks. A lot of detection and prevention techniques have been suggested and different methodologies have been proposed to secure the sensor networks but good security for wireless sensor networks and IoT is hard and requires exertive time and effort due to the diverse, mobile, and resource-constrained nature of the problem domain [13]. The term 'perfect security' for this types of network is just an illusion. People usually think that the system they are working on is perfectly secured but there are some loopholes, weaknesses, and flaws in security mechanisms, which are only needed to be approached.

The DoS or denial of services is among of the most harmful cyber-attacks in which attacker disrupts the network resources illegitimately and makes the services unavailable to its legitimate intended users. Blackhole attack is the type of DoS attack. The DoS attacks are among the top attacks which were observed in the digital world. The figure 1.1 shows the DoS attack occurred in past three years. The change in the DoS attack statistics variation during past three years is given in the figure 1.2. The proportion of different types of DoS attacks in past year is depicted in the figure 1.3, which shows that SYN flooding.

We are going to discuss some of the notable and topmost DoS attacks observed in the past three to four years, which shows that security is never

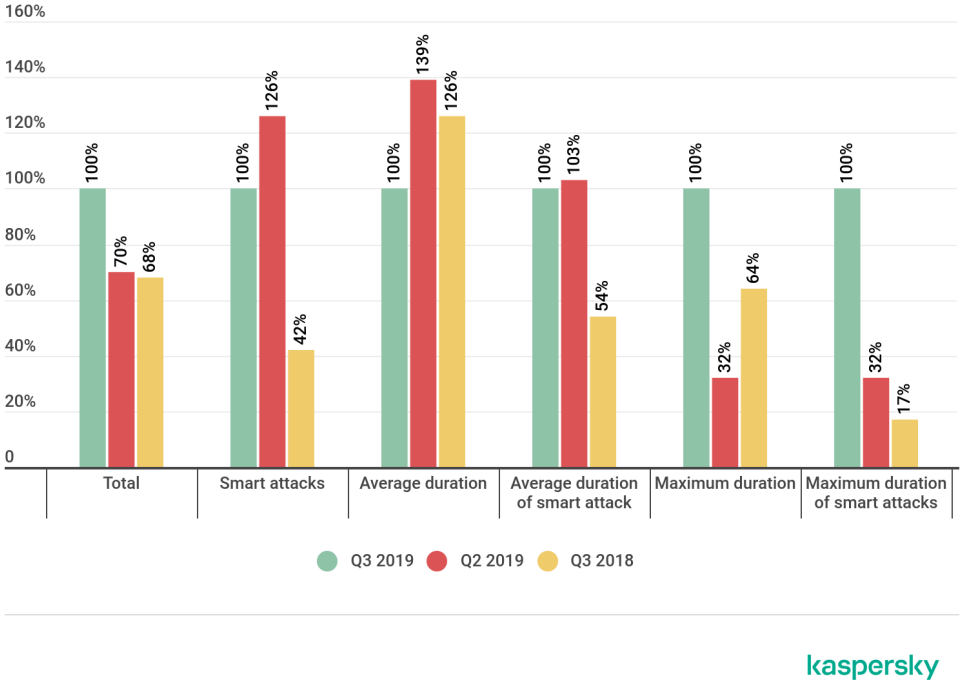

Figure 1.3: Denial Of Services Attacks Statistics in Past Three Years [14]

ultimate or perfect. The big names in the digital world have always been a target of illegitimate activities to gain unintended benefits. Most of the attacks have been prevented but some of them have been successfully implemented. One of the most discussed attacks is the Distributed Denial of Services attack (DDoS) attempted back in October 2016 on Dyn [15], a renowned Web Application Management and Internet Performance Management, Web Application Security, and domain name service (DNS) company . The little innocent IoT devices became the part of an IoT army to commit DDoS attacks. The attack affected Twitter, Paypal, Amazon web services, and Netflix either. The Dyn stated attack as a complicated and sophisticated attempt by using port 53 with masked UDP and TCP traffic. The

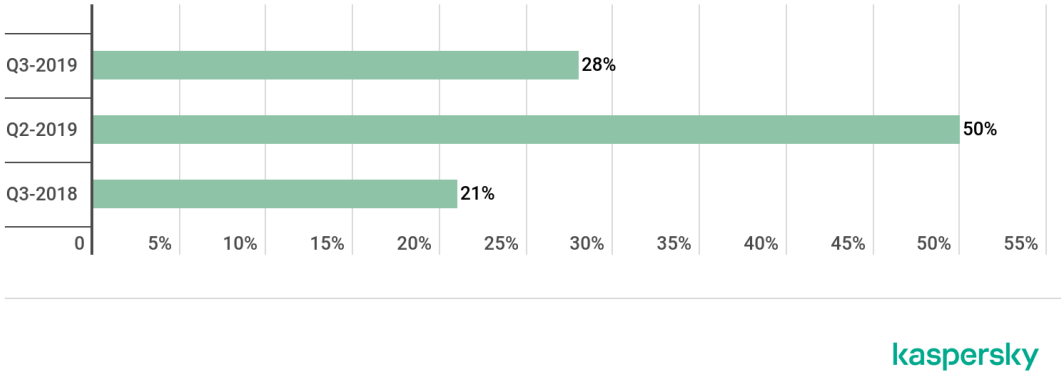

Figure 1.4: Denial Of Services Attacks Statistics Variation [14]

Mirai botnet was a key source of illegal traffic and the attack was originated by recursive DNS retry traffic. The recursive DNS worsened the impact of the attack. There was another noticeable malicious activity observed back in 2017 when one of the largest American credit bureaus named Equifax faced a cyber-attack resulting in 143 million of its customers compromised. The invaders stole sensitive private data of the customers including their birth-dates, identities, licenses data, and residential addresses with the credit card data of 209 thousand customers [16]. The attacked originated in the mid of May 2017 and exposed at the end of July 2017. The application vulnerability caused the lethal attack. There was a noticeable DDoS attack on UK national lottery scheme when their website and mobile phone application taken offline due to the massive DDoS attack in September, 2017 [18]. One of the most popular developer platforms named GitHub faced the greatest DDoS attack of all time back in February 2018. The sudden immense traffic was observed and recorded at a rate of 1.35 terabits per second(Tbps), so it is also called 1.35 Tbps GitHub attack [17]. The amount of traffic was enor-

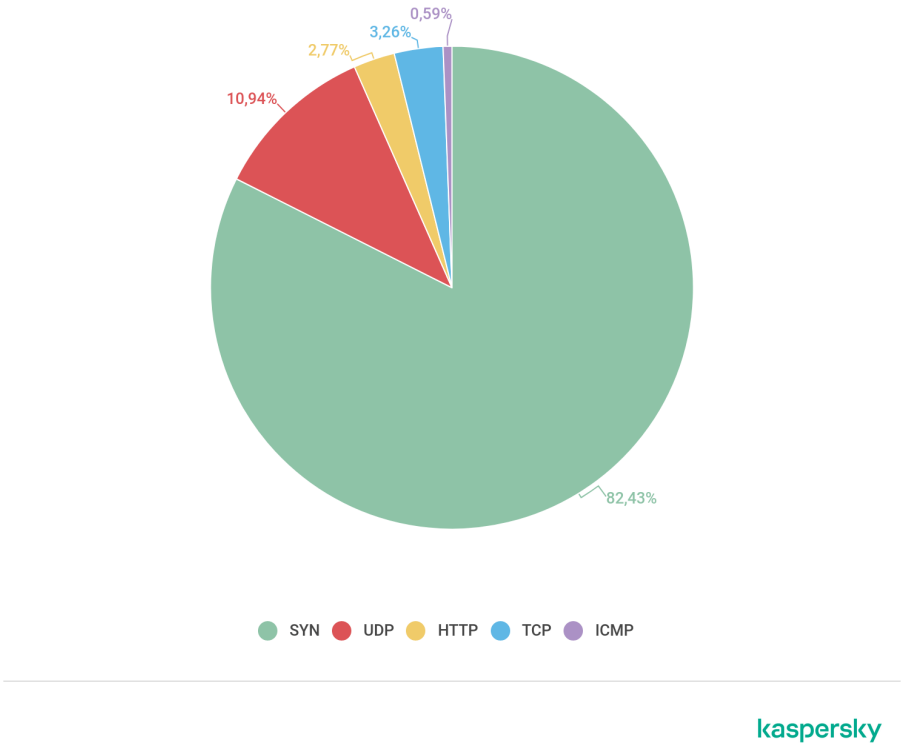

Figure 1.5: Denial Of Services Attacks Types [14]

mous and record-breaking. According to the official statements GitHub, the traffic was tracked down from the points of origination, and over a thousand multiple autonomous systems across thousands of unique endpoints found. The attack consisted of two phases. In the first peak, the onslaught of traffic at 1.35 Tbps via 126 million packets per second, and in the second phase 400 Gigabits per second (Gbps) offensive traffic was recorded. The attack was mechanized by manipulating the Memcached instances that were unconsciously available and accessible on the Internet with the user datagram protocol (UDP) support enabled. The spoofed internet protocol (IP) addresses permitted the Memcached responses to be targeted against further

addresses, like the data which was used to serve GitHub. This vulnerability was unique in its nature. The above paragraphs comprise some of the prominent attacks in the most recent past and the statistics in the figures show that the Blackhole attack and DDoS attack still occur despite the facts of hardest security efforts. There is nothing that exists like perfect security. The security can be better and better but at some points or levels. There is always a loophole or weakness in the so-called perfect plan, and ultimately attackers find that to breach the system for malicious benefits. According to the statement of the Visual Network Index (VNI) forecast by Cisco Systems [19], there will be 28.5 billion network devices in the world by the end of 2022. The exponential increase in the volume of WSN and IoT devices will also result in numerous cyber-security risks.Now, If the attack or something unusual happens, and the security teams finally mitigate the attack. After all, The most important questions arise.

- The Incident itself?
- The Incident Time?
- The incident behavior?
- The Victim nodes in-network?
- The compromised or malicious nodes?
- The behavior of the compromised nodes?
- The flaws in the security system?
- The damage?
- External Attribution?
- Internal Attribution?

So logically we come to the conclusion that despite the security mech-

anisms, we still have to develop and strengthen forensics mechanisms to conduct the investigations. The Forensic investigations of the cyber-attacks in wireless sensor domains are very important because this domain is comparatively more prone to security attacks and resource-constrained in terms of power and memory. The detailed discussion regarding forensic studies of WSN and its sister domains will be documented in the upcoming section. We have chosen the Blackhole attack in the sensor domain to implement the forensic analysis because to the best knowledge there is not research paper found specifically on the topic of forensics analysis of Blackhole attack in the sensing domain. The reason behind choosing because we have observed its detrimental effects on the systems. The digital forensics of wireless sensors networks domain and the difficulties with a brief analysis will be discussed in literature review section.

1.6 Objectives and Goals

The purpose of this research is the forensic analysis of detrimental blackhole attack in WSN. We will deeply investigate and analyze this attack and will briefly discuss the WSN vulnerabilities causing this attack. We will unravel the facts behind this attack. A brief root cause analysis will help to construct the better mechanisms to guard the network systems in the future.

Chapter 2

Literature Review

The Wireless Sensor Networks (WSN) are prone to Blackhole attack and other disastrous attacks due to their mobile broadcast nature. In this section, we are going to discuss the previous research efforts dedicated to detect and prevent the sensor networks from the Blackhole attacks, the vulnerabilities of sensing domain, digital forensics complexities for sensing domain, and forensics investigations studies carried out in mentioned domain.

Now we will briefly discuss the characteristics of sensor networks which make them vulnerable to different security attacks. WSN communication operations entirely depend upon the wireless media for data transmission. Data communication and transmission via the mentioned medium is financially economical because it reduces the consumption of expensive physical media for data transmission. It resulted in reducing the human exertion to install network devices and transmission cables over vast geographical ranges [7, 21, 23]. WSN devices cooperatively operate to gather and transmit data for several economical objectives. The nodes in the sensing domain

not only operate in regular environments and normal circumstances but in dangerous situations monitoring critical infrastructures. The insecurity of WSN is categorized into three classes. First, the insecurity of nodes for example the common sensor nodes and the heads, insecurity of communication hops and routes between sensor nodes, and insecurity of data traffic transmitting via the wireless media. The resource-constrained environment of the wireless sensing domain makes it very problematic to operate an entire collection of wireless sensor network nodes steadily at a time. It will affect the cost and power of the WSN [20]. The MANET sensing domain is usually composed of several mobile devices with restricted transmission range, power, and battery resources [4]. In sensor networks, the sensor nodes are very cost-effective and installed in comparatively problematic terrains where human sustainability and approach is not conceivable. These nodes are accomplished to observe the environmental surroundings and then disseminate the data . In general, the WSNs contains a base station (BS), with various cluster heads (CH) and the member nodes in multiple clusters. The CH collects the data from their nodes and directs the obtained information to the BS. In the Ad-hoc environment of the sensing domain, the mobile nodes can spontaneously join or vacate the network. There is no explicit organization in MANET infrastructure. The self-building nature of the mobile nodes is the key reason behind the popularity of these networks in military operation applications and tragedy controlling applications [4]. The nodes in the wireless sensing environment always depend upon other fellow nodes for forwarding data. This multi-hop dependency between nodes is also a notable weakness of WSN. The attackers generally take advantage of this hop

to hop dependency and inject malicious nodes in the routes. The malicious nodes then start to drop data resulting in the black hole attack [22]. Other notable vulnerabilities of WSN nodes are the limited transmission range, computational capacity and less power. These limitations are the key obstacle to apply customary cryptographic techniques.There are multiple reasons such as interference, multi-path effects, shadow effects, external noise, and weather which affects wireless communication. As we know, the nodes in WSNs are prone to diverse security problems and attacks, and the Blackhole attack (BH) is among the top detrimental attacks which is a form of DDoS attack. There are several notable methodologies, technologies, and schemes proposed to mitigate the Blackhole attacks. We are going to discuss those schemes. An interesting multiple WSN zoning environment Black Hole Attack detection scheme was proposed [24]. In the proposed methodology, the wireless sensor network is distributed into multiple small zones of similar size by assigning a unique ID to each zone. The nodes know their respective locations and position by Localization algorithm. Every node in the network broadcast its energy level with all other nodes and BS. The BS then picks a node with uppermost energy and make that node the head of the cluster head (CH). The main authorities of CH are receiving the data from all the nodes in the zone, and then forward it to the BS. Several mobile agents support the system by observing and monitoring every node and CH. If the mobile agent observes some node or the CH not forwarding the data packets, then it will declare that specific node as a Blackhole node. After that, the mobile agent triggers an alert message to the CH and BS to eliminate that adverse node from the WSN. A Cluster Reputation-based

Cooperative Malicious Node Detection Removal (CRCMD and R) technique for securing a mobile ad-hoc network (MANETs) from the Blackhole attack was proposed [25]. This scheme finds an adverse node during the route setup phase. So, the information will not be transmitted through the neighbor's nodes and malicious routes. The CRCMDR extends the advance on-demand distance vector (AODV) routing protocol with supplementary features. The network consists of several clusters and every cluster has a cluster head (CH). The CH preserves three tables. These tables are called legitimacy value (LV) table, neighbor's table, and Reputation value (RV) table. The routing table of neighbor encloses the IDs of adjacent sensor nodes and the CH identity (ID). The LV table is used for storing the history account for sensor nodes. Total numbers of instances when a specific node takes part in a transmission procedure, and the ratio of successfully transmitted packets to the all packets transmitted. This supports the calculation of LV for a node and this legitimacy value decides the honesty of nodes. Fundamentally, The Reputation Value (RV) table provisions the reputation value of nodes. The RV is counted by adding an extra cluster head identity (CH-ID) field to route request (RREQ) packet, and this additional field also preserve the ID of the source node with CH-ID. Correspondingly, the route reply (RREP) packet is also adapted to the supplementary modification. RREP field in the CH-ID stores the node ID of the replying node, the node ID of the node next to the replying node, and source to destination prime product number (PPN) value of all nodes. The nodes with the maximum RV are considered as able for the transmission of the data packets. So in the RV table, the standing of the nodes must be greater than the threshold reputation value. As we know, in

the discovery for route process, the source node generates and broadcasts a RREQ packet for the safe and shortest path from source to the destination. Then the other nodes in response compile their route reply (RREP) packets, which contains the node ID with the prime product (PP) and their CH-IDs. The source node then divides the PP by the number of all nodes from the source node to the destination node. And If the given PPN is dividable by the number of entire nodes in the entire route, then the node is considered as partially trusted (PT) node. The source node then sends mock packets to that node. If the route replying node is in the same CH, then the CH moves into the unrestrained mode and computes the RV for the node. If the source node and the responding node are not in the same Cluster, the CH of the source node generates the encrypted info to the CH of intermediate node (IN). The encrypted info is then sent via a reliable route. The CH of IN go in the unrestrained mode, then computes the LV of IN, and then the next node triggers the algorithms for detection and elimination of the Blackhole nodes. A scheme with the help of an intrusion detection system (IDS) proposed to detect and prevent the network from Blackhole attack by identifying the adverse nodes by using the network simulator (NS2). The Tool command language (TCL) is used to observe the complete functionalities of a network. The TCL creates three diverse files. The network animator (NAM) files, trace files, and the terminal files. The path followed by the packet and the status of the packet are included in the terminal files [26]. The NetAnim (NAM) is the simulation tool for NS2 and is used for the visual demonstration of the nodes and their data packets flow. Trace file contains the traces of the received, sent, and lost packets with time and other details

in the network. In the anticipated system, a general WSN contains several nodes. A malevolent node is then inserted into the network to manipulate the determined traffic by promoting the shortest path to destinations. An IDS is mounted on each node in the network to observe its behavior. Every node has an exclusive identity. So when a node repetitively fails to forward the received data packets to the destination paths. The IDS considers that specific node as an adverse node by awaring the BS about it. After that, the base station eliminates that distrustful node from the network. The Blackhole attack detection scheme using response data packets and their validation was suggested for WSN. A particular WSN has several clusters and every cluster includes a coordinator and member sensor nodes. The selection of a node for the position of Cluster Head or Cluster Coordinator (CH or CC) is elected on the standard of efficiency. So The node having the highest efficiency is selected as the CC. The CC bears the responsibility to detect the Blackhole nodes and save the identities (IDs) of all neighbors and intermediate sensor nodes. The CC transmits the authentication validation packets by adding an additional bit to it, which represents the packet as a validation packet for the network by specifying the exclusive IDs of the neighbor nodes. The network nodes then send the response packets for the validation packet as an acknowledgment. These acknowledgment packets include the IDs of neighbor nodes and the acknowledgment (ACK) field. The CC accumulates the data from the member nodes via immediate neighbors. A threshold time or average packet time is considered for collecting data packets. And, If the CC does not get a data packet from the specific immediate neighbors within the threshold time, then the node or nodes is declared as a Blackhole and

ultimately eliminated from the WSN and the cluster are regenerated [27]. An active detection routing (ADR) protocol-based scheme offered to detect the wicked routes [28]. The ADR protocol works to reveal the intruders. The Routing protocols appeal the malicious ID for attacking the route when data packets are absent. Such distrustful routes fail their reliance and should be excluded in the future. Correspondingly, the confidence value of the effective route will be increased. The network nodes with maximum confidence value and adjacent to the sink node will support data transmission. In case, if this type of node is absent, a report back to the higher node is generated that the destination is not accessible. Then another node with high confidence value will be selected for data transmission. Another interesting scheme to mitigate the denial of services (DoS) attacks in WSN was proposed [29]. The scheme was constructed on a population-based search algorithm named The Honey Bee algorithm. This algorithm involves the food-seeking behavior of honey bee colonies. There are multiple Employed Bees, Scouts, and Onlookers. The Scouts are accountable for an optimum exploration of fresh flowers. The Onlookers are actually spectators or observers and have the right to make choice about whether the food source is selected or rejected. The Employed Bees then take food from the source. So by using that model with the help of a reverse tracing technique (RTT), a detection scheme for DoS attack is introduced in this scheme. Firstly, A node transmits a route request (RREQ) packet to all of its neighbors. If the neighbor node reply to the packet, then it will send data packets, otherwise it will consider the node as a blackhole node. Each sender will follow the procedure. So The nodes in the network transmit their data packets via their neighbors. A Hierarchi-

cal Trust-Based Blackhole Detection (HTB-BHD) scheme was suggested to secure Smart Grid stations in Wireless Sensor Networks [30]. Usually, The WSNs are divided into multiple divisions, and each division posses a CH node. The CH is selected on the basis of the weighted selection algorithm for the CH. CH collects the data packets and forward those towards the sink node. A data aggregation model operates to eliminate the chances of replication, additional energy consumption, and network overhead concerns. A hierarchical trust evaluation model is applied to discriminate normal nodes from malicious nodes. This model also supports the CH to decide that a node is legitimate or not. The CH bears the responsibility for the maintenance of the history of dropped packets. A threshold is set for dropped packets, and if the ratio of the drop packets exceeds that threshold. Then the clusters are regenerated as a refresh function. An interesting mechanism constructed on a game theory-based security model and potential threat messages (PTM) [31]. A game theory model (GTM) consisted of two players which are playing for their particular interests. In the suggested scheme, legitimate nodes and illegitimate nodes play a game but with dissimilar objectives. The idea behind Potential Threats (PT) messages supports to identify the malevolent nodes. Fundamentally, these potential threat messages aid the network nodes to decide a connection with a particular node or terminate a connection with a node. In the commencement phase of the network, an average delay time (DT) or a threshold for legal nodes is defined. In the primary stage, the time consumed by a network node for transmitting a message is noted. If the time exceeds the threshold, PT messages will be propagated into the network. The node participation in the network and PT associated with

the particular node identities (IDs) are observed in the second phase. If the difference of transmitting a message and PT against it is more than the set threshold, then a link will be established with the requesting node, and if it is less than the threshold the request will be rejected. An additional possibility of game theory is its use to facilitate the legitimate entities to collaborate or terminate the link with other entities. In this specific approach, the legitimate and malevolent entities implement similar strategies except for the malevolent attacks and legitimate node defends.

Another methodology based on the Hybrid Trust-Based (HTB) powered with an Intrusion Detection System (IDS) [32]. The Base station (BS) bears the administration responsibility of cluster heads (CHs) and other member nodes of relevant clusters. The BS assigns exclusive IDs to the network members, the authentication keys which nodes share with each other and prime trust values (TV). The WSN is generally distributed into the three-layered model. The sensor nodes, the clusters of the sensor nodes, and a base station (BS). The described identities exchange control packets (CP) for the effective performance of the network. The CPs support the BS to chose a CH if the existing CH fails to cope with queries. And If a sensor node discovers that its CH as a malevolent, the node will trigger a CP straight to the BS via a defined substitute path. The CP is comprised of sensor node IDs and associated trust values (TV) of member nodes, and cluster heads identity (CH-ID). If a sensor node links with BS directly then CP encloses CH-ID and trust value of that CH. Each node has the responsibility to compute the TV of its CH and immediate neighbor nodes. The trust values (TV) or Reputation values (RV) are kept in a Function Reputation table (FRT). The

FRT is then broadcasted into the WSN. Actually, each sensor node observes its immediate neighbor nodes and computes their FRT. The computed values in FRT are comprised of this sensed information.

- Data sensed by each node
- Forwarding of that data
- Replies of nodes
- The trust value of event reporting
- Response value to the threshold

The nodes in a cluster use data forwarding (DF) feature to decide the honesty of their CH. The CH transmits the Control Packets to the BS before transmitting further information. The member sensor nodes must inspect through those CP and note their ID, and if it does not discover its own ID in the CP, then it should increase Fail Count (FC) for its CH. In other cases, the success count will be increased. There are two classes of FRTs maintained by each identity. The FRT of their own, and the FRT of the other fellow entities. The combined TV is intended by relating these two FRTs. The entities include the base station too. The sensor node can also send messages straight to the BS if they find any CH compromised by encrypting the CH-ID into their data packet. The BS then decrypts the packet, and ultimately it eliminates the CH from the network. A scheme based on Two-Tier trust management [33] to secure the WSN from the Blackhole nodes in WSN was proposed. The trust value of the nodes depends upon the data trust and communication of nodes. The CH issue the keys to the legitimate nodes. After registering the nodes successfully, the nodes are allowed to communicate in the network. The sensor nodes that are not new in the network

are assigned fresh keys when their trust value (TV) outstrips the threshold value. These TVs supports the BS to segregate illegal nodes from the honest nodes. The sensor nodes that do not take part in the communication process fail in maintaining their trust level, hence removed from the WSN. In the subsequent part, the CH starts to observe the entire network. The nodes communicate with their immediate neighbor by receive-acknowledged (RCV-ACK) and request-reply (REQ-REP). The malicious nodes are not capable of following this scheme. The honest nodes can receive data packets from their immediate neighbor nodes and send back the Acknowledgement. The TVs fluctuate on the basis of traffic. The nodes with the roundabout values to the threshold are assigned fresh keys and the nodes with less value are eliminated from the network. There was another scheme based on a hybrid trust-based intrusion detection system (HTB-IDS) to detect the detrimental blackhole attacks in the sensing domain was proposed [34]. This HTB-IDS scheme categorizes the security attacks by analyzing received packets and their time delay. The source node waits for a predefined threshold time after broadcasting the RREQ packet in the network, and the member nodes must send back RREP before the threshold. If it does not happen, the failed node is considered as the Blackhole node. The Source node then aware the entire network by triggering an alert message to avoid the malicious node. Another approach focusing on the role of cluster head was suggested to secure WSN from the Blackhole attack. The CH is the key and easy target for an attacker to capture because by compromising this entity the attacker can manipulate a complete segment of the network. If the CH gets compromised, a significant damage can be implemented to the aggregation of the network. This

approach specifically concentrated on mitigating a blackhole attack in the clustered WSN. The sensor node follow the Low-energy adaptive clustering hierarchy (LEACH) protocol for the selection of their cluster heads (CH) [35]. The CH is designated on the basis of energy and the distance of the node from the base station (BS). In a unique case, if multiple nodes posses same energy value, then the distance from base station decides the CH. This process is repeated after a fixed amount of time to select the CH again. The BS has the responsibility to overlook and observe the energy levels of the elected CHs. If the selected CH presents the same energy level twice or seamless fluctuations in energy level, then it is considered as malicious CH. The BS then triggers an alert message in the network about the adverse CH.

A scheme for detection and prevention of Blackhole attacks in mobile ad-hoc networks (MANETs) was proposed, which uses a comprehensive extended data routing information (EDRI) approach The EDRI methodology is fundamentally an updated form of the data routing information (DRI) methodology [36]. The extended data routing information (EDRI) table includes the source node IDs, neighbor nodes IDs, source node to destination node path and BH node record. There are several pieces of information included in the ID field. • Neighbor ID

- FROM (source)
- TO (destination)
- BHN (Blackhole node)

There are binary numbers used to specify if the node is honest node or dishonest node. If a malevolent node is discovered, the value in BHN field is changed from 0 to 1. All nodes try to maintain their peculiar EDRI

table. The EDRI approach is also powered with control packets (CP). The CP has the ID of source node, IDs of neighbor nodes and random number (RN) security value. This RN is persistent all over the data path. The data CP can not be transmitted by the adverse nodes so it works for detecting single Blackhole attack but it will fail to detect the community attack when there are more than a single Blackhole attack. The suggested methodology operates in three diverse phases.

- Discovery of the route
- Scrutiny of the route
- Eliminating the cooperative Blackhole nodes

The RREQ is broadcasted to discover the shortest path. The member nodes respond with the RREP packet along with Next-Hop-Node (NHN) and EDRI tables. The Malevolent nodes may transmit their cooperative BH-ID in Next-Hop-Node (NHN) to dodge the detection mechanism. Further, If it is the trustworthy route then the node starts transmitting data packets, and if it is not a trustworthy route then the route is inspected by using the anticipated schema. The source node will use a random number generator (RNG) to produce an RN and declaring itself to the intermediate node (IN). The source node will transmit the data CP to the NHN and waits for the response. If the RN of the ACK is similar to intermediate (IN), then it updates its EDRI table entries by setting to value 1. If the response generated from the end node then it will stop the process and end the checking. If the RN is not similar, the node is considered as malevolent and an alert is sent to the source node. If the NHN is not the end node in the network then the NHN is considered IN. Then it discovers a path to INs and starts inquiry

for next-hop to IN and update EDRI table entries. Then it relates its EDRI table entries of IN with the prior one. If the FROM and TO entries of IN is 1 for the prior one, then the node is trustworthy otherwise it is malicious. If the node is malevolent then alert the entire network by telling the bad node ID. The scheme propose the iteration of the procedure until success. When network nodes know about the BH node in network, they update BHN entry value to 1 against the BH-ID and ultimately eliminate the node from the network. A scheme named smart attack detection (SAD) [37] to mitigate multiple types of denial of services (DoS) attacks in the ad-hoc sensing domain proposed by using network simulator (NS2.35). The approach is beneficial to detect four types of attacks. This approach emphasizes to detect the particular types of DoS attacks. This approach primarily detects the types of attack then it proceeds for the solution of the attack because the approach considers that the type detection is more important than the attack mitigation. The types of attacks detected are wormhole, sinkhole, Blackhole, and botnet. The botnet attack occurs when a specific node suffers overflow. Wormhole attack takes place when a specific node disrupts the neighbor nodes and when a particular node disrupts a specific node repetitively then the sinkhole attack occurred. The Identification depends upon the node axis, mobility and node number. Another Blackhole attack analysis approach on the advance on-demand vehicular (AODV) network routing protocol proposed. The study observes the harm of the Blackhole attack on the AODV protocol performance. The Blackhole attack affects the performance of the network cumulatively because the end to end packet delay increases infecting the throughput of the network. This study uses the network simula-

tor 3.25 for their simulation [38]. In another approach studying the Blackhole attack and focusing on secure data transmission (SDT) with a presumption that routes have already formed from sources to destination. This approach presents a scheme that is constructed on an ad-hoc on-demand multipath distance vector (AOMDV) routing protocol to learn active routes for data transmission [39].

The analysis of the safety and security of the AOMDV routing protocol is done in the scheme. The AOMDV is a multi-path extension to the AODV routing protocol against detrimental blackhole attacks. When the routes from a source node to the destination node are configured, then a message is fragmented into several parts and every part of the message is encrypted using the homomorphic encryption scheme in advance before the sender forwards the partial message to the end destination. Now the most important part comes, If an adversary stands in the route then it may drop the packets and perform the blackhole attack. This scheme specifically discourses the issues of the attacks in the AOMDV protocol. The scheme is not an IDS or intrusion isolation system (IIS), but we can state that it is an intrusion avoidance system (IAS) from adversaries. The key conception behind this scheme is to allocate a set of separate routes into a set of clusters several active separate routes are assigned to each cluster, where entire sets of the separate paths are associated among a sender and a receiver. A message is fragmented into several parts before transmitting, and then every fragment is encrypted by the homomorphic encryption scheme. Then, the message fragment is transmitted to each cluster in a fashion that only one encrypted fragment of the message arrives in each group, and each every node in every

group receives the same message fragment. If a transitional node drops the fragment of the message, then that fragment of the message can be carried to the destination through an alternative route. Ultimately, the receiver obtains the complete encrypted fragments of the message, then it decrypts those fragments, reassemble those, and then finds the message.

Maximum methodologies suggested for protecting WSN from Blackhole attacks use other fellow nodes for detecting the illegitimate node or involves the positioning of other supporting systems, for example, Intrusion Detection System (IDS). Those methods are costly and bear the overhead and complexity issues resulting reduction in network lifetime. Furthermore, one particular methodology is proposed mainly used to cope with a single type of attack only. This methodology [40] has planned a defending technique that easily encompasses wormhole and Blackhole attack mitigation. This is an approach consisting of multiple phases.

Phase one: The Source node gets the RREP packet after broadcasting the RREQ packet from the fellow nodes, and the middle nodes/senders keep a record for all the RREP packets for a defined time with sequence numbers.

Phase two: Then the average of the all sequence numbers is computed by the given formula S: S= (seq i + seq i+1 + seq i+2 +.....+ seq i + n) / n

The sequence number seq i is for a specific RREP and n is the total numbers of RREP packets.

Phase 3: The RREP packets with sequence number more than the value of S are declined.

Step 4: At last, the route with a value less than or equal to the value of S is chosen.

The possibility of selecting the RREP of attacker will be very low because the malicious entity generally picks the highest number to pledge that their RREP packets get chosen for transmission. We have studied many Blackhole attack mitigation techniques presented in past literature. Now, We will look into the complexities and challenges for digital investigation and forensic studies for wireless sensing domains such as WSN and IoT. We will inspect past literature discussing the issues related to this topic in investigations held in the specific domain.

The WSNs and IoT are all about sensing critical data, storing the data, and processing the data for desired operations. Hence, we have studied in the past theory, that the data which is stored, processed and cumulatively computed by renowned organizations is a substantial subject for future digital investigations and digital forensics. The digital evidence that is provided by IoT or WSNs to the forensic investigators will be far finer as comparing to what the investigation community currently possesses. Furthermore, the IoT and WSNs correspondingly propose innovative and enhanced prospects for data that is at times misused, through the development growth in the procedures of the forensic community [13]. The algorithms, methodologies, and techniques that were implemented and established were constructed on the digital forensics (DF) process model entailing the processes of collection, examination, analysis, and reporting of the digital evidence (DE). We can identify and isolate data by using these proved operations. This data is not only important for the on-going investigation process but for future investigations as well because the information has been filtered throughout an evolving cycle of extraction, collection, processing, and presentations. The DF in IoT

and WSN is challenging particularly when it approaches accuracy issues due to the intensity of data analysis. Sometimes it bears the consequences of losing the granularity of the data as systems may present different semantics. However, it has the capability to accept different formats and may possess a proprietary format. The WSNs and the IoTs produce heterogeneous data which is very challenging in the aspects of DF investigations [13]. Especially when we specifically discuss the complexities and challenges for forensic investigations in the IoT domain which possesses the snowballing volume of items of digital forensic interest. The complexities occur due to the significance of identified and collected devices, indistinct network confinements, and edge-less networks. The realm of ubiquitous computing, it is really complex and problematic to conduct DF investigations at both logical and physical levels. Data acquisition, data extraction, and analysis of the data are very challenging in UbCom.

The IoT is not only limited to a single or few computing devices like old fashioned personal computer (PC) or small local area networks(LAN) [41]. The IoT realm has increased the challenges for digital investigators. The security breach in IoT has the complexity of heterogeneity of devices, encryption of data, third party involvement and so on. The so-called "Thing" in IoT may be a pet, vehicle or a household item. With the integration of client-side forensics with cloud-native computing forensics, the development of a connection to support practical digital forensics mechanisms is possible to cope with the modern challenges. Furthermore, the idea of the internet of anything (IoA) will explode the number of devices connected to the Internet [41]. The fundamental complications regarding the extraction of

data from the IoT devices and environment are a big obstacle to the digital investigator's aptitude to yield rigorous, forensically sound and admissible DE. [42] There is a number of challenges, complexities and uncertainties are listed below.

- The uncertainty around the source of the data, the location of storing and process of retrieving
- The problems in the secure chain of custody process due to the digital data volatility and complex data transmission routes among the IoT infrastructure layers
- The application of customary DF extraction techniques is not possible to the aggregated data which is stored in the cloud
- The miscellaneous and proprietary data storage and data interchange formats decrease the granularity of data due to capacity limitations used by IoT services.

Now we are going to discuss in detail the complexities and challenges for forensic studies in WSN and the IoT. Basically, there are two main parts of the system from where we can extract the DE, the internal and external parts. The table 1 contains the details of it.

We have discussed digital forensics in the sensing domain along with challenges and complexities. There are comparatively fewer research efforts has been dedicated to the area of digital forensic of WSN and IoT. WSN does not have any methodology to establish or check the broadcast of information through the sensor nodes. The sensor nodes are independent to transfer the data to the BS, which is of great susceptibility to these systems and the collected data. An investigating study on rushing attacks concluded that the

Table 2.1: The Digital Evidence (DE) in Sensing Environments [43]

	Internal			External			
Sources of DE	Perimeter Devices	Sensor Nodes	The Network	M- Area Networks	Web-Environments	End Nodes	Cloud
Example	NAT server, AAA server, firewall, IDS, IPS	Wired and Wireless media, mobile communications GSM, sensor networks	IoTware fridges, mobile devices, smart meters, readers, tags, embedded systems	Public, Private, and Hybrid cloud systems	Web clients, web-servers, social networks	Mobile devices, sensor nodes and network	BAN, PAN, LAN
Expected Evidence	Admin Level evidence	Network, Logs	Sensor data, IP addresses, Rime number, sensor ID, SSID	Client Virtual Machines; logs	User Activity Details and Web Logs	Sensor data IP address, Rime number, sensor ID	Network Logs

increase in the number of infested entities worsens the harm of attack [44].

In another study [4], the simulated environment for MANET has been set and the simulation results for single Blackhole attack and multiple Blackhole attack in advance on-demand vehicular ad-hoc (AODV) routing protocol and optimized link state routing (OLSR) protocol is studied by using Network Simulator 3.27 (NS3). The study is based on the quest for the number of nodes and the effect of the attack on the network by the variation in the number of nodes. The impact of the attack is measured by taking into account the metrics like the end to end (E2E) delay, network overhead, packet delivery ratio or packet drop ratio (PDR), and throughput [4, 45, 46]. The IEEE 802.11ac is applied at the physical layer to imitate the real scenario. In the AODV protocol, the attacker issues a zero metric message for all destinations. In response, all nodes around the source nose route their data packets through it. A malevolent node publishes illegitimate routing information that it has the most appropriate route towards the destination and then drops the data packets. The Blackhole attack in the pro-active OLSR protocol takes place in two steps [45]. First of all, the attacker obtains a

multi-point relay (MPR) position in the network. Then it performs a link spoof attack mechanism by compromising by its all two-hop adjacency. Then in the second step, the attacker starts to drop all data and control packets, that are supposed to be transferred.

Another simulated environment study [38] for the Blackhole Attack using the NS3 network simulator held on the AODV protocol. This study focused on the mobility speed of the network nodes. The network scenarios of simulation comprised of variations in the mobility speed with the changes in the number of nodes with the varying number of malicious nodes. They incorporated their study with the Gauss Markov Mobility Model. They found that the speed of the nodes degrades the cumulative performance of the WSN. The attack did not affect the end to end delay badly. They used IEEE 802.11b. A digital investigation study [47] on the wormhole attack in wireless sensor network was presented. The investigation performed by setting the observer nodes or investigative nodes in the network. These nodes are set as in-charge in the network and spatially distributed in the network. These nodes observe the packet or datagram monitoring in the network. There are some algorithms that were suggested for the aggregation of collected digital evidence and reconstruct the potential scenario for the attacks. The observers are liable for their area of coverage only. These observer nodes make the DE and securely forward that DE which has the information regarding the monitored data packets, their routes, and the node IDs with malicious behavior. On the other side, the set of algorithms that are used by the BS in order to aggregate the info received from the observer nodes. The BS also reconstructs the scenarios of the attacks. The scheme is tested in a simulated

environment. The simulation calculates two things.

I. The communication Overhead

II. The Memory Overhead

The approach [47] successfully detects wormhole because the network in thoroughly observed and all communication between all nodes is strictly monitored. This caused network overhead to increase. There are possibilities of false negatives due to bottlenecks. MANETs are decentralized, dynamic, transitory, and anywhere settled networks composed of freely moving wireless mobile nodes, which improves scalability and time efficiency. MANETs usually applied in a mission-critical domain, such as in combat arena, disastrous areas and war games. The criticality of this application requires a sound security investigation system. This work proposes an analytical overview of launching a DDoS attack in MANET by exploring network traffic patterns to define the time of the attack. These qualities have some vulnerabilities too. Security is a key dilemma in ad hoc networks such as DDoS DoS. In another study distributed DoS attacks are inspected by NASF (Non-address spoofing flood) in MANETs [48]. Statistical investigation of flow rate information and IDS log files is used to set detection features. False Detection rate, detection ratio, and detection time are three parameters to evaluate the NASF attack. Various NASF constraints are simulated and studied with multiple degradations of network throughputs. Malicious users perform DDoS attacks to paralyze networks by simultaneous flooding illegitimate traffic from various hosts. In this way, they block out the access of legitimate hosts. Generally, the DDoS attack is initiated by one or more nodes say 'MASTER' and multiple hijacked systems called 'ZOMBIES'. They create an intense and

huge demand to exhaust the system and network resources. This work focus on flooding DDoS attacks, in which the attacker creates huge traffic to exhaust network or critical system, which results in compromised resources i.e. saturation of bandwidth. So, it will deny services to legitimate users. Network Forensics is a branch of digital forensics to identify, preserve, investigate, visualize and present digital evidence to expose illegitimate and harmful activities. In-network forensics analysis is the key to the investigation. Network forensics is all about what happened, where, when, how, who was involved, and why? The forensics process is compiled of pattern recognition, correlation fusion and network traffic disability [48]. Digital evidence usually composed of captured traffic and network device's data i.e. Configuration settings, log files and routing tables. Live network traffic is also captured as a practiced attacker may compromise or delete log files. This approach of forensics analysis of DoS traffic involves the only the network forensics. The analysis of the traffic was done with the help of an analytical model. The MANET investigations base on the digital evidence identification, preservation, analysis and presentation. There are three main questions [48, 49].

I. If there is an adversary in the traffic?

II. If this adversary causes DoS

III. The Time of the Attack?

The detection of the attack based on the detection features (DF I and DF II) which are based on the statistical analysis of flow rate info and IDS log files. The detection time, rate and false detection rate are used as metrics of performance [48].

An investigative study [50] to measure the adversity of the Blackhole attack in WANETs. The severity of the harm of the attack to a system is helpful to create good mechanisms to guard the systems from such attacks. The study set the threshold of the harm of the attack and the rate of increasing malevolent data packets to check the effectiveness of the proposed scheme. New metrics for Blackhole attack introduced. The names of the metrics are corruption routing table (CRT), compromising originator node (CON), and compromising relay node (CRN). These metrics support the measurement of the intensity of the BH attack in MANET. The CRT computes the number of malicious route entries in the table. The CRN measures the number of forwarded corrupted packets by relay nodes. The CON calculates number of despoiled packets received by the source nodes. Interestingly, they introduced a new type of the Blackhole attack the Hybrid Blackhole Attack. The hybrid Blackhole attack consisted of two variations. The simulator used for the study is JiST/SWANS. The variants of attacks are independence and cooperation. They concluded by computing the above metrics that the independent variant of the hybrid attack is the most severe attack. The cooperative variant is most efficient attack.

Another study [51] investigates how the BH attack disturbs the performance of dynamic source routing (DSR) based ad-hoc networks. The Blackhole attack is studied in the DSR because it is a reactive and ON-demand protocol. There is a need to discover a route whenever a source needs to send data to a specific destination. So the reactive protocols are more prone to the BH attacks. In reactive protocols, the sources frequently inquire for routes. They used Network Simulator (NS2) for their study. They also concluded

that the throughput of the network was reduced by 32 percent, PDR reduced by 31 percent, and the end to end delay was reduced by 78 percent.

The Jamming attack is a notable type of denial of service (DoS) attacks in computer and wireless networks that can easily be conceded out. In the Jamming attack, a malicious entity transmits a high-range signal in the network to disturb the normal performance of the network. In the result of a high range signal, the legitimate and intended communication in the network has interfered [54]. We have another study in the investigative domain forensically examining the Jamming attack in the sensor networks [55]. They emphasized on the location of the clogged zone and jammed nodes that damaged the network performance. They suggested a Q-learning design algorithm for the identification of the node location. The model is integrated with the Optimized Link State Routing (OLSR) protocol. The learning model is asynchronous and distributed. It is capable of identifying the location of the jamming area in run-time when the attack occurs. It is of key importance to identify the location of the jammed node in order to repair the network. They applied two different network topologies in network simulator (NS3) and performed naive and intelligent attack scenarios. The key objective behind their localization schema was the confinement of good nodes in the network which are proximate to the source of congestion or jamming area. This approach works in a distributed manner and involves an online Q-learning algorithm designed to identify a jammer and malevolent entity. The Grid topology and random topology was used for the nodes positioning.

The goal of the described scheme is to develop a digital forensic tool to identify the malicious node in the network which is jamming the area

communication. The attacker they assumed for their approach is of the congestion type attacker. The attacker plays a bombardment style attack by transmitting format compliant packets. This results in seizing the other nodes for using traffic resources. Usually, the victim nodes are the nodes that are generally adjacent to the attacker node. Specifically, the consequences of the attack on the neighbor nodes of the attacker can be classified into two approaches [55].

I. The legitimate nodes drop packets at the first two layers. The physical and MAC layers.

II. The growth in the number of control packets in the entire network. As the network keeps operating, the routing protocol must have to send more and more control packets.

The study focused on a specific single node as a victim. As a result, that node will suffer from other fellow nodes. It will face more degradation than other nodes. There are two variations as discussed above.

I. The naïve jammer to simply inserting blocker packets.

II. The clever jammer, which intelligently separates the network and sends blocker packets and manipulates the localization algorithm by sending false info.

Chapter 3

Critical Analysis

This chapter is comprised of the critical analysis of the investigative studies which have been discussed in the literature review chapter. As there is always a need to be improved so those studies lack comprehension some qualities and need improvement. The limitations in the past work exist which encompasses several aspects. When we look into that, we come to know that most of the techniques [4,38,44–47] generally discussed the attacks. They did not discuss briefly the concerned attacks at the node level. The behavior of the nodes was not mentioned. These studies generally described the variations in the number of nodes ratio to the performance of the network. It is definitely understood that if we will increase the number of malicious nodes in the network, they will drop more and more packets. So The damage to the network will increase with the number of the nodes. As the best of our knowledge, there is no study that emphasizes the position of the malicious node in the network. It is very important to capture the most important position in the network which may lead to maximum output routes. So the

malicious node can publish the shortest route to the maximum number of nodes seeking a route to their desired destinations. In this case, they will be able to damage the network with maximum efficiency. A study [47] on the wormhole attack introduced the interesting idea of including the observer nodes in the network to overlook and monitor the nodes. The network data collection and integration is helped with some algorithms on the base station (BS). This will increase the network overhead due to the extra calculations of the data. The cost of network operation and energy consumption will also increase. Those researches were merely implementation studies on the performance of the networks except two approaches. We will briefly discuss those approaches.

The first of them is the forensic analysis of DoS attack traffic in MANETs [48]. That study is a brief analysis of the traffic in the response of the DoS but it only examines traffic by investigating IDS logs. The study was based on the non-address spoofing attack (NASF). These types of attacks are flooding attacks. Multiple nodes burst the network with the unnecessary request which seizes the intended user to use the resources. The packet dropping behavior of the node was not taken into sight. They used the network simulator GloMoSim (Global Mobile Information System Simulator). The GloMoSim is a discrete event simulator specially designed for massive and wire-line communication. Thousands of heterogeneous individual entities can be corporated by this simulator. It also supports modular simulation for the network protocol stack. But this simulator is not good enough for forensic studies in the sensing domain. Because there is no specific routing protocol exists for wireless sensor networks. There is no energy consumption model that exists

for transport layer [52]. There are also lacks energy consumption models for the internet protocol (IP) addresses support. The GloMoSim also depicts the random waypoint mobility (RWM) model. The RVM model is not suitable for all sorts of simulations. The GloMoSim is not a good simulator for the state of the art IoT or sensor networks due to the above-discussed shortcomings. The remnants of the traces of network communication are very important to conduct postmortem investigations. The study uses an analytical model for the analysis of the communication traffic data. There may be some other reasons which may disturb the performance of the network, such as bad weather. So this analytical model should be well focused and granule. While that approach introduced the detection feature I and detection feature II (DF I and DF II). The DF I is based on the statistics of the IDS log files and the DF II is based on the data flow rate information. This is a good approach like divide and conquer.

On the other hand [50], a study investigated the severity of the Blackhole in wireless ad-hoc networks by defining a threshold. The threshold is the harm intensity of the Blackhole attack on the network. There were three novel metrics measurement standards introduced named compromising relay node (CRN), compromising originator node (CON), and corruption routing table (CRT). This was a good and novel approach. There is an issue of the 'Threshold' value of the severity. This will not be beneficial in the case of selective types of the Blackhole attacks. Such as, we assume that an attacker knows about the operational infrastructure and operations of the system. And then he will deliberately keep the severity of the attack below that defined threshold, so it will not cross that threshold and the system will

never know about this. This will be extremely detrimental for the critical systems which are based on the aggregation of the data received from the network nodes. Even a little manipulation with time and type of critical data will destroy the objectives of the systems. There are three different types of metrics that are generated through different metrics. This will also increase the cost and overhead of the network. They also introduced a new type of Blackhole attack named the hybrid Blackhole attack. They did not mention that will it be beneficial for the conventional Blackhole attack and its other type? On the other hand, they used the simulator JiST/SWAN based on java. This is not a more realistic simulator because Java has some defense regulations and due to this simulator is forbidden to be persistent in stats [53]. This simulator demands a perfect idea of a queuing algorithm.

The forensic study of jammer attack [55] in the wireless network was an interesting addition in this domain. The network topologies were applied by using network simulator 3, which is one of the best network simulators. They have used a good approach of dividing the attack into two bases. The naïve based and intelligent based. The approach of the algorithm was distributed and scattering which made it easy to locate the culprit node. The Q-learning operates locally at every node, and every node must know the network figures for that one and one-hop neighbors. On the other side, the localization Q-learning is asynchronous. This algorithm can converge if some data is missing. Even it can converge the old data which is not obsolete. Apart from the approach, the procedure seems complex so this could cause some overhead.

Chapter 4

Research Methodology

This chapter includes the approaches and workflow of the research carried out for this document. There are multiple research approaches being used to conduct research in academia and industry. Generally, this research work is the hybrid type, multiple methodologies have been adopted while conducting this research. We will briefly discuss the methodology in upcoming sections in this chapter. This will include the topic hunting, identifying the problem, the observations, and evaluating our ideas to the problem.

4.1 Introduction

The research is the thirst or quest of information particular to the area under consideration. We can precisely state that it is a scientific procedure to discover novel information and facts [56]. Whenever a problem needs a solution, then questions arise. These questions need answers to construct the appropriate solution for that problem. This is called research. Clifford

Woody defined research as the progression in the defining and redefining the acknowledged problem, articulating the hypothesis and suggesting the solution to that problem, assessing the composed data, assembling suppositions, deriving results, and ultimately testing to verify the stated hypothesis [57].

4.2 Types of Research

This section will discuss the research methodologies and their applications to our research.

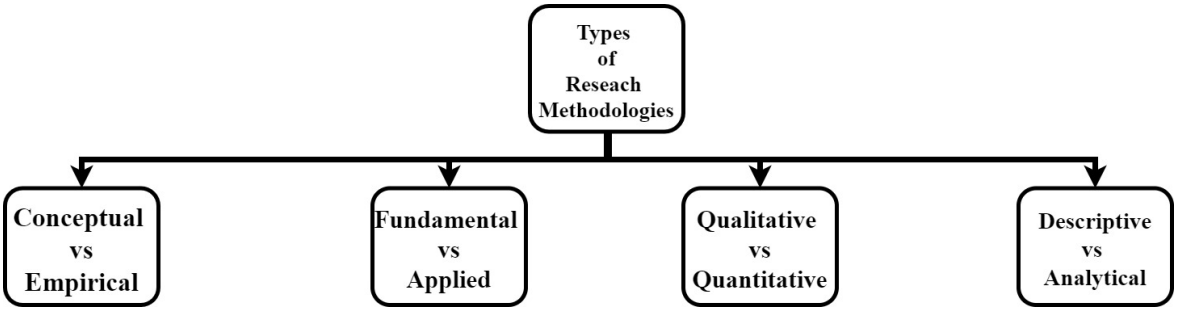

Figure 4.1: Research Methodology Types

4.2.1 The Empirical vs Conceptual Research

The Empirical Research counts on the observations and experiments deprived of trusting on any existing schemes or conceptual methods. It only depends upon the observations, experiments, and conclusions of the researchers themselves. This type of research starts from the hypothesis which is based on the facts and assessing the results. The researcher may reject or accept the hypothesis on the basis of proof. On the other side, the conceptual research

entirely depends upon the abstract ideas and the concepts introduced by the theorists [58].

4.2.2 The Quantitative Vs Qualitative Research

Computable or measurement-based research is called quantitative research. It is deployed in the domains where we can rationalize ideas to the quantity. And qualitative research is a scientific methodology of observation to collect non-computable or non-numerical data. It is based on quality. The qualitative research is mere the ideas of the people. [58]

4.2.3 The Descriptive Vs Analytical Research

The descriptive research consists of the discovery of recent work, then conducting little reviews to seek necessary and interrelated information and evidence. It is objected to describing the study about the particular domain of research that can furthermore be used in future research work. The core characteristics of descriptive research are that the researcher does not have any regulation and control over the data and recent literature. They can just find methods and proofs. While in analytical research, the researcher takes all the collected data from the reviews and perform the critical analysis and assessment to find the conclusion [58].

4.2.4 The Fundamental Vs Applied Research

Based on the depth of the knowledge required, we can divide research into applied and fundamental researches. The fundamental research aims to gather

the basic knowledge and find the preliminary info of a phenomenon. While the applied research aims to seek efficient solutions to the difficulties and problems faced by the research community and industry. There are several experiments are performed by the researcher to examine and investigate the problem to acquire in-depth knowledge of the problem domain. The performed experiments are very helpful to find solutions to the existing problems [58].

4.3 Research Methods and Research Methodology

Researchers use multiple methodologies, procedures, and techniques to conduct research. The process of applying these techniques is called research methodology. The process is incepted with reviews until we do not reach any conclusion, and this process is known as the research method [57]. Actually, research methodology is the scientific process adopted to find a solution to a specific problem. The research methodology is not the same for all types of problems. We must have to identify the problem first, and then we will have to choose the best methodology for our problem in order to find the best solution. It is extremely required that the objective of the result must be clear to adopt the methodology. In order to conduct this research, we have followed these steps.

• Exploring the wireless sensor network (WSN), Internet of things (IoT), WSN and IoT security, attacks in sensing domain, the Blackhole attack, and

the denial of services (DoS) attack.

• Exploring The Digital Forensic, The notable attacks in recent history, and Digital forensics for WSN and IoT. Exploring the challenges for the targeted domain.

• Choosing some topics for further research work in the targeted domain.

• Deriving the hypothesis from the current literature.

• Proposing a solution to the problem domain.

• Exploring the suitable tools and techniques

• Validating the hypothesis by the implementation.

4.3.1 Thesis Research Methodology

This research incorporates the hybrid approach throughout the process, which comprises conceptual, applied and fundamental researches. The steps which are followed throughout this research activity are written down.

• Defining a Research Domain

• Literature Review

• Critical Analysis

• Targeting a research topic

• Identification of problem

• Developing a Hypothesis

• Observations

• Proposing a solution

• Implementation

• Presentation

4.4 Summary

This chapter contained the research methodology introduction, types of research methodology, types of researches. The above-mentioned topics were concisely discussed and elaborated.

Chapter 5

Strategy for Forensic Analysis

This chapter includes the strategy for conducting the research and various critical and important discussion factors for the problem statement and approach. This chapter will contain the strategical primitives and their discussion. The introduction of tools and the reasons behind using those tools and techniques will be discussed in upcoming section.

5.1 Approach of the Research

The solution strategy for the problem statement is consisted of step by step approach. The figure below demonstrates the flow of the research.

We started from the first step of studying the past literature of our research interest. Then we chose an attack-type to investigate in our research. We chose the Blackhole attack due to its detrimental damages to the cyber world. Then we formulated a strategy for the next phases of the research. We simulated a wireless sensor network in NS3 and performed a Blackhole

Figure 5.1: Research Strategy

attack by random and selected nodes. The simulation runs for a fixed defined time and stops after it. The nodes are clear and the representation of the animation depicts the bad nodes dropping the packets by a red line. The traces and the pcap files are collected after the attack.

The detailed strategy for the research is given above in figure 5.2. Before starting the further work we must know what kind of digital evidence will help us to pursue our study and get beneficial outcomes. So the first step in the strategy is the identification of digital evidence. We can search it

from the past literature that what type of evidence the network and devices would generate. The second step contains the process of the simulation of the attack. In this step, a WSN containing the multiple numbers of nodes is created in NS3. The malicious nodes are defined and then the simulation is run. When the simulation is stopped on defined time. The protocols for the routing of the network nodes are defined. Then the traces and artifacts of the network are collected from defined locations. The evidences contains the extensions like .tr, .pcap. We can conduct a comprehensive node by node analysis of the network. The important question may be of this type.

I. Which node behaved maliciously?

II. What type of malicious behavior was observed?

III. What is the number of malicious nodes in the Network?

IV. What type of damage they are causing to the network?

The nodes can be analyzed by the NS3 PyViz, NetAnim, and tracemetrics tools. We can also inspect the flow monitor of the NS3.

The number of nodes may be so large that it may not be feasible in terms of time and space to analyze all nodes for forensic analysis. So it will be good to analyze some of the nodes on the basis of the packet drop ratio. This will be briefly discussed in the analysis section of .

5.2 Simulation

In the past fifty years, there has been a ground-breaking advance and development due to the astonishing growth of the use of digital computers and devices. The era of information technology revolution has exponentially ac-

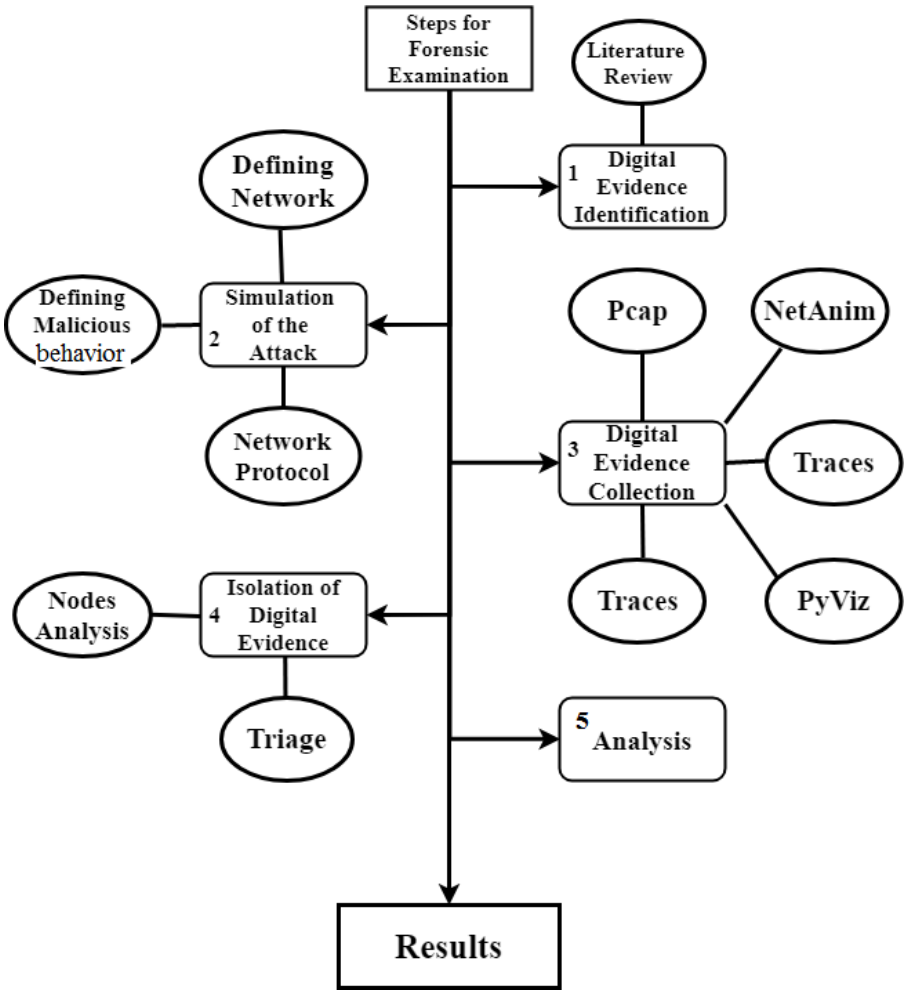

Figure 5.2: Workflow of Research Strategy

celerated the advancement of every domain. It is estimated that the 'think' power of a single computer device will surpass the combined human brain-power on the earth in the upcoming 30 years. The growth in digital sciences has influenced almost all branches of sciences, in fact, it boosted up the research pace of every science. The growth in computing kingdom resulted in using simulation and modeling in it. The emergence and widespread availability of computing power and resources resulted in the exploration of the

new heights of experimentation for innovative, enhanced and improved solutions [58].

5.2.1 Why we use Simulation?

In several conditions and circumstances, experimentation is not affordable because working with real objects and media, it is unaffordable, dangerous, or even impossible to build, modifying, and even demolish systems. The simulation is a risk-free life, as we can make mistakes, go back and forth in time, undo actions, and start over again. An on the other side experimenting with the real-world is disruptive, irretrievable, costly, time and resource consuming, unethical, and in some cases impossible..

5.2.2 Simulation Domains

The complicated models and their simulations are very significant for this purpose. We have a wide and significant problem range encompassing computational methods, conceptual models, uncertainty and fidelity issues, conventional and cutting-edge paradigms and re-usability for the solution range all over the industries and institutions such as cyber-security, smart cities, agriculture and so on [60]. The Simulation is used for the training, study, and exploration of complex and large-scale systems. It is the finest and safe approach to get understanding and comprehension over the operation of existing and prevailing systems without disturbing and troubling the actual systems. We can test novel ideas and concepts for the systems before implementation in real-time. The prediction of the future behavior of the

conceptual systems is performed by simulation before investing a large number of resources. The simulation aids critical decision making by analyzing, and solving complex problems. We can easily state that it is the branch of science and mastery over experience.

5.2.3 Objectives of Simulation

The main objective of the simulation is to find the answers to questions in all domains of life. In the descriptive aspect, we can use it to understand how a system works, and in the perspective aspect, we can use it to compare different alternatives [59]. We can use it to evaluate the proposed system and the existing system to analyze the correctness and performance of a system. There are several objectives behind simulating an environment such as uncertainty reduction, acquiring the knowledge of the system, procurement decisions, education, research, training, sensitivity analysis, safety assessment, risk assessment, forecasting, prediction, alternative choices, prototyping, designing, and evaluations of decision.

5.2.4 Network Simulation

In the computer networks domain, the network simulation is a method in which software analyzes the performance and comportment of a network by calculating the links and association between several network nodes and entities. A typical network simulator real-time animations, visualization, packet flow, efficiency, scalability, performance, cost efficiency to design a network. There are generally two categories of simulators available in aspects

of purchases, the commercial and open-source simulators [61]. Simulation tools have a vigorous role in real-world implementation of the ideas because practically hardware implementation of network topologies in real-life and on real environment is extremely costly and even impossible to modify. The simulators are the prototypes of actual systems.

5.3 Simulation for Forensic Studies

Simulation at several stages of fidelity has been used in research, training, and education for several years. The use of simulation in the domain of information technology and computer science education plays a vital role in order to produce a well-trained investigator. The DF education is a span that includes the secure forensically seizure of digital evidence (DE), digital memory and device imaging, the examination of the DE and images, presentation and acting as an expert witness in court. Several of these activities are appropriate for simulation-based research and education. Multiple universities teach digital forensics to their students by simulation, i.e. the University of Portsmouth. This generally includes constructing a situation where a computing device is seized and imaged. Numerous universities nowadays have 'forensic houses' which are simulated crime scenes [62]. Almost all of the the research studies and investigation which were discussed in the literature review chapter and critical analysis chapter has used network simulators for their study. The forensics analysis of jamming attacks, digital investigations of DoS attack, forensic analysis of DoS traffic data, forensic analysis of wormhole attack used the network simulators such as NS2, NS3,

MATLAB, JiST. Those studies were briefly The benefits of using simulation has been discussed in the previous section. Simulations are intended to be secure, given that many of the effects of a potentially high-stakes scenario without the fear of failure or damage. The simulation environments for the forensic investigation research and education are of two type [63].

I. Physical Simulation

II. Virtual Simulation

The universities and training institution take into account both types of environment in order to train students. Interestingly, a Microsoft research study for robust cloud forensics used a simulator. The malevolent manipulation of machine time is a severe challenge in computer forensics. It is of key importance to timely detect such manipulation and reconstructing the genuine timeline. It is usually very difficult to do this because the attacker always has an escalation ladder in his hand. Microsoft research study proposed a forensic framework by implementing it on a simulator [64]. We will use network simulator 3 (NS3) for our forensic study of blackhole attack.

5.3.1 Network Simulator 3

The Network Simulator (ns-3) is a discrete-event network simulator. It is specially designed for research and educational objectives. It provides animation for the packet flow. NS3 is executed in C++ with discrete python scripting. It also has a special feature of emulation for the integration with real networks [65]. It is a flexible simulator. It is the best simulator in aspects of comparison with real-time hardware because of its realistic environment

with organized source code. The basic architecture of NS3 is given in the below figure.

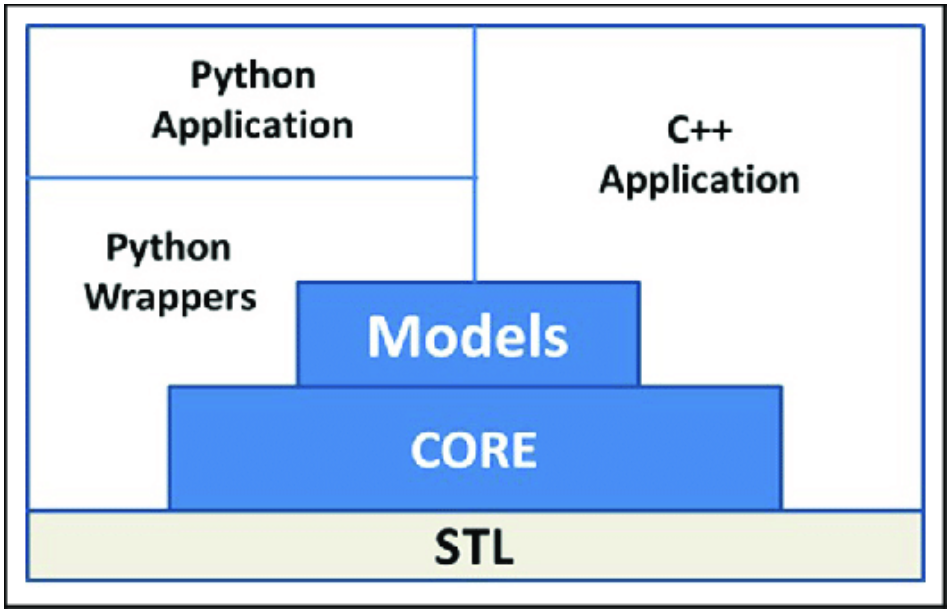

Figure 5.3: Basic architecture of NS3 [65]

5.3.2 NS3 Insight

NS3 is objected to provide enhanced support by the modularity of the components, integration and reuse of utilities, emulations, scalability of simulations, tracing, statistics, and validation. NS3 runs on UNIX and LINUX based OS. NS3 is particularly focused on modern IPv4 and IPv6 networks, as well as non-IP infrastructures and architectures. NS3 supports for the construction of virtual networks (VN) and network emulation. It also facilitates for topology generation, event scheduling, random variables, timers. The general composition of NS3 is given in the figure below.

There are some important facilities which will be very important for this

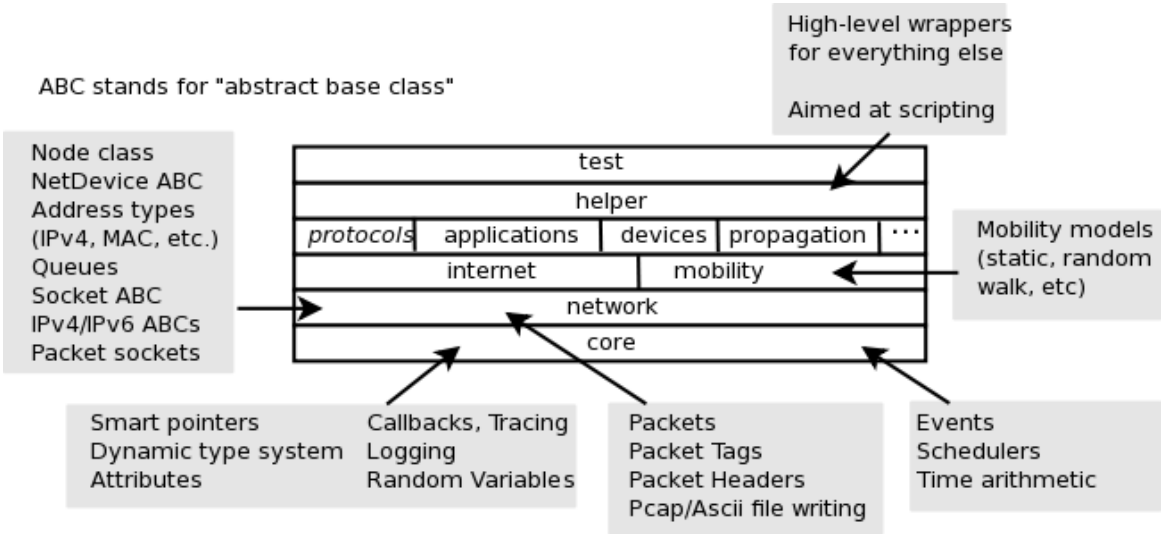

Figure 5.4: Organization of NS3 [65]

research.

- Nodes, Applications, and Channels
- The ability of the simulator to emit and consume REAL NETWORK PACKETS
- Tracing
- Logging
- Statistics

An architecture for the insight of NS3 functioning is given in the figure below.

We will briefly discuss the statistical and tracing parts in upcoming section. We will compare the remnants which we can find from real networks and from the NS3.

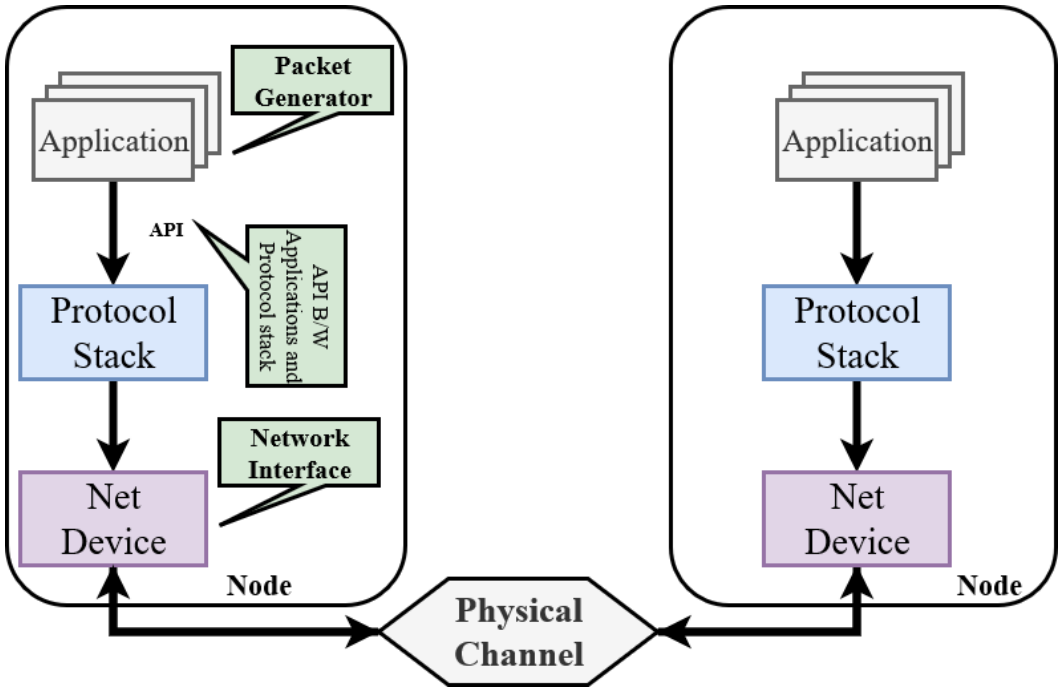

Figure 5.5: NS3 Architectural Functioning

5.3.3 NS3 Statistical Framework

This section summaries the process of data collection from the simulation and the statistical framework for ns-3. The process is very important regarding our research. This is all about the remnants and DE. The main goal of the statistical framework is to provide the functionality to record and show data and statistics for the analysis. It boosts the simulation process. It integrates with the NS3 tracing system, which we will discuss in the upcoming section. The statistical framework can be used independently without incorporating the tracing system. It helps users to create, aggregate, and analyze data over multiple trials. It reduces the network overhead when a package is not in use [66].

The core principles behind the framework are given below.

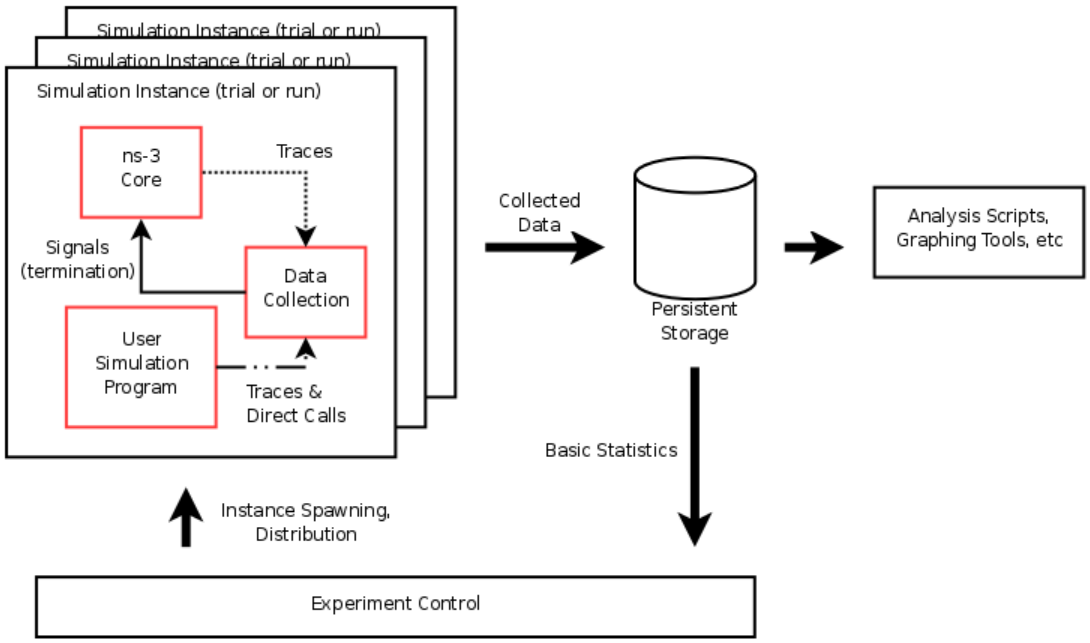

Figure 5.6: NS3 Statistical Framework Architecture [66]

• Each experimental trial is piloted by every single instance of the simulation program, whether in a serial or parallel manner.

• A script executes the instances of the simulation program in a controlled manner, varying parameters as necessary

• After this, data is composed and stored for making plots. This data will be used for analysis.

• The analysis may be performed by external scripts and helping tools

One of the key objectives of the framework is to collect data and make it accessible for further manipulation is other helping tools [66].

5.3.4 NS3 Traces

The NS3 structure contains a callback-based tactic which is called tracing. The tracing fetches tracing sources from tracing sinks and that is dedicated to flexibility for the user. Packet traces available in the libpcap format to allow for post analysis and the tools built around that trace format. We will use a tool named tracemetrics for the analysis of the traces. Built-in statistics will also be extensively available [66].

ASCII Traces

NS3 offers a helper functionality that wraps the detailed low-level tracing system to support the user with the particulars involved in configuring some easily understood packet traces. If the user enables this feature, he will see the output in an ASCII file.

5.3.5 NetAnim

NetAnim is an offline network tool for animation that now comes with the NS3 package. The NS3 network simulation is animated by NetAnim using an XML trace output file. NetAnim is much more than it is thought. The nodes position, packet flow details, flow monitoring, packet delivery can also be depicted by this tool [66].

5.3.6 Flow Monitor

The objective of the Flow Monitor module is to be responsible for a flexible system to measure the performance of the network protocols. This module

tracks the packet exchanged by nodes by triggered probes installed in the network nodes. The packets are recognized by their flow. Every flow is defined by its probe. As an example, a flow will be defined by protocol and port from source to destination nodes [66].

5.3.7 PyViz

Python Visualizer (PyViz) a simulation visualization tool of NS3. It does not use any trace files. It is a live simulation tool. It is generally used for the debugging process. It is used to figure out if the models are working appropriately. PyViz is written in python but it works for C++ and Python [66].

5.3.8 Tracemetrics

TraceMetrics is a useful tool for the trace file analysis for NS3. The main objective of this tool is to perform a rapid analysis of the trace file produced by NS3 simulations and compute useful metrics for performance measurement and research purposes [66].

5.3.9 Wireshark

Wireshark is also a network analysis tool previously named Ethereal. It captures packets in real-time and displays them in a human-readable design. Wireshark is facilitated with color codes, filters and other features that let a user to deeply analyze into network traffic and inspect transmission packets individually.

5.3.10 Gnuplot

GNUPLOT is a graph representation tool which can produce 2D and 3D plots for functions, data, and data fits. It is a command-line program supported by almost all OS platforms.

5.4 Comparison between the NS3 and Physical Prototypes of WSN

The network simulation tools address several design characteristics and propose numerous simulation abstractions to characterize and model real-life behavior. A comprehensive comparative study [67] on simulation tools examined the key open-source network simulation tools for wireless sensor networks. The study investigated that if the simulation tools produce equivalent results to the real-world networks or not. They designed two standard applications to evaluate their idea by comparing several features of WSNs. The evaluation was based on metrics such as power consumption accuracy, network throughput, packet reception rate, latency, communication media modeling, and run-time performance of the simulation. These metrics are also assessed against measurements on WSN physical models. The experiments confirmed that the network simulation tools yield equivalent outcomes from a functional aspect and have a capability to model communication singularities, while the capacity to model particulars of the execution platform considerably influences the run-time simulation performance and the power estimation accuracy.

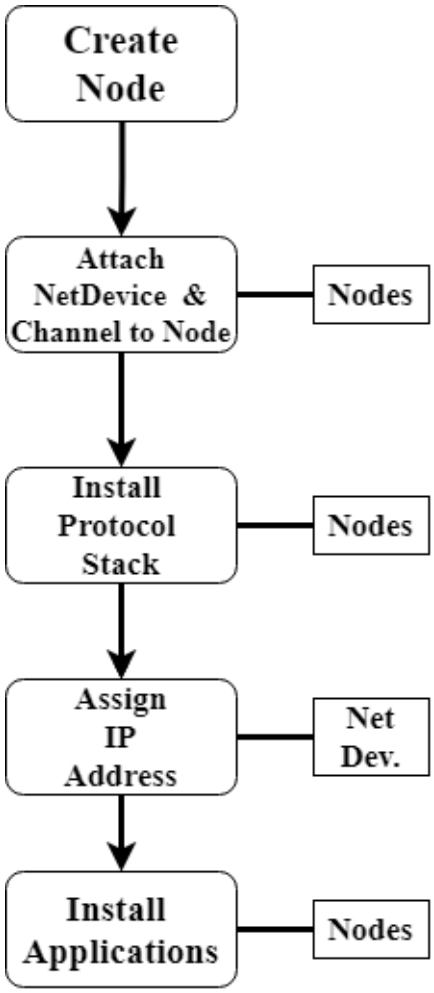

Figure 5.7: Build Topology of NS3 Networks [66]

If we look a the node or a network device definition in NS3, we come to know that the process is the same in real networks.

5.5 Network Implementation in NS3

This section contains a detailed discussion of the simulated network. We used the Ubuntu 19.04 Operating System on the 64-bit processor. We have used NS3.30 for simulation which is the newest version of NS3. A NetAnim

snapshot of our implemented network is depicted in the image given below.

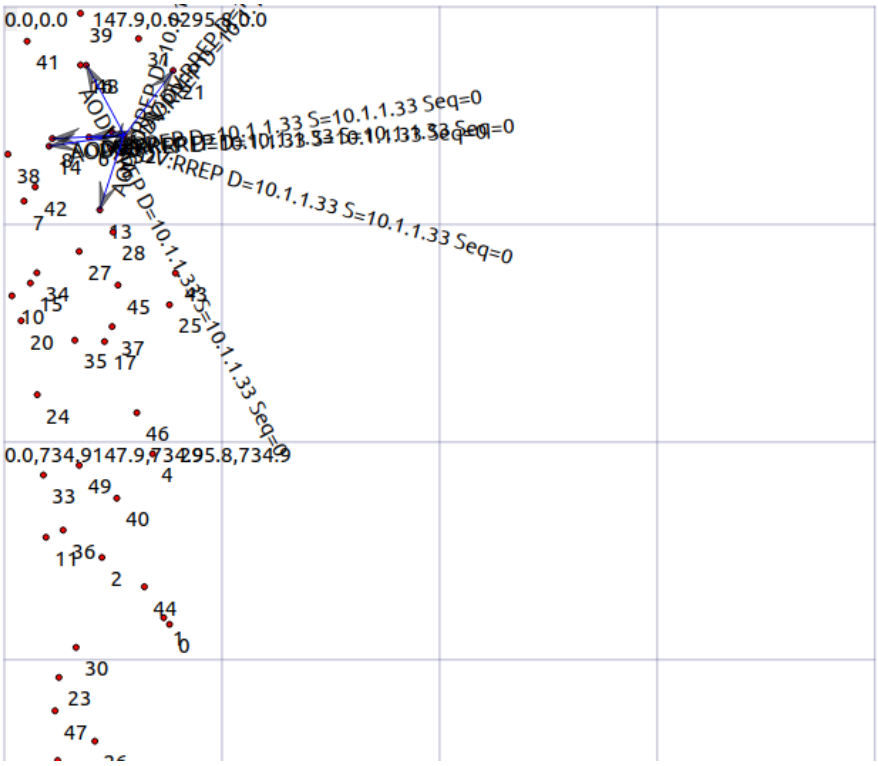

Figure 5.8: Network Animation

5.5.1 Implementation Parameters for Networks

The network is comprised of random mobile ad-hoc sensor nodes. The sensor environment uses the RandomWaypointMobilityModel class of NS3. In this class, every object opts a random destination at a random speed with a random pause time. In our network, the nodes move at a speed of20 meters per second with no pause time within a region of 300x1500 meters. The total numbers of nodes are 50 and the simulation run-time is 200 seconds, and we can increase or decrease the mobility speed and number of nodes in the network. The 802.11b wifi protocol is used. We can also change the transmit

Table 5.1: The Parameters used in the Simulation of WSN

Parameter	**Values**
Nodes	50
Sink Nodes	10
Mobility Model	RandomWayPointMobility
Position Allocator	RandomRectangularPositionAllocator
Protocol	AODV
Time	200 seconds apprx.
Loss Model	Friis Propagation Loss Model Class
MAC Protocol	IEEE 802.11b
Bits per Sec	20
Mode	Ad-Hoc Wifi
Propagation	ConstantSpeedPropagationDelay
Power	7.5 dBm
Region	300 x 1500
Wifi Rate	2 Mb per second

power of the nodes. We used and modified a GNU licensed base free file from NS3 example.

The most important thing in our implementation is that we defined the behavior of the network as random. The mobile nodes in the network adopt a random waypoint mobility model. The network starts as a normal network until almost the first 50 to 100 seconds. Then the attack starts in a random way. We defined the behavior of the attack only in our source code. We did not assign malicious behavior to any node. There is no malicious node defined by default in our network, the nodes will behave malevolently randomly and we will have to find that which node was malicious by performing an analysis of the traces by above discussed tools. This behavior of the Network and the attack will help us to follow the forensic activities thoroughly. As we do not know which specific node or flow will be going to be malicious. We will go through all the nodes and will look deeply that which node dropped the

packets.

Our Network simulation will produce different types of files for the analysis.

- A comma separated file
- A flow monitor file
- A trace File
- PCAP files for Wireshark
- An XML file for NetAnim

These traces types are briefly discussed above.

AODV

Advance on-demand distance vector routing protocol based on the Bellman-Ford distant vector algorithm and is a type of reactive routing protocols. It constructs a route to the desired destination only when it is needed. The route is maintained until needed by the source otherwise it is destroyed. In AODV every node maintains its table which stores information about the neighbors to reach destinations. AODV ensures the freshness of the routing table by sequence numbers [70].

5.5.2 Friis propagation loss model

The power level of a signal reduces as the signal traverses through the atmosphere at a rate directly proportional to the wavelength of the signal and inversely proportional to the traversed distance. In antenna theory the Friis Equation is one of the most fundamental equation. It is used to compute the

power received from antenna A when transmitted to antenna B with their respected gains. The antennas are separated by a distance R operating at frequency f with wavelength lambda.

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi d)^2 L} \quad (5.1)$$

The equation 5.1 is known as the Friis propagation loss equation. The parameters which are included in the equation are described below.

λ : wavelength (m)

d : distance (m)

L : system loss (unit-less)

P_r : reception power (W)

P_t : transmission power (W)

G_t : transmission gain (unit-less)

G_r : reception gain (unit-less)

In the implementation in NS3, The lambda λ is computed as $\frac{C}{f}$, where the constant $C = 299792458$ m/s is the speed of light in a vacuum, and f is the frequency in Hz which is user configure-able via frequency attribute.

The validity of Friis model is only proved for propagation of signal in a vacuum or free space within the so-called far field region, which is considered as an approximate region for $d > 3\lambda$. The model will still return a value for

$d < 3\lambda$, rather than creating a fatal error. So this is a true practical model for many simulation scenarios. However, we stress that the values obtained in such conditions shall not be considered realistic [69].

Chapter 6

Forensic Analysis of the Attack

The key role of this chapter is to analyze that the attack has occurred in the network. We have to analyze the traces and the traffic flows between the nodes to find the malicious nodes and root causes of the attack. We will perform postmortem analysis of the attack as well as we will perform an analysis of the performance of the four different protocols in the presence of Blackhole nodes. The AODV protocol will be analyzed under the Blackhole attack. The Number of nodes in our Network is 50. In which multiple nodes behaved maliciously but we will analyze only some of them due to the restriction of time and space. The nodes and flows for the analysis will be chosen on the basis of three filters.

I. The Maximum loss ratio of Flow ID

II. The average loss ratio of Flow ID

III. The Minimum Loss Ratio of Flow ID

The flow monitor is a powerful tool for NS3 simulation traffic flows. It works by the probes which are installed in the network nodes for the packet

tracking which are exchanged by the network nodes. Flow monitor also measures a number of parameters and it is designed by a modular approach. The network probes are of four types.

- Packet sent by the source node (SendOutgoing IPv4 and IPv6 traces)
- Packet is forwarded by a node (UnicastForward IPv4 and IPv6 traces)
- Packet received (LocalDeliver IPv4 and IPv6 traces)
- Packet dropped (Drop IPv4 and IPv6 traces)

The tracking is performed at IP level, so the retransmissions by layer 4 protocols such as TCP will be seen as a new packet. The data composed for each flow by flow monitor is given and explained below [71]:

- timeFirstTxPacket: the time when the first packet in the specific flow was transmitted.
- timeLastTxPacket: the time when the last packet in the specific flow was transmitted.
- timeFirstRxPacket: the time when the first packet in the specific flow was received by an end node.
- timeLastRxPacket: the time when the last packet in the specific flow was received
- txBytes, txPackets: the total number of transmitted bytes or packets for the specific flow
- rxBytes, rxPackets: the total number of received bytes or packets for the specific flow.
- lostPackets: total number of packets that are assumed to be lost.
- packetsDropped, bytesDropped: the number of packets and bytes lost in the flow.

• delaySum: the sum of all end-to-end delays for received packets.

• jitterSum: the sum of all end-to-end delay jitter for all received packets of the specific flow.

• timesForwarded: the number of times a packet has been reportedly forwarded.

• delayHistogram, jitterHistogram, packetSizeHistogram: histogram versions for the delay, jitter, and packet sizes, respectively.

There is also an important thing about the Flow monitor packets counting. After the simulation ends, the Flow Monitor report about the "lost" packets in the flow, i.e., packets that Flow Monitor has the missing track of. It is essential to consider that the Flow Monitor records the statistics of the packets by intercepting them at a given network level such as IP level. So the packets queued for transmission below that level are considered as lost. So the NS3 team suggests to deliberately end the simulation before the actual simulation end time. Some seconds are enough for it. We did it.

6.1 Attack on The Network

First of all, we will need to know about the workflow of the AODV protocol. As we know that the AODV is a reactive routing protocol which constructs routes on demand. This is an table driven and on-demand protocol and supports uni-casting multi-casting. Every route has a lifetime after that it expires and never used again. The AODV node routing table contains the destination IP, Dest. Sequence number with valid flag, state and routing flags, network interface, next hop, Hop-count to the destination, and life

time. In AODV, there are three types of addresses.

I. Source Address

II. Destination Address

III. Next Hop

The message set and explanation is given below.

I. Route Request (RREQ) : Route needed

II. Route Reply (RREP) : Route Replied/published

III. Rout Error (RERR) : Route demolish

IV. Hello (Link status monitoring)

The RREQ is broadcasted in the network by a node, if the nodes have a route then they reply otherwise they forward the packet. A reverse pointer is used to keep back track of the source node. When the RREQ reach the destination, then the destination node send RREP through the reverse path and the nodes update their routing table.

We have performed a Blackhole attack in the network using the AODV protocol for routing in first place. We will briefly analyze the nodes on the described standards.

Figure 6.1 represents the Blackhole attack in which malicious nodes dropping packets which are shown by the red lines dropping down to the bottom. This is the screenshot image of the python visualizer (PyViz) live animation of the attack.

Moreover, Figure 6.2 shows the screenshot of the statistics of the node 0 in the network. We can see clearly the transmitted bytes, received bytes, number of transmitted packets, and number of received packets with packet rate per second. In the black box, we can also note the details of node. In

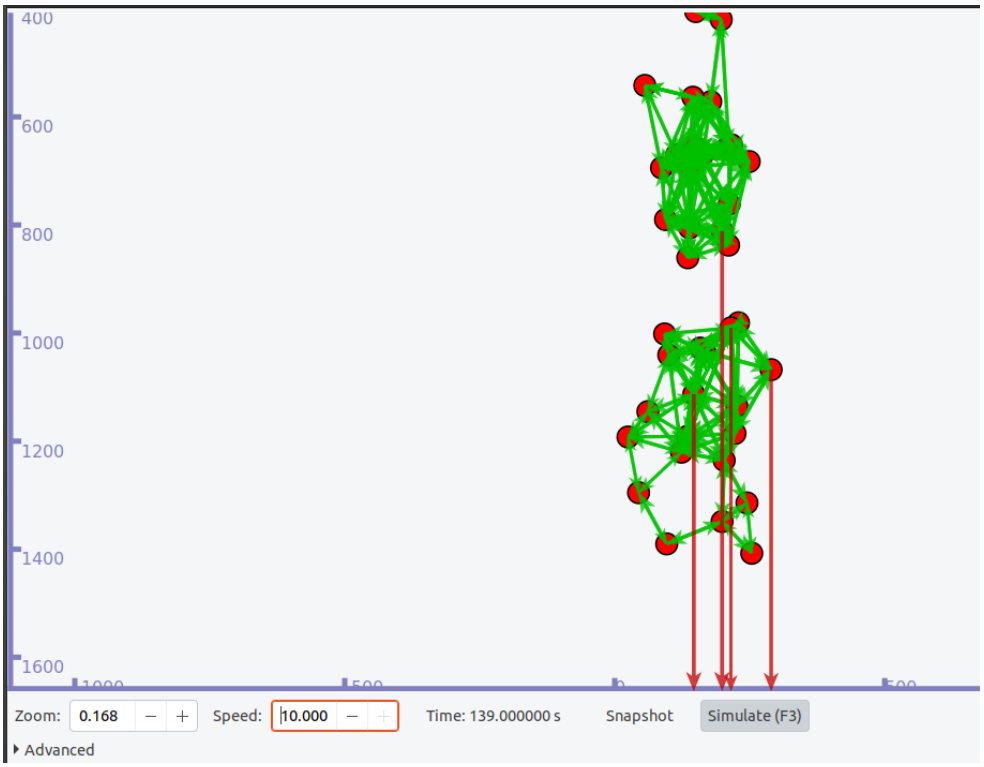

Figure 6.1: Depiction of Blackhole Attack

which the node number is shown as Node 0. The Mobility model the node is following is also shown. The type of the devices installed on the node O. There are two types of net devices on each node.

I. Wifi Device

II. Loop Back device

The IP and MAC address of the devices are also shown in image.

Figure 6.3 contains the screenshot image of the NetAnim animation. The XML file of the animation contains the traces of the Network. We will analyze the imaging of both live and post remnants of the network transmission. In the second image, we can see the nodes transmitting to their neighbors by AODV protocol.

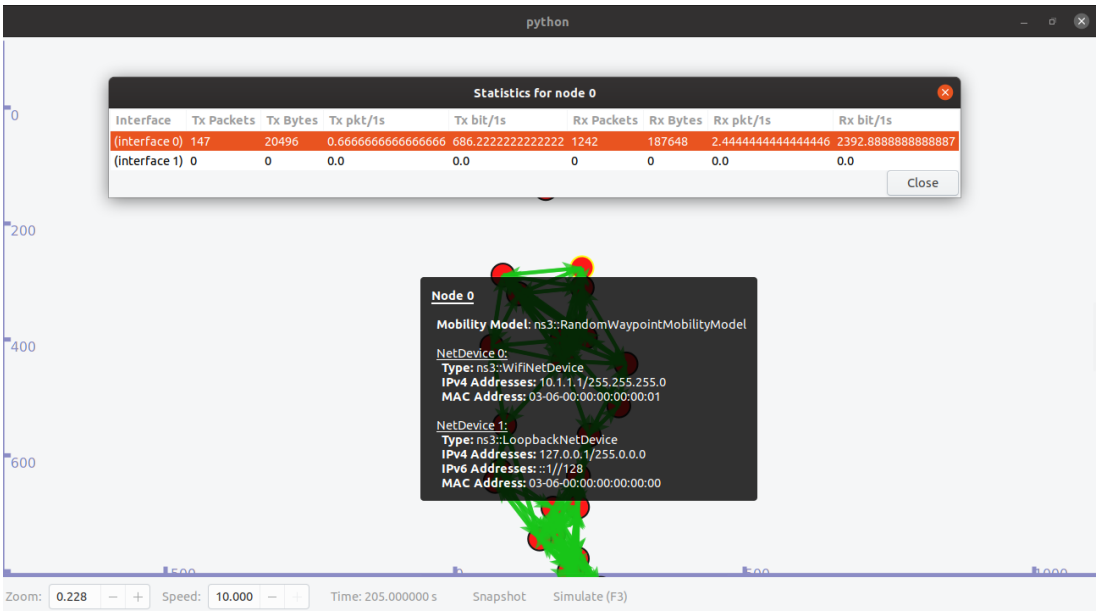

Figure 6.2: Details of the Node

AODV is a reactive routing protocol, so we have a great number of flows because the routes are constructed on demand and then they are deleted after a time limit. There are almost 950 flows in 200 simulated seconds. The images of these flows are given below. We will consider the packet loss ration of the flows. The Flow Ids 1 to 10 have packet loss ratio of 60, 68, 71, 87, 96, 30, 38, 0, 100, and 0 percent subsequently. The fluctuations in the packet losses are because nodes try to find new paths. We will analyze the flow 2, 4, 8 and 27.

6.1.1 Flow ID 2

In this flow, the packet loss ratio is 68.59 percent and it is pointed by a red line. So we can find that there is a malicious node in the route that dropped the packets in the flow. The Blue lines show the information that

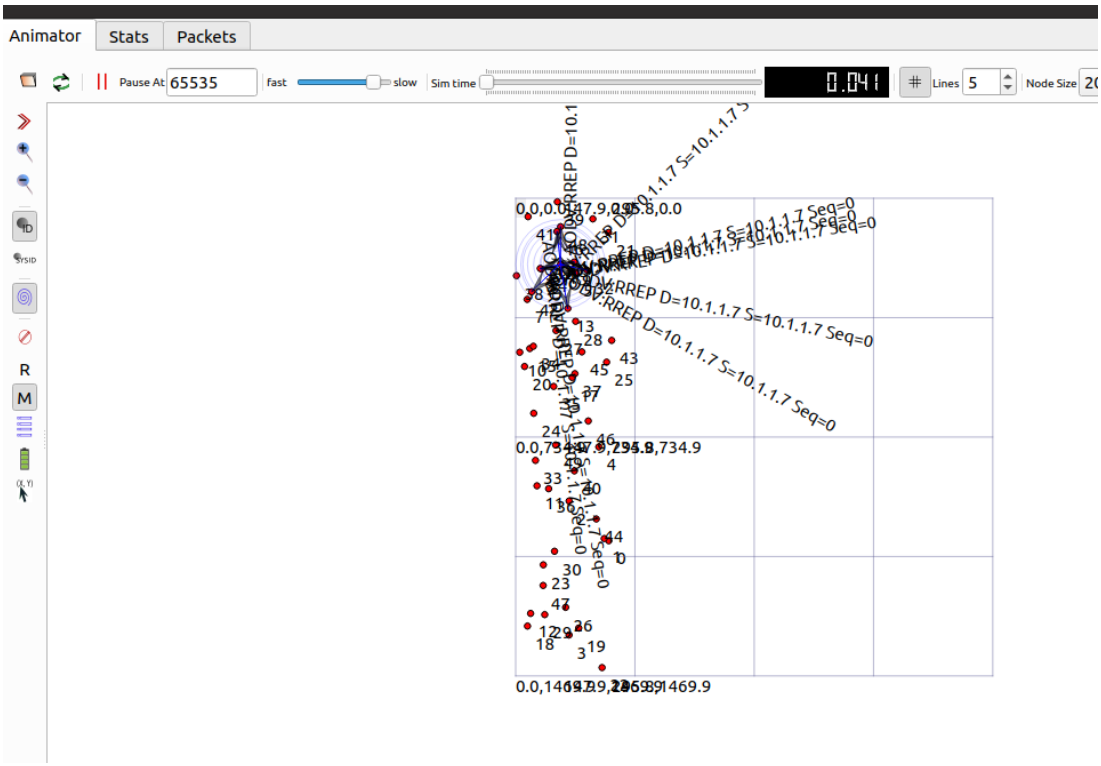

Figure 6.3: Network Animation of AODV Protocol in NetAnim

the total number of the transmitted packets is 398 and the packets received are 125. The bytes transmitted are 36616 and received are 11500. This flow is generated by using UDP from Ip Address 10.1.1.11 to the Ip Address 10.1.1.1. It means that the node number 10 to node number 0, because the node 0 have the IP address 10.1.1.1 and so on for the next nodes. The flow has a comparatively high loss ratio. There is no TTL expired so it means that the packets are dropped intentionally by a node. The Fragment time out incidents were 79 and No route incidents were 2.

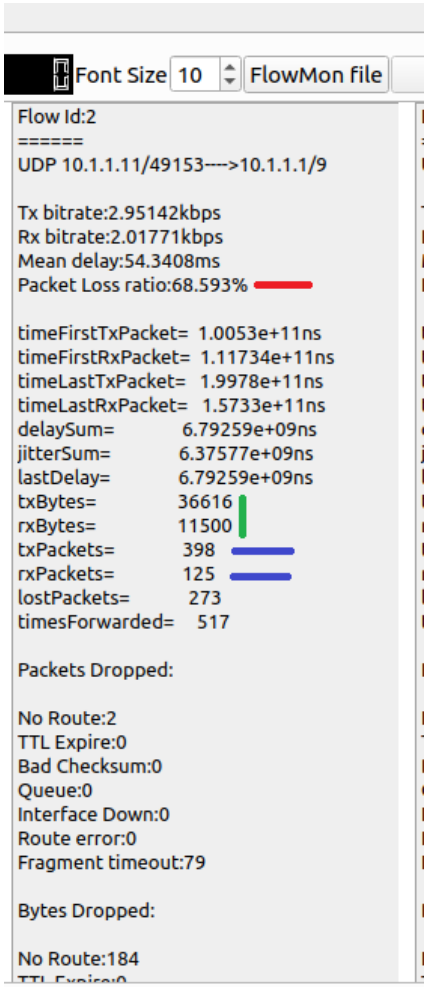

Figure 6.4: NetAnim Image of the Flow ID 2

6.1.2 Flow ID 4

In this flow, the packet loss ratio is 87.18 percent and it is pointed by a red line. So we can find that there is a malicious node in the route that dropped most of the packets in the flow. The Blue lines show the information that the total number of the transmitted packets is 398 and the packets received are 51. The bytes transmitted are 36616 and received are 4696. This flow is generated by using UDP from Ip Address 10.1.1.13 to the Ip Address 10.1.1.3.

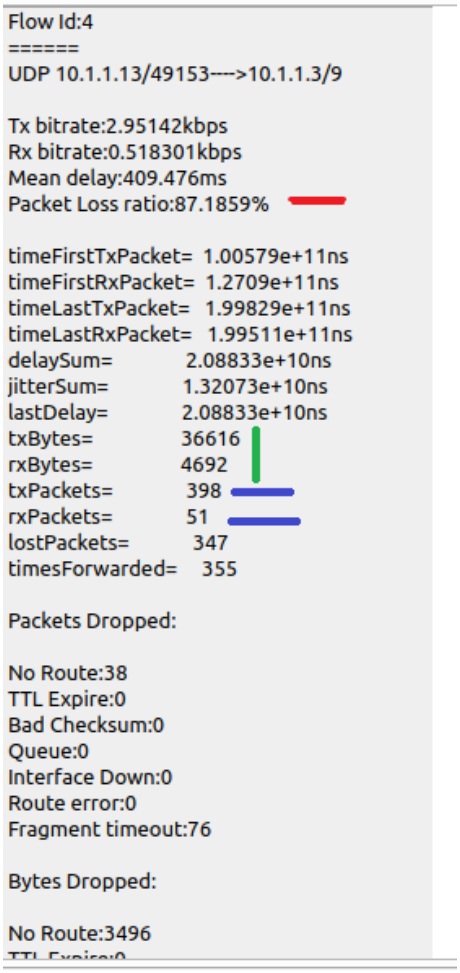

Figure 6.5: NetAnim Image of the Flow ID 4

It means that the node number 12 to node number 2, because the node 0 have the IP address 10.1.1.1 and so on for the next nodes. The flow has a comparatively very high loss ratio. There is no TTL expired so it means that the packets are dropped intentionally by a node. The Fragment time out incidents were 76 and No route incidents were 38.

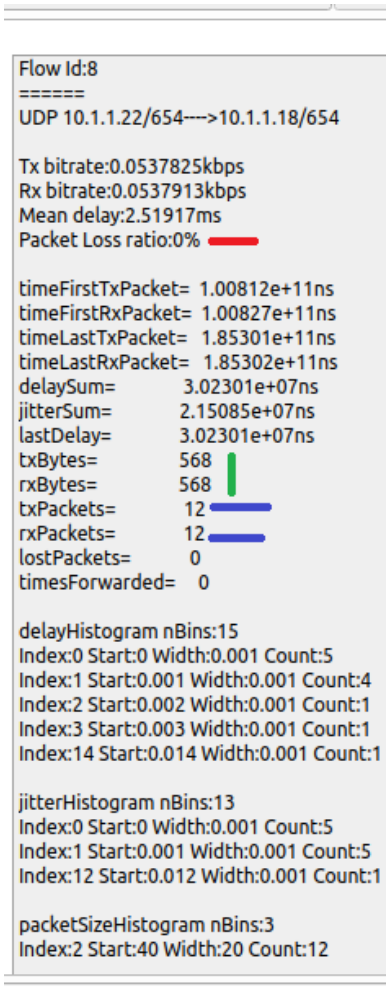

Figure 6.6: NetAnim Image of the Flow ID 8

6.1.3 Flow ID 8

In this flow, the packet loss ratio is 0 percent and it is pointed by a red line. So we can find that there is no malicious node in the route so all of the packets in the flow reached safely. The Blue lines show the information that the total number of the transmitted packets is 12 and the packets received are 12. The bytes transmitted are 568 and received are 568. This flow is generated by using UDP from Ip Address 10.1.1.22 to the Ip Address 10.1.1.18. It means

that the node number 21 to node number 17, because the node 0 have the IP address 10.1.1.1 and so on for the next nodes. The flow has no loss. This shows that the nodes between the route are honest.

6.1.4 Flow ID 27

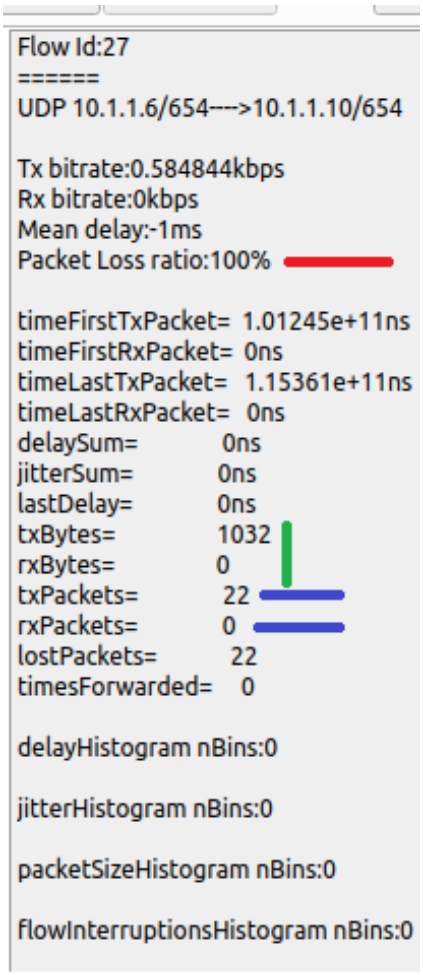

Figure 6.7: NetAnim Image of the Flow ID 27

In this flow, the packet loss ratio is 100 percent and it is pointed by a red line. So we can find that there is a extreme malicious node in the

route that dropped all of the packets in the flow. The Blue lines show the information that the total number of the transmitted packets is 22 and the packets received are 0. The bytes transmitted are 1032 and received are 0. This flow is generated by using UDP from Ip Address 10.1.1.6 to the Ip Address 10.1.1.10. It means that the node number 5 to node number 9, because the node 0 have the IP address 10.1.1.1 and so on for the next nodes. The flow has a comparatively highest loss ratio. There is no TTL expired so it means that the packets are dropped intentionally by a node.

6.1.5 Results of the Flow Monitor

AODV is a on-demand routing protocol, and when a source node constructs a route towards the destination, then it expires after a fixed amount of time. Whenever the same source node wants to communicate with the same destination then it will have to broadcast a RREQ packet again. The all process will be repeated and maybe the previous path assigned again. Although it is not always possible.

We can not discuss briefly all flow IDs one by one due to the time and space but we will analyse those flows by plotting graphs and table.

Table 6.1 contains the information of some flow IDs from ID 1 to ID 950. It was not possible to discuss each and every ID one by one, so we copied the Flow ID record of each file and created a CSV file and a table to analyze. It could take a lot of space to put a table of 950 entries so we are not putting all of them. The table contains information about some of the initial IDs and some of the final IDs. We can see that as the transmission

Table 6.1: The Flow IDs Details

Flow ID	Transmitted Packets	received Packets	lost Packets	PLR
1	399	159	240	60.150
2	398	125	273	68.593
3	398	114	284	71.357
4	398	51	347	87.186
5	398	14	384	96.482
6	398	275	123	30.905
7	397	243	154	38.791
8	12	12	0	0.000
9	14	0	14	100.000
10	6	6	0	0.000
11	2	0	2	100.000
12	7	7	0	0.000
13	7	7	0	0.000
14	2	1	1	50.000
15	29	29	0	0.000
16	5	0	5	100.000
17	12	12	0	0.000
18	8	8	0	0.000
19	3	3	0	0.000
20	1	1	0	0.000
21	13	12	1	7.692
22	20	20	0	0.000
23	397	194	203	51.134
24	396	108	288	72.727
25	396	112	284	71.717
26	4	3	1	25.000
27	22	0	22	100.000
28	15	13	2	13.333
29	1	1	0	0.000
30	1	1	0	0.000
37	7	6	1	14.286
.....				
944	4	3	1	25.000
945	1	1	0	0.000
946	5	5	0	0.000
947	1	1	0	0.000
948	1	1	0	0.000
949	2	2	0	0.000
950	3	3	0	0.000
Total	**10693**	**7621**	**3072**	**28.729**

Table 6.2: The Statistics of all Flows of the simulation

No.	Description	Outcome
1	All Transmitted Packets	10693
2	All Received Packets	7621
3	All Lost Packets	3072
4	Packet Delivery Ratio	71%
5	Packet Loss Ratio	29%
6	Delay	0.03
7	End To End Delay	19.76 sec
8	Throughput	31.49 b/s

started at a high rate. In the first 7 Flow IDs, the transmitted packets were round about 398 for each flow. After the attack started, the transmission started to decline. There are also great variations among the Packet Loss Ratio (PLR) of the Flows. We have more than a hundred flows in which the PLR is 100 percent. We have briefly discussed one of these flows above. The total number of packets traces found by flow monitor is 10693 packets from all flows. In which, the received packets are 7621 and lost packets are 3072. Our cumulative loss is about 29 percent of all flows. It means that the Blackhole nodes destroyed the routing performance of the network by 29 percent. This tells a lot about the adverse behavior of the Blackhole attack.

The second table contains the detailed cumulative details of the network flows extracted from the flow monitor file.This contains the information of All packets transmitted, received and lost in the flows, end to end delay, and throughput.

The figure above shows the statistics of all 950 flow IDs with respect to their number of packets transmission. The initial bars show that the packets transmission up-to 400 packets per flow ID. But then it declined badly.

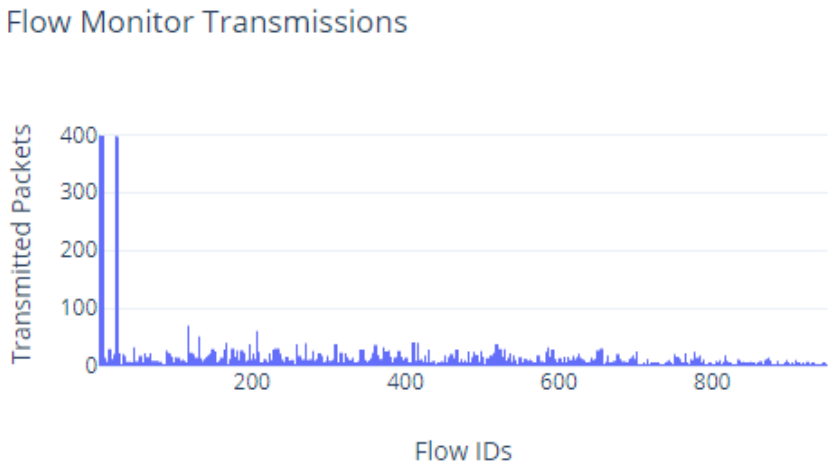

Figure 6.8: Graph of All Flow ID's Transmitted Packets

While the second figure contains the information about the received packets from all flow IDs. As proportional to the transmission, the number of received packets also declined. We can see that It kept variating throughout the process but never touched the highest again.

The third figure shows the number of lost packets. In the start, the number of packet loss was high. It almost hit 400 packets per flow at the worsen state of attack. But when the transmission packets number declined, the received packets and lost packets number also declined.

The final figure shows the packet loss ratio (PLR) of all flow IDs from ID 1 to 950. The Flow IDs on X-Axis show the losses they suffered. The line graph frequently touching the maximum. The packet loss ratio is given in percentage. We have a lot of flows in which not even a single data packet was received by the destination IP. The PLR is 100 percent repeatedly throughout the axis. From the above tables, we notice that the number of packets

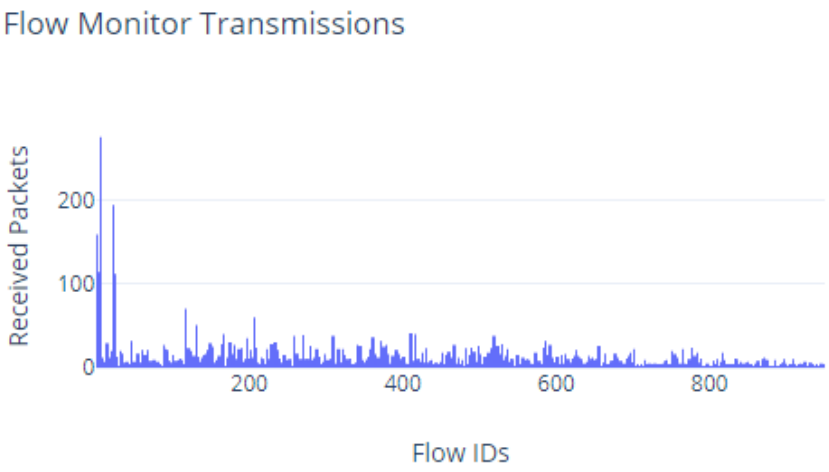

Figure 6.9: Graph of All Flow ID's Received Packets

declined when the attack started. Even the number of packets declined but the damage scale remained same till the end. In some flows the number of packet were very few, for example from 3 to 10. They were all dropped by the Blackhole nodes. So the PLR hit the hundred percent scale-point.

This reason of such harmful behaviour is that some of the specific malicious nodes were in an intermediate cluster of the nodes. Those nodes almost jammed the traffic flow of several nodes from the above and below parts of the Network.

The significant of the analysis of the Flow Monitor traces is that it focuses on the IP layer. Flow monitor tracks the packets routing in the Network. The IP level transmissions and their statistics were discussed in this section. The brief analysis of the traffic of these flow verify that the Blackhole attack is severely detrimental for the routing protocols.

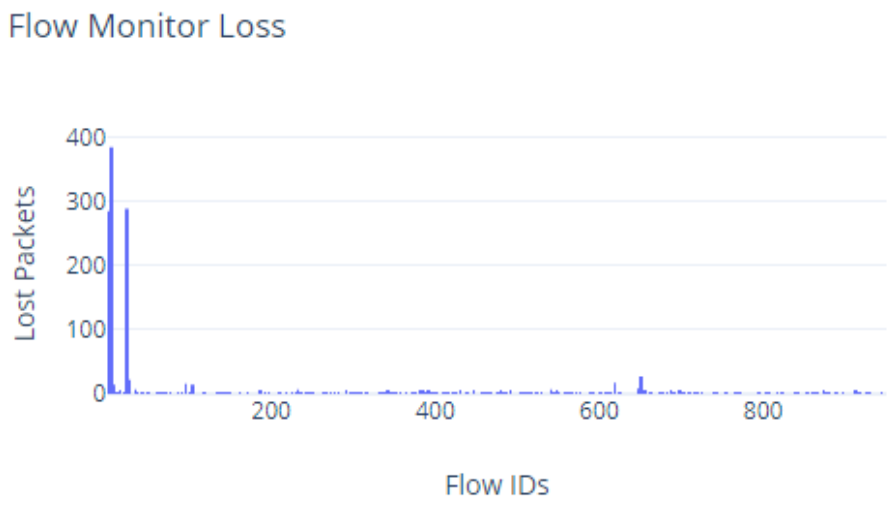

Figure 6.10: Graph of All Flow ID's Lost Packets

6.1.6 Network Animation Traces

When we run an XML file of the simulation. We find different kind of statistics. The node activities regrading concerned protocol and characteristics, data transmission, the types of data transmission. We can export a CSV file of that data to analyze further.

We extracted the graph of the UDP traffic from the animator which is given below.

The figure shows the data flow by horizontal lines and node IDs by vertical lines. The packets used the port number 654 for the transmission. The first flow is from node 35 to the node 10 on the top most. So by this figure we can see that almost all of the traffic passed through the intermediate nodes from node 15 to node 34. Second most congested area of the traffic is between node 2 to the node 10. So the blackhole nodes which extremely affected the network may be in these number of nodes.

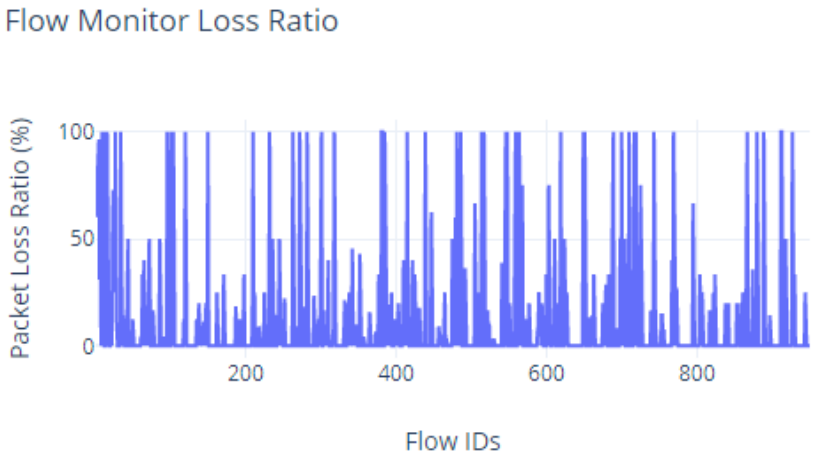

Figure 6.11: The Packets Loss Ratio (PLR) of Flow IDs

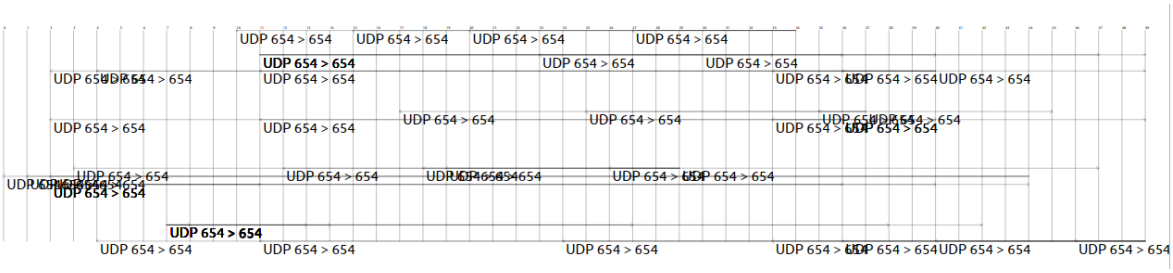

Figure 6.12: Graph of the UDP data Flows

Now we will analyze node to node UDP data transmission. The graphs contains only the data transmissions of UDP.

The graph of the data packets contains the sender nodes at Y-Axis and the UDP flows with receiver nodes at X-Axis. These flows only show the data flows which are intended from a sender to the receiver nodes.

Now we will look upon the AODV messages transmission in figure 6.14. The graph contains the transmission of only route reply packets from different nodes. Each source appends it's own address as reverse pointer for the route reply when it forwards the RREQ. The intermediate senders also appends

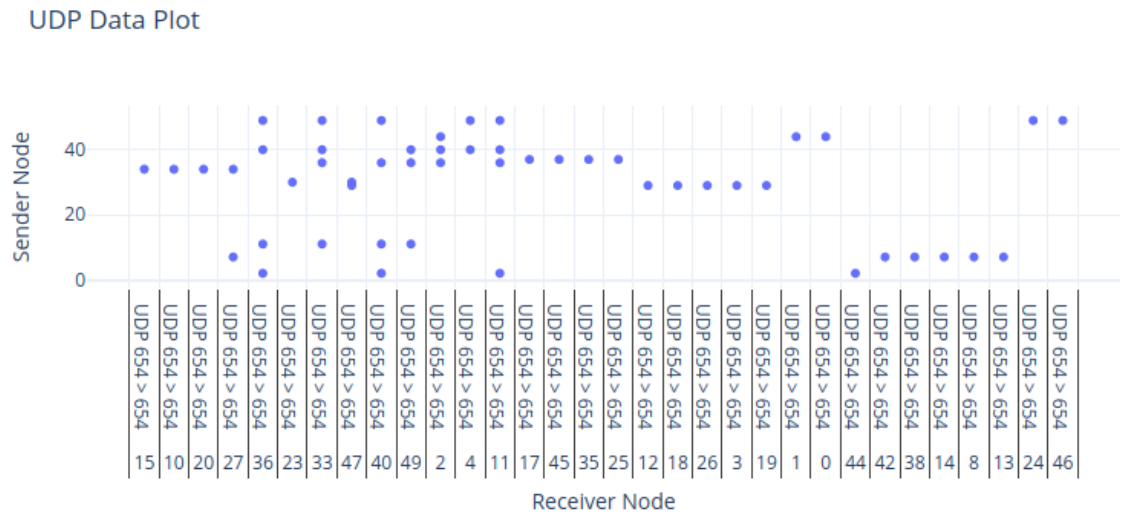

Figure 6.13: Graph of the UDP data Flows

their IP address for back-path pointer. The RREP is a uni-cast message

We can see that the RREP sender nodes with their subsequent IP address and reverse pointer on the Y-Axis with sequence numbers 0. On the X-Axis we have the receiver nodes and the time of the transmission.

The node 34 with an IP Address of 10.1.1.35 forward the RREP to the node 15 with an IP Address of 10.1.1.16. So the node by which most of the RREP packets may be the detrimental node. It also may be an honest node, but it is an important point in the forensics and network security aspect. The position of the node in the network is of key importance. As if I am an attacker, I will definitely choose a narrow position to perform attack as all data packets will pass through it.

The graph shows the overhead of routing due to the excessive control information of AODV control messages and Blackhole nodes. Due to the Blackhole attack nodes started to find newer shortest routes. So we can

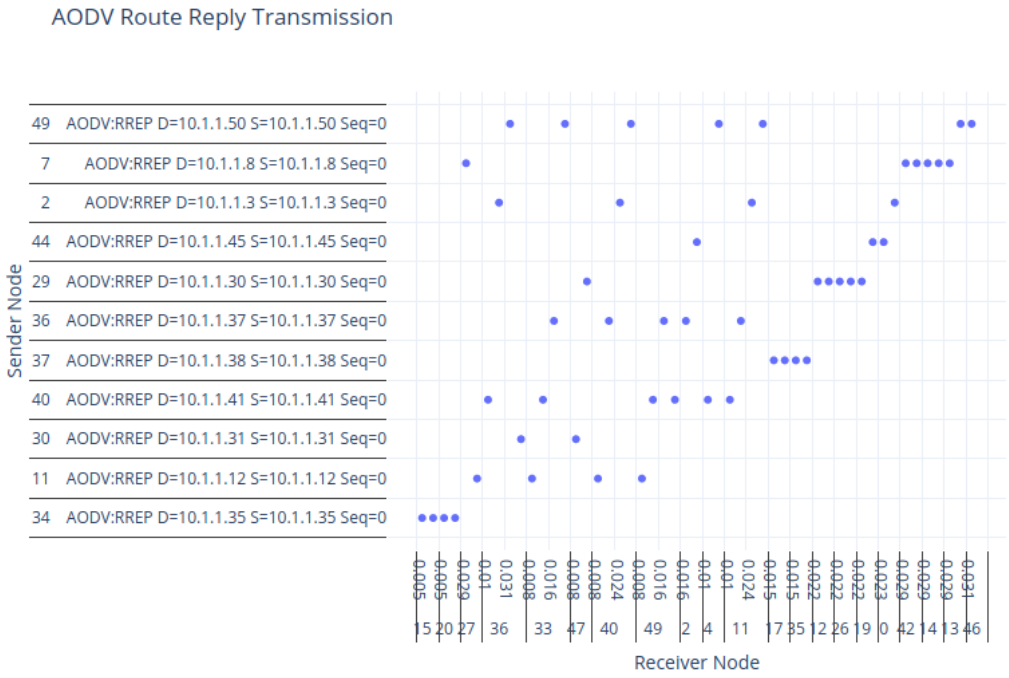

Figure 6.14: Graph of the AODV RREPs

verify that the Blackhole attack is detrimental for routing of the network.

6.1.7 PCAP Files Analysis by Wireshark

There is also an important form of digital evidence which we must go through. The captured packets files of the transmission. We will also analyze these PCAP files for specific nodes. We selected the nodes according to the Flow IDs from the flow monitor. The Flow IDs which suffered from the maximum packet loss have these nodes as their intermediate nodes or hops. So it is important to analyze these nodes. Wireshark works by putting the network interface card (NIC) into a promiscuous mode. It tells NIC to accept every packet it receives. It helps us to analyze traffic in real-time. Again due to the restriction of time and space we will only analyze some of the nodes from the

network. There are 15 to 24 nodes that remain in the middle of the network. We can not analyze all of them. There are two reasons. First of all, time and space would not allow that. The second and most important thing, the nodes have shown similar behavior. So the analysis of few nodes will also describe the behavior of other nodes.

PCAP of Node 5

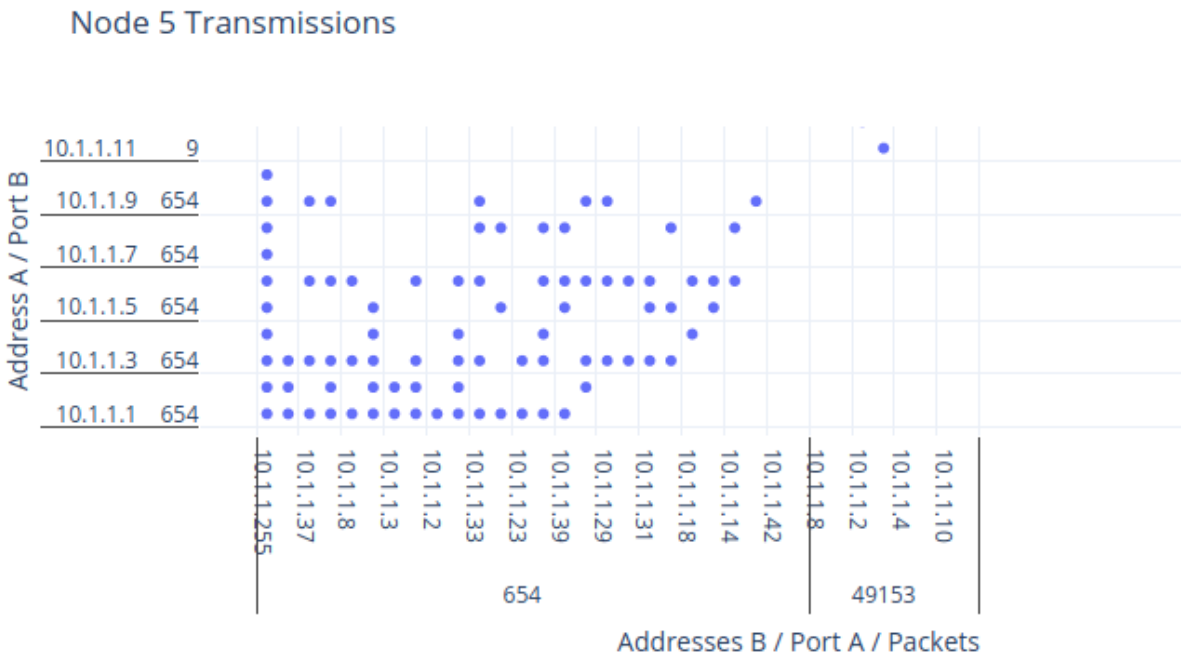

Figure 6.15: Graph of the Node 5 Conversations

In this graph we can see the packets exchanged from the ports of the node 5. The IP address of the node 5 is 10.1.1.6. Most of its conversation belongs to port 654. Some of the packets belongs to both port Addresses. The packets captured at this nodes belongs to 20 nodes including it self. The scattered points in the graph depict the enormous activity of the node in the

network.

Protocol	Percent Packets	Packets	Percent Bytes
Frame	100.0	6521	100.0
IEEE 802.11 wireless LAN	100.0	6521	29.1
Logical-Link Control	65.3	4261	68.8
Internet Protocol Version 4	59.9	3905	18.2
User Datagram Protocol	59.6	3886	7.2
Data	16.0	1045	15.6
Ad hoc On-demand Distance Vector Routing Protocol	43.6	2841	13.4
Internet Control Message Protocol	0.3	19	0.2
Address Resolution Protocol	5.5	356	2.3

Figure 6.16: The Protocol Hierarchy of Node 5

The figure 6.16 shows the protocol hierarchy of the packets captured at node 5. We can see that the total number of captured packets at node 5 are 6521 in which the UDP packets are 3886 with 1045 data and 2841 AODV packets.

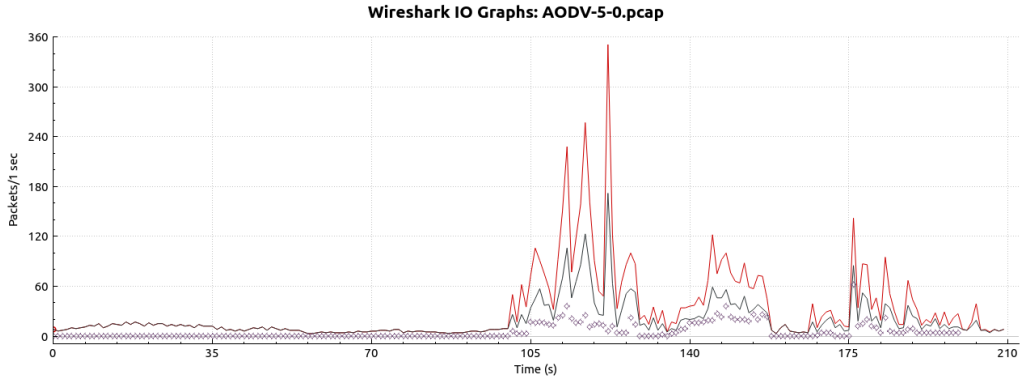

Figure 6.17: The I/O Graph of Node 5

Figure 6.17 is the Input/Output graph of the packets with respect to time at node 5. The I/O graph of the Wireshark depicts the statistics of the overall traffic on a captured file. By default, the Y-Axis is the packets per tick, while X-Axis is the tick interval per second. The ticks are the different filters Wireshark use. We used the filters of TCP errors, UDP, and data for

this graph. The red line is for all packets, for example, AODV and UDP. The dark grey line shows the UDP traffic. The diamonds show the data. We can see that the data packets increase from 100 seconds and then start to decline periodically for little spans. There are two long spans when the captured packets are very and data packets are almost 0. This means the attack is worse in these spans. The black hole nodes dropped most of the packets in this span.

PCAP of Node 22

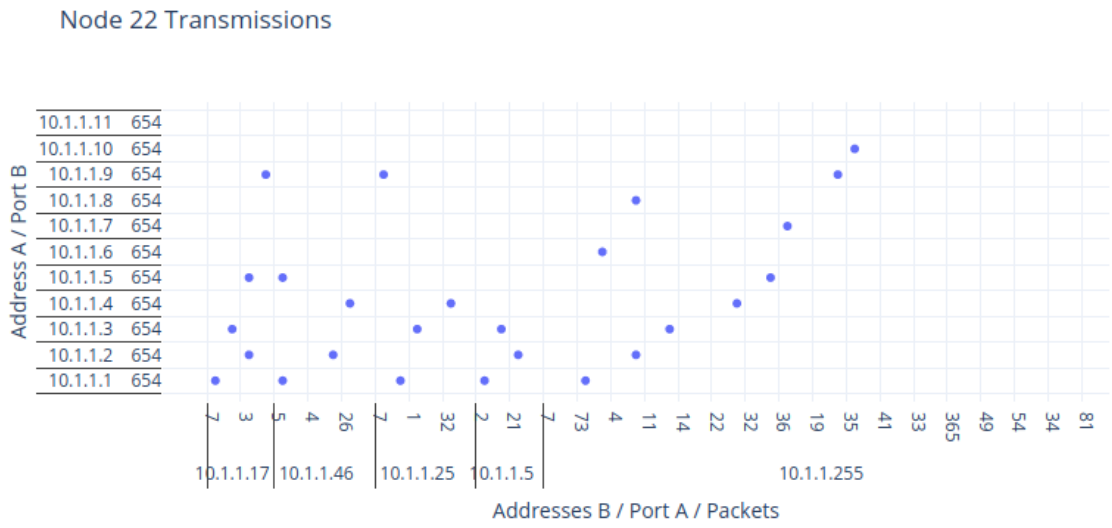

Figure 6.18: Graph of the Node 22 Conversations

18In figure 6.15 we can see the packets exchanged from the ports of the node 22. The IP address of the node 22 is 10.1.1.23. Most of its conversation belongs to port 654. Some of the packets belong to both port Addresses. The packets captured at these nodes belong to 15 nodes. The number of packets is also given at x-axis w.r.t their IP addresses. The scattered points in the

graph depict the activity of the node in the network.

Wireshark · Protocol Hierarchy Statistics · AODV-22-0.pcap

Protocol	Percent Packets	Packets	Percent Bytes
Frame	100.0	11086	100.0
IEEE 802.11 wireless LAN	100.0	11086	28.1
Logical-Link Control	67.4	7477	70.0
Internet Protocol Version 4	62.5	6932	18.1
User Datagram Protocol	62.4	6917	7.2
Data	20.3	2253	18.8
Ad hoc On-demand Distance Vector Routing Protocol	42.1	4664	12.3
Internet Control Message Protocol	0.1	15	0.1
Address Resolution Protocol	4.9	545	2.0

Figure 6.19: The Protocol Hierarchy of Node 22

Figure 6.19 shows the protocol hierarchy of captured packets at node 22. We can see that the total number of captured packets at node 5 are 11086 in which the UDP packets are 6917 with 2253 data and 4664 AODV packets.

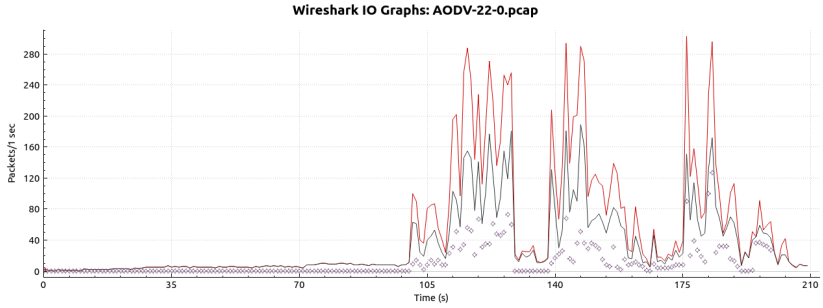

Figure 6.20: The I/O Graph of Node 22

We can see that the data packets increase from 100 seconds and then start to decline frequently for for little t spans. There are also two long spans when the captured packets are very low and data packets are almost 0. This means the attack is worse in these spans. The black hole nodes dropped most of the packets in this span.

PCAP of Node 32 and 36

We have also the PCAP details of node 32 and 36 with almost similar results but the number of packets are different at all nodes.

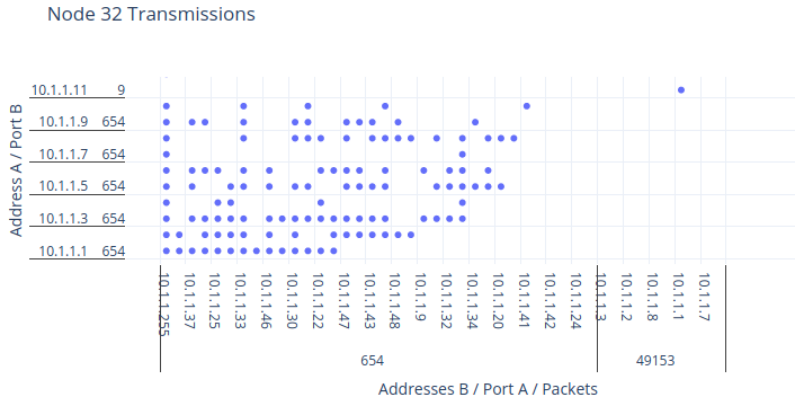

Figure 6.21: The I/O Graph of Node 32

Protocol	Percent Packets	Packets	Percent Bytes
Frame	100.0	9610	100.0
IEEE 802.11 wireless LAN	100.0	9610	29.1
Logical-Link Control	67.6	6500	68.9
Internet Protocol Version 4	62.5	6002	18.7
User Datagram Protocol	62.1	5970	7.4
Data	14.9	1431	14.3
Ad hoc On-demand Distance Vector Routing Protocol	47.2	4539	14.1
Internet Control Message Protocol	0.3	32	0.2
Address Resolution Protocol	5.2	498	2.2

Figure 6.22: The Protocol Hierarchy of Node 32

We put filter of All packets, UDP packets and UDP data on the I/O graphs of the PCAP files in Wireshark. The data packets of the I/0 graph show that the line at highest point of packets per second is consisted of all packets. Then the second grey line is consisted of the UDP packets. The Third line is consisted upon the data packets. In the 'all packets' filter the packets of all types included which are shown in the protocol hierarchy. While the UDP filter contains the UDP AODV and UDP data packets. And the

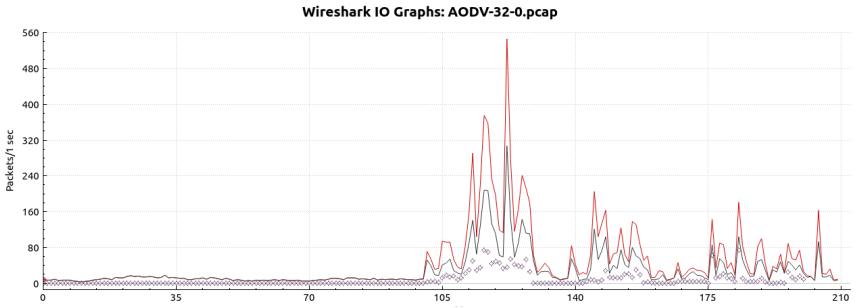

Figure 6.23: The I/O Graph of Node 32

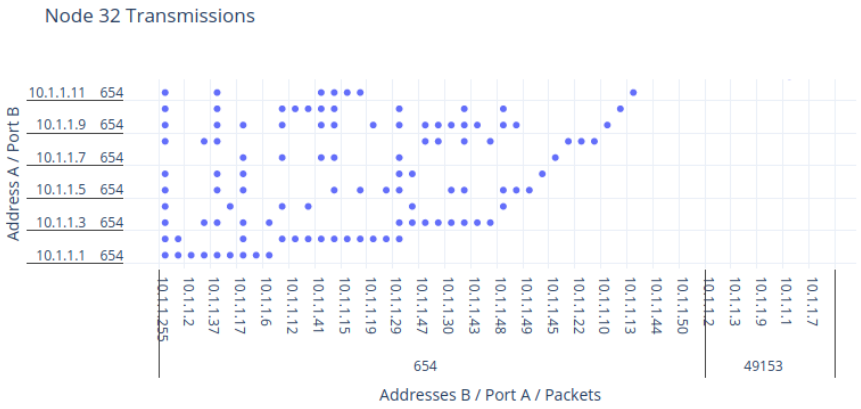

Figure 6.24: The I/O Graph of Node 36

Diamonds line is consisted of all UDP data packets. The Graphs of almost all severely bad nodes show a similar behavior like the above nodes. From all graphs, it is clear that the performance of the network declined badly in two-time spans.

6.1.8 Analysis of the Merged PCAP Files

We have merged all 50 PCAP files of the nodes to visualize the cumulative packets transmission in the network. We cam visualize the packets fluctuations in the network with respect to time.

The total number of packets captured are 456656 in which UDP packets

Wireshark · Protocol Hierarchy Statistics · AODV-36-0.pcap

Protocol	Percent Packets	Packets	Percent Bytes
Frame	100.0	10214	100.0
IEEE 802.11 wireless LAN	100.0	10214	27.5
Logical-Link Control	68.5	7001	70.7
Internet Protocol Version 4	64.5	6591	18.1
User Datagram Protocol	64.4	6581	7.2
Data	22.2	2270	20.0
Ad hoc On-demand Distance Vector Routing Protocol	42.2	4311	12.2
Internet Control Message Protocol	0.1	10	0.0
Address Resolution Protocol	4.0	410	1.6

Figure 6.25: The Protocol Hierarchy of Node 36

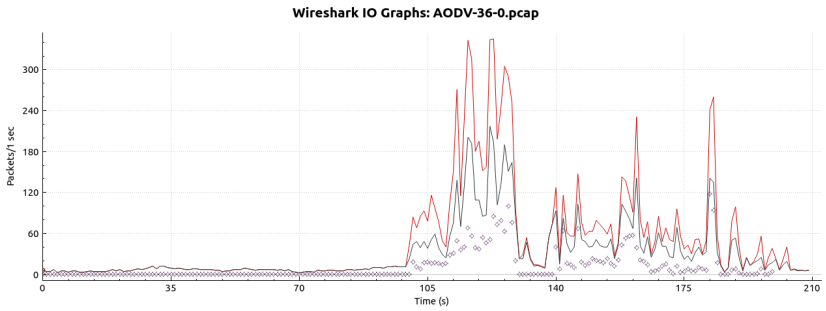

Figure 6.26: The I/O Graph of Node 36

are 298837 further composed of 107152 data and 191686 AODV Packets.

We can see that during the worse state of the attack during the timespan of 135 second where the loss of the packets boosted up and the second worse phase is during 160 to 175 seconds. We have put four filters to draw the graph. The red line indicates all types of packets, the blue line depicts the all UDP packets, the yellow line indicates the AODV Packets, and the diamonds show the data packets. In the first 100 seconds, the network sets up. On the 101th second, the data transmission starts. On the 105th second the attack generates and affects the network performance.

Wireshark · Protocol Hierarchy Statistics · Merged.pcap

Protocol	Percent Packets	Packets	Percent Bytes
Frame	100.0	456656	100.0
IEEE 802.11 wireless LAN	100.0	456656	27.2
Logical-Link Control	70.0	319498	71.1
Internet Protocol Version 4	65.7	299827	18.1
User Datagram Protocol	65.4	298837	7.2
Data	23.5	107152	20.7
Ad hoc On-demand Distance Vector Routing Protocol	42.0	191685	11.8
Internet Control Message Protocol	0.2	990	0.1
Address Resolution Protocol	4.3	19671	1.7

Figure 6.27: Protocol Hierarchy

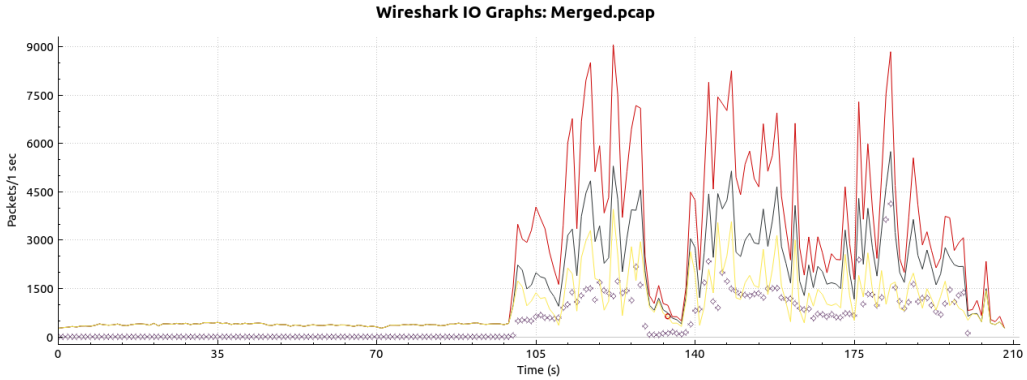

Figure 6.28: I/O Graph

6.2 PyViz Simulation

PyViz is a live simulation visualization tool of NS3. It does not use any traces. It demonstrates the nodes dropping packets and working of the mobility models. The PyViz is written in python but it works for both C++ and Python.

We can see the live interface statistics of the nodes by pausing simulation at any time. We can also snapshot the event of the simulation. So here are some of the images of the nodes.

We can clearly see the detrimental behavior of the nodes in the figure. Image 6.29 contains the interface statistics of the four different nodes. The

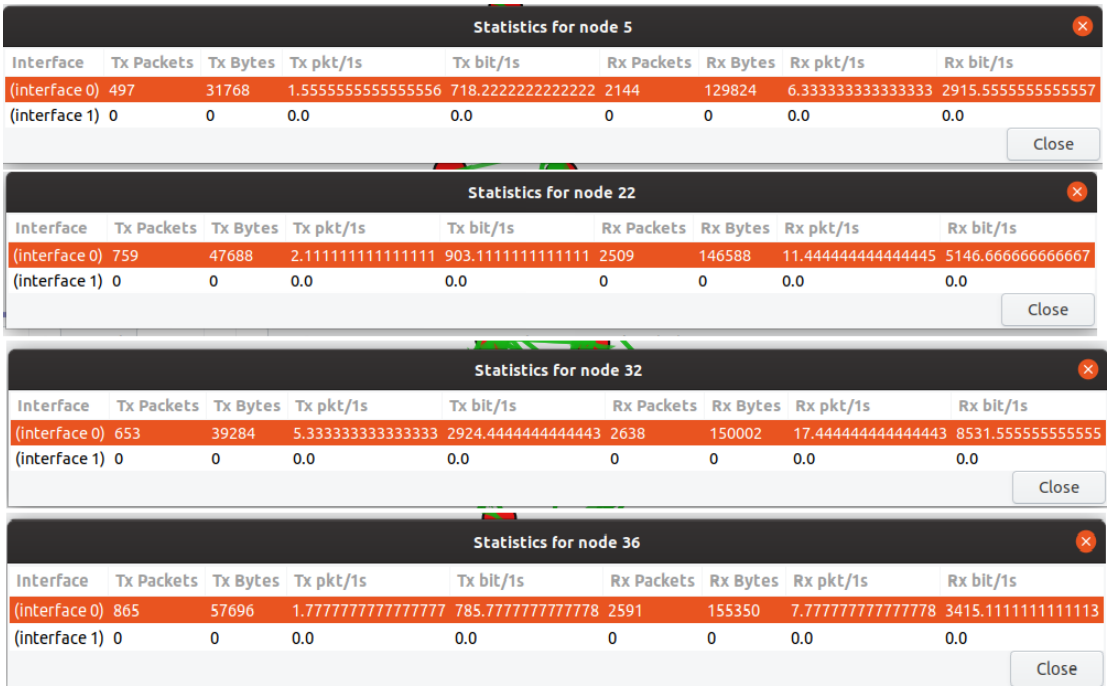

Figure 6.29: The Interface Statistics of Node 5

nodes are node 5, node 22, node 32, and node 36. These are the same nodes that we analyzed in the previous section. We can analyze the behavior of the nodes from the number of packets the node received and the number of packets is transmitted. If a node transmitted messages extremely less than it received, it means that there is something abnormal with it.

First of all, we are going to look into the statistics of node 5. The node 5 received 2144 data packets. While it transmitted only 497 packets to other nodes. It means that it discarded round about 1650 packets. The node discarded almost 76 percent of its packets.

The second node in our list to analyze is node 22. The node received 2509 data packets and it transmitted only 497 packets. The node dropped 1750 packets. It dropped 70 percent of its packets.

The third node to analyze is node 32. It received 2638 packets and transmitted only 653. It caused a loss of almost 2000 packets. It is also among the most detrimental node among all. It caused a loss percentage of 75 percent packets.

The fourth node is node 32. This node received 2591 packets and transmitted 865 packets. It dropped 1726 packets. It dropped 66 percent of packets.

The difference between the number of data packets of PyViz snapshots and the PCAP captured file tell us about the detrimental effect of the Blackhole nodes. Wireshark works on the NIC as we have mentioned above. It cannot capture the packets which node discarded or dropped intentionally. The number of detrimental nodes and the location of the detrimental nodes which they acquire has a great impact on the cumulative performance of the Network.

6.2.1 Little's Results

In Queuing theory, the little's law is an interesting theorem that is used to calculate the average numbers of entities in a static queuing system based on the average waiting time of an entity within a system and the average number of items arriving at the system per unit of time. This law was presented by John Little.

$$L = W\lambda \tag{6.1}$$

L is the long term average number of items in the stationary system,

while lambda is effective long term arrival rate. The W is the average time an item spends in the system.

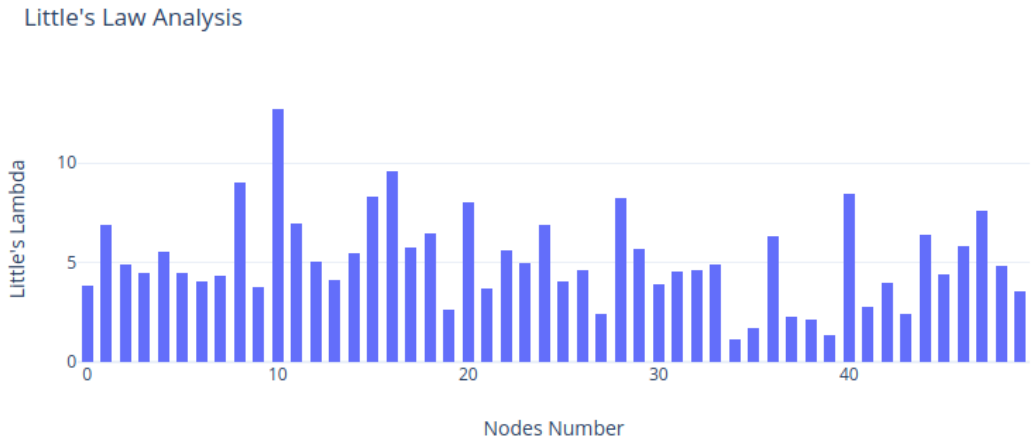

Figure 6.30: The Little's Lambda

The diagram is consisted of the results of the little theorem. We have plotted a graph of the Lambda values of the packets at the specific nodes per unit time. This informs us about the busy entities in the Network. The X-axis contains the specific node number and Y-axis contains the Lambda value of the node per unit time. The busy nodes can easily be noticed by the graph.

Figure 6.31 contains the analysis of the throughput and good-put of the network. These results were extracted through the tracemetrics. Which is a NS3 trace analysis tool. We can clearly observe the throughput to good-put ratio of the nodes. Throughput is the measurement of the amount of all data flowing through a node or link. While the goodput is the measurement of only useful data.

TraceMetrics - a trace analyzer for Network Simulator 3

File Tools Help

Simulation | Nodes | Throughput / Goodput | Little's Result | Streams

Node	Throughput	Goodput
0	126.07902560935324	10.1116010513767
1	209.5093096629945	47.80029587923531
2	191.45014339131225	40.4464042055068
3	166.25731918092202	27.57709377648191
4	194.8972801133725	36.156634062498505
5	149.06951246953832	37.99510698093063
6	121.88500926417994	15.01419550052904
7	180.98425328794605	60.976018461332224
8	351.75157634689685	101.42242266683903
9	167.17655564013808	27.27068162340989
10	952.0895872532544	553.6867606011424
11	422.82962047982227	200.08713595602987
12	298.7422738654372	118.27509108580018
13	303.98000660701206	161.17279251588317
14	296.71229335133506	103.56730773834317
15	491.1499552350995	236.55018217160037
16	568.2892147709808	282.81841728547556
17	327.40138555745466	152.59325222986658
18	375.259133715391	160.86638036281113
19	162.9633885353978	67.7170858289167
20	390.4744121913735	137.27264457626552
21	134.0170154498753	27.57709377648191

Figure 6.31: Throughput and Goodput of the Nodes

6.3 Results, Discussion and Recommendations

We simulated a mobile environment for 50 sensor nodes and defined the attack behavior in the model in the AODV routing class of the NS3. We did not define any node as the malicious node, because the aim of our approach was to forensically analyze the behavior of the network and the traffic in the presence of an attack. A significant portion of the network nodes behaved maliciously. We have analyzed and discussed the different types of traces from the simulated environment and live statistics of the simulation in the PyViz. First of all, we analyzed the flow monitor remnants of the simulation.

There were 950 flows between different Ip addresses at the IP level. We copied each and every flow ID's received, transmitted, and lost packets and made a table and CSV file to draw the graphs of those Flow IDs. The results depicted the detrimental behavior of the attack. The total loss of packets were 28.729 packets at the IP layer. The statistics of the graphs have proved the toxicity of the Blackhole attack to the routing protocols and the data traffic. After that, we briefly discussed some of the flow IDs.

After that, we analyzed the statistics from the Network Animator (NetAnim) of the NS3. We analyzed the node to node packets exchanged and plotted the graphs of the UDP packets and the AODV RREPs of the nodes.

After that, we analyzed the PCAP files of some nodes and analyzed the statistics of the type of traffic captured at those nodes. We extracted useful data from the statistics tools of the Wireshark. In the end, we finally analyzed the statistics of some nodes from the PyViz live simulation visualizer. The statistics proved the past analysis and the damaging of the blackhole attack. The figure below contains the overall packets received and receive rate statistics of our Network under the Blackhole attack.

The graph is plotted by the overall traces which we got by the outcomes of the simulation in the shape of a CSV file. The plot is made by the NS3 Gnuplot. We can see that the transmission beginning from the 100th second of simulation and then showed variations. But as we have mentioned earlier, that the attack was most detrimental in the time span of 135 seconds to 145 seconds. We can see that the receive rate dropped to zero in that phase. our previous outputs also have depicted similar behavior. So These results also prove our previous analysis.

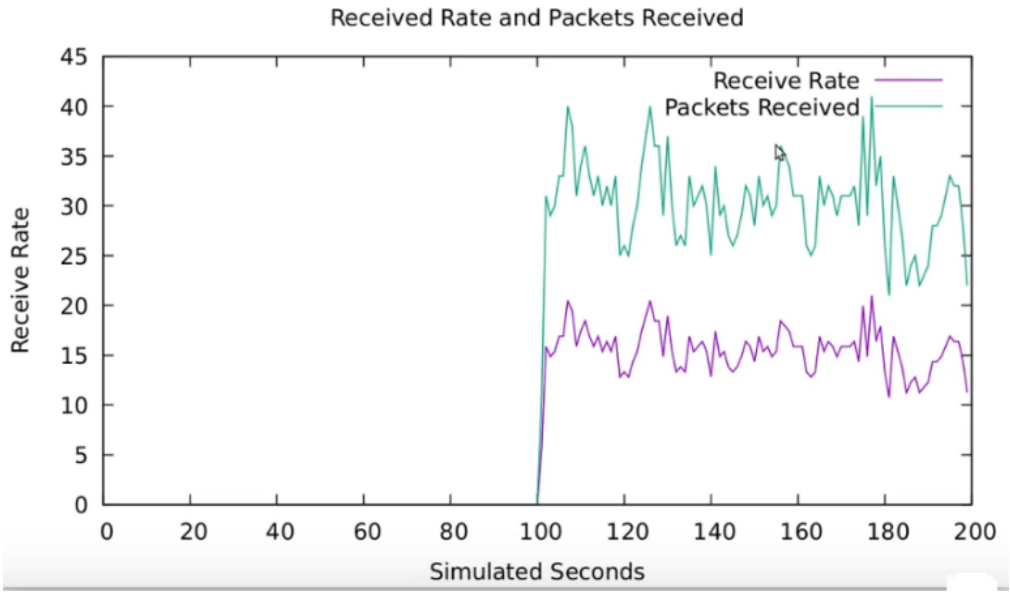

Figure 6.32: The Simulation Statistics of the Network Without Attack

By analyzing the behavior of the mobile sensor networks in a forensic sense, we have found some interesting challenges. First of all, it is a very challenging task to forensically analyze these types of networks. The continuous mobility with very low memory resources and ad-hoc traffic is like a nightmare for an investigator. The routing protocols should be consistent and firmly table-driven. In the on-demand routing protocols, the nodes construct the route and then demolish it after using it. This is not a good approach to the aspects of digital forensics. We also analyzed the total number of packets received, transmitted, and dropped. This is almost impossible to isolate all types of all AODV control packets due to the on-demand behavior. The results may be more worsen with the growth in the size of the Network. For the sake of argument, let us assume that if we make a mechanism for all network nodes to submit each routing table information to a third party

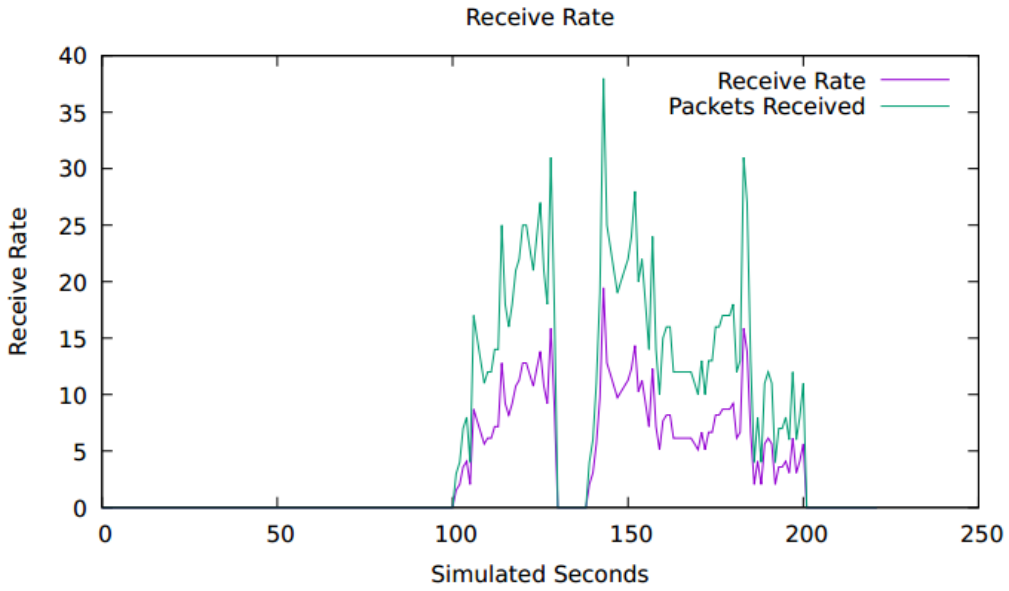

Figure 6.33: The Simulation Statistics of the Network Under Attack

node or a base station (BS). The on-demand protocols then also produce a large amount of request and reply traffic to find routes, especially in mobile networks where the position of the nodes are continuously varying. So the Networks using on-demand or reactive routing protocol are not good to produce forensically useful data. The case may get more complicated with the increasing time span of the attack. The variations in the graphs also showed the low self-healing ability of the AODV protocol as the attack got worse.

From the perspective of the attacker, the position chosen for the attacking node is very important. What if an attacker introduces his malicious node at a location which can destroy a significant portion of the network traffic on the basis of the location. If an attacker enters a pseudo-random mobile node in random mobile networks and attacks the network severely by occupying the prime location. There must be a counter to it using the same pseudo-random

Table 6.3: Comparative Analysis of Different Network types

Outcomes	**Tx**	**Rx**	**Lx**	**PDR**	**PLR**	**DL (Sec.)**	**E2E DL (Sec.)**	**TH (b/s)**
Normal Network	2316	1206	210	90 %	10%	0.01	1.03	83.09
Mobile Network	10676	7604	3072	71%	29%	0.051	6.6	31.49
Mobile Network (35)	3612	2737	875	75%	25%	0.03	14.6	13.81
Static Network	7882	7137	745	90%	10%	0.03	4.67	37.95
Controlled	15911	13331	2580	83%	17%	0.08	10.49	53.58
Tx	All Transmitted Packets							
Rx	All Received Packets							
Lx	All Lost Packets							
PDR	Packet Delivery Ratio							
PLR	Packet Loss Ratio							
DL	Delay							
E2E DL	End to End Delay							
TH	Throughput							

approach. It means that the nodes with the high trust values should not be moving randomly. We may define their area by some localization algorithms. Although, node localization is one of the basic challenges in WSN.

Table 6.3 also verifies our findings and discussions. We have constructed four different networks using AODV protocol regarding their nature and compared their outcomes accordingly. First of all the network under blackhole attack is the network which we have analysed above. The second type of network is the same type of network as above but with less number of nodes. The number of nodes for this network is 35. We can see that by decreasing only 15 nodes caused a big difference to the network performance. The number of packets decreased more than half in the flows. Packet loss ratio has fallen from 29% to 25% and E2E delay and throughput increased. The Third type of the Network is same network as above but static. We can clearly see the harm of mobility on the network in forensics sense. It is very hard to follow the record of mobile nodes. Mobility causes great amount of overhead on the network. Packet delivery ratio increased even in the presence

Table 6.4: The Stats of the Static Network Under Attack

Total	**Mal**	**Tx**	**Rx**	**Lx**	**PDR**	**PLR**	**DL**	**E2E DL**	**TH**
50	10	14383	9742	4641	67%	33%	0.09	9.42	41.99
	14	17778	12762	5017	70%	30%	0.08	8.19	53.12
	15	13435	9882	3553	73%	27%	0.08	8.19	42.12
	19	11888	8865	3023	74%	26%	0.10	11.61	38
	20	12844	9913	2950	76%	21%	0.09	9.71	44.01
	25	10803	8732	2071	79%	21%	0.08	9.75	34.06
	26	11050	8996	2054	79%	21%	0.08	9.3	35.01
Mal	Number of malicious nodes								
Tx	All Transmitted Packets								
Rx	All Received Packets								
Lx	All Lost Packets								
PDR	Packets Delivery Ratio								
PLR	Packet Loss Ratio								
DL	Delay								
E2E DL	Average End to End Delay								
TH	Throughput								

of attack. AODV performed better in the presence of attack in static nodes. E2E delay also decreased and throughput increased. The above three network are ad-hoc networks but the last is controlled WSN in which malicious node IDs are broadcasted to others. The malicious nodes are defined and almost half of the total nodes are malicious in the network. So we can see in the presence of almost half blackhole nodes the network performed better than the mobile WSN networks.

Table 6.4 contains the comparative analysis of the number of malicious nodes in the traditional static WSN in which we used the total number of nodes 50. We can clearly observe that with increasing the number of malicious nodes in the network the number of packets is also variating in the specific static network. We have tested and analyzed the subject networks by increasing the number of malicious nodes deliberately. We have defined the number of malicious nodes in a random manner in our code. In usual

Table 6.5: Comparative Analysis of the Number of Malicious Nodes in Mobile WSN

Total	**Mal**	**Tx**	**Rx**	**Lx**	**PDR**	**PLR**	**DL**	**E2E DL**	**TH**
50	10	9150	7310	1840	79%	21%	0.13	19.06	39.24
	11	4654	3125	1529	67%	33%	0.16	53.71	23.08
	13	10092	8231	1861	81%	17%	0.13	16.25	37.97
	14	5583	4166	1417	74%	26%	0.14	33.94	26.51
	15	4984	3707	1277	74%	26%	0.14	40.21	19.04
	19	4911	3601	1310	73%	27%	0.14	38.97	19.85
	20	4275	3279	996	76%	24%	0.13	39.10	18.36
	21	5081	3669	1412	72%	28%	0.14	40.75	16.95
	24	2724	2036	688	74%	26%	0.11	55.79	13.92
	25	3524	2777	747	78%	22%	0.11	40.49	16.792
Mal	Number of Malicious Nodes								
Tx	All Transmitted Packets								
Rx	All Received Packets								
Lx	All Lost Packets								
PDR	Packets Delivery Ratio								
PLR	Packet Loss Ratio								
DL	Delay								
E2E DL	Average End to End Delay								
TH	Throughput								

behavior, increasing the number of nodes increases the flows of the control packets, but this is not always true. The reason for this behavior is the strategic positions of the malicious nodes. As we have described earlier. The location is of extreme importance and it affects the cumulative calculations of the Network. When we increase the number of nodes more than half of the total number of nodes, then the Network Performance will be the same as under intense Smurf attack.

In the mobile ad-hoc wireless sensor network, we have performed the analysis on the same basis. We can easily observe that even with changing a single number of a malicious node can cause a significant change in the cumulative performance of the Network. A single malicious node can cause

big differences.

The WSN and other sister wireless network will be the significant source of digital evidence in upcoming future which will be totally based on these type of networks. But due to the heterogeneous mobile nature and the complicated processes of data aggregation, there are real challenges which digital forensics will must have to cope with. Some of the challenges regrading network traffic are discussed above. So we recommend constructing more controlled and with well memorized infra-structured wireless sensor networks to cope with the challenges of upcoming cyber threats. There should be detailed forensics frameworks for the sister domains of the sensor network. The IoT will change the digital picture of the world. So There should be special operating systems for these types of Networks based on the perspectives of digital forensics.

Chapter 7

Conclusion & Future Work

This chapter will conclude the thesis research and will highlight some future research directions. The proliferation of wireless sensor networks also alarmed the threats of security and safety in these networks. We all know that security is never ultimate. There is a need for building strong forensic methodologies for new era networks. We analyzed the Blackhole attack in wireless sensor networks by inspecting the traffic generated by the network. Different kinds of traces were analyzed by different tools. We performed a postmortem analysis of the IP level traffic by flow monitor tools. Then we analyzed the XML traces by NetAnim, and finally, we analyzed some blackhole nodes statistics by PyViz. We analyzed and explained the detrimental level of Blackhole attack for Wireless sensor networks especially in the case of mobile sensor networks. Finally, we critically discussed the problem domain in light of our research and recommended some solutions for that. Digital forensics still has several critical research problems for the domain of upcoming Networks.

7.1 Future Work

The future work that can be carried out regarding this research is the comparative investigations of different pro-active and reactive routing protocols for WSN and IoT to design a pro-forensic routing protocol for this domain. There is a lot of research problems open from the perspective of network forensics for next-generation networks.

Bibliography

[1] A. Karakaya and S. Akleylek, "A survey on security threats and authentication approaches in wireless sensor networks," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya,2018,pp.1-4.

[2] R. Gurunath, M. Agarwal, A. Nandi, and D. Samanta, "An Overview: Security Issue in IoT Network," 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud)), 2018 2nd International Conference on, Palladam, India, 2018, pp. 104-107.

[3] E. Elmahdi, S. M. Yoo, and K. Sharshembiev, "Securing data forwarding against blackhole attacks in mobile ad hoc networks," 2018 IEEE 8th Annu. Comput. Commun. Work. Conf. CCWC 2018, vol. 2018-Janua, pp. 463–467, 2018.

[4] O. Sbai and M. Elboukhari, "Simulation of MANET's Single and Multiple Blackhole Attack with NS-3," Colloq. Inf. Sci. Technol. Cist, vol. 2018-Octob, pp. 612–617, 2018.

[5] R. Gurunath, M. Agarwal, A. Nandi, and D. Samanta, "An overview: Security issue in IoT network," Proc. Int. Conf. I-SMAC (IoT Soc. Mobile, Anal. Cloud), I-SMAC 2018, pp. 104–107, 2019.

[6] S. Sezer, "T1C: IoT Security: - Threats, Security Challenges and IoT Security Research and Technology Trends," 2018 31st IEEE International System-on-Chip Conference (SOCC), Arlington, VA, 2018, pp. 1-2.

[7] S. Ali, M. A. Khan, J. Ahmad, A. W. Malik, and A. Ur Rehman, "Detection and prevention of Black Hole Attacks in IOT WSN," 2018 3rd Int. Conf. Fog Mob. Edge Comput. FMEC 2018, pp. 217–226, 2018.

[8] A. Yasin and M. Abu Zant, "Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique," Wirel. Commun. Mob. Comput., vol. 2018, 2018.

[9] G. Palmer, 'A Road Map for Digital Forensic Research', in Digital Forensic Research Workshop (DFRWS), 2001.

[10] S. Saleem, Protecting the Integrity of Digital Evidence and Basic Human Rights During the Process of Digital Forensics. 2015.

[11] International Organization on Computer Evidence, 'G8 Proposed Principles For The Procedures Relating To Digital Evidence', 2000.

[12] M. Hikmatyar, Y. Prayudi, and I. Riadi, "Network Forensics Framework Development using Interactive Planning Approach," Int. J. Comput. Appl., vol. 161, no. 10, pp. 41–48, 2017.

[13] U. Karabiyik and K. Akkaya, "Digital Forensics for IoT and WSNs," Stud. Syst. Decis. Control, vol. 164, no. December, pp. 171–207, 2019.

[14] "DDoS report Q3 2019 — Securelist." [Online]. Available: https://securelist.com/ddos-report-q3-2019/94958/. [Accessed: 02-Jan-2020].

[15] "Dyn Analysis Summary Of Friday October 21 Attack — Dyn Blog." [Online]. Available: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/. [Accessed: 02-Jan-2020].

[16] "Home — Equifax Data Breach Settlement." [Online]. Available: https://www.equifaxbreachsettlement.com/. [Accessed: 06-Jan-2020].

[17] "February 28th DDoS Incident Report - The GitHub Blog." [Online]. Available: https://github.blog/2018-03-01-ddos-incident-report/. [Accessed: 05-Jan-2020].

[18] "UK National Lottery knocked offline by DDoS attack — WeLiveSecurity." [Online]. Available: https://www.welivesecurity.com/2017/10/02/uk-national-lottery-ddos-attack/. [Accessed: 06-Jan-2020].

[19] "VNI Global Fixed and Mobile Internet Traffic Forecasts - Cisco." [Online]. Available: https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html complete-forecast. [Accessed: 02-Jan-2020].

[20] K. Katayama and H. Ohsaki, "Fluid-based Modeling of Large-Scale IEEE 802.15.4 Wireless Sensor Networks," Proc. - Int. Comput. Softw. Appl. Conf., vol. 2, pp. 543–548, 2019.

[21] Di. Bharti, N. Nainta, and H. Monga, "Performance Analysis of Wireless Sensor Networks under Adverse Scenario of Attack," 2019 6th Int. Conf. Signal Process. Integr. Networks, SPIN 2019, pp. 826–828, 2019.

[22] A. Johnson, J. Molloy, J. Yunes, J. Puthuparampil, and A. Elleithy, "Security in Wireless Sensors Networks," 2019 IEEE Long Isl. Syst. Appl. Technol. Conf. LISAT 2019, pp. 1–3, 2019.

[23] O. Belej, N. Nestor, O. Polotai, and J. Sadeckii, "Features of Application of Data Transmission Protocols in Wireless Networks of Sensors," 2019 3rd Int. Conf. Adv. Inf. Commun. Technol. AICT 2019 - Proc., pp. 317–322, 2019.

[24] Dr. Shreenath K N, Manasa V M "Black Hole Attack detection in Zone based WSN" International Journal on Recent and Innovation Trends in Computing and Communication, pp 148–151, Volume:5, Issue:4, April 2017

[25] Saurabh Sharma, Dr. Sapna Gambhir, "CRCMDR: Cluster and Reputation based Cooperative Malicious Node Detection Removal Scheme in MANETs", IEEE, 11th International Conference on Intelligent Systems and Control (ISCO), pp 36 – 340, Coimbatore, India, 5-6 January 2017

[26] Abhinav Kaurav, Kakelli Anil Kumar, "Detection and Prevention of Black hole Attack in Wireless Sensor Network Using Ns-2.35 Simulator" IJSR CSEIT, Volume 2 — Issue 3, May – June 2017

[27] Abdullah Aljumah, Tariq Ahamed Ahanger, "Futuristic Method to Detect and Prevent Black-Hole Attack in Wireless Sensor Networks" IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.2, 05 February 2017

[28] Pavan Kumar Gupta, M. Madhu, "Improving Security and Detecting Black Hole Attack in Wireless Sensing Networks" International Journal of Professional Engineering Studies, Vol VIII, Issue 5, August 2017

[29] P. Hemalatha, J. Vijithaananthi, "An Effective Performance For Denial Of Service Attack (DoS) Detection" IEEE, International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)", pp 229 – 233, Palladam, India, 10 – 11 February 2017

[30] Safa Otoum, Burak Kantarci and Hussein T. Mouftah, "Hierarchical Trust Based, Black Hole Detection in WSN based Smart Grids" IEEE, international conference on Communications (ICC), Paris, France, pp 1 – 6, 21-25 May 2017

[31] Anshuman Chhabra, Vidushi Vashishth and Deepak Kumar Sharma, "A game theory based secure model against Black hole attacks in Opportunistic Networks" IEEE, Information Sciences and Systems (CISS), pp 1 – 6, Baltimore, MD, USA, 22-24 March 2017

[32] Mert Melih Ozcelik, Erdal Irmak, Suat Ozdemir "A Hybrid Trust Based IDS for WSN" IEEE, Networks, Computers and Communications (ISNCC), pp 1 – 6, Marrakech, Morocco, 16-18 May 2017

[33] Moutushi Singh, Rupayan Das, Mrinal Kanti Sarkar, Koushik Majumder and Subir Kumar Sarkar "A Key-Based Two-Tier Trust Management Filtering Scheme for Intrusion Detection in WSN" Springer, Proceedings of the Second International Conference on Computer and Communication Technologies, pp 679-690, Volume 1, Springer India, January 2016

[34] Arshdeep Kaur "Detection and Isolation of Black hole Attack in WSN using Hybrid Technique (Received and Time Delay)" IEEE, International Conference on Inventive Computation Technologies(ICICT), pp 1 – 5, Volume: 2, Coimbatore, India, 26-27 August 2016

[35] Gurjinder Kaur1, V.K. Jain, Yogesh Chaba "Detection and Prevention of Black hole Attacks in WSN" Springer, International Conference on Intelligent, Secure, Dependable Systems in Distributed and Cloud Environments (ISDDC), pp 118-126, Vancouver, BC, Canada, 25-27 October 2017

[36] Ali Dorri "An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET" Springer Wireless Networks New York, Volume 23, Issue 6, pp 1767–1778, Springer US, Aug 2017

[37] J. V. Ananthi and S. Vengatesan, "Detection of various attacks in wireless adhoc networks and its performance analysis," Proc. Int. Conf. Inven. Comput. Informatics, ICICI 2017, no. Icici, pp. 754–757, 2018.

[38] G. Li, Z. Yan, and Y. Fu, "A study and simulation research of blackhole attack on mobile adhoc network," 2018 IEEE Conf. Commun. Netw. Secur. CNS 2018, pp. 1–6, 2018.

[39] E. Elmahdi, S. M. Yoo, and K. Sharshembiev, "Securing data forwarding against blackhole attacks in mobile ad hoc networks," 2018 IEEE 8th Annu. Comput. Commun. Work. Conf. CCWC 2018, vol. 2018-Janua, pp. 463–467, 2018.

[40] T. Kaur and R. Kumar, "Mitigation of Blackhole Attacks and Wormhole Attacks in Wireless Sensor Networks Using AODV Protocol," 2018 6th IEEE Int. Conf. Smart Energy Grid Eng. SEGE 2018, pp. 288–292, 2018.

[41] Á. Macdermott, T. Baker, and Q. Shi, "Iot Forensics: Challenges for the Ioa Era," 2018 9th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2018 - Proc., vol. 2018-Janua, pp. 1–5, 2018.

[42] M. Chernyshev, S. Zeadally, Z. Baig, and A. Woodward, "Internet of things forensics: The need, process models, and open issues," IT Prof., vol. 20, no. 3, pp. 40–49, 2018.

[43] Oriwoh and P. Sant. The forensics edge management system: A concept and design. In Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC), pages 544–550. IEEE, 2013.

[44] Di. Bharti, N. Nainta, and H. Monga, "Performance Analysis of Wireless Sensor Networks under Adverse Scenario of Attack," 2019 6th Int. Conf. Signal Process. Integr. Networks, SPIN 2019, pp. 826–828, 2019.

[45] S. Djahel, F. Naït-Abdesselam, and Z. Zhang, "Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges," IEEE Commun. Surv. Tutorials, vol. 13, no. 4, pp. 658– 672, 2011.

[46] A. Kumari and S. Krishnan, "Simulation Based Study of Blackhole Attack under AODV Protocol," Proc. - 2018 4th Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2018, pp. 1–6, 2018.

[47] B. Triki, S. Rekhis, and N. Boudriga, "Digital investigation of wormhole attacks in wireless sensor networks," Proc. - 2009 8th IEEE Int. Symp. Netw. Comput. Appl. NCA 2009, pp. 179–186, 2009.

[48] Y. Guo and I. Lee, "Forensic analysis of DoS attack traffic in MANET," Proc. - 2010 4th Int. Conf. Netw. Syst. Secur. NSS 2010, pp. 293–298, 2010.

[49] Y. Guo and M. Simon, "Network forensics in MANET: Traffic analysis of source spoofed DoS attacks," Proc. - 2010 4th Int. Conf. Netw. Syst. Secur. NSS 2010, pp. 128–135, 2010.

[50] S. Mandala, M. A. Ngadi, J. M. Sharif, M. Soperi Mohd Zahid, and F. Mohamed, "Investigating severity of blackhole attack and its variance in wireless mobile ad hoc networks," Int. J. Embed. Syst., vol. 7, no. 3–4, pp. 296–305, 2015.

[51] L. Mejaele and E. O. Ochola, "Analysing the impact of black hole attack on DSR-based MANET: The hidden network destructor," 2015 2nd Int. Conf. Inf. Secur. Cyber Forensics, InfoSec 2015, pp. 140–144, 2016.

[52] L. Sharma, S. K. Bharti, and D. K. Yadav, "Vehicular Ad Hoc Networks (VANETs): A Survey on Security issues and challenges," Int. J. Adv. Res. Comput., vol. 6, no. 2, pp. 19–22, 2017.

[53] C. Gayathri,R. Vadivel, "An Overview: Basic Concept of Network Simulation Tools", ICITCSA 2017, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Special Issue 1, January 2017, DOI 10.17148/IJARCCE

[54] Osanaiye O, Alfa AS, Hancke GP. A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks. Sensors (Basel). 2018;18(6):1691. Published 2018 May 24. doi:10.3390/s18061691

[55] Y. Liu and W. Trappe, "Jammer forensics: Localization in peer to peer networks based on Q-learning," ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc., vol. 2015-Augus, pp. 1737–1741, 2015.

[56] Z. Wang, S. Dang, S. Shaham, Z. Zhang and Z. Lv, "Basic Research Methodology in Wireless Communications: The First Course for Research-Based Graduate Students," in IEEE Access, vol. 7, pp. 86678-86696, 2019.

[57] S. Saleem, O. Popov, and I. Baggili, 'Extended Abstract Digital Forensics Model with Preservation and Protection as Umbrella Principles', Procedia Comput. Sci., vol. 35, pp. 812–821, 2014.

[58] S. Rajasekar, P. Philominathan, and V. Chinnathambi, "Research Methodology", 2013. [Online]. Available: http://arxiv.org/pdf/physics/0601009.pdf. [Accessed: 24-jan-2020].

[59] Winsberg, Eric, "Computer Simulations in Science", The Stanford Encyclopedia of Philosophy (Winter 2019 Edition), Edward N. Zalta (ed.), URL = ¡https://plato.stanford.edu/archives/win2019/entries/simulations-science/¿.

[60] S. Idwan, J. A. Zubairi and I. Mahmood, "Smart Solutions for Smart Cities: Using Wireless Sensor Network for Smart Dumpster Management," 2016 International Conference on Collaboration Technologies and Systems (CTS), Orlando, FL, 2016, pp. 493-497.

[61] R. L., M. J., and A. J., "Survey on Network Simulators," Int. J. Comput. Appl., vol. 182, no. 21, pp. 23–30, 2018.

[62] J. Crellin, "The use of simulation in digital forensics teaching," 11th Annu. Conf. High. Educ. Acad. Inf. Comput. Sci. Gr., no. July 2016, pp. 24–26, 2010.

[63] J. L. Malone, "Fight crime. Unravel incidents ... one byte at a time.," SANS Comput. Forensics, p. 125, 2004.

[64] R. Battistoni, R. Di Pietro, and F. Lombardi, "CloRoFor : Cloud Robust Forensics," pp. 1–12, 2013.

[65] "About — ns-3." [Online]. Available: https://www.nsnam.org/about/. [Accessed: 27-Jan-2020].

[66] "ns-3 vns-3-dev documentation." [Online]. Available: https://www.nsnam.org/docs/release/3.13/models/singlehtml/index.html. [Accessed: 27-Jan-2020].

[67] I. Minakov, R. Passerone, A. Rizzardi, and S. Sicari, "A comparative study of recent wireless sensor network simulators," ACM Trans. Sens. Networks, vol. 12, no. 3, 2016.

[68] [Online].Available: https://www.nsnam.org/doxygen/classns31friispropagationlossmodel.htr [Accessed: 2-Feb-2020].

[69] T. S. Chouhan and R. S. Deshmukh, "Analysis of DSDV, OLSR and AODV Routing Protocols in VANETS Scenario: Using NS3," 2015 International Conference on Computational Intelligence and Communication Networks (CICN), Jabalpur, 2015, pp. 85-89.

[70] "Flow Monitor — Model Library." [Online]. Available: https://www.nsnam.org/docs/models/html/flow-monitor.html. [Accessed: 04-Feb-2020].

[71]