T.C.

ALTINBAŞ UNIVERSITY

Electrical and Computer Engineering

A COMPREHENSIVE APPROACH ON IMPACTS OF GRAYHOLE, BLACKHOLE AND SYBIL ATTACK BASED ON AODV PROTOCOL IN WIRELESS SENSOR NETWORKS

SUFIAN ABDULQADER AL-MAJMAIE

Master Thesis

Supervisor
Asst. Prof. Dr. Oguz Ata

Istanbul (2019)

A COMPREHENSIVE APPROACH ON IMPACTS OF GRAYHOLE, BLACKHOLE AND SYBIL ATTACK BASED ON AODV PROTOCOL IN WIRELESS SENSOR NETWORKS

by

Sufian Abdulqader Al-Majmaie

Electrical and Computer Engineering

Submitted to the Graduate School of Science and Engineering

in partial fulfillment of the requirements for the degree of

Master of Science

ALTINBAŞ UNIVERSITY

2019

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Asst. Prof. Dr. Oğuz ATA

Supervisor

Examining Committee Members (first name belongs to the chairperson of the jury and the second name belongs to supervisor)

Prof. Dr. Hasan Huseyin BALIK	Air Force Academy, National Defense University	_________
Asst. Prof. Dr. Oğuz ATA	School of Engineering and Natural Science, Altinbas University	_________
Prof. Dr. Osman Nuri UCAN	School of Engineering and Natural Science, Altinbas University	_________

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Asst. Prof. Dr. Çağatay AYDIN
Head of Department

Approval Date of Graduate School of
Science and Engineering: ____/____/____

Assoc. Prof. Dr. Oğuz BAYAT
Director

I acknowledge that all information contained in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have referred to all the articles and findings that were not original to this work and have referred to them fully.

Sufian Abdulqader Al-Majmaie

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude Asst. Prof. Dr. Oğuz Ata for all the knowledge and support he provided during my study for the master's degree and throughout the work to complete this thesis. You have made my dream comes true. And I would like to present a special thanks for Asst. Prof. Dr. Ameer Kadhim Hadi for his support and efforts to accomplish this work.

ABSTRACT

A COMPREHENSIVE APPROACH ON IMPACTS OF GRAYHOLE, BLACKHOLE AND SYBIL ATTACK BASED ON AODV PROTOCOL IN WIRELESS SENSOR NETWORKS

Sufian Abdulqader Al-Majmaie,

M.Sc., Electrical and Computer Engineering, Altınbaş University,

Supervisor: Asst. Prof. Dr. Oğuz ATA

Date: April 2019

Pages: 74

In the current days, Wireless Sensor Networks (WSNs) have grabbed extended attention in engineering sectors due to their ability to address big engineering tasks in relatively lower cost. It records specific variation environments such as temperature, pressure etc. also it can be deployed in places where human can’t be reached due to their small size (Nano and Micro). The small nodes of WSN is considered as corner stone that plot the performance and time line of overall network. In this article, we concentrate of routing protocol in IEEE 802.11 static wireless sensor network from security perspectives. Three malicious attacks over network layer of AODV routing protocol are studied. The objective of this study was to realize the impact of Black Hole, Gray Hole and Sybil attacks on the AODV routing protocol. Network is implemented to detect the temperature information by adopting 49 sensors in grid topology, each sensor is transmitting the sensing data by multi-hop communication to a supper node called as sink node. Simulation is performed using MANASIM integrated in Network Simulator. Temperature information is generated virtually according to number of sensors and simulation time using the CPR tool in NS-2, hence 933 packets are generated as payload of the network; for each attack, throughput, PDF and NRL are determined after 1300 iterations of the experiment and with effects of 1 to 4 malicious nodes. The network is found more resistive to the Gray Hole attack where optimum results are obtained, the detected average throughput was 3.8375 whereas the PDF and NRL are found 99.065 and 3.2175 respectively.

Keywords: AODV, malicious, Gray Hole, Black Hole, Sybil, Sensor, Temperature.

ÖZET

Kablosuz sensör ağlarında AODV protokolüne dayalı (gri delik kara delik ve sybil) saldırılarının etkilerine dair kapsamlı bir yaklaşım

Sufian Abdulqader Al-Majmaie,

M.Sc., Elektrik ve Bilgisayar Mühendisliği, Altınbaş Üniversitesi,

Danışman: Yrd. Prof. Dr. Oğuz ATA

Tarih: Nisan 2019

Sayfalar: 74

Günümüzde, Kablosuz Sensör Ağları (WSN'ler) göreceli olarak daha düşük maliyetle büyük mühendislik görevlerini yerine getirme yetenekleri nedeniyle mühendislik alanında büyük ilgi görmüştür. Sıcaklık, basınç vb. Gibi belirli değerleri değişkenlik gösteren ortamlardan verileri kaydeder; ayrıca küçük boyutlarından (Nano ve Micro) dolayı insanın ulaşılamadığı insan ulaşımın uygun olmadığı yerlere yerleştirilebilir. WSN'nin küçük düğümleri, genel ağın performansını ve zaman çizgisini gösteren köşe taşı olarak kabul edilir. Bu çalışmanın amacı, Kara Delik, Gri Delik ve Sybil saldırılarının AODV yönlendirme protokolü üzerindeki etkilerini değerlendirmektir. Ağ topolojisinde 49 sensör ile sıcaklık bilgisini algılamak için bir ağ kurulmuştur, her bir sensör çok sıçramalı iletişim yoluyla algılama verilerini SINK düğümü adı verilen ana düğümüne iletir. Simülasyon, Ağ Simülatörü olarak NS2(Network Simulator) içerisinde bütünleşik olarak gelen MANASIM kullanılmıştır. Sıcaklık bilgisi sanal olarak üretilmekte olup, sensör sayısına ve NS-2'deki CPR aracını kullandığı simülasyon süresine göre üretilir. Her saldırı için 933 paket üretilmiştir.Verim, PDF ve NRL, hesaplamaları için 1300 tekrarın ortalaması ile ve kötü niyetli düğümün etkisi ağa yerleştirilen 1 ile 4 arasındaki kötü niyetli düğüm ile belirleniri . Ağ, optimum sonuçların alındığı Gray Hole saldırısına daha dirençli bulundu, tespit edilen ortalama verim 3.8375, PDF 99.065 ve NRL 3.2175 olarak bulunmuştur.

Anahtar Kelimeler: AODV, kötü amaçlı, Gri Delik, Kara Delik, Sybil, Sensör, Sıcaklık.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

LIST OF ABBREVIATIONS

AODV	:	Ad Hoc on-demand Distant Vector
RP	:	Routing Protocol
RREQ	:	Routing Request
RREP	:	Routing Reply
SHC	:	Single Hope Communications
MHC	:	Multi Hope Communications
MN	:	Mobile Network
BH	:	Black Hole
GH	:	Gray Hole
RERR	:	Route Error
H	:	Header
SN	:	Sensor Network
WSN	:	Wireless Sensors Network
QoS	:	Quality of Service
BS	:	Base Station
IP	:	Internet Protocol
ID	:	Identity Number
RX	:	Receiver
TX	:	Transmitter

1. INTRODUCTION

1.1 OVERVIEW

Generally, sensors are transducers that detect the physical and chemical variations in any environment such as pressure, temperature, the pH changes etc. and send the sensing data to remote servers (gateway). It can work in various environments such as free space, water and gas or any feasible surroundings alike working inside petrol pipe lines or any other chemical fluid conditions. Sensors are required a particular protection while they are functioning in different atmospheres, a plastic cover can be used to isolate the sensor circuits from the water or fluid impacts and metal cages can be used for protecting the sensors if they were in high areas alike hills where the chances of lighting are high. Usually, sensors are forming what is so called network and hence it is called sensor network. Sensors network that perform its function wirelessly is termed as wireless sensor network (WSN). Such networks are constructed by participation of three main sectors: monitoring unit, core unit and sensing unit; in monitoring part usually, graphical user interfaces are made to display the sensing information to the specialist bodies who is taking an action according to the observations, sensing information can be monitored by using large laboratories or even using a small screens like mobile phones; the core unit is performing the data processing and establishing the communication between the sensors and monitoring units. Consequently, Core unit may involve communication module and processing model with work sequentially with sensing unit that in turn collecting the data from the surrounding object. Core unit is mostly formed by using a microcontroller which is programmable to perform any kind of functions, it acts as gateway to the sensor network. Each sensor is having its own position (location) in the sensors array and this location is called as node, each node is connected to the core unit and/or to the neighboring nodes for network formation. sensors are designed by reupdated manufacturers such as SHARP, MicroStrain, MOTOROLA, DeltaTRAK, ELECTROCHEM, Crossbow etc. however, sensor may have a single sensing task or multiple sensing task more likely, it may be used to sense the temperature, pressure, dust etc. companies of interest are competing to produce tiny and passive sensors that take a nanometer dimensions and consume less energy. Ultimately, whole structure of sensors is being empowered with a DC power source usually batteries for sensing unites and power supplies for core and monitoring units. Wireless sensor networks (WSNs) are being used in several applications as low cost and efficient alternative solution that may substitute the complex and costly solution like remote sensing by satellites. It being used in health applications [1] [2] to monitor the brain or muscles electrical activity and agriculture applications to monitor the plants condition remotely [3]; furthermore, it being used to monitor the high-powered engines health as given in [4].

1.2 PROBLEM FORMULATION

Commonly, wireless sensor networks (WSNs) are sub divided into smaller and tiny sensors formed in specific topology such as tree or stat structure. The main agenda of the said wireless sensor network is to monitor a particular change in project fields. However, some participants in the said sensing environment are distorting the functionality of sensors network. Malfunctioning of sensors due to malicious attacks is trending concern of researches.

wireless sensor networks (WSNs) are fallen in two categories base on their method of connectivity. However, literature survey reveals that WLAN and ZigBee are exploited for providing connectivity in WSN paradigms. Depending on the requirement of data rate; ZigBee is used for applications that not exceed Kbps whereas WLAN network is used for applications that demand higher data rates. In this project WLAN wireless network is deployed for connecting the network nodes with server due to their data rate and autonomous characteristics.

The simplicity and autonomous in network infrastructure are the major considerations in wireless sensor networks, for this reason; wireless Ad-Hoc network is the predominant network standard in this field. This standard comes with two varieties: Wireless Local Area Network WLAN and Bluetooth [4]. since they are ensuring an acceptable data rate, WLAN IEEE 802.11 is the preferred network backbone for wireless sensors. Nonetheless, the autonomous nature of this network standard may cause serious treat from security perspectives. In other word, any node within the range of the network can join automatically without granting any permission from higher administration, actually, admin tasks are not seen in this type of network. The new node that may arrive into the network can malfunction the entire network performance if malicious activity is conducted.

The curriculum of Ad-Hoc network has drawn big security drawback in terms of ability to combat the malicious attacks, with such disadvantage, WSNs are more subjectable for passive and active attacks that could take place by any node within the range of sensor network.

1.3 PROPOSED PARADIGM

In this thesis, wireless sensor network is simulated for monitoring a temperature in virtual environments. Hence the security of the said network was concerned in our research problem, we have conducted the simulation in such way the malfunctioning of sensors is taking place due to malicious attacks. Wireless IEEE 802.11 Ad-Hoc network is relied as a method of connectivity in our paradigm where we can analyze the impact of autonomous mechanism of this network. For testing the network security level, we made the simulation with three attacks: Sybil attack, Black Hole attack and Sybil attack. Hence the impact of each attach is studied individually; experiment is repeated with same attack by changing the number of malicious nodes as (one node, two nodes, three nodes and four nodes). In each iteration, throughput is obtained for known sent packets and known received packets, PDF and NRL are obtained as well.

1.4 THESIS ORGANIZATION

This thesis report is contained of five technical chapters detailing the core work of our project and describing the results for making conclusions. Conclusion and future work are listed at the end of this thesis; all references and important data are tabled in the appendix.

- Chapter one: “Introduction”, that imply wireless sensor network importance and reveals the problem statement of this work with objectives and the structure of this thesis report.
- Chapter two: “Literature survey”, contains the similar studies and timeline of wireless sensor technology and emphasises the sensors applications in various daily life and industrial sectors.
- Chapter three: is about the research methodology, describes the key technology used in establishment of our simulation results.
- Chapter four: discuss the thesis outcomes
- Chapter five: is the conclusion.

2. LITERATURE SURVEY

2.1 SENSORS TECHNIQUES

Wireless sensors are defined at [4] where the sensors form a network deployed in safety applications more likely, protecting the workers in constriction industry. In this application ZigBee standard used form initiating the communication between network participants; author at [4] emphasis that using ZigBee may reduce the cost of signaling as lower frequency with narrow bands are used. Wireless sensor network is designed in this study to protect the labors from harmful agents alike strong rays and viruses due to dust, the same was done by fabricating a wearable sensor to be placed in labor's cloth in such way that both nodes and antenna are integrated within the fabric. To be able of implementing the above characteristics, Mobile Wireless Sensor Network will need to be deployed. Furthermore, author reveals that three main sections have to be integrated to fulfill the design requirements of mobile wireless sensor network: the sensing node, the gateway and far nodes; the sensing nodes must be selected to be rudest enough to tolerate the outdoor environments also need to be light in weight so that workers can wear it in their garments. The major task of sensing node is to collect the variation in outdoor environment and send it to the gateway that in turn collect all the data from all sensing nodes and re-rout it to the remote nodes (servers) by using the internet network. It is important to mention that two sensors are used in this study: SGLux TOCON-ABC1with output sensitivity of 280 and consumption of 2.4 mW of power for sun rays' detections; furthermore, Sharp GP2Y1010AU0F with 0.5 sensitivity and 60 mW of power consumption is used as dust detection sensor.

At [5], the wireless sensors are highly exposed to surrounding impacts such as wireless noise and other environmental conditions, however performance metrics in wireless sensors can be defined upon two factors more likely the latency and the throughput. In this study, author says that sensors performance is critical when applications alike real time actuators are in the image; for such applications highly-reliable sensors are needed. Basically, parameters such as sensor's type and node location in the network are directly affecting the functionality of sensor. As per this study i.e. [5], simulators can be used to validate the sensors performance where real world conditions are coded for creating a clear vison of sensor reliability. OPENT software is used for sensors virtual test; it provides big enough library and graphical user interface so it eases dealing with wireless sensors network. However, this approach had drawn a conclusion that sensor positioning is directly affecting the performance, furthermore, two network topologies: mesh and star are tested for sake of performance optimization and results shown that star topological network is suitable for mechanical applications alike actuators which demands a good latency.

Wireless bands are sub-divided into three working groups for operating a wireless sensor networks with different licensed bands that are varying depends on the geographical location. IEEE 802.15.4 is the popular standard of ZigBee that underlaying the wireless sensor networks in most of applications. Bands of 915 MHz, 2.4 GHz and 868 MHz are the working frequencies of wireless sensors in USA, Australia and Europe respectively. Furtherly, we are going to denote the wireless sensor networks and wireless sensors and networks (as termed by most researches in the literature) in abbreviation as WS and WSAN respectively.

At [6], saving the electricity of public lighting in cities is a challenge for electrical engineers and also forming an economical challenge in terms of man power and machines costing. However, WSAN are deployed in here for sensing the level of sky light in the cities and then sending the information to the actuators that is in turn switching the required number of lights for this time of the day; this process is obviously related to the weather and environmental conditions such as clouds, rains and snow which are directly shading the sun light; dealing with such circumstances is worthy by involving WSAN approach.

At [7] , sensors for chemical reactions parameters are also designed; as an example of such sensors: the pH sensor that designed in here using wireless sensor triggered by LC capacitors. This study is concentrated on testing LC capacitors that used for pH status detection. The capacitor was tested under different frequencies and results shown the feasibility of deploying such capacitor for performing such tasks.

At [8], Sporain Microsystems developed a pressure sensor with oscillator 131MHz Clapp type, this pressure sensor is developed for monitoring the aircraft engines. In order to design sensor network for conducting the above task, set of devices are used such as MESFET, Clapp oscillator Compex chip capacitor and film inductor; all to be used with Sporain Microsystem pressure sensor. Wireless sensor is interfaced with antenna by magnetically coupling circuit made up from oscillator (resonant circuit); however, antenna was kept one meter away from the sensor. It’s obvious that such sensing circuit in similar applications may require energy to trigger the devices, in this study; author said that thermal model can be used to fulfil this corner and hence to design a pressure sensor operating up to 100 psi with temperature tolerance of 400 C. The applications similar to the aircraft engine health measurement may demand a rudest sensing network that tolerate harsh environments and perform an accurate measure (sensing) with acceptable error.

At [9], the number of sensors in the network is posing a big economical challenge. Pan-Tilt-Zoom wireless visual sensor (PTZWVS) is demonstrated, author mentioned that traditional wireless visual sensors differ from PTZ sensor in terms of coverage and visual operations; PTZWVS can tilt, Pan and zoom the objects and have extendable coverage. While using the PTZ virtual wireless sensor, two regions can be identified in the field of view (FOV): PTZ Coverage region and Direct coverage region (DCR). In this PTZ mode of coverage sensor may require to change the camera angle to cover the object while in direct coverage mode merely a particular side can be covered. Adjusting the visuality angle is happening with PTZ coverage mode where sensor is in process to tilt, zoom and pan the sight; ultimately, performing all these process in the same time may lead to noticeable delay in visual data capturing, this study is proposed using of multiple sensor to fulfil delay matter. Form the other hand, deploying large number of visual sensors is maximizing the cost of the project, this problem can be tackled using heuristic algorithm alike PTZA. In this algorithm, field of view can be divided into several nodes and then calculating each sensor visuality (how many nodes are covered by each sensor) in that the number of deployed sensors will be limited to those sensors can cover the maximum nodes.

At [10], wherever sensors are found the sources are required to empower them; however, this approach is proposing a zero power sensor. The same is essential for increasing the population of sensing; technologies alike IoT devices will be the biggest beneficiary from deploying zero powered sensors. Designing a zero empowered sensing device is listed under passive sensing circuits; in this approach, passive sensor is implemented by using the principles of third order intermodulation. Nonlinear devices are forming the majority of passive sensing components where the same may open the door of non-linear effects that degrade the performance. Nonlinear effects is another drawback that need to be sorted while dealing with passive sensors; these effects are degrading the performance of the said sensor by negatively impacting the accuracy of sensing data.

At [11], the study deals with post sensing procedure where sensing data are being processed to extract the sensing information. Physical wireless parameters conversion sensing network (PhyC-SN) is new terminology defined in this study as the process that convers the sensing data into sensing information by exploiting the frequency components in the sensing data and performing the required frequency modulation. Information separation is another task to be tackled; sensing data transmission is varying in accordance with event changes in sensing environments, hence the separation between the two consecutive entries is hard task for PhyC-SN module. In such circumstances where quick processing the sensing data is required similarly as stated in [9] where large number of sensors are required for performing the accurate and fast sensing; here we realized that using algorithms may ease the mentioned difficulty; the separation between consecutive entry of data tackled by using probability approach that guess the future entry of sensors before it actually exists.

PhyC-SN is a paradigm that used to carry the sensing information to the processing unit Fusion center (FC), however, different frequency components can be realized in PhyC-SN unit. Separation of those frequencies is achievable by frequency conversion methods such as Fourier transform or Fast Fourier Transform (FFT), sensor network may have the ability for quick recognizing of frequency variation. Transmission control protocol can ease this problem by using the probability concept to anticipate the next sensing data.

At [12], sensors manufacturers are tending to miniaturizing the sensors and fabricating tiny batteries with long life span to empower sensors. Basically, sensors are responsible to sensor the physicals changes with known ambience whereas the wireless sensor networks are responsible to transmit the sensing data gathered by the sensors into the processing station where further possessing of this data are performed. Depending on the nature of application that sensors networks have been employed for; sensor data are treated individually at the stage of data processing base on application nature; the same is discussed in this study where star topology is used with base node that mainly empowered. Author mentioned that star topology is a popular network topology used by most sensor applications with small sensor sized in few cubic centimeters empowered by small battery lasting for several months.

The IEEE 802.15.4 is common standard used by most wireless sensor networks; it has power efficient topologies with low data rate; the physical layer of this standard is compatible with the most available transceivers. Multiplexing techniques such as Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) can be used in MAC layer in IEEE 802.15.4 to facilitate the handover process when node exiting or entering the network.

For strengthen the WSN, sensors should be connected to remote node (outer node) so nodes should adopt a good routing mechanism; said by the author.

At [13], this study is conducted to recognize the performance metrics such as latency, power consumption and throughput while using star topology and cluster topology of wireless sensor nodes with IEEE 802.15.4 standard. However, up to 100 nodes are used in this experiment to obtain the performance measure in different topologies. Study shows that clustered nodes are reporting higher throughput. For signaling and sensing data exchanging, WSN may adopt a ZigBee IEEE 802.15.4 or Wireless Personal Area Network (WPAN) IEEE 802.15 standards, in case of ZigBee based wireless sensor network, the parameters and network specifications are easier than wireless personal area network also ZigBee is far less expensive than WPAN. In order to measure the performance as per the above description, NS2 used to simulate two network topologies (sate and cluster tree) in each scenario, network is tested in terms of energy consumption, delay and throughput; it was found that cluster tree topology is anyhow better than star as star network is consuming larger power and packet transmission may take longer time. Author experienced the NS2 network simulator and stated that NS2 is best simulator to test communication networks due to its ability to virtualize the dynamic behaviors of the said networks.

At [14], study involves designing of slop monitoring wireless sensor with ZigBee based communication scheme. The main purpose of this approach is finding the land deformation happening due to rains and heavy floods in hills areas. The proposed system contains of router to spread the monitored data through internet; data is collected from the end device (sensor) that forward the data to the coordinator. Routing the data from sensors is being the focus of IoT researches; in this prototype author said that ZigBee IEEE 802.15.4 is most suitable derive to start the communication among network nodes whereas it permits large number of connections in relatively low power consumption, a six thousand connection is possible in case of ZigBee as reported in this study, sleeping mode is activated in ZigBee where device can go into sleep if no communication is made which minimize the power consumption. In other word, ZigBee still partially rout the data during the sleeping mode by delimit the power if only low data rate is required. Two major concerns are involved in this study: the environment is directly affecting the WSN as the last is in touch with surrounding particles more likely impacted by weather, hence lighting is one of those effects that need to be encountered when designing WSN; in this approach authors have made a simplified lighting rod to discharge the lighting if any; A cage is made to protect this prototype. Furthermore, the Received Signal Strength Indication procedure is to be done for accurately design the antenna.

At [15], study involves designing of wireless video sensor for detection of air targets. The use of ZigBee for video sensors are not meeting the required performance as ZigBee supports low data rates only (250 kbps can be achieved while using ZigBee). In this approach, WIFI IEEE 802.11 are used as communication (up to 11 Mbps) backbone that supports high data rate and fits video transmission. Traditionally, UART interfaces are used along with ZigBee that provide relatively low data rate, in case of this study, Serial peripheral interface (SPI) is used with WIFI sensor node that supports high data rate, those interfaces are nothing but manner to connect the device to the host computer or servicers where data can be processed. Sensors that used in this study are tableted in Table 2.1.

Table 2. 1: Sensors that used in the study [15] for developing air target monitoring systems.

Sensor model	Function
GP2Y1010AU0F	Dust detection made by SHARP
TPM-300E	Air sensor made by DOVELET
DHT21	Humidity and temperature by ROPO

The circuit is empowered by lithium 3.7 V rechargeable battery.

At [16], the approach proposes semi-passive autonomous sensor for monitoring the temperature, pressure and gas at indoor environments using the Radio Frequency Identification. This study aims to produce a very small size sensor by printing the sensor using a single walled carbonate nanotube (SWCNT) printed on substrate paper. This study is focused on using inkjet printing technology to develop a green wireless sensor.

At [17], wireless sensor network differs from the single\standalone sensor (wired sensors) in their ability to provide a wider scanning information for bigger sensing field. WSNs have more importance in their uses over complex sensing tasks specially when the wired sensor can not stand due to mobility requirement. An acoustic wireless sensor is made to monitor the health level of underground pipe lines by detecting the breaks (leakage) in the pipe or any abnormal particles; this sensor is functioning by measuring the pressure along the pipe while moving within the path. For protection purpose, two precautions are made which isolate the sensor circuit from the water and external radio frequency; for that sensor circuit is shielded against

RF effects and isolated by plastic cover from surrounding water. Sensor is made as random shape to friction avoidance while moving in water. Sensor is governed using a PIC 32 microprocessor, the data is sent from sensor entity to the microprocessor using of radio frequency board, the following specifications are noticed as wireless parameters that chosen in this study:

Table 2. 2: Wireless sensor specifications that chosen by [17].

Subject	Details
Usable band	ISM: industrial, scientific and medical band.
Wireless method	RF board
Transmitted power	27 dBm
Input level of sensitively	-117 dBm
Data rate	115.2 Kbps

At [18], a study that focused in designing resonant circuit that act as passive sensor for multiple physical parameters. Those sensors are totally zero powered sensors that support sensing temperature, strain, humidity, pressure. Substrate circuit printing is newly invented approach that utilizes a small area for making the hardware electronic circuits; this approach lies about developing a multilayer electronic board as shown in figure 2.1.

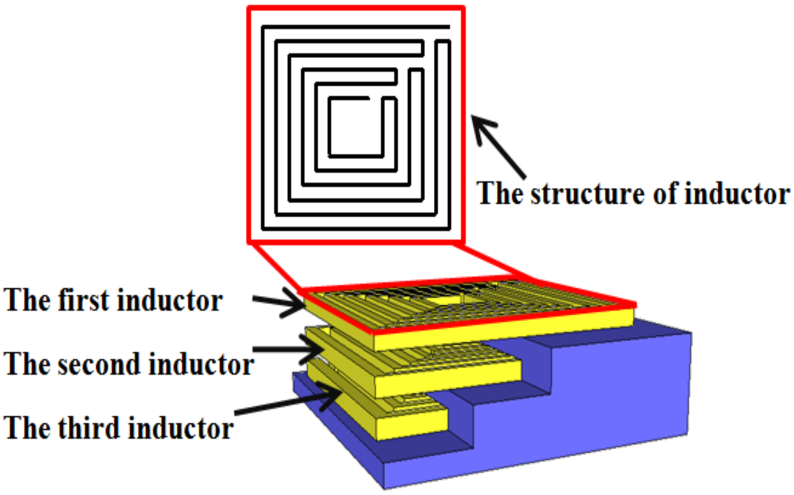

Figure 2. 1: Substrate design of electronic circuit.

At [3], smart farming is achievable using a wireless sensor network that supports multimedia sensing facility. A CMOS camera is integrated with this multimedia sensor for controlling the farm equipment. This approach is inheriting the concept of multilayer PCB for hardware that allows space utilization and consequently compacted PCB is yielded. While concerning to assess the status of plants, usually remote sensing is involved more likely, large scales of green lands can be monitored by satellite and hence all the health information is provided in form map. The remote sensing (satellite-based sensing) is highly costing and complex procedure to be developed; this limitation is eased with using wireless sensor network to monitor the plants health level. WSN can be established inside the field (farm) and detect high quality pictures along with weather parameters detection alike temperature and dryness of the surrounding; all those data can ease the agronomist job to accurately and remotely monitoring the plants without needing to be presented in the field. The communication is set using the SimpliciTI protocol which is yielding image transmission up to 100 Kpbs data rate. Further sensors specifications can be listed as follow: receiver end sensitively is -90 dBm, the throughput range is 20 Kbps to 40 Kbps. Microcontroller of PIC 32 series is used for governing the tasks and connected with WSN using UART port. In this study, relatively low data rate is established which may not help to detect the expected image quality.

At [1], a study that make use of another application of wireless sensor network, however, this approach is extending the ways to extract the EMG (brain and muscles activity detection) that is happening by EMG device that is installing over the muscles (none-invasive). However, this study aims to extend the use of EMG signals after it being detected from the muscles and sent through some prototype to the monitoring device that ease the access to this data anywhere and anytime so that doctors or health specialists can diagnose the case flexibly. Wireless body area network (WBAN) is used to create the necessary communication between the sensor end and monitoring end. WIFI module that is using IEEE 802.11 standard is used for communication purpose, this prototype is in turn provides a high data rate capability that looks more than the necessary to transmit the data in this application.

At [2], EMG and EEG signals are the essential components that underlay any neural activity control so detection of EEG and EMG is respectively reflecting the brain electrical activity and muscles electrical activity. The detection of those signals is reported in this study using of tiny electrodes acts as sensors on particular (predefined) region in the scalp. However, this approach is proposing another alternative to empower the EEG and EMG sensors by providing a wirelessly power option.

At [19], the wireless sensing actuator network (WSAN) is the backbone of IoT and required to operate in more reliable form and self-configurable techniques that maximize the overall efficiency. The main contribution of this work lies on the module capability to support multiple purpose sensing and multiple communication schemes. ISM, IEEE 802.15.4a (ZigBee) and IEEE 802.11 b/g/n0 (WIFI) are set to be the communication methods that provides connectivity in various data rate that matches the purpose of sensing more likely, for video related sensors, higher data rate is required which needs to be ensured using the WIFI of WPAN standards. The user end system is made to be graphical user interface supportive, the same is done as microcontroller of model PIC 32 is used which is supporting these powerful tasks.

At [20], none infrastructure sensor network is grabbed extra attentions in wireless sensor network due to their tiny structure and small power consumption. Ad Hoc wireless network is the core concept of none infrastructure wireless network, it comes in two standards: IEEE 802.11 WLAN and IEEE 802.15.1 Bluetooth. The first standard used to establish long distant communication whereas Bluetooth is set for short distant communication. The power consumption of such network is relatively low where some researches are clearly mentioned that passive nodes are deployed at many cases where the presence of battery is not possible. More likely, mall power requirement may produce from smaller power supplies.

At [21], wireless sensor networks based on Ad-Hoc network are demanding routing administration only where packets can across around the nodes efficiently. The main goal of routing protocols is to ensure efficient power management and reduce the network computational cost. However, AODV protocol seems the feasible option for wireless sensor network.

At [22], Ad Hoc on demand distant vector is the routing protocol used by most wireless sensor networks that deploy IEEE 802.11 model. This routing protocol is existed to reduce the number of hops packets made to reach destination node. It works base of two stages: discovery of status and exchanging of node information. Nodes may broadcast a hello request where it can tell each other about their location and their willing to reach a particular destination, in hereafter, routing protocol may compare the requests in each node to obtain the lesser cost path and then forward the packets through that path.

At [23], [24] and [25], wireless sensor networks are designed initially to serve the military applications where small sensors can be deployed in tough geographical area and capture information which is difficult to be done by human. Sensors presence at the harsh environments make it more susceptible for malicious attacks. Ad Hoc core is the more subjected topology for attacks where network functions and performance are distorted. Attackers are accessing the network by snooping on the nodes and overhear the coordination and other routing (confidential information) from the legitimate node. They use this stolen information for designing a malicious node and inserting it in the network. Such kind of nodes may work either to drop all data packets that it receives or drop a particular packet that is predefined by attacker. Malicious node is working to fool the normal nodes as it pretends to be a legitimate node. Different kind of attacks are seen targeting the wireless sensor networks, the attacks may target different kinds of layers in OSI system so that some attacks are for application layer, others for network layer and so on.

At [26], a study that proposed a threshold of high energy is presented as key point of Blackhole and Grayhole attacks where the LEACH routing protocol is targeted by attacker in wireless sensor network. The system is simulated in Network Simulator II and performance measured on energy threshold bases. Outcomes of this study reveals that Blackhole attack is more effective on LEACH protocol.

At [27], attacks alike Blackhole, Flooding, Grayhole, Rushing can be targeting AODV and AOMDV routing protocols and effect of the said attach can be monitored using Packet Loss Count, throughput, end to end delay and hop count.

At [28], malicious nodes behaviors can be analyzed in wireless sensor networks using the packet drop count. This study involves analyzing the opportunistic routing protocols while the same is undergoing a Blackhole attack, analytical techniques are used to calculate the behaviors of Blackhole attack in this type of routing protocol. Impact of Sinkhole and Blackhole attacks are presented along with their threat to wireless sensor network security at [29] also the key metrics to evaluate the network level of security are presented as well. Routing protocols are said to be in three categories such as proactive, reactive and hybrid routing protocols and however, the protocols of the same are presented with Wormhole attack in [30]. The AODV protocol is an reactive routing protocol whereas OLSR and ZRP are proactive and hybrid routing protocols; Qualnet 5.0 is the network simulator used to perform the experiments at [30]. Blackhole attack is presented in several studies and said to be that attack where data packets from network are being sinked and routed to unknown destination after using a fake node pretending as legitimate node; another attacks such as Grayhole, Wormhole, Sinkhole, Sleep deprivation and Byzantine attack are very popular attacks that targeting the AODV routing protocol as said by [31].

2.2 SUMMARY

In the beginning of this literature survey, we emphasis to state the working bands that used to fulfill the main corner of the topic which is being wireless. The sensors are said to detect the surrounding physical or chemical variation and technically sensors can perform a bigger task if they would form a network. Furthermore, wirelessly signaling is another term that make the sensor network more recognizable in addressing the industrial problems. Three standers are observed from the literature as a communication method which provides a different data rates for matching application demands. ZigBee is considered as efficient way to link the sensors with monitoring zoon by permitting a moderated data rate with highly power efficient process. Other studies are preferring to use IEEE 802.11 family to enhance the data rate while working on such application that uses video sensing. While formation of wireless sensor network, two network topologies are recognized in which either to be star or tree topology, the worthiness of tree topology is reported to be more feasible as compare with the star topology. We realized that most of studies in the literature are focused on developing the sensor node in such way concerning about their data rate and hardware efficiency such as space utilization, researchers are paid efforts to minimize the size and weight of the said wireless sensor which is actually become feasible using the substrate PCB prints that enable the electronics components to be formed in layers on the top of each other which reduce the space and miniaturizing the overall circuit. The observations of this literature survey reveal about lake resources in measurement of multi attack effects in wireless sensor network. Articles of the same concern are listing the preliminary information about the attacks without tending to measure the network immunity with multiple attack presence.

The AODV is common routing protocol in Ad Hoc wireless network, it leaks of security due to the nature of none infrastructure Ad Hoc network so that nodes are join and leave by merely adjusting their location to be within network range. Malicious nodes are majorly pretending as legitimate nodes where they can fool the legitimates and pass their secret credentials. While doing this project, efforts are paid to study of malicious attacks that take place in network layer and target the AODV routing protocol. The main objectives of our paradigm is to understand the strength of attacker so that prevention method can be implemented on future work.

3. METHODOLOGY

3.1 SENSOR UNITS

In wireless sensor network, two different structured are introduced which are the infrastructure sensing networked and non-infrastructure sensing network [20]. the both are similar in conducting the sensing operations but differs by the application of interest. Well, the infrastructure sensing network is termed to that network that involving an administration block for controlling the hosts connectivity (nodes manger in case WSN), the administrator is regulating the process between the nodes itself and between the nodes and severs, it also responsible to broadcast the sensing information across a public network like internet, it uses routers and switches for performing routing operations if more than a one network is existed. This kind of network is usually used where the security is required and no matter about the size as higher power is required to run such setups where bigger batteries and devices are coming into image. An example about the infrastructure sensor network is those wireless sensor networks using the cellular systems as backbone.

From the other hand, none infrastructure sensing network is defined as an option for those application seeking for simplicity. None infrastructure means tiny (microelectronic) devices powered by smaller power and could be self-empowered devices such as passive sensor [14] [18]. Small battery can be used to run such network as size is concern by the beneficiaries. This type of network is used in this project for sensing the temperature variation, however, the network backbone and the administration block is omitted in none infrastructure sensing network, that means nodes can join and leave at any time form the network without central permission. Ad-Hoc network is the best common example of none infrastructure model, it has two slandered which is IEEE 802.11 Wireless Local Area Network (WLAN) for long coverage connection and IEEE 802.15.1 that stands for Bluetooth as wireless personal area network for short range of connectivity. This network is considered as autonomous system consisting of nodes that act as routers connected by wireless links to the sink node (server) these nodes can move freely within the network coverage. Single hop network is termed to the mobile mode where sensors are moving within the coverage radius so connection is established between the particular node and the server whereas the multi hop network is ensuring bigger coverage area as data packets can be forwarded to other nodes and then to the destination in which enhance the coverage area. Figure 3.1 demonstrates the Ad-Hoc network topology for single hop and multi-hop process.

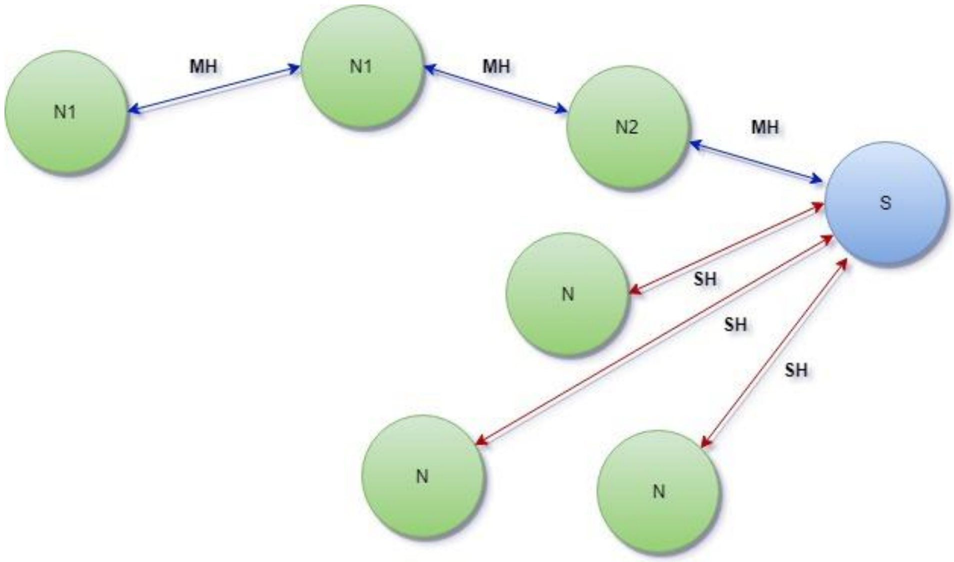

Figure 3. 3: Single hop versus multi hop communication in Ad-Hoc network.

The Ad-Hoc as none infrastructure network is preferred by the application due to their dynamic topology, however, the following characteristics can be seen in such kind of network:

a. Energy harvesting devices;
b. Bandwidth is very limited;
c. Security incompatibility if high security is required;
d. It can be deployed quickly and easily;
e. Nods are self-configured so that network is independent of back office operations;
f. Both single hop and multi hop are supported;
g. Autonomous node operations;
h. Furthermore, know that all information in point (e.) is validated then; networking equipment such as switches and routers are not required for this network;
i. Cost of implementation is very feasible since a less budget may be needed for the network adaptation;
j. Know that all information of point (b.) is validated, that means high data rate sensors such as virtual sensors may not fit with this network standard;
k. Security degradation as stated in point (c.) is very critical event as any node can joint the network without grating permission, for that; prevention procedure must be taken for smooth operation of none infrastructure sensing network.

3.2 SIMULATION ESTABLISHMENT

As a special type of Ad-Hoc wireless network, the wireless sensor network should be designed by deploying number of nodes over the environment of interest so that, sensor can detect required data from the said sensing environment. As soon as sensor granted the data, it may forward the sensing data to the remote node called as server node or sink node. The server node is categorized as highly setup powerful node that can brae the multi-flow of data from network nodes. Compare to the real work experiments, computer virtual environment simulates wireless network scenarios with far less expensive budget. Different kinds of sensors can be establishes using the simulator with the possibility to change the parameters for selecting the optimum sensing settings. For this project, wireless sensor network can be efficiently simulated using MANNASIM which is termed as an extension for network simulator (NS-2). However, using MANNASIM is providing flexibility for simulating the wireless sensors by simply changing the classes of this tool (MANNASIM). Furthermore, the back office operations in the standards and protocols can be adjusted along with network monitoring process that records the packets flowing and other analytical details about the network [21].

The main objective of this project is finding out the level of distortion raised due to the malicious attacks on wireless sensor network, hence a complete simulation of the said sensor network is required. For doing so, MANNASIM is used a simulation environment and is provided framework of wireless sensor network. The framework of this tool is developed to simulate the wireless network scenario and uses the procedure of Network Simulator 2 (NS-2) to do the same. Whereas the simulation outcomes and creation of the said simulation is achieved by the other solution called as script generator tool (SGT) which works side by side with framework codes of network simulator (NS-2) to establish a compete procedure. In other word, simulation should start with creation TCL file (the frame work of the same is provided in general public license which make it possible for users to update the code according to the required network), TCL file is containing the general scenario of wireless network. Soon after, script generator tool (SGT) is providing front end monitor to the TCL procedures. MANNASIM is platform coded in JAVA and integrated with network simulator (NS-2); as described in [21] this entity is addon feature in network simulator NS-2 that making it capable to simulate the wireless sensor networks with different sensing requirements. Dealing with MANNASIM is fall into four sub bundles that demonstrated in figure 3.2. first of all, the general parameters of wireless scenario in NS-2 will need to be adjusted.

Essentially, simulation of wireless sensor network is depending on TCL code in network simulator 2 (NS-2) that plots the network components and the methods handling the data within this network. However, as declared above, NS-2 is the mother land of wireless network simulation, a mobile and wireless node are already existed in this software; talking about sensor network, situation of NS-2 nodes to be upgraded for sensing networks fulfilment, however, new characteristics to be applied on currently existed node for make it compatible with sensing operations; energy consumption, stop time, sleep time, type of sensor to be mainly applied on core nodes. Energy requirements is another concern of simulation where different standards of batteries are in use within sensor networks; furthermore, nodes to be individually treated for establishment of their behaviors in the network. Generally, TCL coding is major task for simulating the wireless sensor network; this language is error susceptible and unexcited tools to accommodate the wide scenarios of wireless simulation so MANASIM has paved the road for simulation without actually needing to use TCL commands. The presence of script generator tool (SGT) make the simulation more feasible specially with large wireless networks. User may need only to adjust the existed values and change the protocols name using the script generator tool (SGT) friendly interface. For the figure 3.2. the details parameters the been used in our paradigm is listed below, where all settings are descried for each step from figure 3.2.

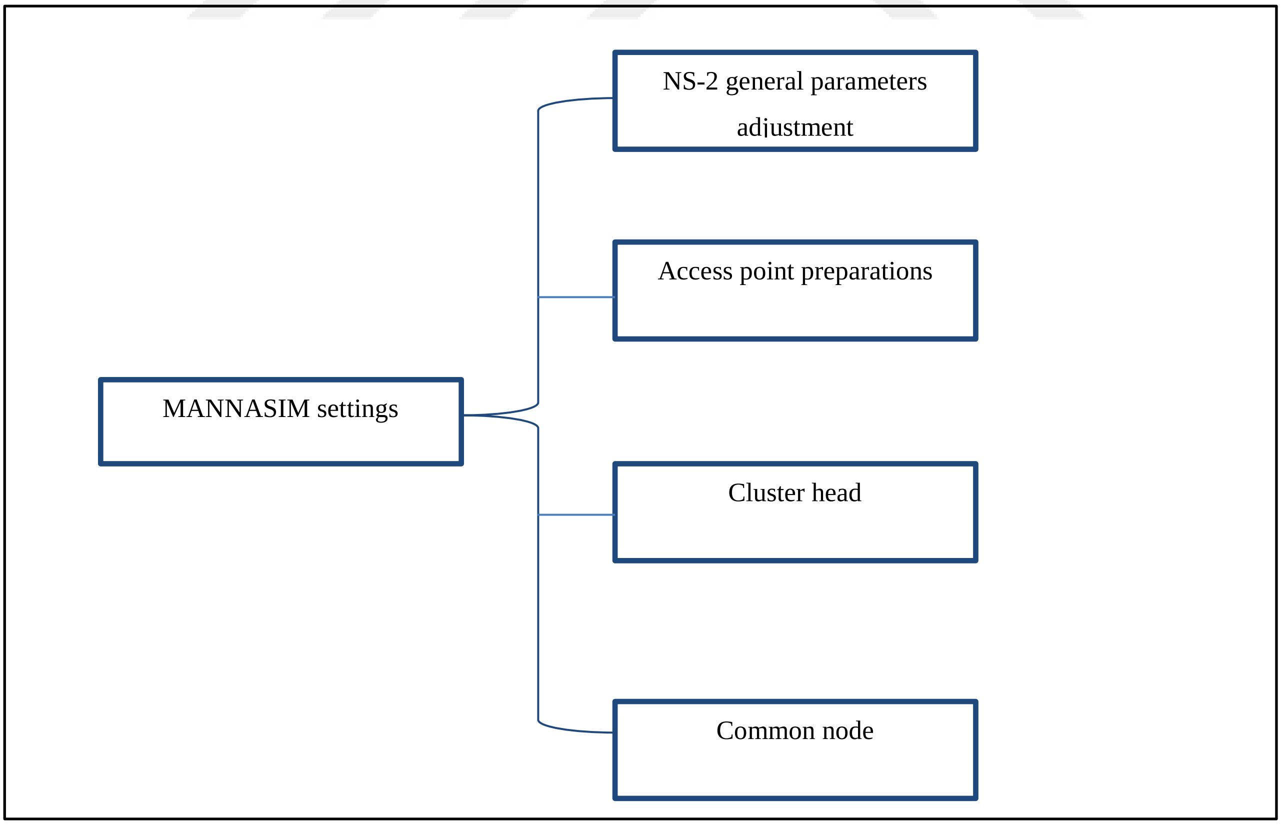

Figure 3. 4: MANNASIM main classes structure.

3.2.1 General simulation procedure

Simulation is performed using Network Simulator 2 (NS-2) where wireless sensor network is fabricated along with the malicious nodes for testing the network reliability in the said abnormal situations. The general scenario of the simulation can be described herein:

1. Simulation is prepared by changing some parameters related to the communication model and power model, however, wireless channel with two ways signal propagation is set for fulfilment of wireless sensor network requirements. It is already described in the preceding sections that none infrastructure communication model is selected in correspondence of IEEE 802.11 wireless Ad-Hoc network, the advantages and drawbacks of this topology is prementioned above. Coverage mode of this network is set as Multi hop communication figure (3.1), as a default property omni directional antenna is proven a good performance as per the literature so that it being used over here, this antenna is installed in (0,0,105) location over the sensor's body. Drop Tail queuing algorithm is an option which is left as default with 300 tolerance of queue length. Ultimately, this network is empowered from battery which was the common option for WSN in previous studies. No concern is given to the life span and dimensions of the cell battery as no supported feature in the simulator is integrated for such task.
2. The paradigm of this project is proposed for testing the effect of malicious nodes in different kinds of attacks on wireless sensor network holding the settings mentioned in point (1). Hence, a forty nine temperature sensor is distributed across topography of 600m x 600m. one (single) node is designated as server node and single hop connect is established between each node and server/sink node. The 49 nodes are arranged corresponding to Manhattan grid of seven rows that consisting of seven nodes, figure 3.3 demonstrates the geometrical structure of the simulation.
3. Simulation is to be performed in four different iterations, that can happen by existence of four possibilities of malicious action. Hence, simulation may begin with zero malicious node and then single malicious node to be added and so on through four malicious nodes. Three attacks i.e. Black hole, Sybil and Grey hole attack to be taking place during each iteration so that, twelve experiments to be performed excluding the core (plane) experiment that take place with no notice attack.
4. Location of malicious nodes {0,1,2,3,4} is made randomly so that we can obtain different results every time we run the simulation, however, the effect of attack is changed depending on malicious node location.

5. As we intended to measure the impact of malicious nodes in various attacks on Multi hop wireless sensor network, we stated before that malicious nodes are randomly distributed throughout the network; that dispense the need of mobility of sensing nodes in current simulation. However, the sensor nodes motion is made static for the purpose of network immunity measurements.

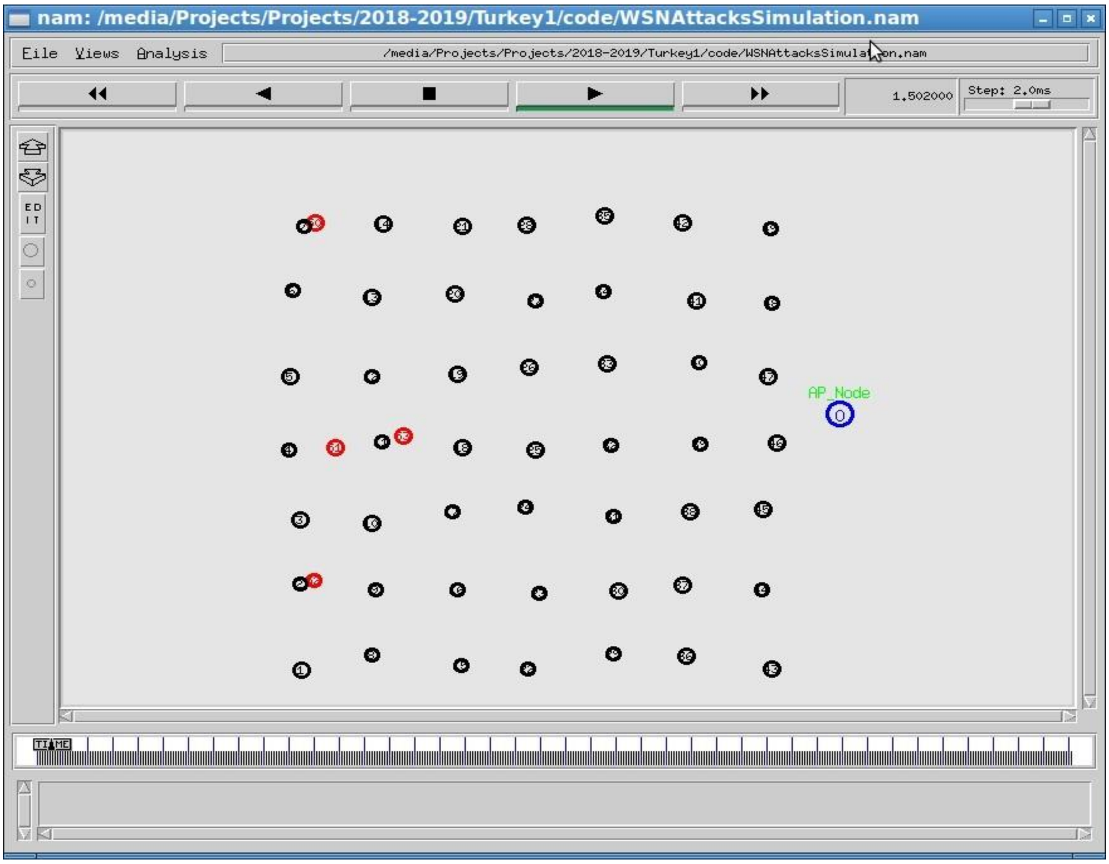
nam: /media/Projects/Projects/2018-2019/Turkey1/code/WSNAttacksSimulation.nam
File
Views
Analysis
/media/Projects/Projects/2018-2019/Turkey1/code/WSNAttacksSimulation.nam
1.502000
Step: 2.0ms
EDIT
AP_Node
0
TIME

Figure 3. 5: The proposed topography that simulated the WSN at present of four malicious nodes.

6. The further step in this simulation was about defining the functioning nodes, nodes is categorized into three groups: common nodes, sink nodes and attacking nodes. A special class is made in the simulation which defines the behaviours of every node during the run time. The normal (common) nodes stands for temperature sensors that distributed throughout sensing arena. Those sensors are designated to gather temperature readings from the said sensing field, they are enabled to grab any data within 50m to 10m range. Taking about the temperature readings sources, practically, MANNASIM is designated to encapsulate the data of any selected sensor with sub class called as DataGenerator [21].

However, the sensor power is very important factor that is explicitly effects the life span of the network. The sensor's parameters are tabulated in Annexure 1.

7. The sink node is characterized by adopting a single node located at farthest side from the sensor grid. This node is designed with super settings in terms of data rate and energy.
8. Malicious nodes are deployed in this simulation so that we can test the network performance with presence of single node malicious, two malicious nodes, three malicious nodes and four malicious nodes. Known that every malicious event is taking place with standalone experiment (iteration).
9. Malicious nodes are deployed between the sensor as one node through four nodes. The mechanism of malicious operations is taking place by employing the autonomous nature of Ad-Hoc network. In other word, any sensing node may forward the packets to nearest node as per routing mechanism. That impose higher probability for malicious node to be nearest intermediate node to any sensor node, in which increase the chance of malfunctions existence.

3.3 ROUTING PROTOCOL

Which acts as main entity in wireless sensing network, it takes the necessary steps for ensuring a smoother propagation of data packets through the network. Routing procedure is depending on network topology and nodes location. Sensors (nodes) are detecting the sensing data post data to the destination node. Data may travel to the destination through several intermediations, that is normally happening by means of routing protocols which take the responsibility for regulating the traffic through the network. There is an intimated relationship between the power sources and the data paths in the wireless sensor networks. Knowing that power consumption is forming big challenges for the designers as smaller batteries is usually integrated with the sensors and it backs up the sensor circuit with the power for limited period of time, the life of battery is only determining the life span of the sensors network. For Ad Hoc networks the micro batteries are usually used as power model, however, routing protocol is essentially designated to find the paths with lesser losses so that minimum energy may consume from the sensor energy model. Currently, many technologies are proposed for enhancing the redundancy of routing protocols. Commonly, large sensor network that consists of more than 100 nodes is more subjectable to data congestion and that may pose many disorders in the performance, the powerful routing mechanism yields smooth transmission of packets by minimizing the length of ques so that minimum delay is resulted , furthermore, the lesser possible energy is radiated for the sensor nodes as shortest path transmission is ensured by powerful routing and hence sensor nodes are not required anymore to transmit the packets to far nodes; with lack of routing mechanism, packet may reflect pack to the source node due to unstable routing and then the node may re rout the same data again which increase the power consumption. The current routing approaches involves data aggregation, in other word, data of same nature that holds same routing information are grouped in one bundle and then transmitted to the destination (all packets are intended to reach same destination), this is utilizing the bandwidth in such way that channel will prevent being busy by processing same destination packets individually, instead of this, packets of same destination may be sent at once so that channel will be free for other data transportation. Many factors are coming to the image when we talk about aggregation; many of real time applications may not tolerate the processing delay that raised from aggregation so, factors like priority transmission may also defined. The packets of impotent information to be sent as soon as possible may cross over the other packets in terms of transmission priority. The same is taking place by labeling the urgent packets with some identity so that the router will aware about such type of nodes and take it first in transmission. Figure 3.4. generalizes the process of routing, various operations to be taken to complete the routing, it begins with generation of data series which is temperature data in our case, this data is intended to reach the sink node by passing through other nodes in the network. It is cleared that. Data is not proffered to be sent in the same fashion as it captured, researchers have developed a technique in which continuous data is breaking up into smaller data trains called as packets, this approach is fall under the concept called packet switching network that is considered as optimized method of circuit switching networks. Packets is more combatable for noise inference as one packet drop is anyways having lesser impact then dropping all data. all nodes in this network are automatically communicating with each other in order to form a packet paths toward the destination sink. That followed by broadcasting of hello message as every node may send this message to all nodes for determining the nearest neighbor, at the end of this stage, all nodes will gather the information about their neighboring and they will gain clear clue about network topology. As the network formed and nodes is trained to capture the nearest neighbors, the time will come for routing protocols for performing their tasks, the information captured by every node is to be integrated with data packets as the source node may transmit packets among several nodes, in every packet, the term header is standing for the information that applied by the particular node on this packet upon the receiving of the said packet by this node. Header information is involving the traffic related data and all the necessary details for successful signaling.

Usually, every routing protocol is having own advantage and drawbacks for particular network topology and data traffic levels. Routing protocols are varying within following protocols: AODV, LANMAR, ZRP, DYMO, RIP [22]. Such protocols can parity from each other in terms of throughputs and noise immunity (the same will be discussed in coming sections of this chapter). The similarity of routing protocols is termed to their essential responsibility of reducing the network load by effectively utilizing the network resources. Form the other hand, their differences are about the performance drawn in particular application. The diagram in figure 3.4 is demonstrating the procedure above where the label "H" stands for the header and "P" stands for packet.

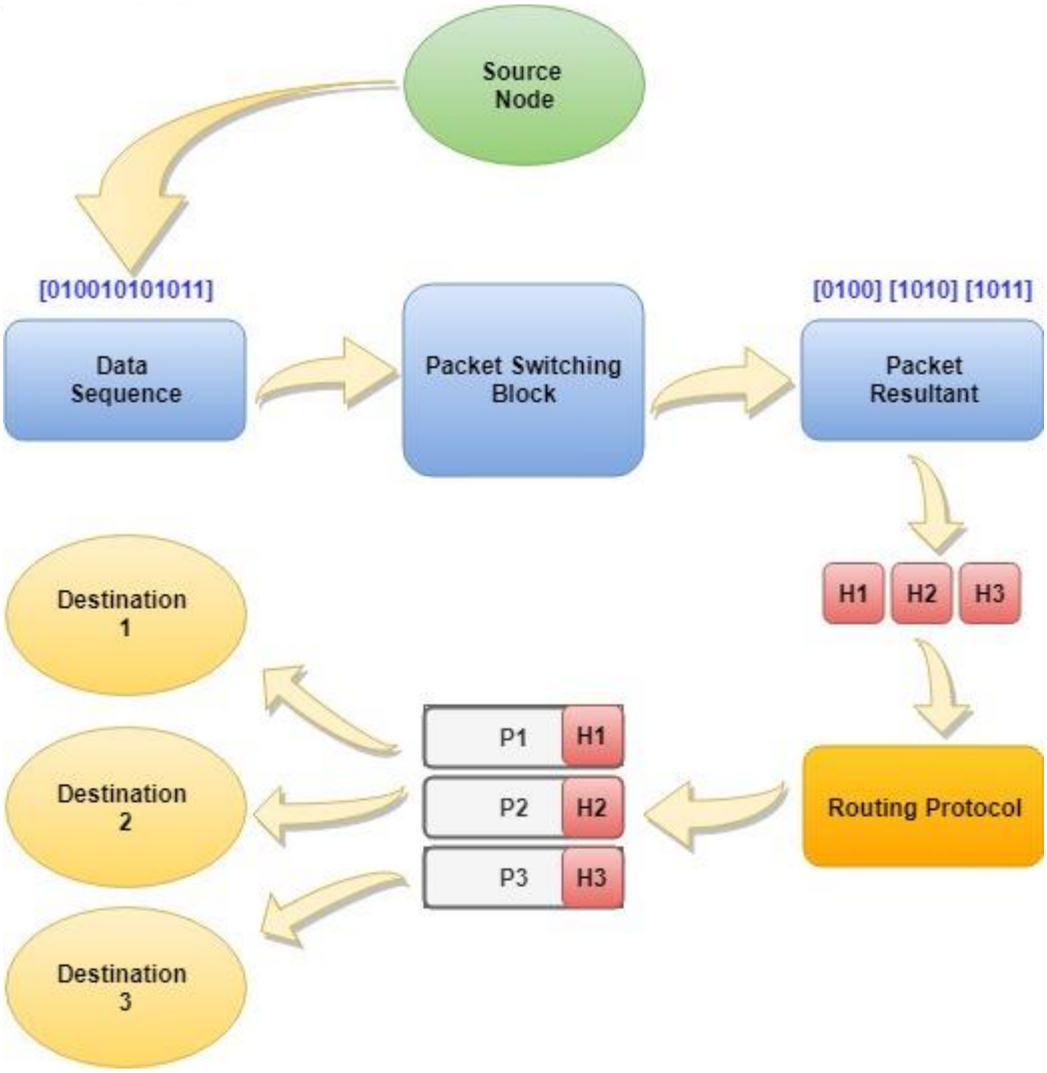

Figure 3. 6: A block diagram reveals the procedure of data handling at any wireless network.

.

3.3.1 Ad-Hoc On-Demand Distance Vector (AODV)

This protocol is very common on none infrastructure networks such as Ad-Hoc wireless network. As the name indicates, it only functioning if routing requirement is seemed in the network otherwise it keeps on idle mode where no energy is consumed (sleeping mode). The main steps taken in this technology are depending on the hello message outcomes in each node. If node is willing to forward the data packets so it is already prepared with path information and topology mapping details, using AODV protocol for routing is taking place by requesting the nearest neighbour for accepting the routing, the node of source may send routing request (RREQ) message to the next nearest node which is in turn response to this request by either approving the data or rejecting it. Request reply (RREP) is reflection of neighbour node ability to accept the packet upon the same is requested by source node. Otherwise, if node is not ready to receive data packets, the request is dropped and feedback is sent to the source node as RERR message. Upon receiving of REPP message, source may start sending the data packets using the windowing concept and hand shaking algorithm. Which means node (x) sending packets number (1) to node (y) then by updating the header information, the node (x) may wait for known time (around milliseconds) so the node (y) is now required to acknowledged the receipt of packet (1) and upon successful receipt of packet (1) node (y) may upload the header information of new message and reply back to the source node with acknowledgment number and the available size that remains empty after this packet arrival. However, every node must be programmed with particular storage tolerance (in fraction or multiplies of bits). Coming back to the point, in the case when destination node (node (y) in the example) is replied with information saying small window size is available, the source node may test the next neighbour node that can accept the next packet. Another scenario is how packets are re-classifying after the reach the destination as last packet may reach first, however, header is solving this problem as the source node is always labelling each packet of data with particular id (sequence number) that used for identifying the packet for decoding (processing) in the sink node. Figure 3.5. demonstrates the mechanism of windowing method. Header’s information is uploaded every time nodes sending the packet out, header information is guiding the destination node in the decision of next routing path. Headers may involves information about the remaining window size; as window is full, new arrival packets (if any) may form a queues where nodes can hold for some time until enough space is getting free in the destination node. Packets with priority transmission must be processed before regular packets in the queue. In our simulation, drop tail queuing is set with 1000 byte of queuing capacity.

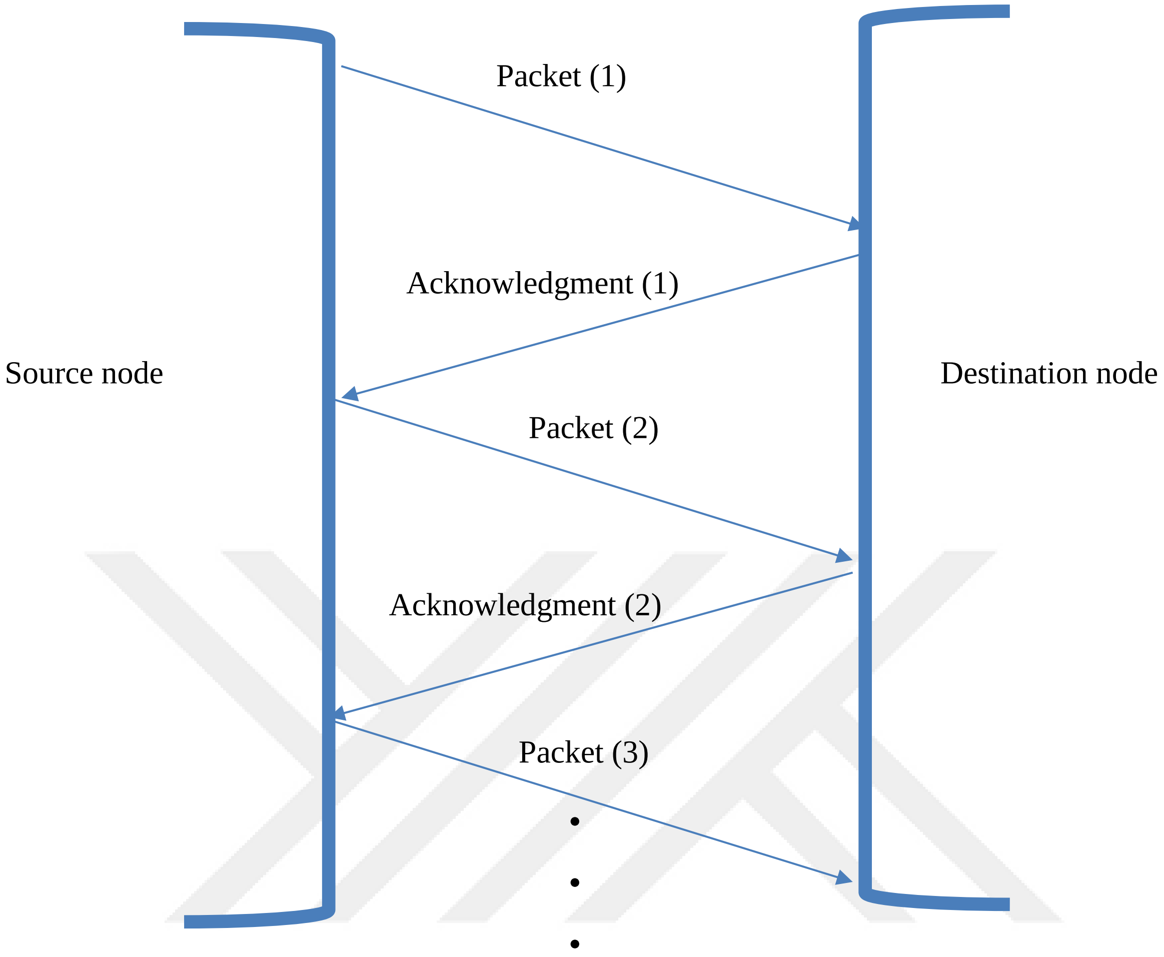

Figure 3. 7: Windowing method which used by nodes for sending the packets of temperature data.

AODV protocol is characterized in the following points:

1. Routing protocol is taking the necessary steps for migration the traffic through the network.
2. Reducing the transmitters duty by reducing the transmission streams.
3. Receivers duty mitigation as packets transition frequency is reduced.
4. Reducing the signalling information in the frame headers and then minimizing the size of the said frame.
5. Maintaining the life span of the sensors by adaptation of stringent management of the power in the network.
6. Reducing the computational cost and processing efforts.
7. Eliminate the unnecessary transmissions among the nodes.
8. Efficient utilization of network resources.

The frame overhead that is generated at the source node and propagated to the destination node is shown in figure 3.6. it involves the necessary information to facilitate the next routing decision in the destination node [28]. Whole arrived packets into particular node; along with their frames overhead may form what is so called routing table as in 3.1.

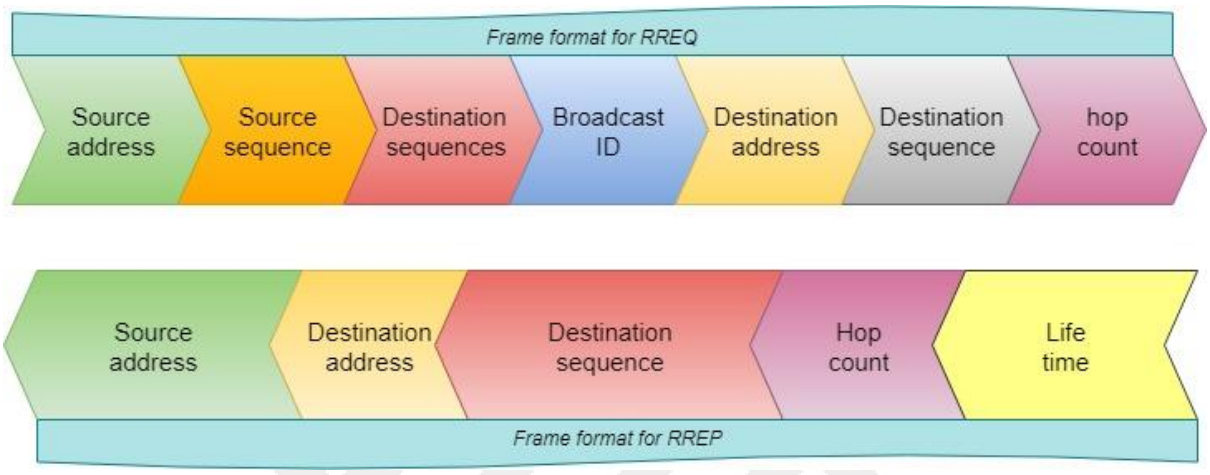

Figure 3. 8: The routing request and routing reply frame that produced by any node in WSN paradigm.

Table 3. 1: A tabulation of routing information for any particular node (routing table template).

Node ID (sent to)	Hope counter	Sent packet sequence number	Previous hops count
5	2	1004	3
0	0	0	0
15	6	1006	2
0	0	0	0

3.4 MALICIOUS ATTACKES

Wireless sensor network consisting multiple wireless sensors termed as nodes is deployed to capture the variation in some parameters in the environments such as temperature and pressure. Wireless sensors are subjected to the harsh effect of the surrounding arena due to the small immunity. Sensors unattended nature is related to their micro circuits and small power supplies where no big infrastructure is possible to be integrated on the nodes. Sensor network is initially developed for military applications and deployed in such fields where human cannot stand. For those application where demand raised from none infrastructure wireless sensor network; and security coroner is also required, there is an option to deploy the traditional wireless sensors based on IEEE 802.11 Ad-Hoc network. It is declared in the preceding section of this thesis that such kind of network is highly susceptible for clone from the unknown nodes. This security drawback raised as any node can join the network without prior acknowledgment as network traffic management is autonomously happening and no stringent administration is seen. The malicious node can take over in all network by pretending as normal node where it broadcast neighboring information to all nodes and accordingly the nearest node may forward its data through this malicious node. This procedure is known as replication where the attacker clones the network by acting friendly through creating a node with similar settings and hence it can inject the malicious credentials. The malicious data may act to copy the network information and forward it into foreign office or it may perform sabotage procedure where only dropping the packets and act against sinking of data in the server node [23]. The pure understanding of attacks mechanism is the corner stone for attack prevention [31], usually attacks can be divided into two categories:

a. **Passive attacks** (eavesdropping) in which don’t have intention and not performing any action to dispute the said network. Such attacks are merely snooping on network for gaining clue about the exchanged information.
b. **Active attacks** which have intention to degrade the performance of network and performing misbehaviors alike packets dropping. These attacks may raise due to internal penetration node.

The wireless sensor network is greatly vulnerable for several attacks such as Black Hole, Gray Hole and Sybil. However, in order to increase the network aid for the common penetrations, those three attacks will be studied extensively.

3.4.1 Black hole

It was seen in AODV routing protocol that two stages are initiated for ensuring packets propagation from source node to destination node. The process are begin with HELLO message that investigates the connectivity status between the nodes where nodes will get to know about the network topology and network coverage. Furthermore, another stage is taken by routing protocol which is traffic control such as determining the minimum and suitable path in the network, the same is performing by sharing of RREQ and RREP between the concern couple of nodes. It is important to state that two types of communications are taking place during routing which is broadcast communication in HELLO stage and unicast communication in RREQ/RREP stage. These processes are ending with rout establishment and this rout is never being a constant and keep changing depending on network traffic condition. The connection between any couple of nodes can be terminated as soon as demand raised to find faster path. That means, rout is keep upgrading as along as network is running, which is the main reason behind network penetration. Hereby, table 3.1 is now understandable since rows are resetting (zeroing) their values after every successful trade. Now the Black Hole attack is targeting the AODV routing protocol in following credentials [31]:

1. Attacker (the individual or organization who willing to clone the network) develops a node and insert it into the network. Initially, attacker have no clue about the topology also no idea about the network coverage so let us assume that location of attacking node is random. There are two sceneries (topics) that might be happening according to random allotment of attacking node: the first topic is that node located in out of network range where no risk is expected from this topic. Form the other hand, risk can only take place if and only if the attacking node is within the network coverage more likely, it located near by any node in the network.
2. Assuming the second topic is existing (point 1), the attacking node (called as Black Hole Node in this condition) is begin to overhear the network and hence it can get the topological information about the nodes of its range.
3. Routing request of fake overhead is created by this node according to the received signalling information from the network. This routing request is established after knowing the routing information from the other nodes in the network. The probable reaction to be taken by Black Hole node is to set the overhead of its routing request to the optimum values so it can fraud the nearest node. As Black Hole node snoops on the network, it works on two major parameters: the next hop and next sequence number. The next hope will be set in the request

frame as shortest hop (equal to 1) whereas the next sequence number is set according to the highest captured number in the network.

4. Frame’s parameters in the Black Hole node alike next hop could be set to minimum (equal to 1 hop) and the sequence number of the next packet is also to be set to the next number of highest snooped number.

5. As it performs the above procedure, the Black Hole node might be seen as best intermediate node to the neighbourhood. Next, it does nothing but dropping any packet as soon as it’s received from nearest node. Figure 3.7 describe in general the vital steps which is used through any malicious node to attack AODV Layer

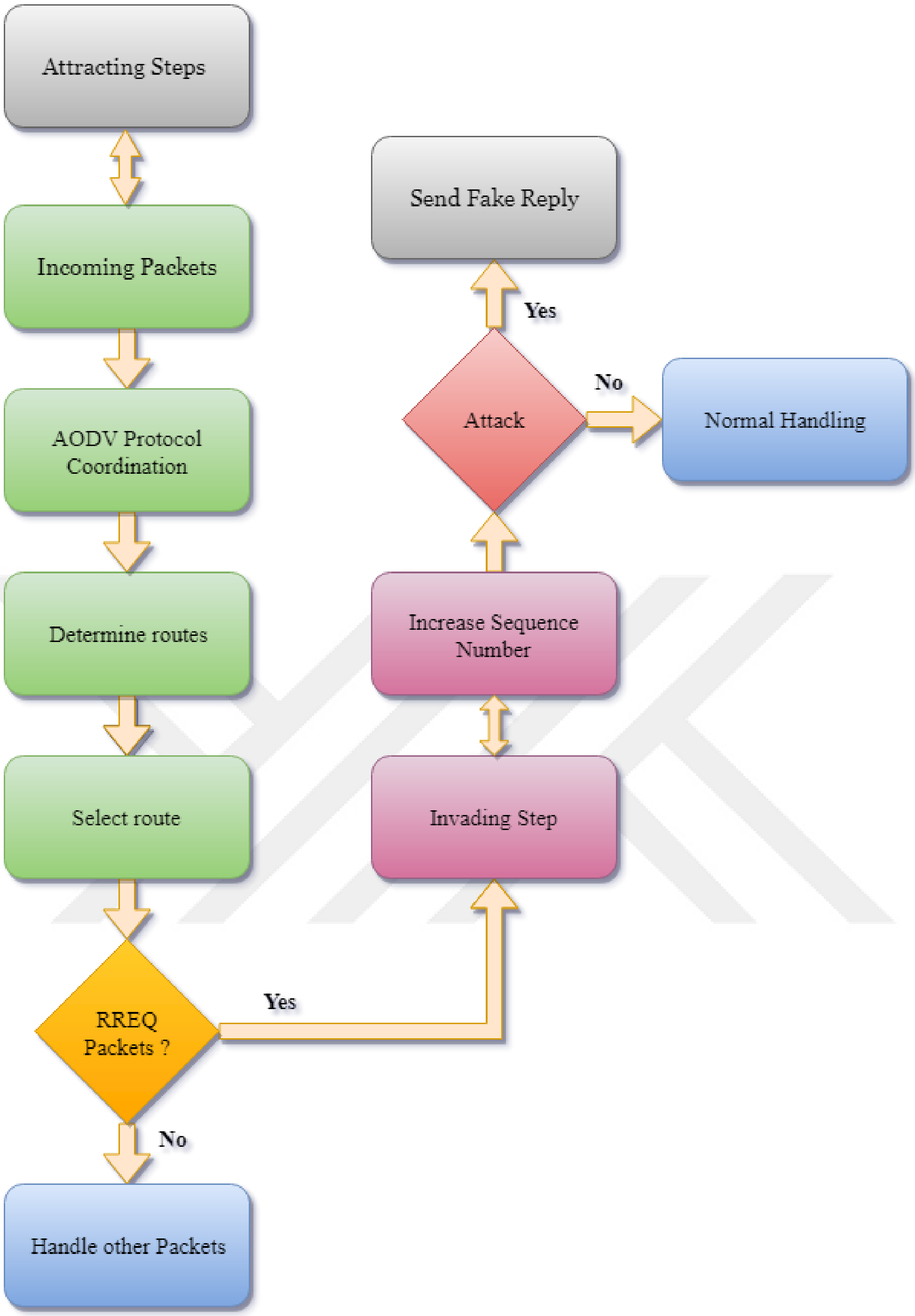

Figure 3. 9: Attack generation at AODV Layer

3.4.2 Gray Hole attack

It differs from the Black Hole Attack in its exclusive task, in the other word, if the attacker willing to target a particular node in the network then only the Gray Hole node is sent for such purpose [32]. More than a single node can anytime merge with network for damaging a wide target (in such networks of high number of nodes). Usually, Gray Hole node can target of particular packet in the stream and dropping this particular packet only. This attack can be happened by single malicious node as in figure (3.8) where this node is merely dropping particular rout in the network. Two or more consecutive nodes can work together in technology to drop a particular path in the network as in figure (3.9).

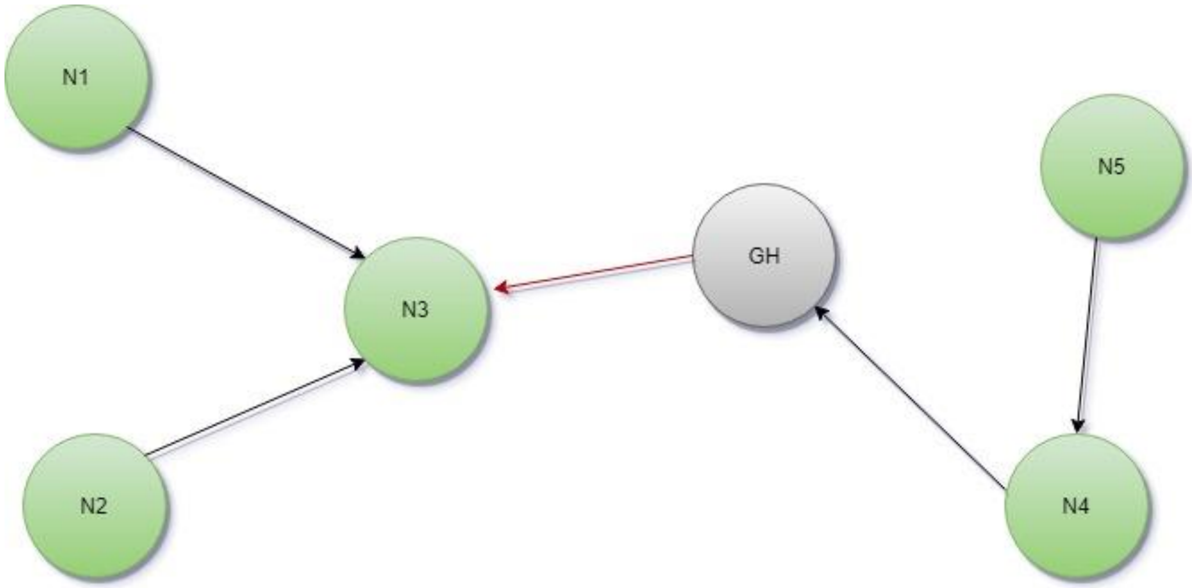

Figure 3. 10: The Diagram reveals the way of rout overtaking by Gray Hole attack in WSN.

Gray Hole attacks differs from Black Hole attacks in their selectivity and predefined mission. Figure 3.9, the Gray Hole nodes is labeled as "GH" where it locates between node (4) and node (3), it works to stop packets flowing between these nodes only.

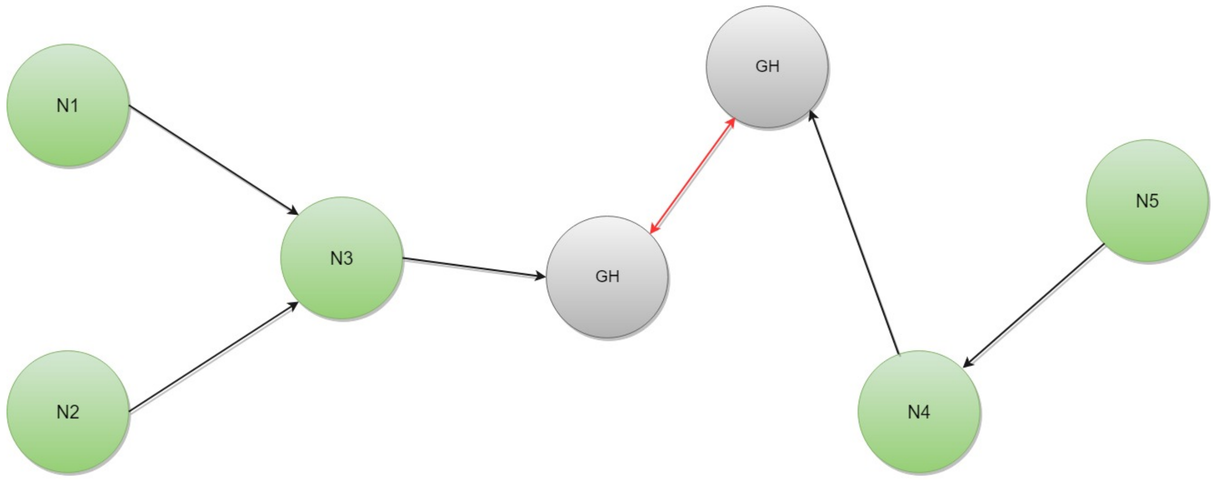

Figure 3. 11: The procedure when two consecutive Gray Hole nodes takeover the rout.

In Gray Hole attack, as packet dropping is taking place in particular path or targeting a predefined packet with known nature, the risk of this particle lies on the difficulty in identifying the victim path for initiation of defense procedure. The attack prevention technique is tough if such attack happened.

The method used by attackers to create the Gray Hole attack is similar to Black Hole as it takes place in network layer and targets the protocols of routing. The only dissimilarity in this attack is more likely their working mechanism in stage after they join the network, they e coded to perform probabilistic drop of packets so there will be no track of this attack for combating it. Furthermore, it may drop packets related to UCP process (the packets entering node) and forward the packet of TDP process (packets leaving the node). This confusion and unclassified mechanism of attack make it difficult to discover, it can perform its credentials while being hidden from the network[33].

3.4.3 Sybil attack

It seems as the hardest attack that may target the routing protocols, Sybil happens by single of multiple malicious nodes and however, the malicious node may create information such as multiple routing request that make it look like many nodes, more likely, the single Sybil node may attract several packets from multiple nodes by fabricating several identities so that, the legitimate nodes will trust and send data packets to Sybil node [33]. This attack can be a gateway for other attacks to hit the network at the same time which may pose big performance degradation. Sybil attack is processing the malicious activity by three methods or connection: when the Sybil node interacts directly (without mediator) with the victim node it calls direct communication; from the other hand when another malicious node is existing within the network, Sybil node can interact with the victim node through the malicious node, however, this called as indirect communication. Another method can by used by attackers which is done by making several identities (routing request) and fooling the legitimate nodes to pass their data through the them, the same is known as steel and fabricate IDs. If the created IDs are attacking the victim at the same time this known as simultaneous attack, whereas if attacker used the fake IDs as one by one then it called none simultaneous attack. Figure 3.10 demonstrates the Sybil attack graphically.

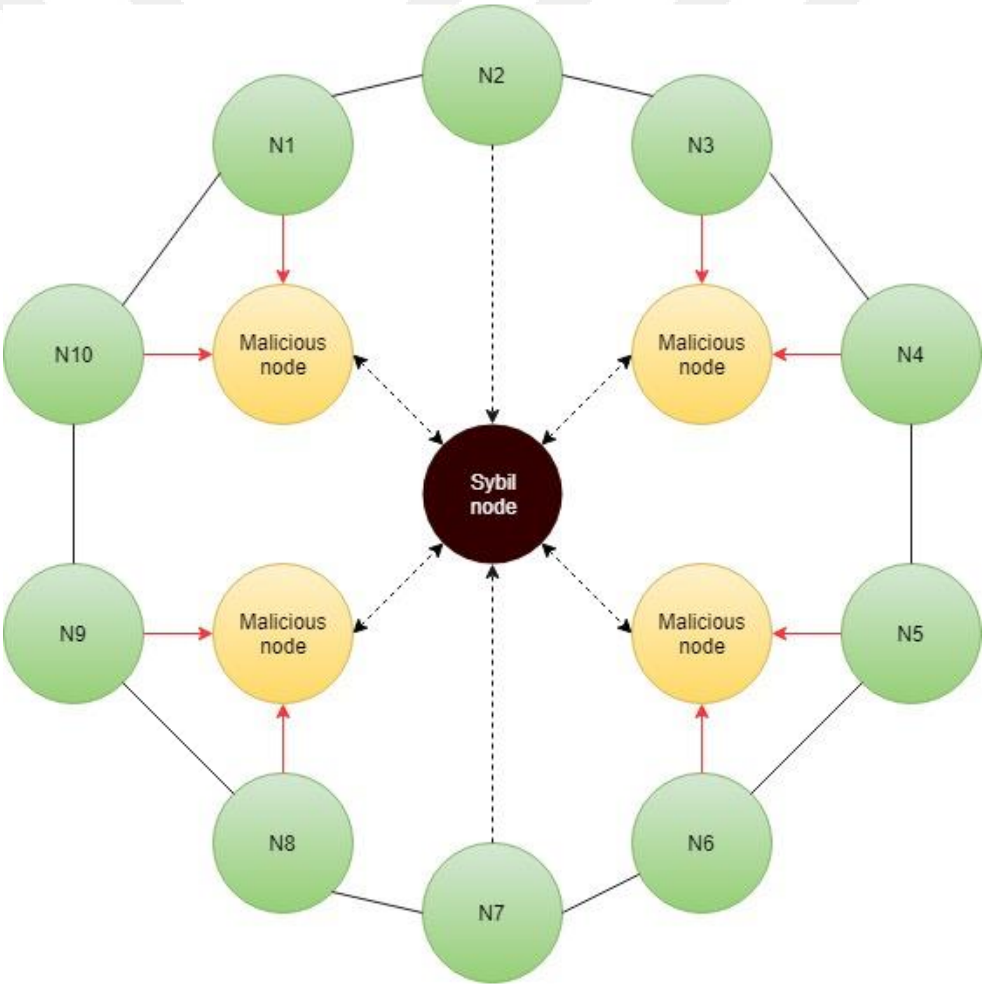

Figure 3. 12: Graphical demonstration of Sybil attacks in different kinds of connectivity

3.5 PERFORMANCE METRICS

In order to compare the performance of penetrated AODV routing protocol and none penetrated routing protocol, set of statistical calculations are made by Ad Hoc network aiming to produce the measure of network immunity for attacks. For measuring any performance in packet switching wireless network, some parameters are mostly required such as the number of packets sent by particular node to the destination through mediator nodes (gate way); the received packets that stands for the actual number of packets that reach the destination without losing their information. Other parameters are associated with this calculations such as throughput and NRL and PDF

3.5.1 Throughput

For particular simulation, the run time of the said simulation is known so that throughput can obtain using the following formula:

$$Throughput\ (avg.) = \frac{number\ of\ received\ packets}{simulation\ time} \tag{3.1}$$

3.5.2 Normalized routing load

Number of those packets that routed using the particular routing protocol (routing protocol must provide the count of actual packets it sends. This number is used to know the load in routing protocol which reflect the number of routed packets with reflect to the packets entering the queue (to be routed), question below is giving the mathematical representation of the same.

$$Normal\ Routing\ Load = \frac{number\ of\ forwarded\ packets}{number\ of\ packets\ prepared\ for\ routing} \tag{3.2}$$

3.5.3 Packet delivery fraction

This factor is calculating by knowing the actual number of delivered packets from source to destination and the number of generated packets in the source (intended number of packets to be sent to destination). The formula below is giving the value of packet delivery fraction PDF where the high value of PFD may represent the powerful routing protocol and lower value is representing weak routing process.

$$Packet\ Delivery\ Fraction = \frac{number\ of\ received\ packets}{number\ of\ sent\ packets} x\ 100\% \tag{3.3}$$

4. SIMULATION RESULTS

4.1 OVERVIEW

Simulation is set so that forty-nine nodes of wireless sensor network to capture the temperature information from 600 meter x 600 meter arena, the simulation parameters can be given in table 4.1.

Table 4. 1: Simulation parameters outline.

Particle	Description
Run time	200 s (adjustable)
Nodes topology	Manhattan grid tree sensor topology
Software	Network Simulator 2 (NS-2)
OS	Linux Ubuntu
Malicious attacks	Black Hole, Gray Hole and Sybil
Number of experiments	1300
Number of sink nodes	1
Legitimate nodes	49
Maximum load	931 packets
Communication model	IEEE 802.11
Attacking type	Network layer attacking

Simulation is established for testing the impacts of above attacks on the routing protocol. In order to study this impact, according to the dense on sensors and the simulation time, NS-2 may initiate packets count; none the less, total packets to be sent throughout the network is realized to be closer to 931 packets. The metrics of performance (section 3.5) is observed at every attack, the results are compared with no attack scenario and the following outcomes are yielded. The location of nodes in the grid is set randomly where it can dominate any location within the limit of network, known this fact, we can predict that simulation may yield different results at every restart of the simulation; for the same we made the simulation to perform 100 runs in order to achieve as accurate as possible readings.

4.2 THROUGHPUT

It measures in sink node according to equation 1, the process of finding this argument and other arguments are inbuilt with simulation scenario. Tables 4.2, 4.3 and 4.4 shows results that average throughput with Black Hole attack, Gray Hole attack and Sybil attack are 0.3275, 3.8375 and 0.74 respectively. The optimum results have seen in the case of Grey Hole attack which yields 6.31 due to their mechanism to drop particular packets in the network by adopting specific fashion of dropping.

Table 4. 2: Results of throughput in Black Hole attack with different number of malicious nodes.

No Mal. Nodes	Sent Packets	Received Packets	Throughput
1	931	109.52	0.46
2	931	86.58	0.36
3	931	67.91	0.28
4	931	49.88	0.21
Avg.	**931**	**78.4725**	**0.3275**

Table 4. 3: Results of throughput in Gray Hole attack with different number of malicious nodes.

No Mal. Nodes	Sent Packets	Received Packets	Throughput
1	931	922.72	3.84
2	931	923.32	3.84
3	931	921.01	3.83
4	931	922.11	3.84
Avg.	**931**	**922.29**	**3.8375**

Table 4. 4: Results of throughput in Sybil attack with different number of malicious nodes.

No Mal. Nodes	Sent Packets	Received Packets	Throughput
1	931	284.63	1.18
2	931	174.53	0.73
3	931	126.97	0.53
4	931	124.01	0.52
Avg.	**931**	**177.535**	**0.74**

4.3 PDF AND NRL

The packet delivery fraction and the normalized routing load are descried in sections 3.5.2 and 3.5.3. however, the results obtained from the experiments for Black Hole attack are given in table 4.5.

Table 4. 5: NRL and PDF obtained at present of Black Hole nodes.

No Mal. Nodes	Sent Packets	Received Packets	PDF	NRL
1	931	109.52	11.76	466.23
2	931	86.58	9.30	497.54
3	931	67.91	7.30	522.74
4	931	49.88	5.36	650.07
Avg.	**931**	**78.4725**	**8.43**	**534.145**

While the results of packet delivery fraction and the normalized routing load for Grey hole and Sybil attacks are given in tables 4.6 and 4.7.

Table 4. 6: NRL and PDF obtained at present of Gray Hole nodes.

No Mal. Nodes	Sent Packets	Received Packets	PDF	NRL
1	931	922.72	99.11	3.11
2	931	923.32	99.18	3.18
3	931	921.01	98.93	3.26
4	931	922.11	99.04	3.32
Avg.	**931**	**922.29**	**99.065**	**3.2175**

Table 4. 7: NRL and PDF obtained at present of Sybil nodes.

No Mal. Nodes	Sent Packets	Received Packets	PDF	NRL
1	931	284.63	30.57	421.10
2	931	174.53	18.75	288.61
3	931	126.97	13.64	204.96
4	931	124.01	13.32	412.23
Avg.	**931**	**177.535**	**19.07**	**331.725**

Now if we combine all the above tables with its results in one table for all performance metrics with different malicious nodes during all attacks in 1300 iterations for placement of malicious nodes, we can get the table 4.8 below.

Table 4. 8: Comparison of average for PDF, NRL, throughput and received packets at sink during all attacks

Attacks	Total Iterations	No. of Malicious nodes	Sent Packets	Received Packets at Sink	PDF	Throughput	NRL
No Attack	100	Average	931	923.83	99.23	3.84	2.98
Gray Hole attack	100	1	931	922.72	99.11	3.84	3.11
	100	2	931	923.32	99.18	3.84	3.18
	100	3	931	921.01	98.93	3.83	3.26
	100	4	931	922.11	99.04	3.84	3.32
	400	Average	931	922.29	99.065	3.8375	3.2175
Sybil attack	100	1	931	284.63	30.57	1.18	421.1
	100	2	931	174.53	18.75	0.73	288.61
	100	3	931	126.97	13.64	0.53	204.96
	100	4	931	124.01	13.32	0.52	412.23
	400	Average	931	177.535	19.07	0.74	331.725
Black Hole attack	100	1	931	109.52	11.76	0.46	466.23
	100	2	931	86.58	9.3	0.36	497.54
	100	3	931	67.91	7.3	0.28	522.74
	100	4	931	49.88	5.36	0.21	650.07
	400	Average	931	78.4725	8.43	0.3275	534.145

Comparing the impacts of malicious attacks of the above results with none attack scenario, we can plot the following graphs. we can represent the comparison between the attacks in terms of throughput, PDF and NRL with respect to number of attacking nodes. The packet delivery at distention can be plotted at presence of single malicious node for all the attacks can be seen in figure 4.1 below.

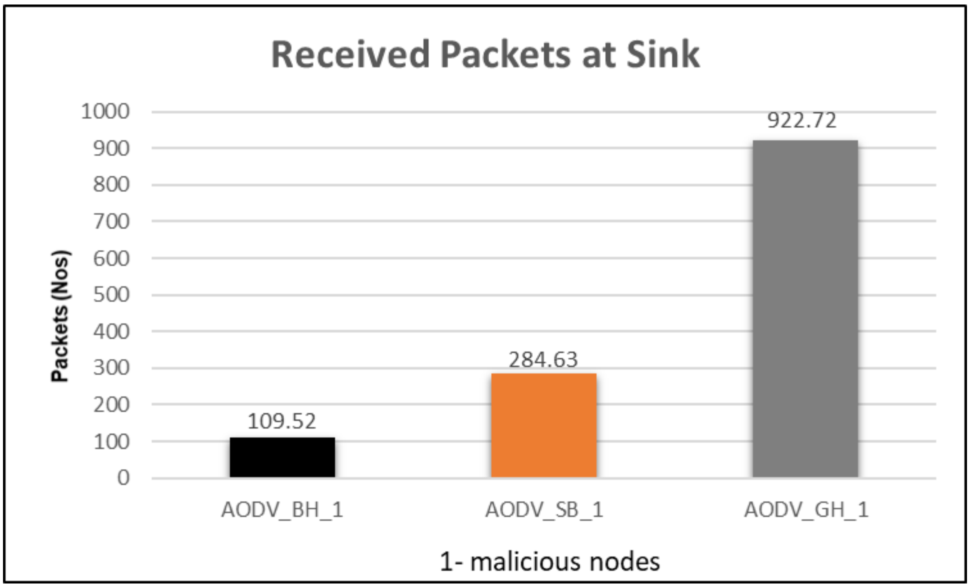

Figure 4. 1: Packets delivery at the sink with single malicious node in all attacks.

The throughput, PDF and NRL can be monetarized for all attacks with single malicious nodes presence, the same is given in figures 4.2, 4.3 and 4.4 below.

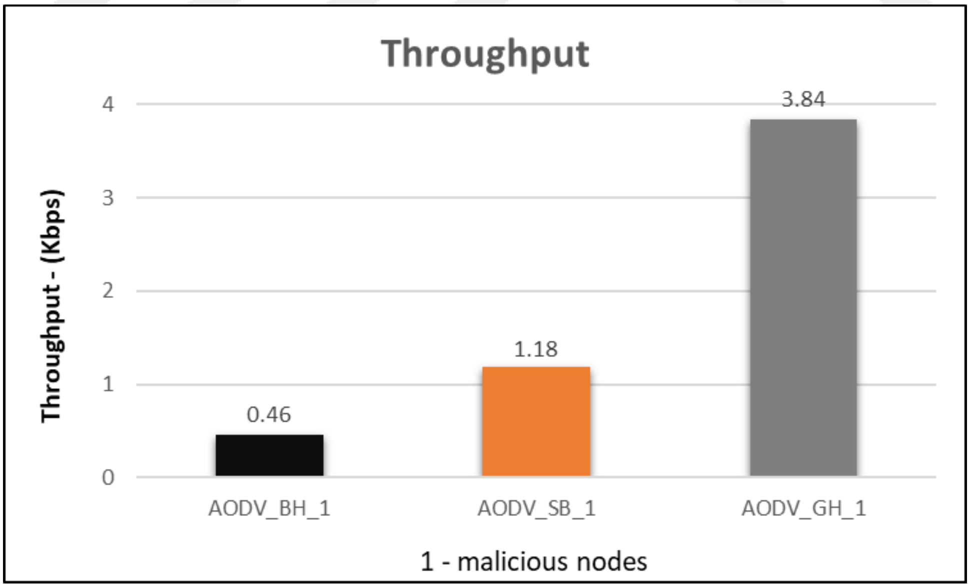

Figure 4. 2: Throughput with single malicious node in all attacks.

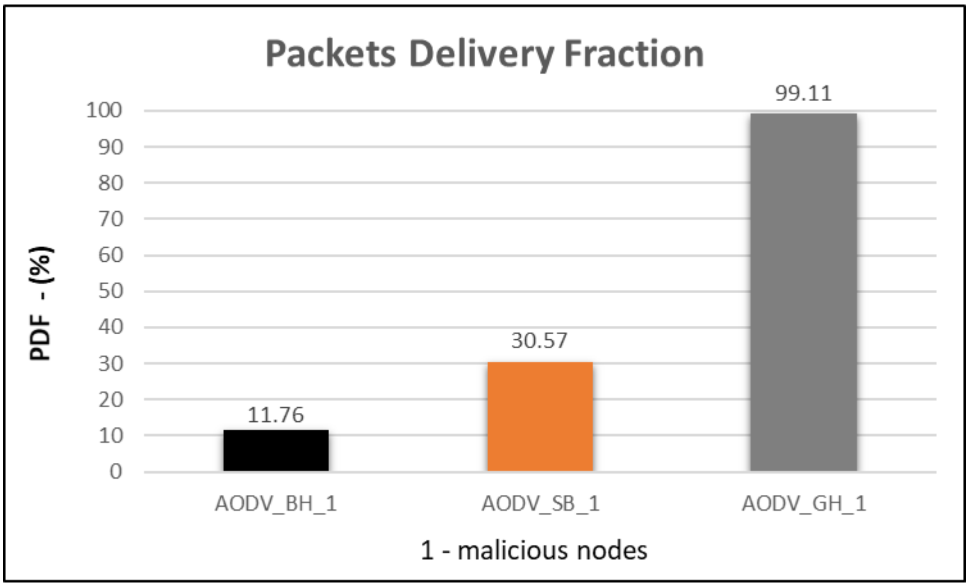

Figure 4. 3: PDF with single malicious node in all attacks.

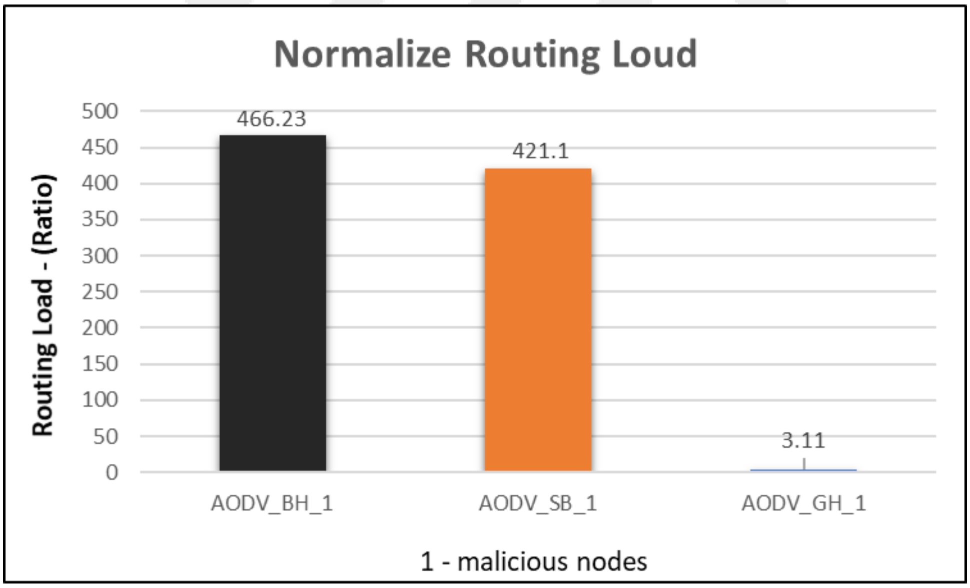

Figure 4. 4: NRL with single malicious node in all attacks.

The same can be repeated for two, three and four malicious nodes and results are graphically given in figures 4.5 through 4.16 thereafter.

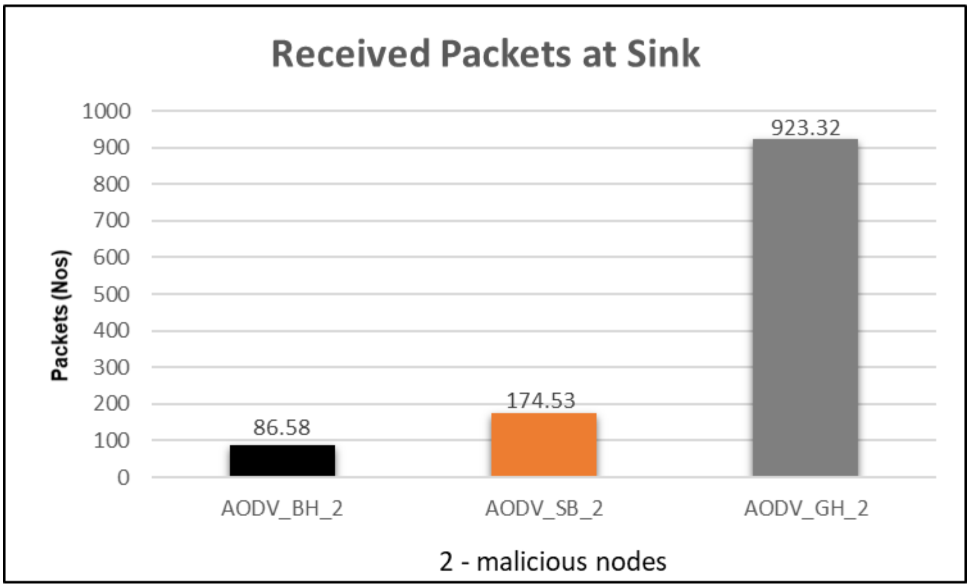

Figure 4. 5: Packets delivery at the sink with two malicious nodes in all attacks.

The Figure 4.5 and 4.6 shows the effect of tow malicious nodes attack on Received Packets at Sink and reflect high packets drop in blackhole while the throughput indicates a good performance with grayhole attack and the worse with black hole then Sybil.

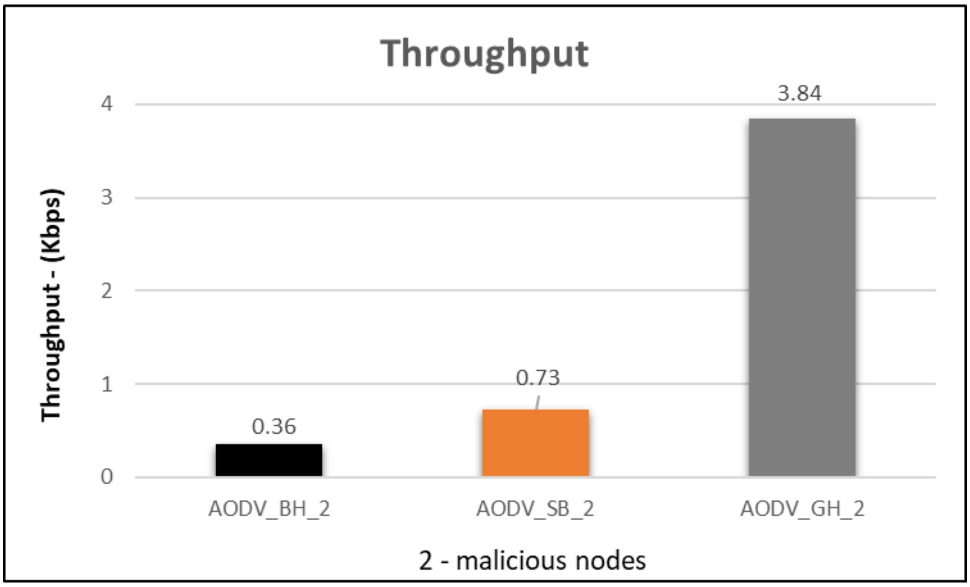

Figure 4. 6: Throughput with two malicious nodes in all attacks.

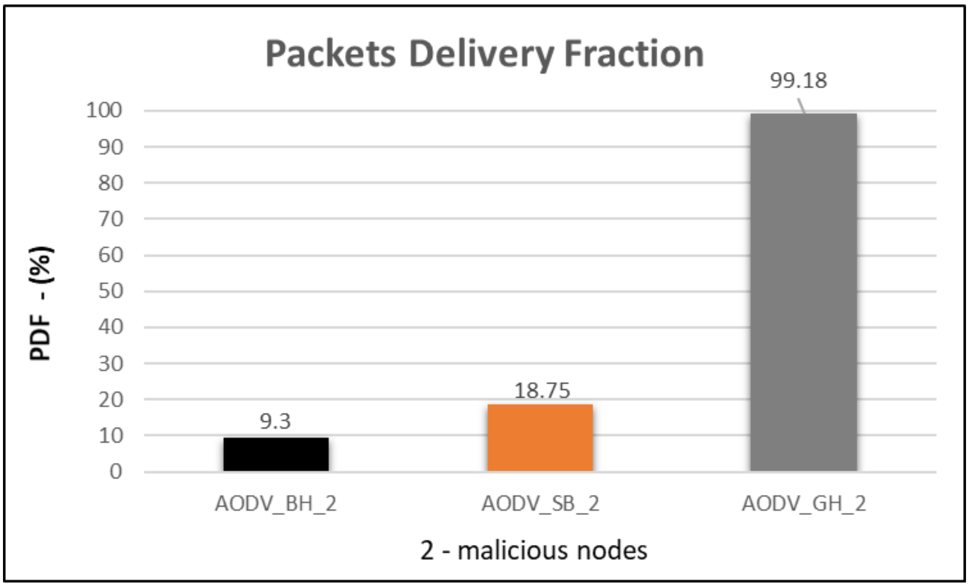

Figure 4. 7: PDF with two malicious nodes in all attacks.

For the PDF metrics in figure 4.7 we find out big mess in blockhole attack then sybil. While we find the NRL ratio in figure 4.8 with two malicious nodes increased which reflect a bad performance in the network.

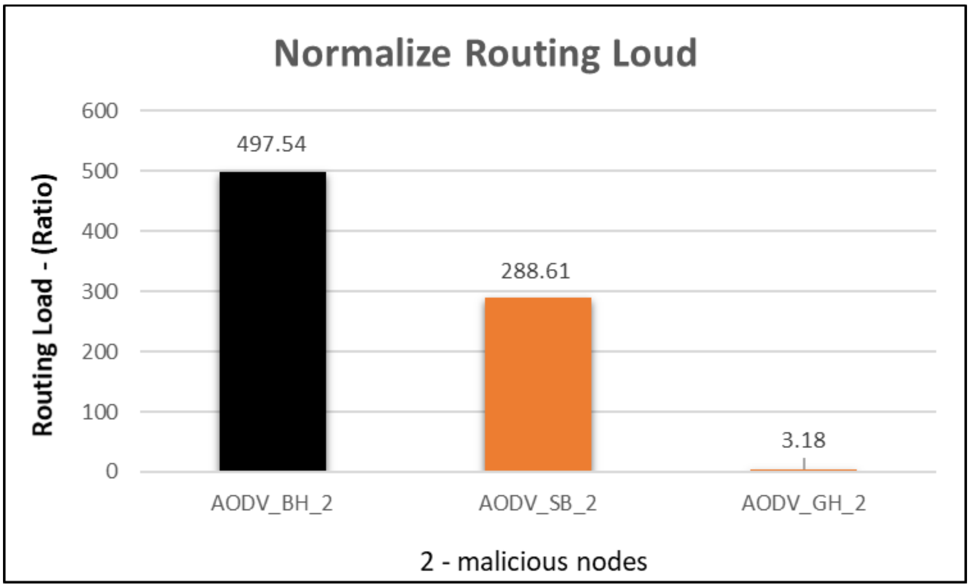

Figure 4. 8: NRL with two malicious nodes in all attacks.

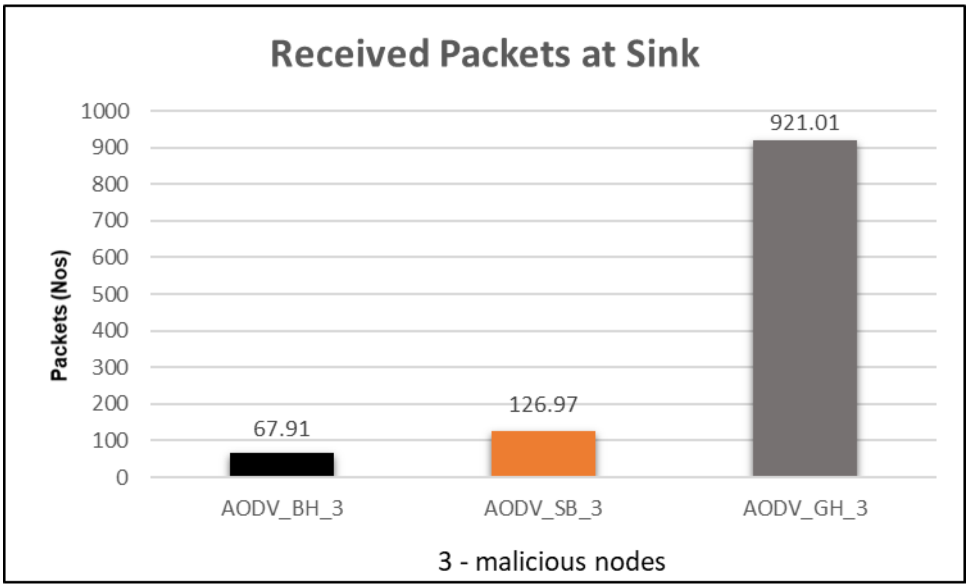

Figure 4. 9: Packets delivery at the sink with three malicious nodes in all attacks.

In figure 4.9 we noticed the highest drop packets at sink with three malicious nodes happened in black hole while in gray hole there is no noticeable change if we compare it with no attack. for the figure 4.10 the better performance is in gray hole and this in contrary with blackhole and sybil attack.

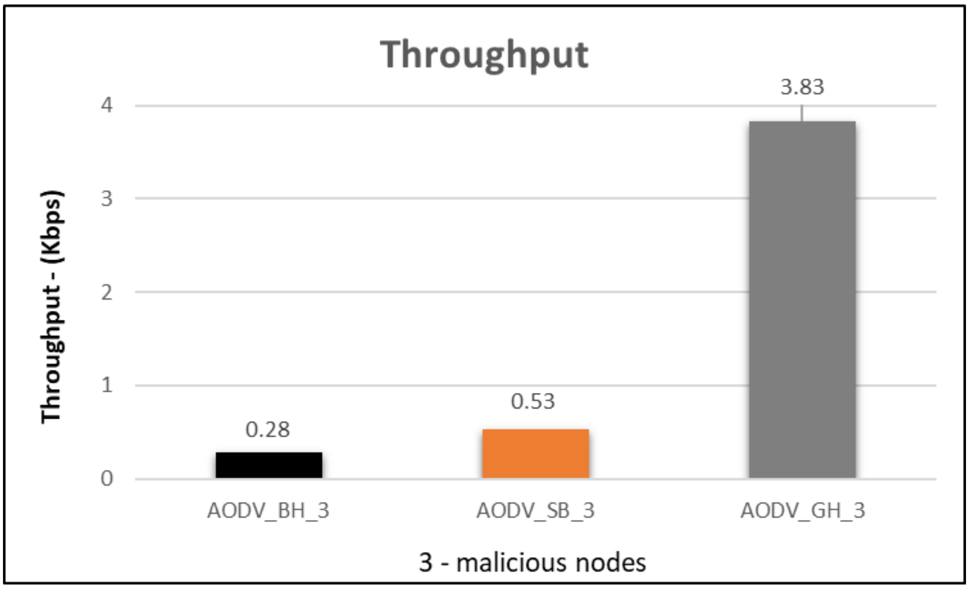

Figure 4. 10: Throughput with three malicious nodes in all attacks.

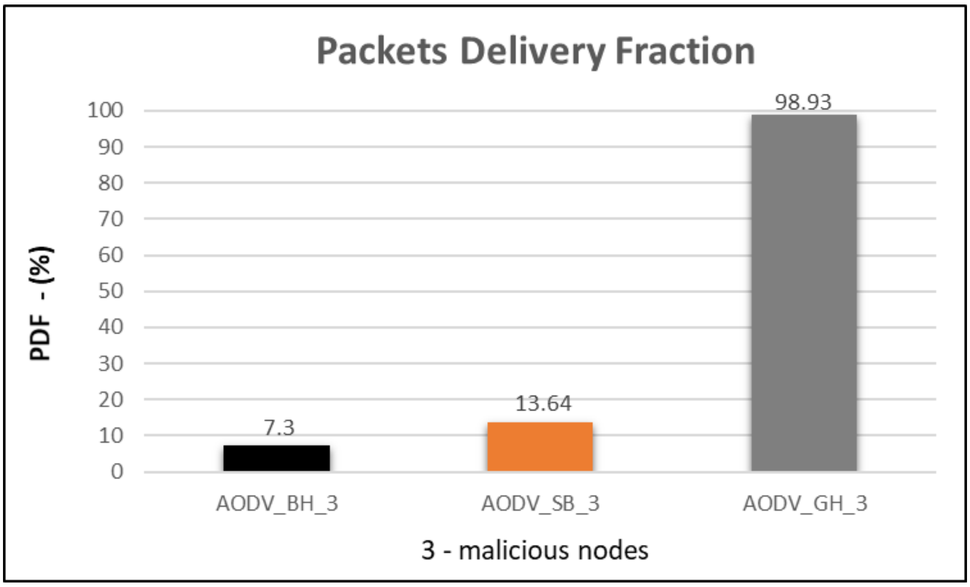

Figure 4. 11: PDF with three malicious nodes in all attacks.

In figure 4.11 the highly rate of packet dropping is high and approximately equal for black and sybil attack with four malicious nodes attacks. While in grayhole the drooping rate optimum to 98.93 which the minimum comparing with the previous states. In figure 4.12 the NRL draw the worst performance with three malicious attack in black hole and sybil while in gray the ratio is minimum with 3.28.

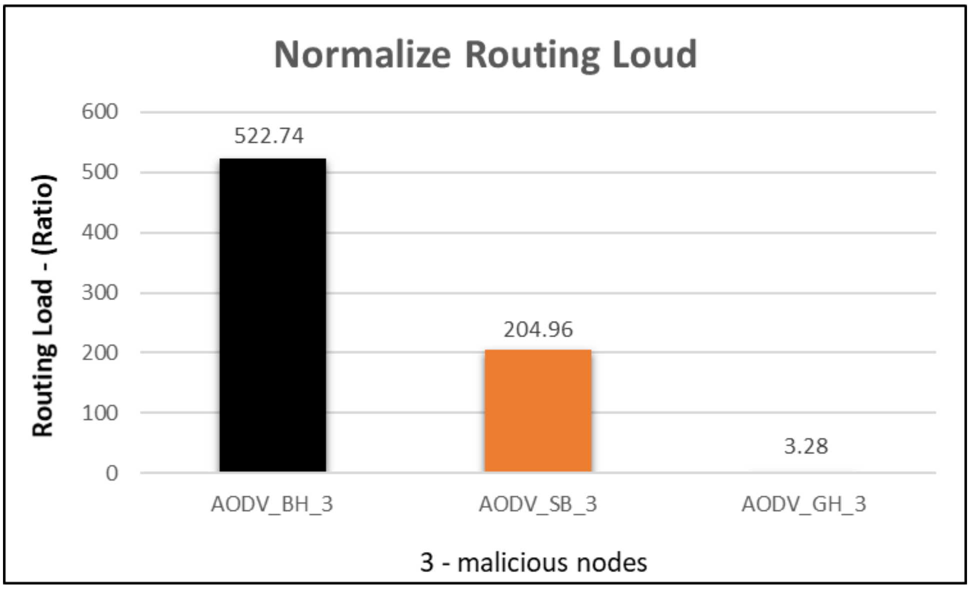

Figure 4. 12: NRL with three malicious nodes in all attacks.

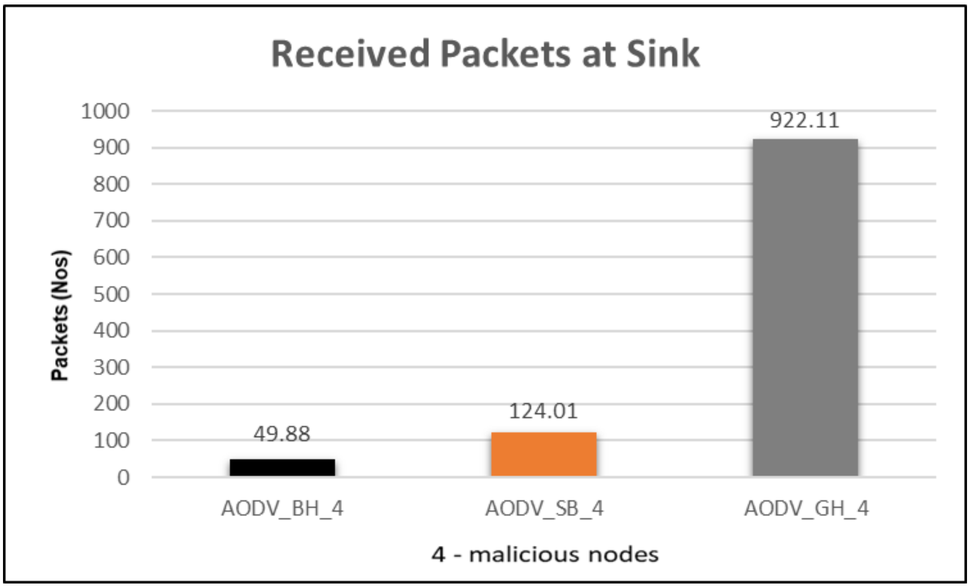

Figure 4. 13: Packets delivery at the sink with four malicious nodes in all attacks.

In figure 4.13 we noticed increasing the malicious node will lead to high packets drops in Sybil and black hole attack. For grayhole we found a big resistance for increasing the malicious nodes which lead too little affect. Figure 4.14 and 4.15 we see a good performance in gray hole according to throughput and PDF values which optimum to (3.84), (99.04).

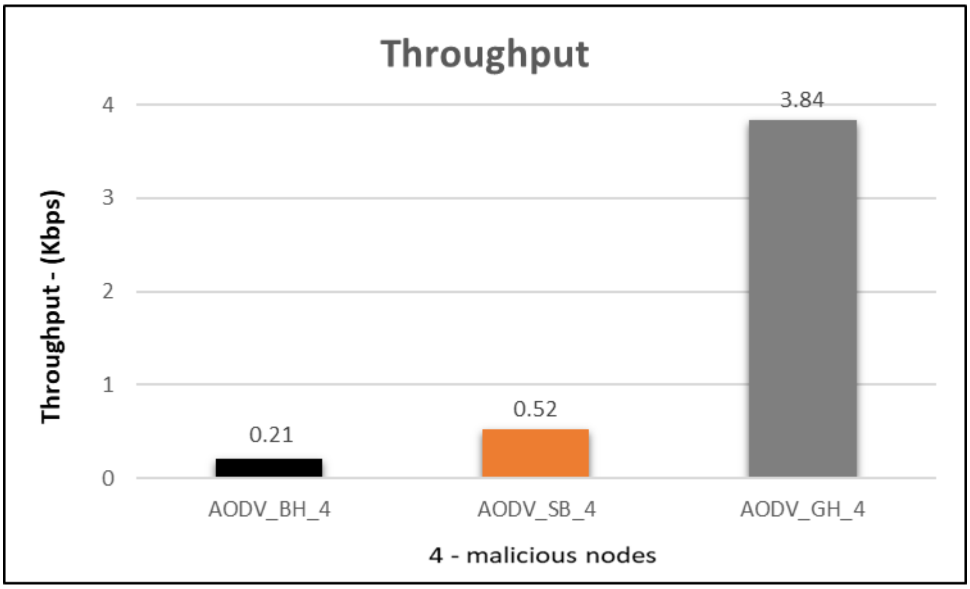

Figure 4. 14: Throughput with four malicious nodes in all attacks.

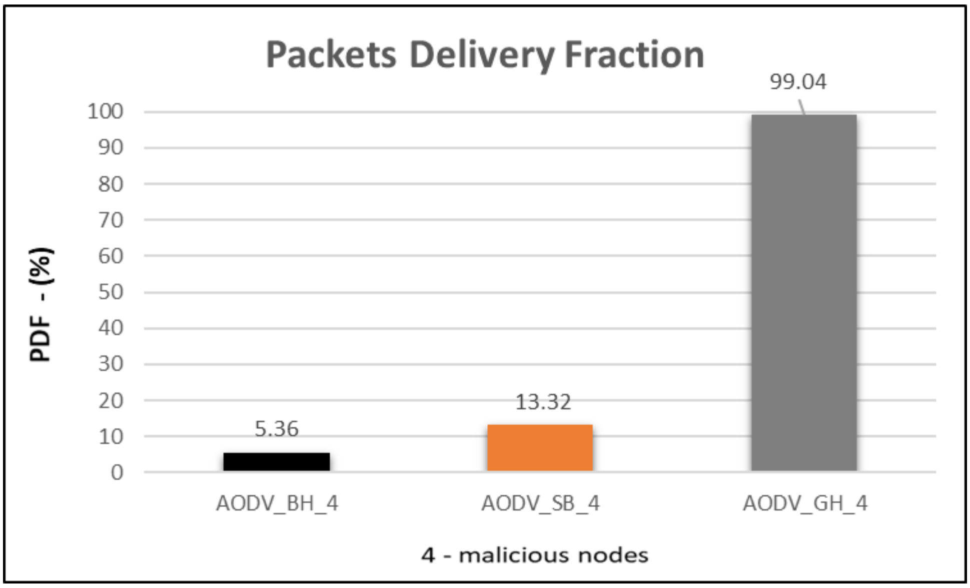

Figure 4. 15: PDF with four malicious nodes in all attacks.

Figure 4.16 implies that NRL ratio is high and still high even with decreasing malicious nodes while in blackhole the situations different. The NRL increasing gradually by increasing malicious nodes and we see it's not that change in value of ratio if we compare it to zero malicious attack.

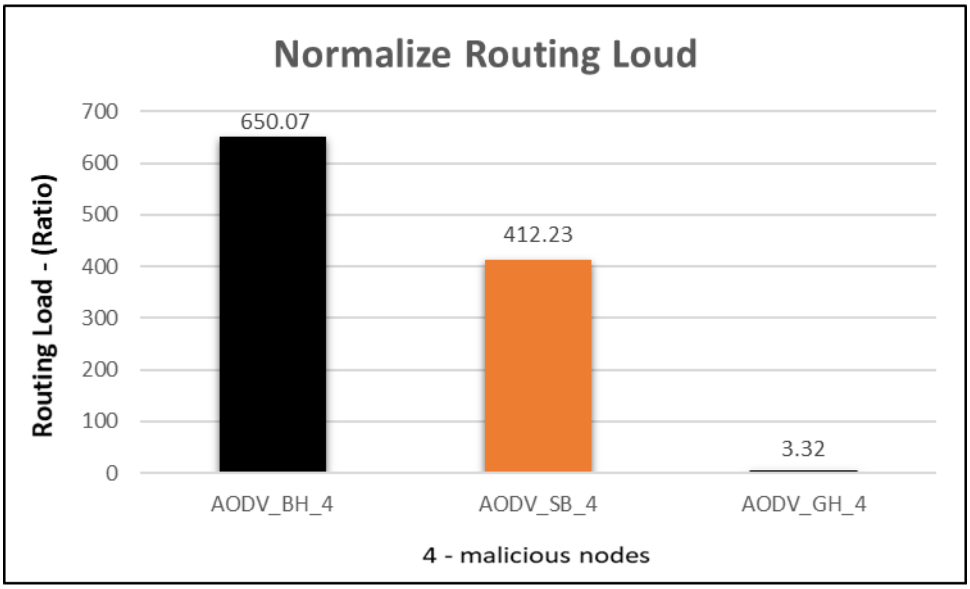

Figure 4. 16: NRL with four malicious nodes in all attacks.

For 1, 2, 3 and 4 nodes the impact of that comparable with no attack stage counted for throughput, PDF and NRL (all in average) are given in figure 4.17 through 4.19.

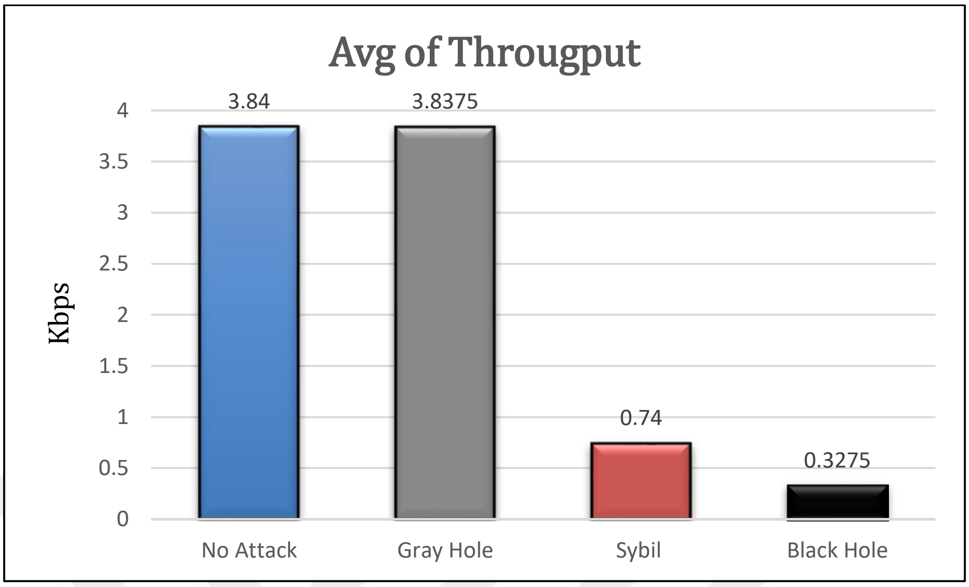

Figure 4. 17: The comparison of average throughput of different numbers of malicious nodes during all attacks.

The comparison in figure 4.17 and 4.18 shows that the highest values for throughput and PDF in grayhole attack and reflect the better performance. While the worst performance is for black hole then sybil attack which have the minimum average values for PDF and throughput.

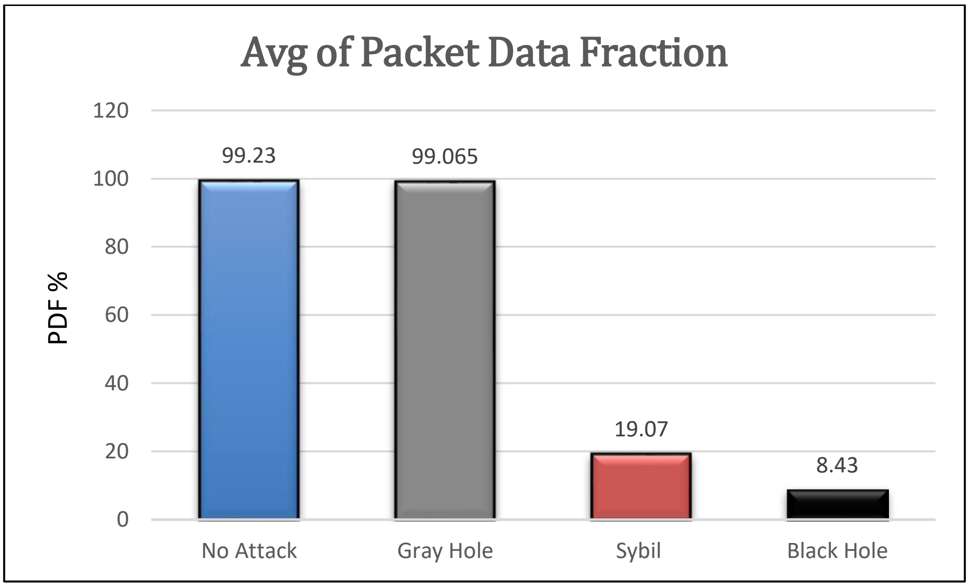

Figure 4. 18: The comparison of average PDF of different numbers of malicious nodes during all attacks.

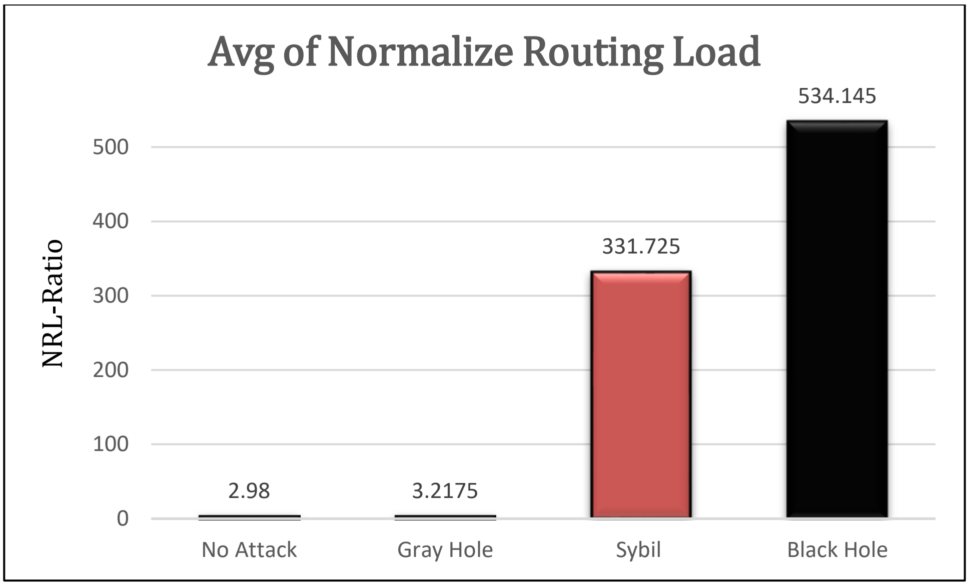

Figure 4. 19: The comparison of average NRL of different numbers of malicious nodes during all attacks.

The figure 4.19 demonstrates that NRL metric average ratio is the highest in black hole attack which imply a big mess in the network, and this is similar to Sybil attack which ratio is optimum to (331.725) for sybil and (534.145) for blockhole attack. We find also that is no change on NRL ratio for grayhole if we compare it with average of no attack. The average of received packets to the destination in all cases are plotted in figure 4.20 and imply highly dropping in blackhole and sybil attacks while the minimum dropping in grayhole attack.

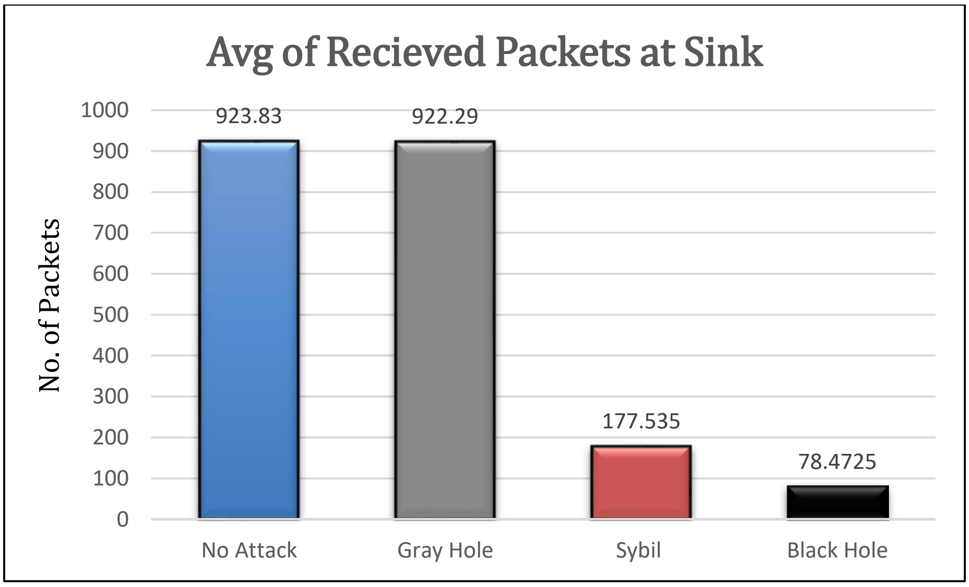

Figure 4. 20: The delivered packets at destination node for all cases.

4.4 RESULTS DISCUSSION

The following observations are made based on the outcomes of these experiments:

1. With more density of Black Hole node, the performance of packet delivery fraction is not degrading as single black hole node is drawing biggest mess in PDF.
2. With Sybil node deployment, the high density of attacking nodes may worsen the performance of packet delivery fraction.
3. At Grayhole attack, there is no sensible impact notice by varying the node’s densities.
4. The throughput is degraded by deploying smaller number of Sybil or Gray Hole nodes.
5. In some traffic conditions, big density of Black Hole nodes may trip the performance of throughput to its worse level.
6. At Grayhole attack, we noticed the largest delivery of packets at sink node 922.29 out of 913 packets.
7. Normalized routing load is optimum (equal to 534.145) with Black Hole attack comparable with no attack condition and other attacks as well..
8. Average packet delivery fraction is optimum with Grayhole attack (equal to 99.065) as compared to no attack condition and other attacks as well..
9. Average throughput in case of Garyhole attack is optimum (equal to 3.8375) as compared to no attack condition and other attacks as well.
10. Grayhole attack is found to be the lesser malfunctioning attack that could hit wireless sensor network or our paradigm.

5. CONCLUSION

In this Thesis, wireless sensor network is fabricated to perform the temperature sensing in particular atmospheres involving arena of 600 by 600 sqm dimensions. The sensors are located to be more likely forming a shape of Manhattan grid with seven rows and seven columns of wireless nodes, all of these nodes are required to report to a single sink node located at the farthest side of the grid. Simulation of the above network was done using MANASIM tool integrated with Network Simulator 2 software in the Linux operation system. Three attacks are established for targeting the network layer of IEEE 802.11 Ad-Hoc network, Black Hole, Gray Hole and Sybil attacks are individually examined on the same network. The simulation is made by MANASIM tool in Network Simulator 2, simulation is first started with single malicious node and proceeded till four malicious nodes. Hence, every malicious attack is designed to harm the AODV routing protocol more likely, all three different attacks is firstly snooping on the nodes broadcasting and keep track of each node requirement, hereafter, in Black Hole attack the attacker node is acting as mediator between the source node and destination node and hence it drops the content fully as it gets in effect. The Sybil attack is also snooping on the network and create a multiple malicious node and try to fool more legitimate nodes, as a result of this, the Sybil attack form the biggest risk on the network as more data dropping can take place due to group of malicious nodes existence. From the other hand, Gray Hole attack is seen to have the lesser negative impacts on the network, this is due to their standard mechanism of dropping particular (selected) packets in random fashion where the malicious node can not be discovered easily due to their randomness behaviors. The outcomes of this study imply that routing protocols are vital to the sustainability of the wireless sensor networks because of their roles of controlling the packets transmission and power control. Since the none infrastructure wireless sensor networks are more deployable at engineering fields, a stringent routing mechanism should be adopted for best utilization. AODV is the most popular routing protocol in Ad-Hoc network and more subjectable to malicious attacks, for the same reason, this study was established to identify the impact of above attacks on this protocol. for different number of malicious nodes, the impact on data dropping is seemed un predictable as revealed by our prototype. The negative effects of malicious nodes may vary according to their location and density in the network.

REFERENCES

[1] M. U. H. Al Rasyid, D. Prasetyo, I. U. Nadhori, and A. H. Alasiry, “Mobile monitoring of muscular strain sensor based on Wireless Body Area Network,” *Proc. - 2015 Int. Electron. Symp. Emerg. Technol. Electron. Information, IES 2015*, pp. 284–287, 2016.

[2] K. Mikhaylov, J. Petajajarvi, M. Makelainen, A. Paatelma, and T. Hanninen, “Live demonstration: Modular multi-radio wireless sensor platform with plug&play modules connection,” *2015 IEEE SENSORS - Proc.*, p. 1, 2015.

[3] M. Demaria, A. R. De La Concepcion, R. Stefanelli, and D. Trinchero, “An efficient platform for low-power, high-definition Multimedia Wireless Sensor Nodes,” *WiSNet 2016 - Proceedings, 2016 IEEE Top. Conf. Wirel. Sensors Sens. Networks*, pp. 38–40, 2016.

[4] E. Pievanelli, A. Plesca, R. Stefanelli, and D. Trinchero, “Dynamic wireless sensor networks for real time safeguard of workers exposed to physical agents in constructions sites,” *WiSNet 2013 - Proc. 2013 IEEE Top. Conf. Wirel. Sensors Sens. Networks - 2013 IEEE Radio Wirel. Week, RWW 2013*, pp. 55–57, 2013.

[5] M. Razfar *et al.*, “Wireless network design and analysis for real time control of launch vehicles,” *IEEE Int. Conf. Wirel. Sp. Extrem. Environ. WiSEE 2013 - Conf. Proc.*, pp. 1–2, 2013.

[6] X. Liu, P. Hu, and F. Li, “A street lamp clustered-control system based on wireless sensor and actuator networks,” *Proc. World Congr. Intell. Control Autom.*, pp. 4484–4489, 2012.

[7] “WIRELESS CHEMICAL SENSORS J. Garcia-Canton, L. Moreno, C. Jimenez, A. Merlos, and A. Baldi Centro Naconal de Microelectrónica (CNM-IMB, CSIC), E-08193 Bellaterra (Barcelona), Spain,” pp. 1903–1906, 2007.

[8] M. C. Scardelletti *et al.*, “Wireless capacitive pressure sensor operating up to 400??c from 0 to 100 psi utilizing power scavenging,” *WiSNet 2014 - Proc. 2014 IEEE Top. Conf. Wirel. Sensors Sens. Networks*, pp. 34–36, 2014.

[9] H. H. Yen, “Novel visual sensor deployment algorithm in PTZ wireless visual sensor networks,” *Proceedings, APWiMob 2014 IEEE Asia Pacific Conf. Wirel. Mob. 2014*, vol. 1, pp. 214–218, 2014.

[10] C. M. Caffrey, J. Flak, I. Marttila, N. Pesonen, and P. Pursula, “Development of a Reader Device for Fully Passive Wireless Sensors,” pp. 2–4, 2017.

[11] K. Fukuda *et al.*, “Transmit control and data separation in physical wireless parameter conversion sensor networks with event driven sensors,” *2018 IEEE Top. Conf. Wirel. Sensors Sens. Networks*, pp. 12–14, 2018.

[12] A. Berger, A. Pötsch, and A. Springer, “Real-time data collection in a spatially extended TDMA-based wireless sensor network,” *RWW 2012 - Proc. 2012 IEEE Top. Conf. Wirel. Sensors Sens. Networks, WiSNet 2012*, pp. 41–44, 2012.

[13] V. C. Woelk, “Innovative Loesungen fuer dezentrale WaermeDirektService Projekte,” *Euroheat Power/Fernwarme Int.*, vol. 29, no. 1, p. 65, 2000.

[14] Y. Nishikawa *et al.*, “Design of stable wireless sensor network for slope monitoring,” *WiSNet 2018 - Proc. 2018 IEEE Top. Conf. Wirel. Sensors Sens. Networks*, vol. 2018–Janua, pp. 8–11, 2018.

[15] C. G. Qian and W. Y. Cai, “The design and implementation of video wireless WIFI sensor nodes with the function of air targets detection,” *Proc. - 2014 Int. Conf. Wirel. Commun. Sens. Network, WCSN 2014*, pp. 222–225, 2014.

[16] J. Dowling and M. M. Tentzeris, “‘Smart house’ and ‘Smart-energy’ applications of low-power RFID-based wireless sensors,” *APMC 2009 - Asia Pacific Microw. Conf. 2009*, no. x, pp. 2412–2415, 2009.

[17] L. Cisoni and D. Trinchero, “An efficient technique for the design of miniaturized wireless sensors within liquids,” *2011 IEEE Radio Wirel. Week, RWW 2011 - 2011 IEEE Top. Conf. Wirel. Sensors Sens. Networks, WiSNet 2011*, pp. 45–48, 2011.

[18] L. Dong, L. F. Wang, Q. Y. Ren, and Q. A. Huang, “Mutual inductance suppressed stacked inductors for passive wireless multi-parameter sensors,” *Proc. IEEE Sensors*, vol. 2014–Decem, no. December, pp. 926–929, 2014.

[19] J. Hayes, S. Beirne, K. T. Lau, and D. Diamond, “Evaluation of a low cost wireless chemical sensor network for environmental monitoring,” *Proc. IEEE Sensors*, pp. 530–533, 2008.

[20] A. Jangra, Swati, Priyanka, and Richa, “Wireless Sensor Network (WSN): Architectural Design issues and Challenges,” *Int. J. Comput. Sci. Eng.*, vol. 02, no. 09, pp. 3089–3094, 2010.

[21] R. M. Pereira, L. Beatrys Ruiz, L. H. C. Davantel, and T. R. D. M. Braga Silva, “PowerMannaSim: An extension with power consumption modeling to MannaSim, a Wireless Sensor Network module of NS-2,” *Proc. - IEEE Symp. Comput. Commun.*, vol. 2016–Febru, pp. 949–955, 2016.

[22] R. P.N, “Analysis on Ad Hoc Routing Protocols in Wireless Sensor Networks,” *Int. J. Ad hoc, Sens. Ubiquitous Comput.*, 2012.

[23] W. Naruephiphat, Y. Ji, and C. Charnsripinyo, “An area-based approach for node replica detection in wireless sensor networks,” in *Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012*, 2012.

[24] D. S. Patil and S. C. Patil, “A Novel Algorithm for Detecting Node Clone Attack in Wireless Sensor Networks,” *2017 Int. Conf. Comput. Commun. Control Autom.*, pp. 1–4, 2017.

[25] M. M. Singh, A. Singh, and J. K. Mandal, “Preventing node replication attack in static Wireless Sensor Netwroks,” *Proc. - 2014 3rd Int. Conf. Reliab. Infocom Technol. Optim. Trends Futur. Dir. ICRITO 2014*, pp. 1–5, 2015.

[26] M. Tripathi, M. S. Gaur, and V. Laxmi, “Comparing the impact of black hole and gray hole attack on LEACH in WSN,” in *Procedia Computer Science*, 2013.

[27] K. Singh, A. Boparai, V. Handa, and S. Rani, “Performance analysis of security attacks and improvements of routing protocols in MANET,” *2015 2nd Int. Conf. Comput. Sci. Comput. Eng. Soc. Media, CSCESM 2015*, pp. 163–169, 2015.

[28] M. Salehi, A. Boukerche, and A. Darehshoorzadeh, “Modeling and performance evaluation of security attacks on opportunistic routing protocols for multihop wireless networks,” *Ad Hoc Networks,* vol. 50, pp. 88–101, 2016.

[29] R. W. Anwar, M. Bakhtiari, A. Zainal, and K. N. Qureshi, “Wireless Sensor Network Performance Analysis and Effect of Blackhole and Sinkhole Attacks,” *J. Teknol.*, vol. 78, no. 4–3, 2016.

[30] T. Jamal and S. A. Butt, “Malicious node analysis in MANETS,” *Int. J. Inf. Technol.*, 2018.

[31] D. Mishra, D. Sukheja, and S. Patel, “A Review on Gray Hole Attack in Wireless Sensor Network,” 2015.

[32] Y. Singh and F. Shan, “Secure Aodv Routing to Prevent Blackhole and Grayhole Attack,” 2017.

[33] M. Kaur, “Sybil Attack in Wireless Sensor Networks : A Survey,” vol. 3, no. 2, pp. 479–481, 2017.

APPENDIX A

THE SIMULATION AND ANALYSIS CODE

```
#####################################################################################
##############################
# WSNAttacksSimulation.tcl
#       Simulation of Wireless Sensor Network Attacks Using Mannasim
#     for the Project "Implementation and Analysis of Different Routing Layer Attacks on Wireless Sensor
Networks"
#       This simulation uses Mannasim for simulating sensor nodes, sensor data and application
#       The normal sensor Nodes will send temperature data and it will be directed to the data sink via the
AP node.
#
# Script developed for the Analysis on the Impact Black Hole Attack, Grey Hole Attack and Sybil Attac on
WSN
#
# A Simulation By
#           Sufian Abdulqader Almajmaie
# Under the Supervison of
#           Ass. Prof. Dr. Oguz Atta
#           Department of Computer Science
#           Istanbul Altinbas University
#           Email: soufian31183@gmail.com
#####################################################################################
##############################

puts $argc
if { $argc != 3 } {
       puts "The WSNAttacks Simulation script requires three input Parameters "
       puts "ns WSNAttacksSimulation.tcl  EvaluationRunNumber Type No_Malicious_Nodes"
       puts "Example : ns   WSNAttacksSimulation.tcl    0 AODV 0"
       puts "Try again."
       exit 0
   } else {
   puts  "Wirelss Sensor Network Attack Simulation : Run-[lindex $argv 0]"
}

set EvaluationRunNumber        [lindex $argv 0]                ; #  if EvaluationRunNumber is 0 then supress event
tracefile generation and record and show nam animation
set NumberofMaliciousNodes      [lindex $argv 2]
#####################################################################################
##############################
# Some Common Simulation parameters
#####################################################################################
##############################
set val(chan)       Channel/WirelessChannel              ; # channel
set val(prop)       Propagation/TwoRayGround       ; # propagation
set val(netif)      Phy/WirelessPhy                      ; # phy
set val(mac)       Mac/802_11                     ; # mac
set val(ifq)       Queue/DropTail/PriQueue              ; # queue
set val(ll)       LL                            ; # link layer
set val(ant)       Antenna/OmniAntenna              ; # antenna
set val(ifqlen) 300                          ; # queue length
#set val(rp)       DumbAgent                       ; # routing protocol
set val(rp)       AODV                           ; # routing protocol
set val(type)   [lindex $argv 1]
```

```
#set all the sensor nodes, CH nodes and AP with normal AODV routing Agent
Agent/AODV set AODV_AttackType_                  0
Agent/AODV set AODV_SybilAttackType_           1
Agent/AODV set AODV_SybilAttack_StartNodeID_    1
Agent/AODV set AODV_SybilAttack_EndNodeID_      30
Agent/AODV set AODV_AttackProbability_         0.90
Agent/AODV set AODV_AttackDebugMode_            0


set val(en)       EnergyModel/Battery             ; # energy model

set val(No_AP_Nodes)       1                   ; # number os access points
set val(AP_Nodes_size)       25

set val(MaliciousNode_Size)          15
set val(No_Normal_Sensor_Nodes)              [expr 7 * 7]       ; # number of common mica2 mote sensor nodes
- should be n x n
set val(Normal_Sensor_Node_size)       15


set val(StarSybilNodeID) 1
set val(EndCybilNodeID) 10


set val(nn)       [expr $val(No_AP_Nodes) + $val(No_Normal_Sensor_Nodes)]                        ; # number
of nodes

set val(x)                        600                          ; # x lenght of scenario
set val(y)                        600                          ; # y Width  of scenario

# Data  setings
set val(Dissemination_Type)            1                     ; # common node disseminating type
set val(Dissemination_Interval)       60.0                    ; # common node disseminating interval

set val(DataPort)                     2020       ; # default data port
set val(SensorDataStart)                 5.0       ; # simulation start time
set val(stop)                         100.0       ; # Sensor Data and simulation stop time

set val(pt_common)                       8.564879510890936E-4
set val(pt_cluster_head)                 0.2817901234567901

set val(SinkAddress)                     0       ; # sink address


##########################################################################################
################################
# Antenna Settings
##########################################################################################
################################
Antenna/OmniAntenna set X_ 0
Antenna/OmniAntenna set Y_ 0
Antenna/OmniAntenna set Z_ 1.5
Antenna/OmniAntenna set Gt_ 1.0
Antenna/OmniAntenna set Gr_ 1.0

##########################################################################################
################################
# Wireless Phy Settings
```

```
####################################################################################################
###################################
Phy/WirelessPhy set CPThresh_ 10.0
Phy/WirelessPhy set CSThresh_ 1.559e-11
Phy/WirelessPhy set RXThresh_ 3.652e-10
Phy/WirelessPhy set Rb_ 2*1e6
Phy/WirelessPhy set Pt_ 0.2818
Phy/WirelessPhy set freq_ 914e+6
Phy/WirelessPhy set L_ 1.0


####################################################################################################
###################################
# Procedure to setup a High Capability Node
####################################################################################################
###################################
proc setup_node { antenna range } {

    puts "Setting up cluster head node with $antenna and range = $range"

    #Phy/WirelessPhy set CPThresh_ 10.0
    #Phy/WirelessPhy set CSThresh_ 1.559e-11
    #Phy/WirelessPhy set RXThresh_ 2.78869e-09      ; # 100 meters
    #Phy/WirelessPhy set RXThresh_ 1.11548e-08      ; # 50 meters
    #Phy/WirelessPhy set Rb_ 2*1e6

    #~ Phy/WirelessPhy set Pt_ 0.281838
    #~ Phy/WirelessPhy set freq_ 2.4e09
    #~ Phy/WirelessPhy set L_ 1.0
    #~ Phy/WirelessPhy set lambda_ 0.125
    #~ Phy/WirelessPhy set RXThresh_ [TwoRay 0.281838 [$antenna set Gt_] [$antenna set Gr_] 0.8 0.8
1.0 $range 0.125]
    #~ Phy/WirelessPhy set bandwidth_ 1000*10e3 ;#1000 kbps

    Node/MobileNode/SensorNode set sensingPower_ 0.064 ;# 64 mW = 0.064 W
    Node/MobileNode/SensorNode set processingPower  0.360 ;# 360 mW = 0.360 W
    Node/MobileNode/SensorNode set instructionsPerSecond_ 150000000 ;# Intel StrongArm 1100 133 MHZ
--> 150 MIPS

}


####################################################################################################
###################################
# Procedure to setup mica type 2 mote
####################################################################################################
###################################

proc setup_mica2 { antenna range } {

    puts "Setting up mica 2 mote with $antenna and range = $range"

    #Phy/WirelessPhy set CPThresh_ 10.0
    #Phy/WirelessPhy set CSThresh_ 1.559e-11
    #Phy/WirelessPhy set RXThresh_ 2.78869e-09      ; # 100 meters
    #Phy/WirelessPhy set RXThresh_ 1.11548e-08      ; # 50 meters
    #Phy/WirelessPhy set Rb_ 2*1e6

    Phy/WirelessPhy set Pt_ 0.281838
    Phy/WirelessPhy set freq_ 2.4e09
```

```
        Phy/WirelessPhy set L_ 1.0
        Phy/WirelessPhy set lambda_ 0.125
        Phy/WirelessPhy set RXThresh_ [TwoRay 0.281838 [$antenna set Gt_] [$antenna set Gr_] 0.8 0.8 1.0
$range 0.125]
        Phy/WirelessPhy set bandwidth_ 28.8*10e3                ;#28.8 kbps

        Node/MobileNode/SensorNode set sensingPower_ 0.015 ;# i = 5mA, V = 3 --> P = ixV = 15 mW = 0.015
W
        Node/MobileNode/SensorNode set processingPower 0.024 ;# i = 8mA, V = 3 --> P = ixV = 24 mW = 0.024
W
        Node/MobileNode/SensorNode set instructionsPerSecond_ 8000000 ;# Atmel 128L 8MHZ --> 8MIPS

}



##########################################################################################
##################################
# Calculating the receiving threshold (RXThresh_ for Phy/Wireless)
# Wei Ye, weiye@isi.edu, 2000
##########################################################################################
##################################

proc Friis { Pt Gt Gr lambda L d} {
  set M [expr $lambda / (4 * 3.14159265359 * $d)]
  return [expr ($Pt * $Gt * $Gr * ($M * $M)) / $L]
}

proc TwoRay { Pt Gt Gr ht hr L d lambda } {
        set crossover_dist [expr (4 * 3.14159265359 * $ht * $hr) / $lambda]

        if { $d < $crossover_dist } {
                return [Friis $Pt $Gt $Gr $lambda $L $d]
        } else {
                return [expr $Pt * $Gt * $Gr * ($hr * $hr * $ht * $ht) / ($d * $d * $d * $d * $L)]
       }
}



##########################################################################################
##################################
# Procedure to create a normal sensor node application
##########################################################################################
##################################
proc create_common_app {destination_id disseminating_type disseminating_interval} {
        set app_ [new Application/SensorBaseApp/CommonNodeApp]
        $app_ set destination_id_ $destination_id
        $app_ set disseminating_type_ $disseminating_type
        $app_ set disseminating_interval_ $disseminating_interval
        return $app_
}


##########################################################################################
##################################
# Procedure to create a access point node application.
##########################################################################################
##################################
```

```
proc create_access_point_app {destination_id} {
        set app_ [new Application/AccessPointApp]
        $app_ set destination_id_ $destination_id
        return $app_
}

######################################################################################################
################################
# Procedure to create a Temperature Data Generator
######################################################################################################
################################
proc create_temp_data_generator {sensing_interval sensing_type avg_measure std_deviation} {
        set temp_gen_ [new DataGenerator/TemperatureDataGenerator]
        $temp_gen_ set sensing_interval_ $sensing_interval
        $temp_gen_ set sensing_type_ $sensing_type
        $temp_gen_ set avg_measure $avg_measure
        $temp_gen_ set std_deviation $std_deviation
        return $temp_gen_
}

set counter 0


######################################################################################################
################################
# Procedure to create a common node
######################################################################################################
################################

proc create_common_node {xx yy} {
        global val ns_ node_ topo udp_ app_ gen_ counter rng

        Phy/WirelessPhy set Pt_ $val(pt_common)
        $ns_ node-config -sensorNode ON \
        -adhocRouting $val(rp) \
        -llType $val(ll) \
        -macType $val(mac) \
        -ifqType $val(ifq) \
        -ifqLen $val(ifqlen) \
        -antType $val(ant) \
        -propType $val(prop) \
        -energyModel $val(en) \
        -phyType $val(netif) \
        -channelType $val(chan) \
        -topoInstance $topo \
        -agentTrace ON \
        -routerTrace ON \
        -macTrace ON \
        -rxPower 0.024 \
        -txPower 0.036 \
        -initialEnergy 10.0 \
        -movementTrace ON


        setup_mica2 $val(ant) 100

        set node_($counter) [$ns_ node]
        $node_($counter) random-motion 0

        $node_($counter) set X_ $xx
```

```
    $node_($counter) set Y_ $yy
    $node_($counter) set Z_ 0.0
    $ns_ initial_node_pos $node_($counter)      $val(Normal_Sensor_Node_size)

    set interval [$rng uniform 0.0 1.0]

    $node_($counter) color "black"


    $ns_ at 0.0 "$node_($counter) color black"


# Setting the Sensor node capacity as mica2 node

    #~ Node/MobileNode/SensorNode set sensingPower_ 0.015
    #~ Node/MobileNode/SensorNode set processingPower 0.024
     #~ Node/MobileNode/SensorNode set instructionsPerSecond_ 8000000
      #~ Phy/WirelessPhy set  bandwidth_ 288000.0



    set udp_($counter) [new Agent/UDP]

    $udp_($counter) set class_ 0
    $udp_($counter) set fid_ 0


    set initial [expr $val(No_AP_Nodes)]




    set app_($counter) [create_common_app $val(SinkAddress) $val(Dissemination_Type) $val(Dissemination_Interval)]
    $node_($counter) attach $udp_($counter) $val(DataPort)
    $node_($counter) add-app $app_($counter)

    set processing_($counter) [new Processing/AggregateProcessing]

    $app_($counter) node $node_($counter)
    $app_($counter) attach-agent $udp_($counter)

    $app_($counter) attach-processing $processing_($counter)
    $processing_($counter) node $node_($counter)

    $ns_ at [expr $val(SensorDataStart) + 1 + $interval] "$app_($counter) start"
    $ns_ at $val(stop) "$app_($counter) stop"

    set gen_($counter) [create_temp_data_generator 3.0 0 25.0 1.0]
    #set gen_($counter) [create_temp_data_generator 5.0 0 27.0 10.0 ]

    $app_($counter) attach_data_generator $gen_($counter)

    incr counter

}
```

```
##########################################################################################
################################
# Procedure to create a access point node
##########################################################################################
################################
proc create_access_point {xx yy} {
	global ns_ val node_ app_ udp_ counter topo
	Phy/WirelessPhy set Pt_ 0.2818
	$ns_ node-config -sensorNode ON \
	-adhocRouting $val(rp) \
	-llType $val(ll) \
	-macType $val(mac) \
	-ifqType $val(ifq) \
	-ifqLen $val(ifqlen) \
	-antType $val(ant) \
	-propType $val(prop) \
	-energyModel $val(en) \
	-phyType $val(netif) \
	-channelType $val(chan) \
	-topoInstance $topo \
	-agentTrace ON \
	-routerTrace ON \
	-macTrace ON \
	-rxPower 0.5 \
	-txPower 0.5 \
	-initialEnergy 100.0 \
	-movementTrace ON

	#Set it as higher capability node
	setup_node $val(ant) 250

	set node_($counter) [$ns_ node]
	$node_($counter) random-motion 0
	set  udp_($counter) [new Agent/UDP]
	$udp_($counter) set class_ 0
	$udp_($counter) set fid_ 0

	set app_($counter) [create_access_point_app [$node_(0) node-addr]]
	$node_($counter) attach $udp_($counter) $val(DataPort)
	$app_($counter) attach-agent $udp_($counter)
	$node_($counter) set X_ $xx
	$node_($counter) set Y_ $yy
	$node_($counter) set Z_ 0.0
	$ns_ initial_node_pos $node_($counter)	$val(AP_Nodes_size)
	$node_($counter) color "blue"


	$ns_ at 0.0 "$node_($counter) color blue"
	$ns_ at 0.0 "$node_($counter) label AP_Node"

	$ns_ at [expr $val(SensorDataStart)] "$app_($counter) start"
	$ns_ at [expr $val(stop)+1] "$app_($counter) stop"

	incr counter

}

##########################################################################################
################################
# Procedure to create a malicious cluster head node
```

```
##########################################################################################################################################
#############################################
proc create_malicoius_node {xx yy} {

global val ns_ node_ topo counter rng

Phy/WirelessPhy set Pt_ $val(pt_cluster_head)

        $ns_ node-config -sensorNode ON \
        -adhocRouting $val(rp) \
        -llType $val(ll) \
        -macType $val(mac) \
        -ifqType $val(ifq) \
        -ifqLen $val(ifqlen) \
        -antType $val(ant) \
        -propType $val(prop) \
        -energyModel $val(en) \
        -phyType $val(netif) \
        -channelType $val(chan) \
        -topoInstance $topo \
        -agentTrace ON \
        -routerTrace ON \
        -macTrace ON \
        -rxPower 0.3 \
        -txPower 0.6 \
        -initialEnergy 100.0 \
        -movementTrace ON

#Set it as higher capability node
        setup_mica2 $val(ant) 100



        set node_($counter) [$ns_ node]
        $node_($counter) random-motion 0

        $node_($counter) set X_ $xx
        $node_($counter) set Y_ $yy
        $node_($counter) set Z_ 0.0
        $node_($counter) color "red"
        $ns_ initial_node_pos $node_($counter)        $val(MaliciousNode_Size)


        if {$val(type) == "AODV_GH"} {
            [$node_($counter) set ragent_] set AODV_AttackType_          1
         #   $ns_ at 0.0 "$node_($counter) label \"GH\""
            $ns_ at 0.0 "$node_($counter) color red "
        }

        if {$val(type) == "AODV_BH"} {
            [$node_($counter) set ragent_] set AODV_AttackType_          2
          #  $ns_ at 0.0 "$node_($counter) label \"BH\""
            $ns_ at 0.0 "$node_($counter) color red "
        }

        if {$val(type) == "AODV_SBL"} {
            [$node_($counter) set ragent_] set AODV_AttackType_          3
           # $ns_ at 0.0 "$node_($counter) label \"SBL\""
            $ns_ at 0.0 "$node_($counter) color red "
        }
```

```
    # $ns_ at 0.0 "$node_($counter)  label-color red "

# In case, the malicious node wishes to behave as a normal node, then it may forward the packets to normal applications

        set udp_($counter) [new Agent/UDP]

        $udp_($counter) set class_ 0
        $udp_($counter) set fid_ 0


        set initial [expr $val(No_AP_Nodes)]

        set interval [$rng uniform 0.0 1.0]

        set app_($counter) [create_common_app $val(SinkAddress) $val(Dissemination_Type) $val(Dissemination_Interval)]
        $node_($counter) attach $udp_($counter) $val(DataPort)
        $node_($counter) add-app $app_($counter)

        set processing_($counter) [new Processing/AggregateProcessing]

        $app_($counter) node $node_($counter)
        $app_($counter) attach-agent $udp_($counter)

        $app_($counter) attach-processing $processing_($counter)
        $processing_($counter) node $node_($counter)

        $ns_ at [expr $val(SensorDataStart) + 1 + $interval] "$app_($counter) start"
        $ns_ at $val(stop) "$app_($counter) stop"


        #~ set udp_($counter) [new Agent/UDP]
        #~ $udp_($counter) set class_ 0
        #~ $udp_($counter) set fid_ 0

        #~  set  app_($counter)  [create_cluster_head_app  [$node_(1)  node-addr]  $val(Dissemination_Type) $val(CH_Node_Dissemination_Interval)]
        #~ $node_($counter) attach $udp_($counter) $val(DataPort)
        #~ $node_($counter) add-app $app_($counter)
        #~ set processing_($counter) [new Processing/AggregateProcessing]

        #~ $app_($counter) node $node_($counter)
        #~ $app_($counter) attach-agent $udp_($counter)

        #~ $app_($counter) attach-processing $processing_($counter)
        #~ $processing_($counter) node $node_($counter)

        #~ $ns_ at [expr $val(SensorDataStart) + 1 + $interval] "$app_($counter) start"
        #~ $ns_ at $val(stop) "$app_($counter) stop"



        incr counter
}



###########################################################################################################################
```

```
# Global variables
##########################################################################################
################################
set ns_ [new Simulator]

##########################################################################################
################################
#Trace File control
#if EvaluationRunNumber is 0 then it enable the recording of nam trace and show nam animation
#Event Trace file will be generated and named with respect to the selected command line options
##########################################################################################
################################

if $EvaluationRunNumber==0 {

   set  NamTraceFileDescriptor [open WSNAttacksSimulation.nam w]
   $ns_ namtrace-all-wireless $NamTraceFileDescriptor $val(x) $val(y)
   $ns_ use-newtrace
   remove-all-packet-headers
   add-packet-header $val(rp) ARP LL MAC CBR IP

   set   EventTraceFileDescriptor                    [open   WSNAttacks-Run-$EvaluationRunNumber-$val(type)-
$NumberofMaliciousNodes.tr w]
   $ns_ trace-all $EventTraceFileDescriptor
} else {

   $ns_ use-newtrace
   remove-all-packet-headers
   add-packet-header $val(rp) ARP LL MAC CBR IP

   set   EventTraceFileDescriptor                    [open   WSNAttacks-Run-$EvaluationRunNumber-$val(type)-
$NumberofMaliciousNodes.tr w]
   $ns_ trace-all $EventTraceFileDescriptor

}


set topo       [new Topography]
$topo load_flatgrid $val(x) $val(y)

set rng [new RNG]
$rng seed [expr 1000 + $EvaluationRunNumber]
create-god $val(nn)


##########################################################################################
################################
# Procedures to control the creation of normal sensor nodes and other node
##########################################################################################
################################


#Create an Access Point for Normal Sensor Data (ID 1)
#setup_mica2 $val(ant) 100

#Possistion the AP at center of the topographical Area

#create_access_point [expr $val(x)/2] [expr $val(y)/2]

create_access_point $val(x) [expr $val(y)/2]
```

```
set GridLileTopology  Yes

if { $GridLileTopology == "Yes" } {
#Create Normal Sensor nodes in somewhat uniform Grid Like location
    for {set i 0} {$i < sqrt($val(No_Normal_Sensor_Nodes)) } {incr i} {
        for {set j 0} {$j < sqrt($val(No_Normal_Sensor_Nodes)) } {incr j} {
            set xval [expr $i * $val(x) / sqrt($val(No_Normal_Sensor_Nodes)) + [$rng integer 20]]
            set yval [expr $j * $val(y) / sqrt($val(No_Normal_Sensor_Nodes)) + [$rng integer 20]]
            create_common_node $xval $yval
          }
    }


} else {
#Create Normal Sensor nodes at Random Locations
    for {set i 0} {$i < sqrt($val(No_Normal_Sensor_Nodes)) } {incr i} {
        for {set j 0} {$j < sqrt($val(No_Normal_Sensor_Nodes)) } {incr j} {
            set xval [expr 10 + [$rng integer $val(x)]]
            set yval [expr 10 + [$rng integer $val(y)]]
            create_common_node $xval $yval
          }
    }

}

# Create Malicious nodes
# Create Malicious nodes at the far end of AP node (left side of the topology)

  if {$val(type) == "Normal_AODV"} {
    puts "Setting Simulation  with  0 Malicious  Nodes"
  } elseif {$val(type) == "AODV_BH"} {
    puts "Setting Simulation  with  $NumberofMaliciousNodes Malicious  Nodes"
    #Place BH node at the oposit corner of Sink node to avoid too much drops
      for {set i 0} {$i < $NumberofMaliciousNodes } {incr i} {
            set xval [expr 10 + [$rng integer [expr $val(x)/5]]]
            set yval [expr 10 + [$rng integer  $val(y) ]]
            create_malicoius_node $xval $yval

      }
  } else {
        #~ for {set i 0} {$i < $NumberofMaliciousNodes } {incr i} {
            #~ set xval [expr 10 + [$rng integer $val(x)]]
            #~ set yval [expr 10 + [$rng integer $val(y)]]
            #~ create_malicoius_node $xval $yval
        #~ }
      for {set i 0} {$i < $NumberofMaliciousNodes } {incr i} {
            set xval [expr 10 + [$rng integer [expr $val(x)/5]]]
            set yval [expr 10 + [$rng integer  $val(y) ]]
            create_malicoius_node $xval $yval

      }
  }


##########################################################################################
################################
# Stop Simulation
##########################################################################################
################################
```

```
$ns_ at [expr $val(stop)+2.0] "finish"

$ns_ at [expr $val(stop)+2.0] "puts \"NS EXITING...\" ; $ns_ halt"

$ns_ at [expr $val(stop)+2.0] "$ns_ nam-end-wireless $val(stop)"



proc finish {} {
        global ns_ EventTraceFileDescriptor NamTraceFileDescriptor EvaluationRunNumber
        #$ns_ flush-trace

        if $EvaluationRunNumber==0 {
            close $NamTraceFileDescriptor
             exec nam WSNAttacksSimulation.nam &

        } else {

              close $EventTraceFileDescriptor
        }

}

puts "Starting Simulation..."
$ns_ run
##########################################################################################
################################
```