PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
Ministry of Higher Education and Scientific Research
Mohamed Khider University – BISKRA
Faculty of Exact Sciences, Natural sciences and Life
Department of Computer Science

Order N°: RTIC14/M2/2022

THESIS

Presented for the Academic Master's degree in

Computer Science

Option: Information and communication networks and technologies

---

INTRUSION DETECTION SYSTEM FOR IOT NETWORKS

By:

HADDOUD MANEL HASNA

Presented in 26/06/2022 Board of Examiners:

Telli Abd Moutie	MCA	President
Sahraoui Somia	MCA	Supervisor
Ben Dahmene Asma	MAA	Examiner

Academic year :2021-2022

Abstract

The Internet of Things is a significant advancement in the field of technology because it stands on several interesting technologies. IoT enables people and objects/devices to connect not just with one another but also with anything at any time and from anywhere via the internet. WSN is one of the domains covered by the diversity of domains covered. Wireless sensor networks, an essential component of the Internet of Things, enable the representation of real-world's dynamic properties in the internet's virtual world. Since the WSNs are used in many domains due to their ease of construction and inexpensive cost. Due to the wide openness of wireless media and the limited resources of WSNs, numerous assaults, such as the black hole attack, may be implemented and integrated with traditional routing protocols used in WSNs. On the other hand, the security of these networks is important, given that possible attackers are always willing to disrupt the vital process of packets routing within WSNs. In our project, we proposed a detective security solution for AODV-based WSNs. The solution is named D-AODV (Detection with AODV) and it has the ability to detect denial of service attacks of type black hole and grey hole, in addition to Sybil attack. This solution is implemented and evaluated with network simulator NS2. The evaluation has shown that the solution takes into account the limitations of the wireless sensor networks while dealing with the aforementioned attacks.

Résumé

L'Internet des objets représente un progrès important dans le domaine de la technologie parce qu'il comprend plusieurs technologies intéressantes. L'IdO permet aux personnes, objets et appareils de se connecter non seulement les uns aux autres mais aussi, à tout moment, n'importe où, via Internet. WSN fait partie des domaines couverts qui sont diverses. Les réseaux de capteurs sans fil, composante essentielle de l'Internet des objets, permettent de représenter les propriétés dynamiques du monde réel dans le monde virtuel d'Internet. Les WSN sont utilisés dans de nombreux domaines, d'une part, pour leur facilité de construction et d'une autre part, leur coût raisonnable. En raison de la grande ouverture des médias sans fil et des ressources limitées des WSN, de nombreuses attaques, comme l'attaque du black hole , peuvent être mises en œuvre et intégrées aux protocoles de routage traditionnels utilisés dans les WSN. Comme la sécurité de ces réseaux est importante et les attaquants éventuels sont toujours prêts à perturber le processus vital de routage des paquets dans les WSN, notre projet propos une solution de sécurité de détection pour AODV basé sur WSN. La solution est nommée D-AODV (Détection avec AODV) a la capacité de détecter les attaques de déni de service de type black hole et grey hole ainsi que l'attaque Sybil. Cette solution est implémentée et évaluée avec le simulateur réseau NS2. L'évaluation a montré que la solution tient compte les limites des réseaux de capteurs sans fil tout en traitant les attaques déjà mentionnées.

Dedication

I dedicate this achievement to my father and my mother, who with love and effort have accompanied me in this process, without hesitating at any moment of seeing my dreams come true, which are also their dreams.

I dedicate this work to my lovely family……

Who always encourage me with passion and endless support. I am

so Lucky to have a them by my side

To my faithful brothers and sisters…

Who have always helped me and believed that I could do it…

To my lovely grandmothers and my aunts who gave me to much support and love

To my firends Marthe , Amine , Taki who has been my support in the difficulties.

Acknowledgments

I wish to thank my supervisor Mme sahraoui she was more than generous with her expertise and precious time, and for guiding me and encouraging me to do professional work.

A special thanks to the jury member for criticizing my thesis.I would like to express my sincere thanks to Dr Mohammed A. Taha Alkhafagey who help me a lot during my work who took his time and effort to answer all my questions and his worthy advice, suggestions, and patience till i finish the work

I would like to express my sincere gratitude to Mohamed Khider University and all the teachers in the department for all the considerate guidance.

I would like to thank other persons from the electrical engineering department who encouraged me all the time and for passing a good time with them during my whole education

List of Tables

List of figures

List of Acronyms

RFID	Radio Frequency Identification
WSN	Wireless sensor network
IoT	Internet of thing
IAB	The Internet Architectural Board
Wi-Fi	Wireless Fidelity
QoS	Quality of Service
IPV6	Internet Protocol version 6
IPV4	Internet Protocol version 4
CoAP	Constrained Application Protocol
MQTT	Message Queuing Telemetry Transport Protocol
EGG	Electroencephalography
BP	Blood Pressure sensor
BG	Blood Glucose sensor
DoS	Denial of Service
MAC	Message Authentication Code
6LoWPAN	IPv6 LoW Power wireless Area Networks
IDS	Intrusion Detection System
RREQ	Route Request Message
RREP	Route Reply Message
AODV	Ad-hoc on Demand Distance Vector Route
RERR	Route Error Message
PDR	Packet Delivery ratio
PDf	Packet Delivery fraction
NS2	Network simulator
D-AODV	Detection with AODV

Content

General Introduction

General Introduction

The development of technology has led to the invention of many promising techniques, networks, and solutions that contribute to the tremendous provision of several domains. The Internet of things is one of the most important topics in this century that will change our lives and make everything connected to the worldwide network (internet).

Wireless Sensor Networks (WSNs) is an important enabling technology. This technology combines the sensing, processing and networking over the sensor nodes with some special features like: autonomous power, ease of deployment, cost-effective and so on. In fact, WSNs have a great capacity to successfully gather diverse types of information about the deployment field. This helps with the identification of early occurrence of events, the remote monitoring and even the prediction of phenomena.

Due to their special nature and several constraints, particularly those related to processing resources, memory storage, and, most importantly, energy WSNs are vulnerable to many attacks. Moreover, the intrusion detection systems (IDSs), are well recognized for being effective security mechanisms for protecting sensor networks from malicious assaults or unauthorized access.

In this project, a D-AODV (Detection with AODV) is proposed. D-AODV is a solution combining AODV protocol with an intrusion detection system, where the main purpose is to detect black hole, grey hole and sybil attacks. The solution takes into consideration the limitation of the wireless sensor network.

This manuscript includes two main parts: the first part consist of the theoretical aspect, while the second part focuses on the presentation of the proposed solution. Part I is divided into two chapters. Chapter 1 presents generalities on the Internet of Things, its history, enabling technologies, application, etc. Chapter 2 deals with an overview of security issues in IoT, as well as a taxonomy protection mechanisms.

Part II concentrates on the presentation of the implementation details of D-AODV and the implementation of the routing attacks. It is composed of two chapters. In chapter 3, we describe the analysis and design of the solution and threat models. In chapter 4, we present the implementation of attacks and D-AODV solution with the evaluation of its effectiveness according to well-determined metrics. The manuscript ends with a general conclusion.

CHAPTER 1: Generalities on IoT

Introduction

The Internet of Things (IoT) is one of the most commonly used technologies because The world has changed in all disciplines, including medical ,industrial , as the world's needs have grown. This chapter is general introduction about Internet of Things and its aspects which include a history of IoT, the architecture used and a brief definition of IoT including some IoT technology such as communication model, transmission technology ,protocols ,IoT application and some challenges of IoT .

1. 1 IoT History

The concept of a network of smart devices was first introduced in 1982, with the first Internet-connected device at Carnegie Melon University.. Not long after, in 1994, Steve Mann created WearCam, which was one of the first camera appeare in the web. WearCam which near-real-time performance consists of recording, processing and broadcasting media camera captured image and monitoring means ability to display image or image stream from camera. The captured images will be transmitted to an entity (a base station) available to the user. In 1999, the name Internet of Things was first coined by Kevin Ashton , MIT Executive Director

He developed an RFID-based globale object identification system the same year. After that, in the year 2000, LG announced the launch of the world's first Internet-connected smart refrigerator. In 2003, the US army used RFID extensively in its Save program, and the same year, retail behemoth Walmart began to use RFID in all of its shops to a greater extent. Many articles about the Internet of Things and its future course were cited in 2005 by mainstream publications such as The Guardian, American, and The Boston Globe. The IPSO Alliance was founded in 2008 by a group of firms to promote the use of Internet Protocol (IP) in networks of "smart objects" and allow the Internet of Things. The Federal Communications Commission (FCC) permitted the use of the "white space spectrum" in 2008. Finally, the debut of IPv6 in 2011 sparked significant interest and growth in this subject, prompting IT behemoths such as Cisco, IBM, and Ericson to launch a slew of educational and commercial IoT efforts.[1][2]

1. 2 IoT Definition

According to technology analysts and visionaries, the Internet of Things (IoT) is a network of physical objects that can be accessed over the internet. To interact with the internal state or external environment, these devices feature integrated technologies such as wireless sensor networks (WSN) and radiofrequency identification (RFID).In general, the

basic objective of IoT is to allow people and things to connect with anything and everyone at anytime, anywhere, utilizing any network and service. [3]

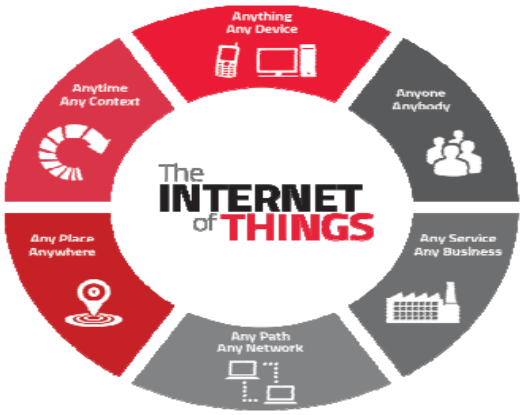

Figure 1: Internet of thing [3]

1.3 Communication Model

In March 2015, the Internet Architectural Board (IAB) published a guiding architecture document for networking smart objects (RFC 7452) this section describes communication models from that document. As a result, it's important to understand the various communication types that enable IoT devices to connect and communicate. Some communication models: [4]

1.3.1 Device-to-Device Communication Model

Communication among two or more IoT devices does not require the use of an intermediary application server; instead, they interact directly. As shown in figure 2

The Internet, IP networks, and other forms of networks are used to communicate. Protocols used to establish direct communication can be Bluetooth [Zigbee]

Small data packets are transferred at a very low data rate in applications like home automation systems, where IoT devices are integrated in locks, lamps, switches, and thermostats ,device-to-device communication is limited because manufacturers employ different communication protocols, and devices can only communicate with devices that use the same protocol.

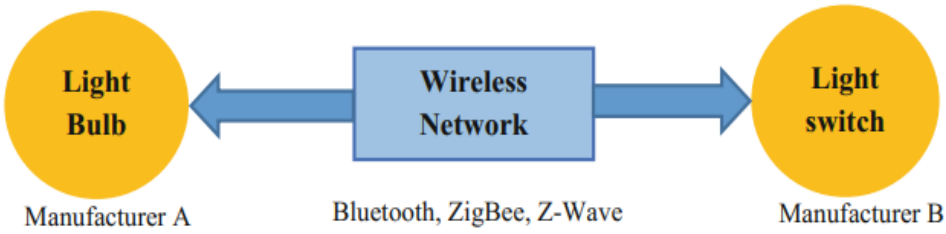

Figure 2: device to device communication [4]

1.3.2 Device-to-Cloud Communication Model

As shown in figure 3, data exchange and message traffic control takes place between IoT devices and internet cloud services (such as application servers).

Traditional wired Ethernet or Wi-Fi connections are used to create a connection between the device and the IP network, which then connects to the cloud service ,Protocols such as HTTP, TCP/IP, TL,S, and others are used by the device to communicate with the cloud service. IoT devices that have implemented the device-to-cloud concept include Samsung Smart TV and Nest Labs leaning Thermostat. These IoT devices collect data and transmit it to a cloud database, where it is evaluated for future use. The cloud technology allows for remote access to these devices, which may be accessed via a web interface or a smartphone .The interoperability issues are frequently encountered in this paradigm when devices made by various manufacturers are attempted to integrate. In the current environment, the device and the cloud should be from the same vendor for this communication model to work successfully.

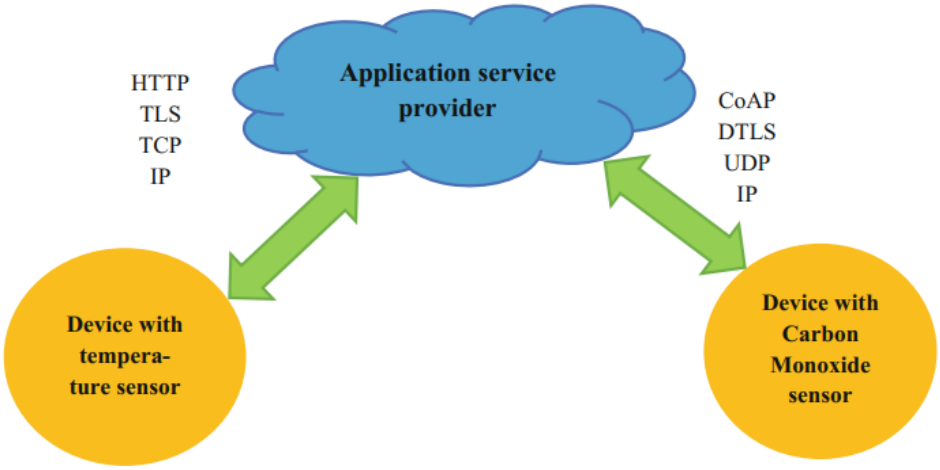

Figure 3: Device-to-cloud communication model[4]

1.3.3 Device-to-Gateway-Communication-Model

As illustrated in figure 4, the IoT device uses a gateway device to communicate with cloud services over the internet for data exchange.

Application-layer-gateway refers to a gateway device that functions at the application layer. The gateway runs application software and serves as a middleman between IoT devices and cloud services, primarily supporting data or protocol translation and providing security. Typically ,smartphones serve as gateway devices that interface with IoT devices and submit data to a cloud service via an App. A fitness app on a smartphone that is connected to a fitness tracker device is an example of such an application layer gateway. Because this device is unable to connect directly to the cloud service, it must rely on the smartphone App as a gateway device .This model integrates new smart devices into a legacy system which further facilitates interoperability between devices. The challenge is the addition of application layer software which adds costs and design complexity to the system.

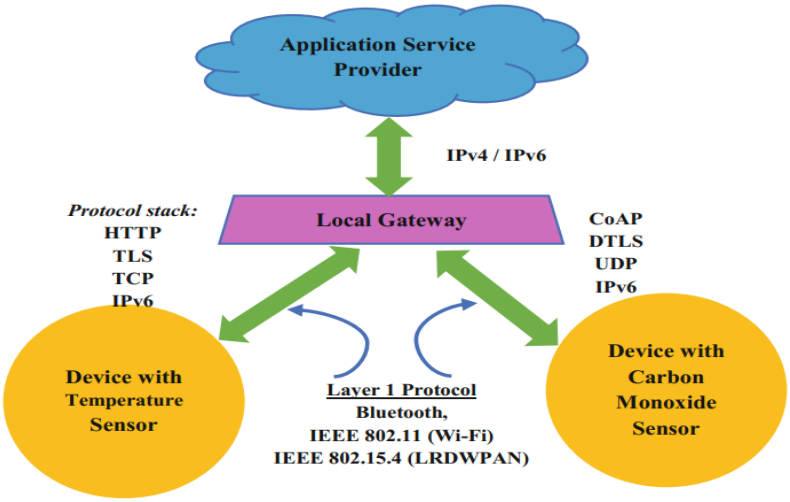

Figure 4: Device-to-gateway communication model[4]

1.4 IoT Characteristics

The Internet of Things is a complicated system with a variety of properties that change from one domain to another. The following are some of the characteristics: [5]

1.4.1 Intelligence

IoT is intelligent because it combines algorithms and processing, software and hardware. Ambient intelligence improves the capabilities of IoT devices, allowing them to adapt intelligently to a given circumstance and helping them in completing specific tasks.

1.4.2 Connectivity

The Internet of Things is made possible by connectivity, which connects common objects. Because simple object-level interactions contribute to collective intelligence in IoT networks, the connectivity of these things is critical. It allows devices to connect to the internet and communicate with each other. The networking of smart things and apps can offer new commercial prospects for the Internet of things with this connectivity.

1.4.3 Dynamic Nature

The Internet of Things' principal function is to collect data from its environment, which is achieved through the dynamic changes that occur around the devices. The condition of these devices changes dynamically, such as when they are sleeping or waking up, whether they are connected or disconnected, and the context of the devices, including temperature, location, and speed. The number of devices changes dynamically with a person, place, and time, in addition to the state of the device

1.4.4 The scale

The number of devices that must be managed and communicate with each other will be far more than the number of devices currently linked to the Internet. Data generated by these devices for application purposes requires more careful control. According to the predicted assessment, 5.5 million new objects would be connected every day in 2016, with 6.4 billion connected devices in use worldwide. By 2020, the number of linked devices is expected to reach 20.8 billion, according to the estimate

1.4.5 Sensing

Sensors that detect or measure changes in the environment to provide data that can report on their status or even interact with the environment are required for IoT to work. Sensing technologies enable the development of capabilities that represent a true understanding of the physical environment and the people who inhabit it.

1.4.6 Heterogeneity

One of the fundamental aspects of the Internet of Things is heterogeneity. Devices in the Internet of Things are based on many hardware platforms and networks, and they can communicate with other devices or service platforms over various networks. Direct network connectivity between heterogeneous networks should be supported by IoT architecture. Scalabilities, modularity, extensibility, and interoperability are the core design criteria for heterogeneous things and their contexts in the Internet of Things.

1.4.7 Security

IoT devices are inherently vulnerable to cyber-attacks. It would be a mistake to ignore security problems while we gain efficiencies, innovative experiences, and other benefits from the Internet of Things. With IoT, there is a high amount of transparency and privacy concerns. It is essential to secure endpoints, networks, and the data that is transmitted across all of them, which necessitates the development of a security paradigm.

1.5 Architecture of IoT

The existing internet architecture, which was adopted in the form of TCP/IP protocols roughly four decades ago, is now incompatible with serving the vast network of Internet of Things.

As a result, a new architecture is required to handle the network of over 25 billion linked objects expected to be available by 2020. To accommodate existing network applications and provide security and Quality of Service (QoS), this new architecture should use open source protocols . Data protection and data privacy are two major obstacles to IoT implementation . As a result, new multi-layered security architectures for IoT are developed in order to improve it further. Hui Sho et al. advocated a four-layer architecture, while Wang Chen proposed a three-layer architecture[6], Hui Sho et al. proposed a four-layer architecture[7], and Xu Cheng et al. proposed a six-layered architecture based on a hierarchical structure [8][4] is shown in figure 5. The six levels of IoT architecture are explained briefly below:

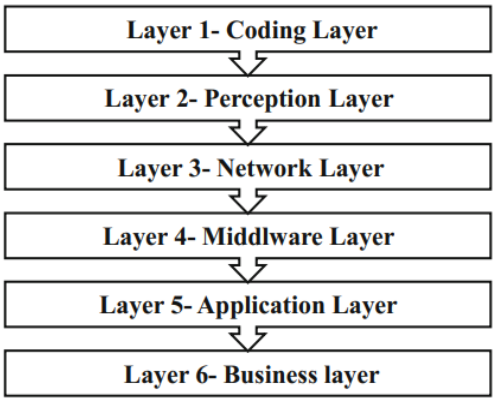

Figure 5: the proposed Architecture of IoT proposed[4]

1.5.1 Coding layer

The Internet of Things is based on this layer. Coding is the process of assigning an id number to each object so that it may be identified throughout the Internet of Things' life cycle.[4]

1.5.2 Perception layer

In IoT architecture, this layer is also known as the sensor layer. Through smart devices, the perception layer interacts with physical devices and components (RFID, sensors, actuators, etc.). Its major goals are to connect items in an IoT network. In this layer, the data sensor collects data from the linked object, transforms it to a digital signal, and sends it to the Network layer for further processing.[6]

1.5.3 Network layer

Secure data transfer between the Perception layer and the Middleware layer is the responsibility of the Network layers. This layer takes information in digital form from the Perception layer and delivers it to the Middleware layer for further processing. This layer is a convergence of internet and communication-based networks that employs multiple transmission mediums such as Bluetooth, Zigbee, and protocols such as IPv4, IPv6, MQTT and others.[7]

1.5.4 Middleware layer

This layer accesses the database directly and stores the relevant information using sophisticated technologies such as ubiquitous computing, cloud computing,among others. This layer primarily uses intelligent processing equipment to process sensor data received from the network layer and then executes a completely automated action depending on the outcome.[8]

1.5.5 Application layer

This layer provides global application management based on the object information processed in the Middleware layer, and this layer provides personalized service based on user needs, using the result of the processed data. As a result, this layer is essential to the growth of large-scale IoT networks.

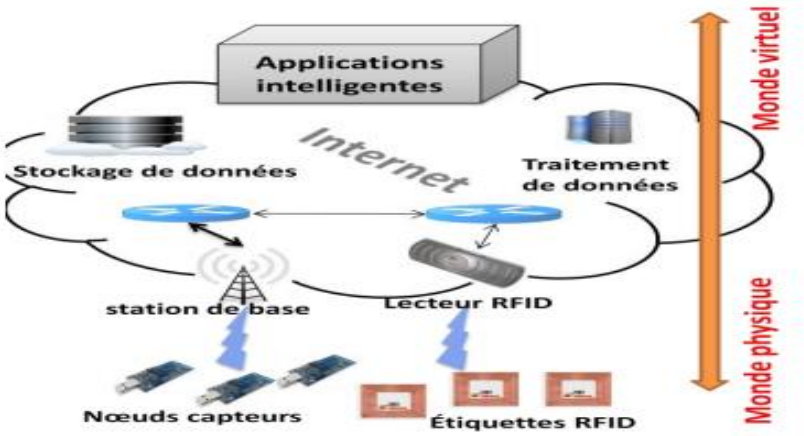

Figure 6: Internet of Things Architecture[1]

1.5.6 Business layer

The Business layer is the top layer of the IoT architecture, where various business models are generated for the effective business strategies. The applications and services provided by IoT is managed in this layer.

1.6 Technologies of IoT

1.6.1 RFID

RFID technology is used to identify and track objects without having to make physical touch with them. It allows data to be exchanged across short distances using radio frequencies. The RFID tags, RFID readers, and antennas make up an RFID-based system. RFID tag can be a microchip attached to an antenna; each RFID tag is attached in an object and has its unique identification number. A RFID reader can identify an object and obtain the corresponding information by querying to the attached RFID tag through appropriate signals. An antenna is used to transmit signals between RFID tag and RFID reader, in comparison with other technologies. Fast scanning, durability, reusability, huge storage, noncontact reading, security, tiny size, and low cost are all advantages of RFID. Because of these advantages, RFID is used at the IoT perception layer to identify and track objects as well as share data.[9]

1.6.2 WSN

In the Internet of Things, WSNs can be highly useful. WSN can detect and monitor device status and send the information to a control center or sink node through several hops. As a result, wsn might be viewed as a new link between the physical and virtual worlds. WSN provides various advantages over other technologies, such as scalability, dynamic reconfiguration, dependability, small size, cheap cost, and low energy usage. All of these advantages aid WSN's integration into various domains with varying requirements. It's worthy to note that both RFID and WSN may be used to collect data in the Internet of Things; the difference is that RFID is mostly used for object identification, whereas WSN is primarily utilized for the perception of real-world [9]

1.6.3 Cloud computing

Cloud Computing is an intelligent technology that is a convergence of many servers into one cloud platform with the goal of sharing resources and allowing access from anywhere and at any time. Cloud technology is an important aspect of the Internet of Things since it saves aggregated data from many IoT devices, analyses it, and provides the results for future action.[4]

1.7 Transmission technologies

In this section, we present the transmission technologies adopted in the IoT:

1.7.1 Short-range technologies

- **Bluetooth**

Is a PAN technology primarily used today as a cable replacement for short-range communication operates in the unlicensed ISM band at 2.4 GHz using a spread spectrum, frequency hopping, and full-duplex signal at a nominal rate of 1600 hops/sec. Its range varies from 1 m to 100 m depending on which class of radio is used. Class 2 is the most commonly used radio. It has a range of around 10 m and uses 2.5mW of power. It supports data throughputs up to 2 Mbps, with up to eight connected devices.[10]

- **NFC**

Is a wireless communication technology designed to build on existing High-Frequency (HF) (13.56 MHz) contactless and RFID technology. Using 13.56 MHz on the ISM band and with a typical operating distance of up to 4 cm, today NFC enables an exchange rate of between 106 Kbps and 848 Kbps. NFC creates a short-range wireless connection able to operate in three different modes of operation: card emulation, read/write, and peer-to-peer. NFC technology enables a wide range of use cases from keyless access to e-wallet in

smartphone and smart tags for medical applications. This is due to ease of implementation and the ability to embed tags into credit cards, smartphones, and other wearable devices.[10]

- **Zigbee**

Is based on the IEEE 802.15.4 link layer and designed, promoted, and maintained by the Zigbee Alliance. The Zigbee protocol suite includes standard commissioning, security, network, and device management procedures. It takes full advantage of IEEE 802.15.4 physical radio standard and operation in unlicensed bands worldwide at 2.4 GHz (global). Raw data throughput rates of 250 Kbps can be achieved at 2.4 GHz (16 channels), 10 Kbps at 915–921 MHz (27 channels), and 100 Kbps at 868 MHz (63 channels). Transmission distances range from 10 to 100 meters, depending on power output and environmental characteristics.[10]

Table 1: The characteristic of ZigBee Wireless Sensor Network[14]

Features	Description
Shorter delay	15ms -30ms
Low rate	1KB/s -250KB/s
Large capacity	Can support up to 255 devices
Band	2.4GHz
Security	Provide data integrity checking
Low power consumption	Battery can be used 6 months to 2 years

1.7.2 Medium-range technologies

- **Wi-Fi**

Is a wireless connectivity technology based on the IEEE 802.11 standards. Initially created for Wireless Local Area Network (WLAN) applications, Wi-Fi is also increasingly used for peer-to-peer and Wireless Personal Area Network connections (WPAN). It provides secure, reliable, and fast wireless connectivity. A Wi-Fi network can be used to connect electronic devices to each other, to the Internet, and to wired networks that use Ethernet technology. It operates in the 2.4 GHz and 5 GHz radio bands, with some products that contain both bands (dual band). It offers low power consumption and low-cost relative to cellular. Unlike cellular, Wi-Fi operates in unlicensed spectrum, resulting also in lower data transmission costs. Range is limited by proximity to a wireless router or relays, and the quality of connection can be diminished by network congestion.[10]

1.7.3 Long-range technologies

- **Mobile cellular networks**

Cellular technologies provide “always-on” connectivity. Similar to mobile phones for consumer applications, cellular data for IoT can be connected over 2G, 3G, or 4G networks. Benefits include broad coverage leveraging existing base station infrastructure as well as mobility (e.g., cars). Potential drawbacks include power consumption, fees associated with data transfer over licensed spectrum owned by carriers, and potential gaps in coverage. The first-generation mobile network (1G) was all about voice and used analogy technology. 2G enabled voice and texting (Short Messaging Service – SMS) using digital technology. 3G was about voice, texting, and data. 4G was everything in 3G but faster, and 5G will be even faster. 5G will be fast enough to download a full-length HD movie in seconds. 5G is much more than just faster networks. It supports the unique combination of high-speed connectivity, very low latency, and ubiquitous coverage, making it natively suitable for supporting IoT use cases. 5G will enable us to control more devices remotely in applications where real-time network performance is critical, enabling new user experiences in many different verticals.[10]

- **Low Power Wide Area Networks**

(LPWANs) are the new phenomenon in IoT. By providing long-range communication on small, inexpensive batteries that last for years, this family of technologies is purpose-built to support large-scale IoT networks sprawling over vast industrial and commercial campuses. LPWANs can literally connect all types of IoT sensors facilitating numerous applications. Nevertheless, LPWANs can only send small blocks of data at a low rate, and therefore are better suited for use cases that don’t require high bandwidth and are not time-sensitive.[11]

Sigfox the first LPWAN technology proposed in the IoT market, was founded in 2009 and has been growing very fast since then. Sigfox low powered connectivity solutions not only improve existing business cases but also enable a new range of opportunities for businesses across all industries. Its physical layer based on an Ultra-Narrow Band (UNB) wireless modulation, it has its proprietary system with low throughput (~100 bps) and low power Extended range (up to 50 km) , 140 messages/day/device ,also it is Subscription-based model , it has its own Cloud platform with and defined API for server access, moreover it offer roaming capability.[12]

Companies select the telecommunications technology that will link their fleet of communication items based on a variety of factors, including technical factors like range, speed.

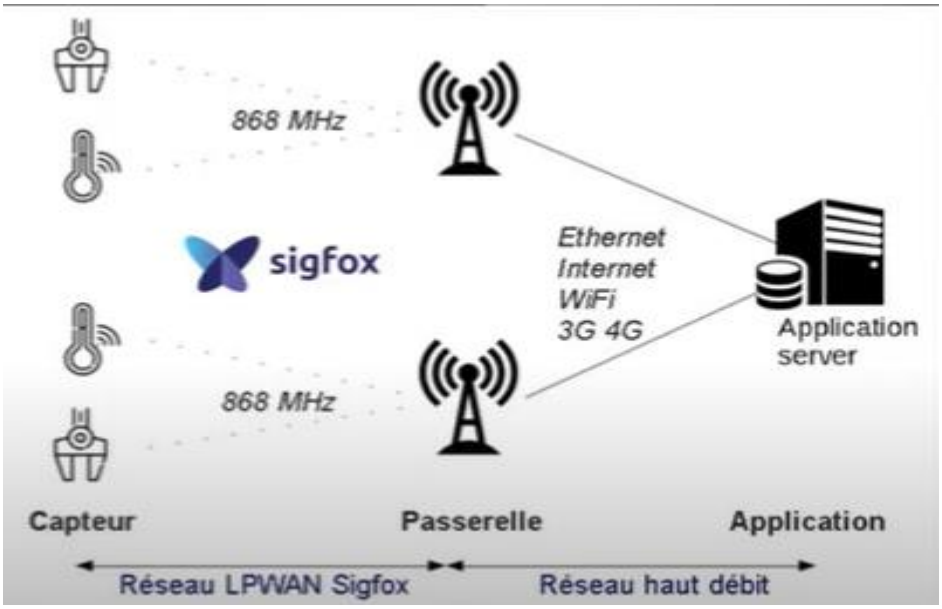

Figure 7: Low Power Wide Area Networks

1.8 Data Transmission Protocols

MQTT, CoAP, AMQP, and HTTP, which are displayed at the top of the protocol stack for IoT network, are the four commonly recognized and developing messaging protocols for IoT systems.[13]

Figure 8 : Protocol Stack for IoT Systems [13]

1.8.1 MQTT (Message Queuing Telemetry Transport Protocol)

MQTT, which was first developed in 1999, is one of the earliest M2M communication protocols. It was created by IBM's Andy Stanford-Clark and Arcom Control Systems Ltd's Arlen Nipper. It's a lightweight M2M messaging protocol built for limited networks that uses publish/subscribe messaging. A MQTT client sends messages to a MQTT broker, which are

then subscribed to by other clients or saved for future subscription. Every communication is sent to a specific address, referred to as a topic. Clients can subscribe to multiple topics and get all messages sent to those topics. MQTT is a binary protocol that typically needs a 2-byte fixed header and tiny message payloads up to 256 MB in size. TCP is the transmission protocol, and TLS/SSL is used for security.[13]

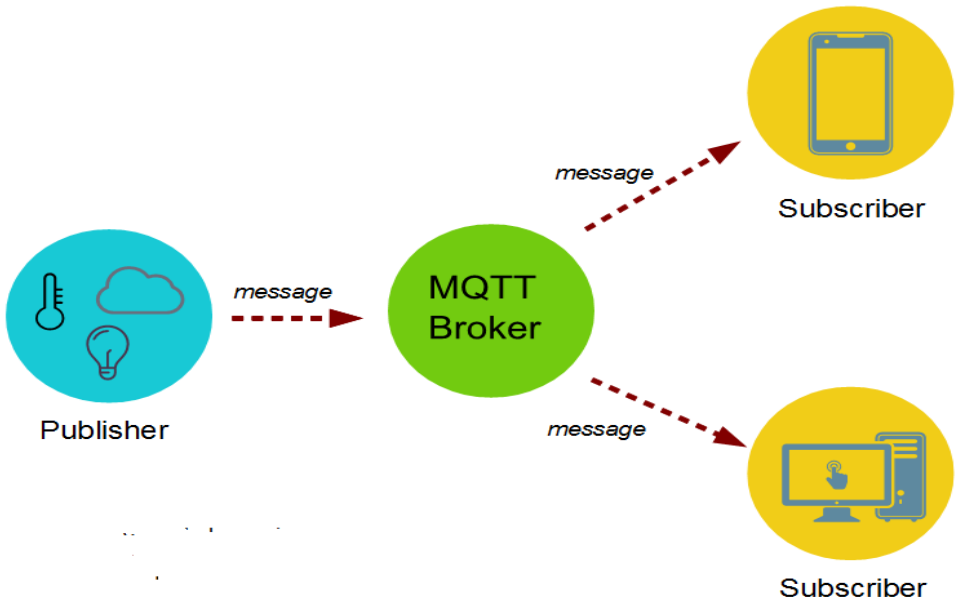

Figure 9: MQTT protocol functionality

1.8.2 CoAP (Constrained Application Protocol)

CoAP is a lightweight M2M protocol from the IETF Core (Constrained RESTful Environments) Working Group. CoAP supports both request/response and resource/observe (a variant of publish/subscribe) architecture. CoAP is mainly developed to interoperate with HTTP and the RESTful Web through simple proxies. Publisher publishes data to the URI and subscriber subscribes to a particular resource Unlike MQTT, CoAP uses Universal Resource Identifier (URI) instead of topic. Publisher publishes data to the URI and subscriber subscribes to a particular resource indicated by the URI. When a publisher publishes new data to the URI, then all the subscribers are notified about the new value as indicated by the URI. CoAP is a binary protocol and normally requires fixed header of 4-bytes with small message payloads up to maximum size dependent on the web server or the programming technology. CoAP uses UDP as a transport protocol and DTLS for security.[13]

1.9 IoT Application Domain

As the world's needs have grown, the Technology of IoT has been used to make people's lives easier it's getting into multiple fields; there is many IoT application domains like, home automation, energy, developed urban areas, transportation, healthcare, manufacturing and agriculture, as depicted in figure 10

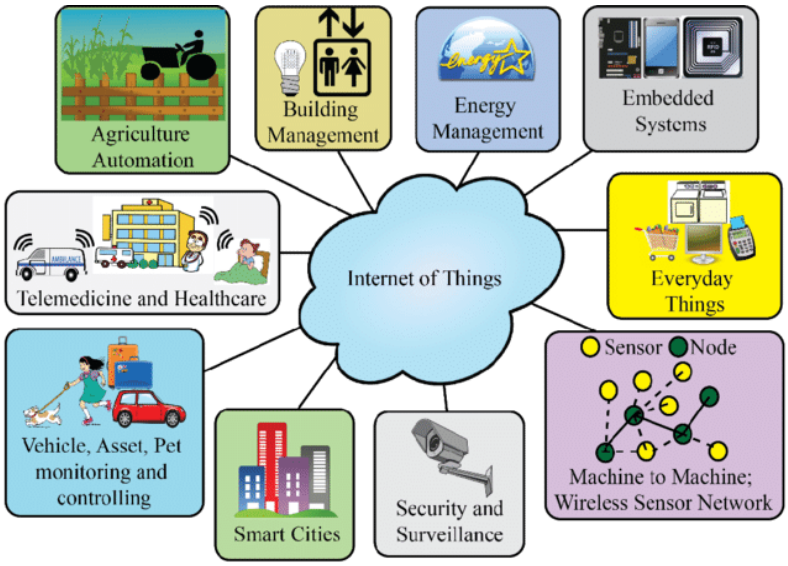

Figure 10: IoT application

- **Smart home system model**

A smart home system has the ability to make our lives much easier. Starting with energy management, which includes the power controls system and the thermostat, all of this is handled to reduce the amount of energy consumed. This includes a door management system, a security management system, and a water management system, all this devices can be remotely monitored and controlled using smartphones, tablets, or laptop computers from anywhere in the World via the Internet or private network. A controller, which may be any IoT home automation hub, a wireless router, and Wi-Fi enabled smart home appliances that can interface with a home automation software platform like OpenHAB and Home Assistant . The software platform enables users to operate devices wirelessly from a smartphone or any computer connected to the home network. The router Ethernet interface connects the controller to the home network. You can also use a Raspberry Pi Single-Board

Computer (SBC) as the controller. MQTT is a message protocol that is frequently used to communicate between the home automation software platform server and smart devices.[14]

Figure 11: Smart home

- **Smart healthcare monitoring system model**

Smart healthcare is a health-care paradigm that allows for remote monitoring and Telehealth, which permits doctors and other medical practitioners to examine, diagnose, and treat patients remotely, A typical smart healthcare monitoring system, shown in figure 12 , comprises of two outpatients, a smart hospital, and an emergency team. A normal patient wearing an Electroencephalography (EEG) sensor, a Blood Pressure (BP) sensor, and a Blood Glucose (BG) sensor, and an elderly patient wearing an Electrocardiogram (ECG) sensor and a Blood Pressure (BP) sensor. The sensors on the patients' bodies constantly gather and transfer data through Bluetooth to their smartphones, which then upload the data to the medical server over the Internet. In the event that a patient is in critical condition, these sensors may rapidly notify the patient's physical status to the emergency team and their doctors, who can then take necessary action. [14]

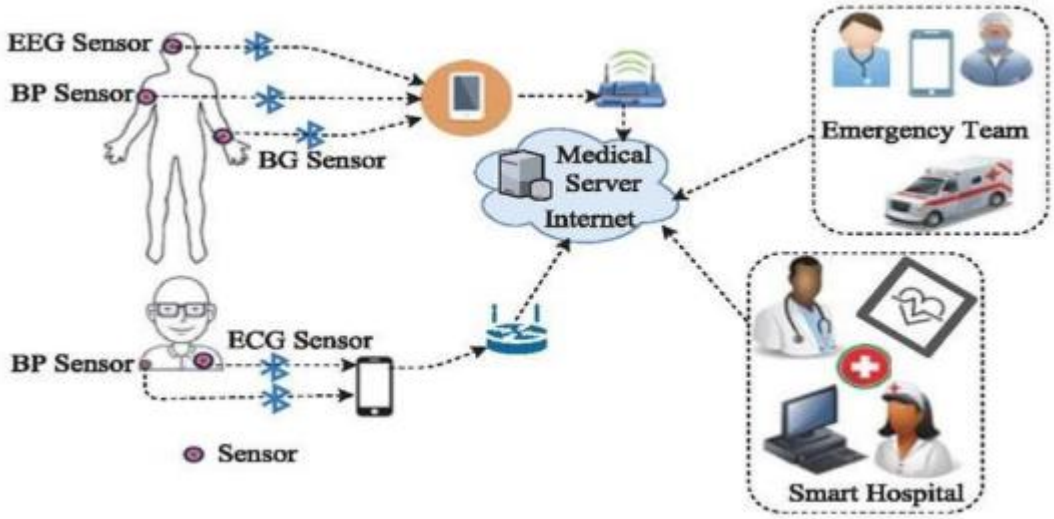

Figure 12: Smart healthcare

1.10 Challenges of IoT

Although the Internet of Things is a promising and helpful idea, and able to deliver efficient solutions to monitoring and remote monitoring problems in a variety of domains. In addition, IoT presents certain critical problems. The following are the most essential difficulties or challenges by IoT:[15][16]

- **Data Management**

Data management is a crucial aspect in the Internet of Things. When considering a world of objects interconnected and constantly exchanging all types of information, the volume of the generated data and the processes involved in the handling of those data become critica.

- **Security and safety**

Health care, smart homes, smart cities, and other essential systems are all highly wanted and in the same time critical , The security and privacy of the IoT network should be supported by the IoT OS. Data integrity, authentication, and access mechanisms are one of the issues that have yet to be resolved ,one of the potential practical ways for addressing privacy and security in the Internet of Things is to use a blockchain-based optimized solution.

- **Interoperability**

Interoperability is the most fundamental core property of the traditional Internet; the first criterion of Internet connectivity is that "connected" devices can "speak the same language" of protocols and encodings. Today's industries employ a variety of standards to support their applications.

- **Device Level Energy Issues**

One of the essential challenges in IoT is how to interconnect “things” in an interoperable way while taking into account the energy constraints, knowing that the communication is the most energy consuming task on devices.

Conclusion

Clearly, the Internet of Things is a revolution in the technology it changed all traditional perceptions and improved human life.In this chapter, we mainly discussed the important technologies as well as the featured applications of IoT. We have also mentioned some drawbacks that should be carefully achieve.

CHAPTER 2: Overview on IoT Security

Introduction

The deployment of huge amounts of constrained IoT devices has the potential to create multiple security issues and cyber-attacks. In this chapter, we focus on studying the likely IoT threats and then, we review the existing countermeasure mechanisms and some related works.

2.1 Security issue in IoT network

While IoT devices play a significant role in the topic of IoT security, due to the larger attack surface of threats that have previously plagued networks, putting all of the attention on this aspect is necessary , the main reason are listed below: [17][18]

- **Software configuration**

Cybercriminals can easily attack IoT devices due to the default software configuration, irregular updates of software installed, a long gap between patch release and its installation, and can have access to each device due to the default login credentials vulnerability. In addition, most of the IoT devices are connected via telnet which is the main perpetrator.

- **Development**

One of the main reasons IoT devices are vulnerable is because they lack the computational capacity for built-in security. Another reason that vulnerabilities can be so pervasive is the limited budget for developing and testing secure firmware, which is influenced by the price point of devices and their very short development cycle.

- **Performance**

Due to the less storage capacity, memory and processing capability, many IoT devices have to be operated on lower power and hence, the security measures fail here and the devices become the victim.

2.2 Taxonomy of attacks in IoT

There are several types of attacks in IoT are listed below: [19][20][21]

2.2.1 Spoofed, Alter, Replay Routing Information

Spoofing, altering, and replay routing are mutual direct attacks that target routing information where data flow between nodes occurs, the attacks are created by generating a false error message, in addition creating a routing loop and many more techniques. Additionally,the spoofer does not emit a signal at first, instead listening to the proper transmitter. Spoofer starts transmitting the unreliable signal when the node transmitter stops providing a signal to the node receiver.

2.2.2 Sybil Attack

The growth of the Internet of Things exposes a system to the Sybil attack, which is defined as a single node with several identities .That implies the opponent might be in several places at the same time. Its goal is to compromise data security and resource consumption.

2.2.3 Denial of Service (DoS)

DoS attack is a particular attack on a network, moreover, there are two categories of DoS attack in IoT:

- **Dos (**Ordinary DoS)

In this attack a tool is required to send packets to an intended system that crash the network or sometimes force the system to restart

- **DDos (**Distributed Denial Of Service**)**

In this attack can be a single attacker, the impact of this attack not only disabled the network but also prevent it to be accessible to a very large network.

2.2.4 Attacks based on Device Property

Low-end devices class or high-end devices class are two types of device properties. The impact of these attacks on the IoT system is varied, because of the power of device property, IoT may result in a fatal error or just a part of the system may operate abnormally.

- **Low-end device class attack**

This class is low-cost since it simply uses a radio connection to connect to the outside world and only a few IoT sensor nodes have access to it , for example, the smartwatch can manage any household device remotely, such as a smart TV or a smart refrigerator.

- **High-end device class attacks**

Full-fledged devices are used to launch attacks against IoT systems in high-end device class attacks. This class connects their IoT devices to the Internet so that they can be accessed from anywhere and at any time by a laptop (powerful device).

2.2.5 Attacks based on Access Level

There are two ways for attackers to get access to the IoT system, depending on their access level:

- **Passive attacks**

Passive attacks involve monitoring and eavesdropping, one of its characteristics is that the attackers do not know anything about the user and do not disturb the communication in IoT they only learn or make use of the information from the system.

- **Active attacks**

Active attacks, in contrast to passive attacks, attempt to evade or break the information or data's protective feature by connecting to the district and disrupting networking communication.

2.2.6 Attacks based on Adversary Location

This adversary can launch attacks to the IoT system from any location means it depends on his location, so that we can define the category of the attack inside or outside

- **Internal attacks**

It's an attack that started by a component inside the security IoT border, to launch the attack, the attacker tries to execute its own malicious code toward IoT devices.

- **External attacks**

These attack characteristics by that the adversary located out of the IoT range and they traying to access remotely also they do not know anything about the IoT architecture.

2.2.7 Attacks based on Attacks Strategy

In this attack, the attacker tries to execute their own malicious code and they have a strategy to launch and destroy the IoT development there are two viewpoints of the strategy:

- **Physical attacks**

A physical attack against an IoT's infrastructure is one approach for successfully blunting IoT devices, an adversary, for example, modifies the behavior or structure of devices in an IoT system.

- **Logical attacks**

A logical attack occurs when the communication channel breaks down as a result of the adversary's attacks on the IoT system. Attackers do not do physical harm to the devices they use to launch their attacks.

2.3 Attack levels in IoT

There are various IoT architecture models. In general, we will explore the attacks that target IoT which can be operated in serval levels of the IoT architecture.

2.3.1 Physical/Perception Layer

At the physical/perception layer, there are a number of important threats include:[19]

- **Eavesdropping on Wireless Communication**

Attackers can deploy devices that appear as end nodes in an IoT system to sniff wireless traffic and gather data about users**.**

- **Loss of Power**

A battery draining attack prevents a node from going to sleep or energy saving mode by bombarding it with a huge number of legal requests.

- **Malicious Data Injection by Forged Devices**

Any determined malicious attacker can introduce a forged device in an IoT system to eavesdrop on the radio traffic, inject fabricated messages or flood the radio channels with fake messages to render the system unavailable to the legitimate users.

2.3.2 MAC/Adaptation/Network Layer

Numerous threats affect security at the MAC layer and at the adaptation layer, there is a likelihood of a attack on 6LoWPAN protocol, moreover, the network layer is exposed to a wide range of attacks that can affect the road construction phase and even the data routing phase which include:[1]

- **Collisions**

Means collisions among sensor communications or between sensors and base station, intensive collisions cause communications breaks and excessive energy consumption resulting from repeated retransmissions of corrupted frames.

- **Sinkhole attack**

The intruder broadcasts falsified messages announcing that it is the best next destination for data streams, according to the metrics adopted by the routing protocol hence, the nodes receiving the falsified messages will be easily corrupted and will all orient their packets to the intruder.

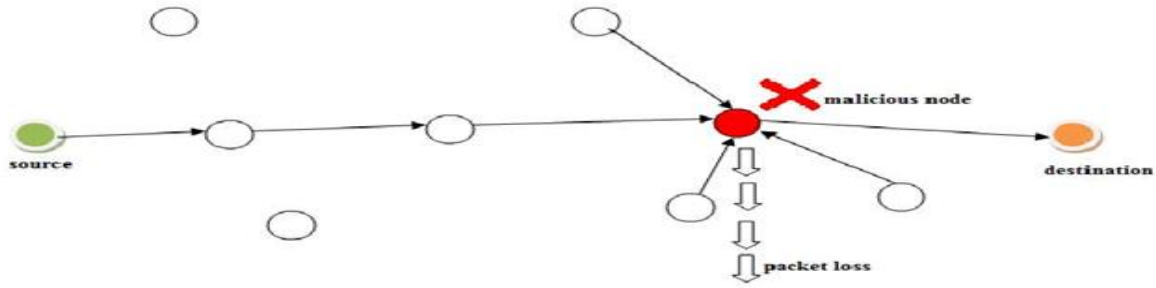

Figure 13 : Sink hole attack

- **Wormhole attack**

A Wormhole assault requires the cooperation of two nodes. These nodes are linked together using higher-performance connections than normal. This link can be made wirelessly or through a wired connection. This link is known as a Wormhole Tunnel. The attacking nodes capture the packets from one location and transmit them to another distant located node that distributes them locally. During the route selection process, these nodes communicate with one another. As a result, they might make it appear as if they had a shorter path to the destination node, then they're included in the route. Because of its distributivity, the wormhole attack is extremely difficult to detect. As a result, a precise placement of the attacking nodes improves the complexity of the attack; for example, an attacker near the base station will entirely destroy the network's routing system.[22][23]

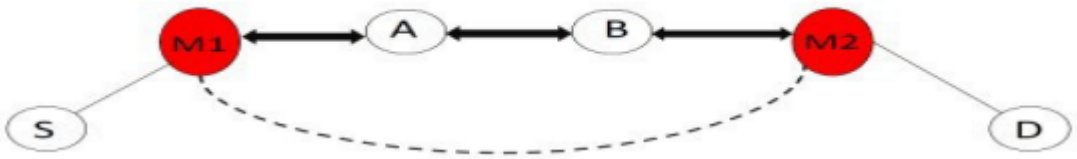

Figure 14:Wormhole attack [22]

- **Hello flooding attack**

The nodes use the 'Hello' message to discover the nodes in neighbor or to announce their current state. An adversary node using a laptop can exploit the fact that the nodes have weak radio ranges, to send via a very powerful signal of messages announcing an optimal route to all nodes in the network; hence, they will update their routing tables with incorrect information. Since the link between the node and the attacker is usually unidirectional, the victim nodes will not be able to use the routes announced by the attacker because it is outside their communication scopes.

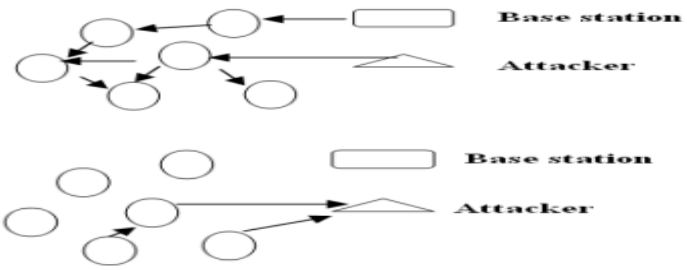

Figure15: Phases of hello flooding attack

Table 2: Summary of attacks and Countermeasures [1]

Attack	Countermeasures
Sinkhole	The authentication
Wormhole	The authentication
Hello flooding	The authentication, Chek the bidirectionality of the communication
Sybil	Symmetric encryption (where each node shares a key secret).

2.4 Mechanisms of protection

Since the IoT facing many security issues hence, this requires a mechanism to prevent and protect IoT devices form threats thus, the researchers developed many mechanism to protect the IoT ecosystem one of this technique is the IDs.

2.4.1 Intrusion Detection System

Intrusion detection is a second line of defense after the cryptography-based solutions that have yet to fit the IoT constraints and limitations. An intrusion detection systems IDS is a system that uses various detection methodologies to identify the assault then sends an alert or report to the system's administrator. The IDS might be a single device that monitors a standalone system or a network system that does local analysis to identify attacks. In addition, IDSs provide the following three critical security services [1] :

- **Data confidentiality**

Which determines whether data is kept in a secure location in the system.

- **Data availability**

Which checks if data are available for an authorized user.

- **Data integrity**

Which checks if data are correct and consistent with other data in the system.

2.4.1.1 IDS types

- **Centralized IDS**

All detection agents in this type of intrusion detection system transmit their results to the base station, which is the only entity responsible for making final choices on intrusion

detection and isolation in this case. Because the base station has the most memory, energy, and processing capability, it will be able to use considerably more complicated and reliable detection methods. Another issue is the periodic broadcast of detection information to a single center might result in excessive energy consumption at the nodes, putting the connections leading to the base station in danger of congestion. [1]

- **Distributed IDS**

The nodes must work together to detect any malicious behavior that may exist in the network. Therefore, detection strategies must achieve a compromise between credible detection and lower cost (low energy consumption, low memory, and a reduced number of control messages and alerts). [1]

- **Hybrid IDS**

The hybrid design combines centralized and distributed architectures into a single intrusion detection system. This will allow both architectures to benefit from the advantages of having ids that perform properly. [1]

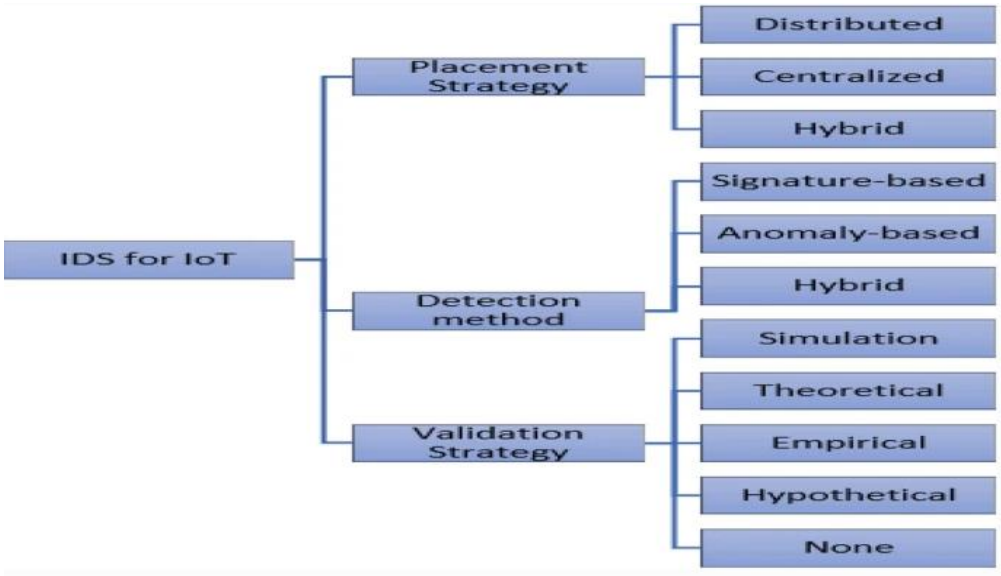

Figure 16: Architecture of IDs

2.4.1.2 IDS Detection approach

Signature and anomaly are two of the most well-known IDS approach, there are some other approach listed below :[24]

- **Signature-based IDS**

Also known as rule-based IDS, is suitable for detecting known attacks with signatures that are already in the database;. An attack is defined as any divergence from the set rules in

the network's behavior. This sort of detection has the benefit of being able to precisely and effectively detect known assaults, resulting in a low false-positive rate. This sort of detection has the drawback of being unable to identify new security assaults or attacks with no preset rules or zero-day attack.

- **Anomaly based IDS**

Statistical behavior modeling is used by anomaly based IDS to monitor network activity and classify them as normal or malicious. The members' normal operations are profiled, and any variation from the typical behavior is marked as an abnormality. The capacity to identify new and undiscovered attacks is the major benefit of anomaly based IDS. Because network activity can change fast, this detection technique has the drawback that normal profiles must be updated on a regular basis.

- **Statistical Based**

The network traffic is collected in this category, and next a profile depicting its stochastic behavior is constructed. A reference profile is created when the network is operating normally. moreover the network is then monitored, and profiles are created on a regular basis, with an anomaly score calculated by comparing the profile to the reference profile. The IDS will report the occurrence of the anomaly if the score exceeds a particular level.

- **Hybrid Detection**

Hybrid IDSs combine anomaly-based and signature-based detection techniques. In general, hybrid systems include two detection modules: one identifies well-known assaults using signatures, while the other detects and learns normal and harmful patterns, or monitors network activity deviations from the typical profile. They are more accurate in detecting attacks and have fewer false positives. These methods, however, need more energy and resources. Hybrid IDSs are typically not recommended for resource-constrained networks like a WSN, although they are still a popular research area.[25]

2.5 IDS Architectures for WSN

In addition, the researchers have divided ad-hoc network IDS designs into three groups, which may be changed to meet the needs of WSN IDS

- **Stand-Alone**

In this approach, each node acts as independent IDS, accountable only for detecting assaults against itself; that is, all network nodes are capable of operating an IDS. The IDS does not share data or collaborate with other systems.[26]

- **Distributed and Cooperative**

In this approach, each node continues to run its own IDS, but the IDSs of all nodes collaborate to establish a global intrusion detection system like it's shown in the figure 17.[26]

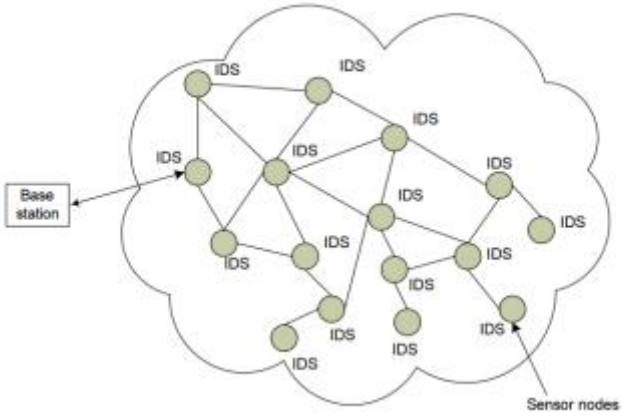

Figure 17: Distributed IDS Architecture.[27]

- **Hierarchical**

The network is organized into clusters with cluster-head nodes in this category. These nodes are responsible for routing within the cluster and accept all the accusation messages from the other cluster members indicating something malicious. Furthermore, being the backbone of the routing architecture, the cluster-head nodes may detect attacks against the network's other cluster-head node.[26]

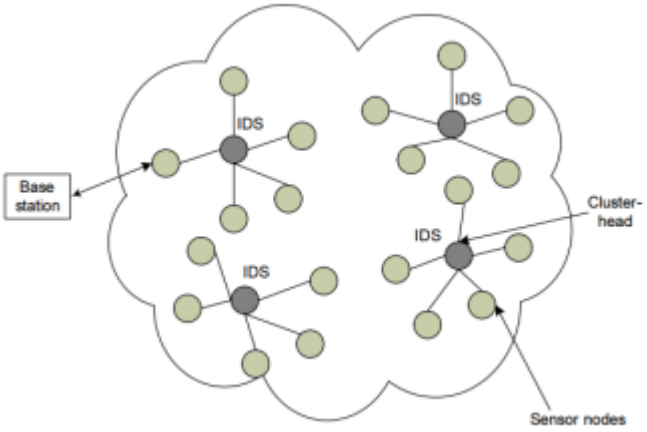

Figure 18: Cluster-based IDS Architecture.[27]

2.6 Related work

2.6.1. Intrusion detection in wsn using modified AODV algorithm

A. Description of the project

The researchers in [28] have developed a scheme for intrusion detection system for the wireless sensor since it's become employed in various application, this proposed dealing with the limited resource and power of the sensors, moreover this solution is for the purpose of prevent and minimize the loss of the information .

B. Principle of work

The Suggested IDs working by modifying the aodv routing protocol from the weakness that maybe cause of the vulnerability .

Moreover all the phases of routing discover, and establishing the link to send data will be the same the only modification based on two main factors which are combo of the source address and the request id that's mean each received request to the node he will verify the combo address of the request message and if it's already excite then the request will be discard.[28]

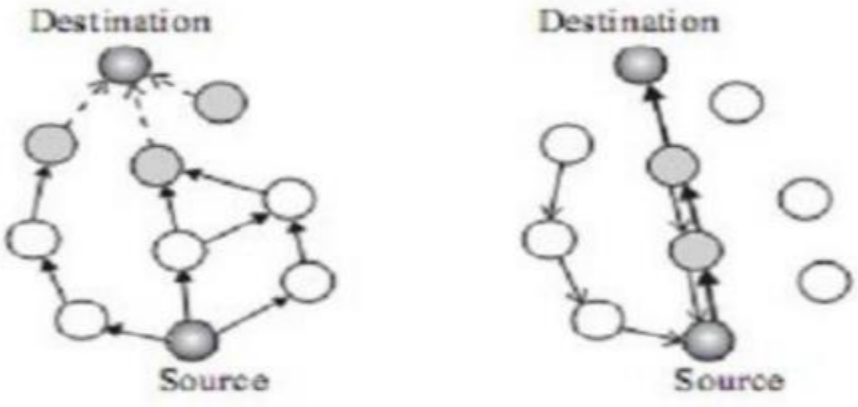

Figure 19: Phases of AODV protocol [28]

C. Outcomes of the solution

Researchers suggest enhanced Ad hoc On-Demand Distance Vector Routing for intrusion detection in wireless sensor networks, which displays high performance under assault.[28]

2.6.2 A Novel Intrusion Detection System for Detecting Black Hole Attacks in Wireless Sensor Network using AODV Protocol

A. description of the project

Since their widespread usage in a range of applications, wireless sensor networks have a number of drawbacks, including low power consumption and limited storage, making them

more vulnerable to assaults. The watchdog methodology, suggested by the researchers, is a method for detecting misbehaving nodes in which each node can hear the communication of neighboring nodes, implying that each packet transmitted in the network is watched by neighboring nodes. They observe the node's activity to verify if it successfully transmits the packets it receives. [29]

B. Principle of work

The presented method for detecting black hole attacks in wireless sensor networks for secure data transfer, as shown in the figure, which signifies if the packet would flow the channel from A to C. By listening promiscuously to node B's transmission, node A may determine if node B passes the packet to node C or not. Because node A is within range of node B, it may listen in on communications between the two.

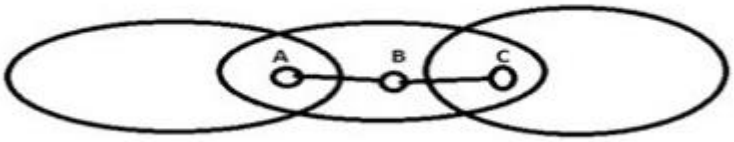

Figure 20: The path of flow data [29]

The proposed method is divided into two phases: Initialization phase and Detection phase.

Initialization phase

⇒ Assuming that the watchdog node cannot be a malicious node, the selection of the watchdog node is based on the fact that the watchdog node is a highly connected node from the neighbor table can be calculated, the watchdog node will monitor the node's end-to-end behavior while communicating.[29]

The second phase is Detection phase

⇒ The watchdog node looks for the malicious node at intervals of time t. The route table, source table, and destination table are all maintained by the watchdog node. When the path from source to destination is discovered, a route table is created. When packets are sent from a source to a destination node, the source table is filtered by the source entry in the route table, and when packets are sent back from the destination to the source node, the destination table is filtered by the destination item in the route table.

All this process it's shown in the figure which happened in the route discovery of the destination when source broadcasts the RREQ packets, The packets are monitored by the

watchdog node, which generates a source table for each RREQ packet and a destination table for each RREP packet. [29]

Notation: Rt =Route table, St=Source table, Se=Source entry, Dt=Destination table, De=destination entry, S=source, D=Destination, Qi=Common node.

Algorithm:

BEGIN

Initialization phase:

1. Create a topology T={q1,q2,q3,-------,q_n}
2. Select a watchdog node W from T (W ∈ T).
3. W monitors the Network traffic.
4.

Detection phase:

5. For each threshold time (t) repeat Step-5 to Step-12.
6. Trace RREQ and RREP packets
7. Create Rt.
8. Filter St from Se in Rt.
9. Filter Dt from De in Rt.
10. Compare route given by S and D.
11. Search Qi.
12. If Qi present

    Then

        No malicious node present.

    Else

        Node is malicious.
13. Stop Simulation.
14. goto Step-3.

END

Figure 21: General steps of detection [29]

Since that the malicious node is blackhole attack so it s the first node to response with RREP .The watchdog node to detect the malicious node uses the following specific rules:[29]

1. First he will analyze the path found from the source to the destination. If the path discovered by the source and destination contains common nodes, then no dangerous node exists; otherwise, any node that is uncommon in the path from any table may be a malicious node.
2. The second one he will check the sequence number and the hop count a according to specific algorithm shown below its depend on two condition the hop count and the sequence number.

.

```
hop count=H, Sequence Number=Sn, Output=Op.
L:
If (H= 1 || Sn = Max)
{
        Op= =1;
  }
Else
{
        Op= =0;
}
if ( Op= =1)
   {
  "Node is Malicious".
   }
Else
{
goto L;
}
```

Figure 22: Algorithm to eliminate malicious reply [29]

C. Outcomes of the proposal

The researchers demonstrated an effective strategy for identifying black hole attacks in a wireless sensor network; the model enhances network performance by eliminating the malicious node from the network.[29]

2.6.3 Secured AODV to protect WSN against malicious

A. Description of the project

The researchers in [30] suggest a new defensive mechanism based on the Ad hoc On-Demand Vector (AODV) routing protocol to secure AODV and protect WSNs from malicious intrusion and adversary assaults. The fundamental feature of secure aodv is that it works well with WSN dynamics and topology changes and offers secure multi-hop routing between sensor nodes. Also to reduce packet loss in the network.

B. principle of work

The primary goal of enhancing AODV is to ensure that data packet loss is decreased or completely handled moreover Several technique were utilized by the researchers to prevent data packet loss in the AODV protocol which is mentioned below :[30]

First Nth Backup Route (AODV nthBR) Technique: in the AODV context, the Nth Backup Route strategies provide a backup route means this approach aids the protocol in locating the closest node to the failing node.

Second Pre-request Receive Reply Technique: It's an algorithm or set of steps at the source node that will delete all of the malicious node's fake replies and ensure that the packets are not lost

```
select Dest_Seq_No from routing table
if (P.Dest_Seq_No > Dest_Seq_No)
        update entry of P in routing table,
        unicast data packets to the route specified in RREP
    else
        discard RREP
else
    if (P.Dest_Seq_No ≥ Src_Seq_No)
        Make entry of P in routing table
    else discard this RREP
```

Figure 23: Algorithm to delete fake reply [30]

Third Using Digital Signatures and Hash Functions: these are primarily used to improve the security and performance of the AODV protocol when it is vulnerable to a black hole attack. Receiving nodes will be able to know that a packet is from a given source node since it will be transmitted with digital signatures. Encrypting the message using a source code that can only be decoded by the node with the key is what hash functions do.

```
if (route does not exist)
    Check cache for already existence request that is sent for destination
    if (the request has not been sent already)
        Create a RREQ packet
        Add (dest addr, broadcast ID) to cache
        broadcast RREQ locally
        the timer is set for RREP_WAIT_TIME for rebroadcasting RREQ
        Increment broadcast ID
```

Figure 24: Pseudo-codes sending RREQ [30]

Fourth Secure AODV: it’s used mobile network, secure AODV may be utilized to improve AODV. It utilized to provide essential security features including non-repudiation, authentication, and integrity to protect route discovery .Each node in this Improved Protocol is assumed to have a signature key pair generated by a suitable asymmetric cryptosystem**.**

Last Using Data Structure Algorithms for Path Compression: this network's nodes deactivate the MAC address, allowing them to listen to all traffic within their radio range. When a network node has a packet for a destination, it accumulates all essential information and determines a route; after that, the node listens for data packets promiscuously

C. result of proposition

The researchers optimized the secured AODV protocol's compatibility with WSN dynamics and topology changes caused by limited available resources, as well as the routing protocol's performance under black hole attack.[30]

Conclusion

Obviously, the security of IoT is a large research field due to the diversity of the threats and the variety of protection strategies. In this chapter, we mainly discussed the important security issues in IoT as well the popular threats also some mechanisms of protection with some related work.

Chapter 3: Presentation of the solution

Introduction

Considering a wide comprehension of the major theoretical principles in the previous chapters, this chapter is primarily concerned with covering fundamental concepts related to the field under study. It will also describe the Ad-hoc on Demand Distance Vector (AODV) routing protocol and demonstrate the black hole attacks and the method of detection also the impact of sybil and grey hole attack in the network. Following that, it will define the architecture of the planned work.

3.1 Ad-hoc on Demand Distance Vector Route Protocol (AODV)

Authors in [31] have proposed the AODV reactive routing algorithm. It is designed for mobile infrastructure-less networks and follows the distance vector routing concept. Because of node mobility, network topology changes often, making the active route useless and necessitating the discovery of a new route. As a route freshness indication, AODV employs a sequence number.

In AODV, routes are found on demand. When a node in the network requires a route to a destination, it broadcasts a route request RREQ. To update its routing table, each nearby node that receives the broadcasted packet must validate the freshness of the routing information through sequence number. This request will be routed to the target node or a node that has an active route to the destination. A destination will unicast a response packet RREP to the source using the shortest path with a sequence number higher than or equal to the one received in the RREQ. After receiving a RREP, a source node begins transmitting data packets to the destination

A route is considered active as long as data packets are sent from the source to the destination on a regular basis. When the source stops sending data packets, the connection expires and is removed from intermediate node routing tables. When a link inside an active route breaks, a route repair procedure is started by sending an RERR packet to the source. When an RERR is received, the node source restarts the route discovery process in order to locate a new path.

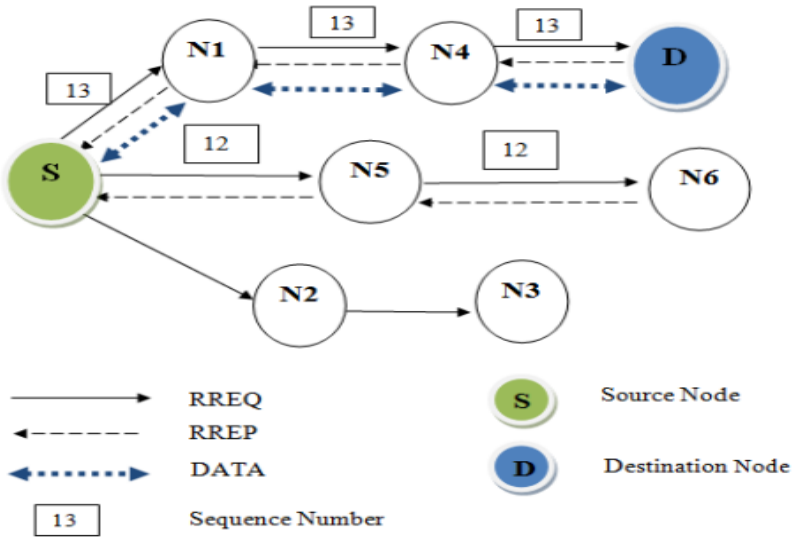

Figure 25: Process of AODV.[31]

3.2 Control Messages in AODV

To discover a path to the destination node in the network, AODV uses three types of control messages

Route Request Message (RREQ)

When a node need a route to a destination but doesn't have one, it sends out an RREQ. The AODV floods the RREQ message.[32]

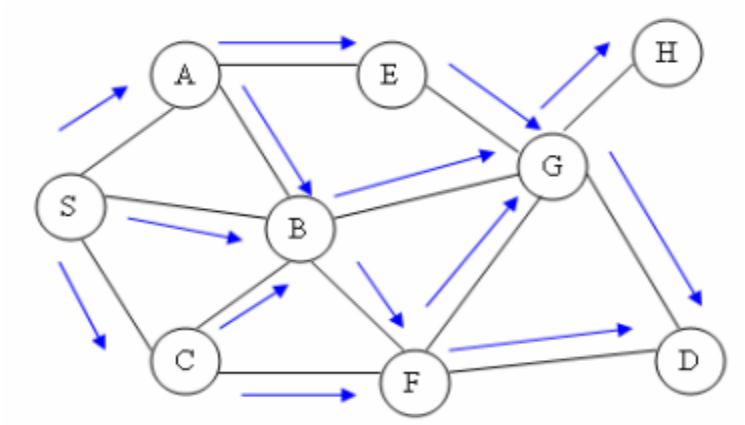

Figure 26: Flooding RREQ in AODV.[33]

Route Reply Message (RREP)

When the destination node or a node with a route to the destination sends a Route reply message (RREP) message back to the originator node, the originator node receives it.[32]

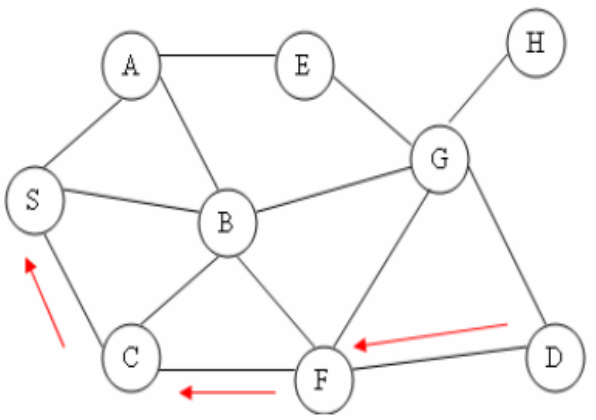

Figure27: Route Reply in AODV. [33]

Route Error Message (RERR)

In an active route, every node in the network maintains track of the state of the links to its neighbors' nodes. If a link fails in an active route, the node route discovery repair procedure by delivering a Route error message (RERR) message to warn other nodes that the link is down. [32]

Hello messages

Since AODV is a reactive protocol, it utilizes Hello messages on a regular basis to notify its neighbours that the link to the host is active. Hello messages are transmitted with a TTL of one, indicating that the message will not be carried further.[35]

3.3 Route Discovery Mechanism in AODV

When a node wants to communicate with another node, the source node first checks his routing table to see if an entry for this destination node exists; if not, the source node sends an RREQ message. This message will be disseminated via limited flooding to neighbours, who will then send it to their neighboring nodes.

This method is repeated until the destination node or a node with a fresh enough path to the destination is found. Then they generate an RREP message and send it unicast to the source node. When the source node gets RREP, a route between the source node and the destination node is established. Once the route is formed, nodes will be able to interact with one another [32]

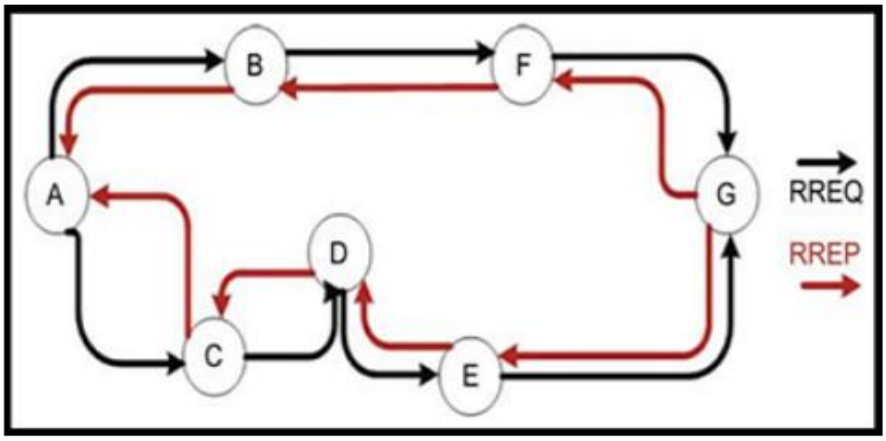

Figure28: AODV route discovery.[32]

3.4 Route Maintenance in AODV

A RERR message is provided to the source node if a link is down or a link between destinations is broken, rendering one or more links inaccessible from the source node or neighboring nodes. When an RREQ message is broadcast in order to locate the target node from the neighbors' nodes.

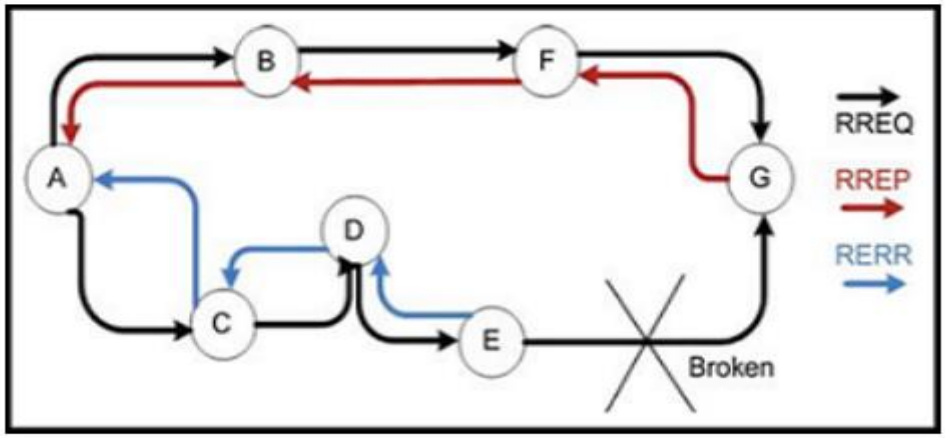

Figure 29: AODV Route Error Message.[32]

3.5 Black Hole Attack

The black hole attack is well-known, active, and dangerous network attack, moreover, it pretended as a legitimate node and took the control of the network by providing false information Therefore, Blackhole nodes allow routing packets, which are used to find a route to the destination node. Moreover, it did not allow any data packets through means when a

source node wants to route a packet to the destination node, it uses a specific route if such a route is available in its routing table. Otherwise, nodes initiate a route discovery process by broadcasting Route Request (RREQ) message to its neighbours. The attacker injects false routing information when he received an RREQ packet to behave as having the best path to the destination in addition the attacker send a fake replay packet in which the sequence number field is set to a higher value, and a smaller number of hops. The source then starts to send out its data packets to the black hole trusting that these packets will reach the destination. In this case, the attacker can intercept all transmitted data packets then drop them.[23]

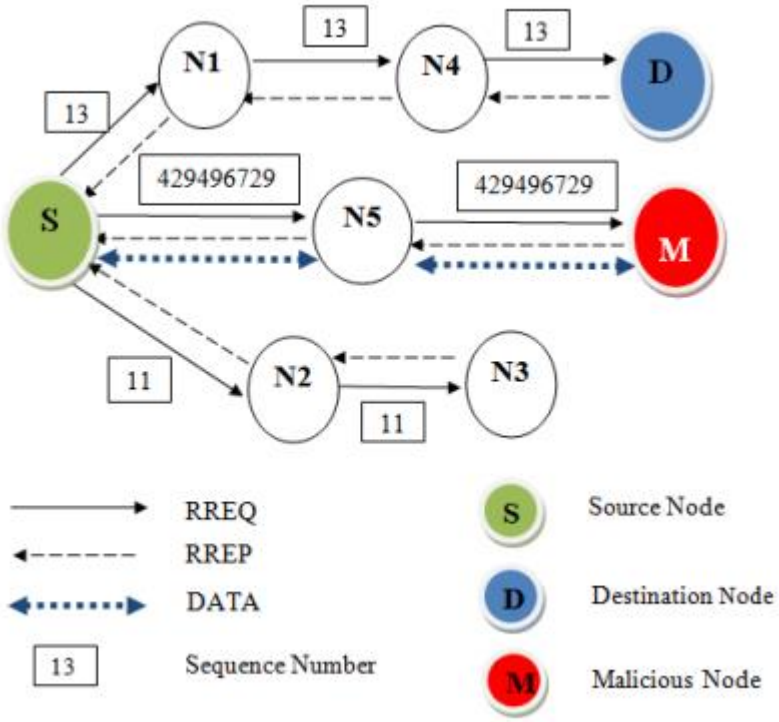

Figure 30: Process of blackhole attack [31]

3.6 The Grey hole attack

The Gray hole attack is a variation on the Blackhole attack.. Although it acts quietly, which are similar in the way they occur at the network layer and target routing. These types of attacks do not put incorrect information into route discovery. The mechanism of the attackers use a selective data packet dropping method; moreover, the malicious node drops the packets randomly or with random selection, the node behaves correctly and replies true RREP messages to nodes that initiate RREQ message this could discard packets entering the node or forwarding packets so there will be no track of this attack and difficult to detect. [23]

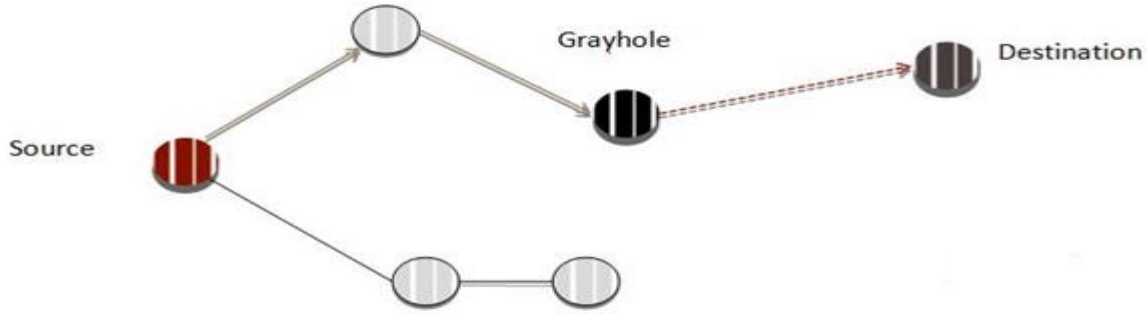

Figure 31: Process of greyhole attack

3.7 Sybil Attack

Sybil appears to be the most difficult attack that may reach routing protocols; even so, the malicious node may create information such as multiple routing requests that make it appear as if there are many nodes; hence, the single Sybil node may attract several packets from multiple nodes by fabricating several identities so that the nodes will trust and send data packets to Sybil node. An attacker can connect or process the malicious activity with its Sybil nodes in two ways: directly and indirectly [34]

- **Directly**: a malicious node delivers messages to legitimate nearby nodes under different Sybil identities.
- **Indirectly:** a malicious node does not send any messages via its Sybil nodes means the Sybil node can interact with the victim node through the malicious node.

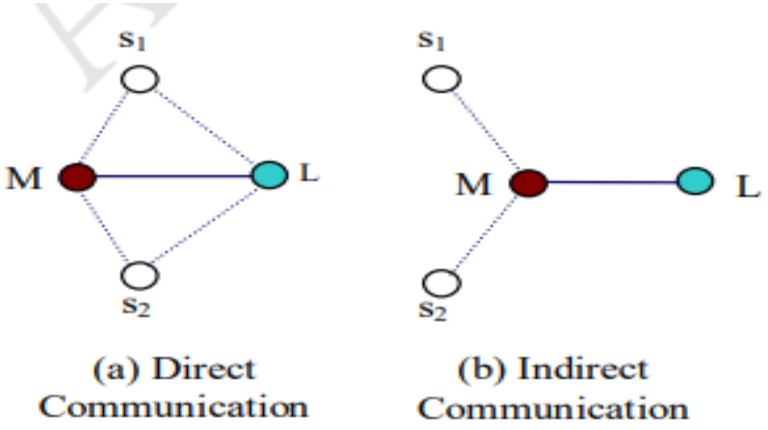

Figure 32: Process of malicious node with Sybil [34]

3.8 Proposed Approach

In this work, we proposed a detection method of blackhole attack and also 2 attacks that can assault and harm the routing phase using the weakness of AODV routing protocol. Before beginning the development or programming process, we must first represent our planned work as an abstract architecture; figure 33 depicts the overall architecture of the experiment.

Figure 33: Global architecture design of the proposed study

Our study is currently divided into five phases, according to our global architecture, which are stated as follows:

- **Phase 1**: Deploy the nodes into the topology
- **Phase 2**: Implement the blackhole attack and the detection method

- **Phase 3**: Analysis and compare results carried out in previous phase to evaluate the performance with blackhole attack then with detection to see the impact of the blackhole attack in the network.
- **Phase 4:** implement the Sybil attack and grey hole attack with multiples malicious nodes
- **Phase 5:** Analysis and compare results carried out in previous phase to evaluate the damage that can be in the network

A. Black hole attack approach

Our solution for black hole attack has two phases as we show in figures number 34 and number 35

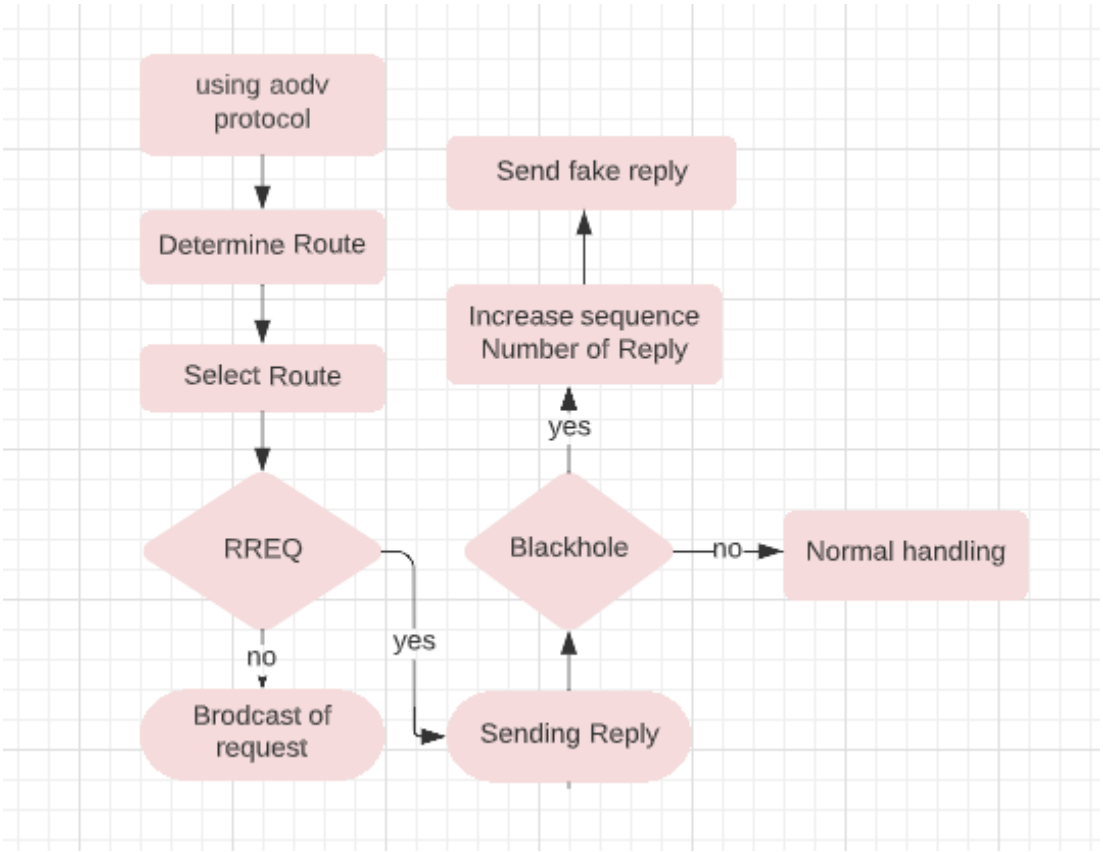

Figure 34: Signal plane for blackhole attack

The blackhole attack has two phases:

1. the first one is shown in the figure 34 which happen in the route discover when a node looking for the destination by sending RREQ packet in broadcast way when the attacker

receive the RREQ packet so he pretend that the destination is in his side by one hope then he increment sequence number to make the honest node think it's new route to the destination after that the attacker node send the fake reply to honest node

2. the second one is shown in the figure 35 which happen when the honest node receive the fake reply and establish the connection and start sending data to the malicious node when the malicious node receive data he start dropping the all packet received.

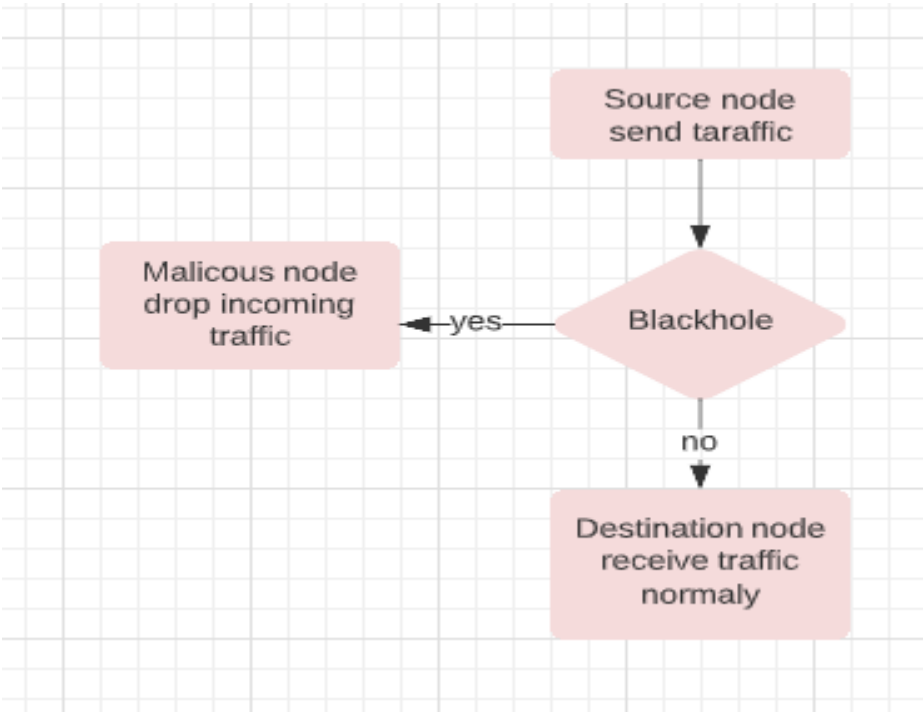

Figure 35: Data plane for blackhole attack

B. Sybil attack approach

Our proposed solution for Sybil attack has two phases as shown in the figures:

1. the first one is shown in the figure 36 which happen in the route discover when a node looking for the destination by sending RREQ packet in broadcast way then the attacker or the malicious node create different identities called Sybil identities if any Sybil node receive RREQ packet the malicious node will send fake reply to the honest node using the identity of Sybil node who receive RREQ packet.

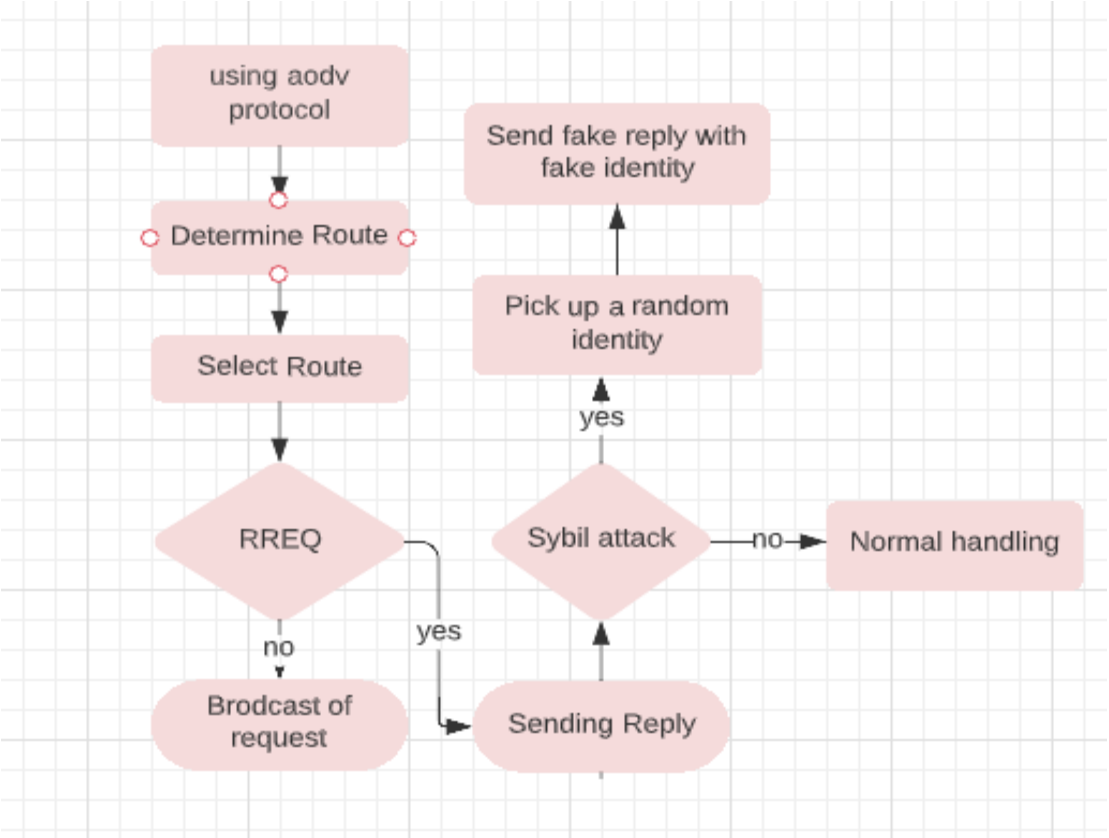

Figure 36: Signal plane for Sybil attack

2. The second phase when the honest node receive fake reply he start sanding data to malicious when the malicious node receive data he start dropping the all packet received this process is shown in the figure 37

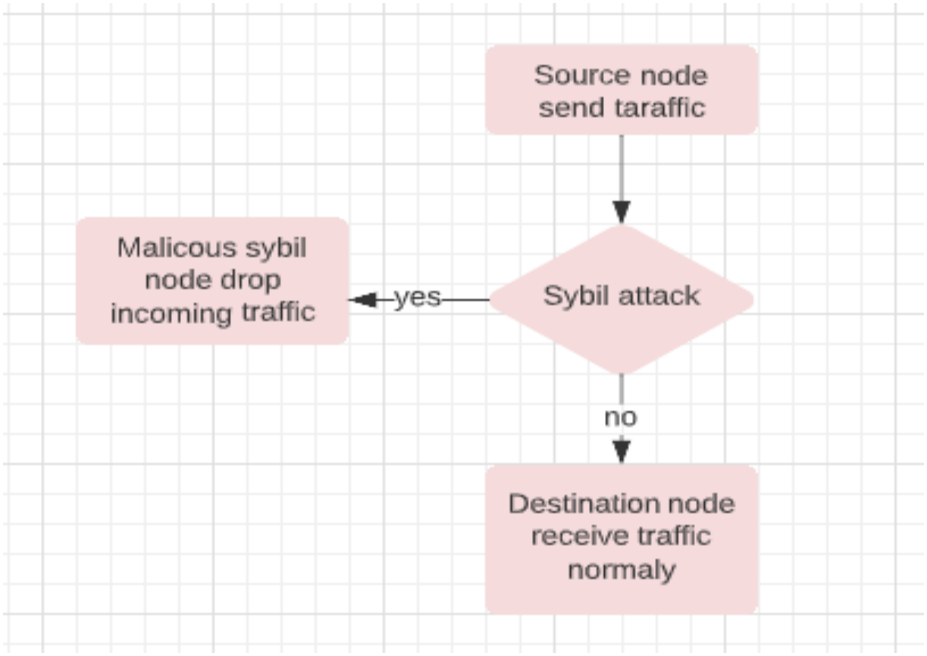

Figure 37: Data plane for Sybil attack

C. Grey hole attack approach

Our solution for grey hole attack has two phases as we show in figures 38 and 39

1. The first one is shown in the figure 38 which happen in the route discover when a node looking for the destination by sending RREQ packet in broadcast way then the attacker or the malicious node receive the RREQ packet so he pretend like he is not malicious node and broadcast the RREQ to his neighbor and sometimes he will drop also the RREQ Packet randomly.

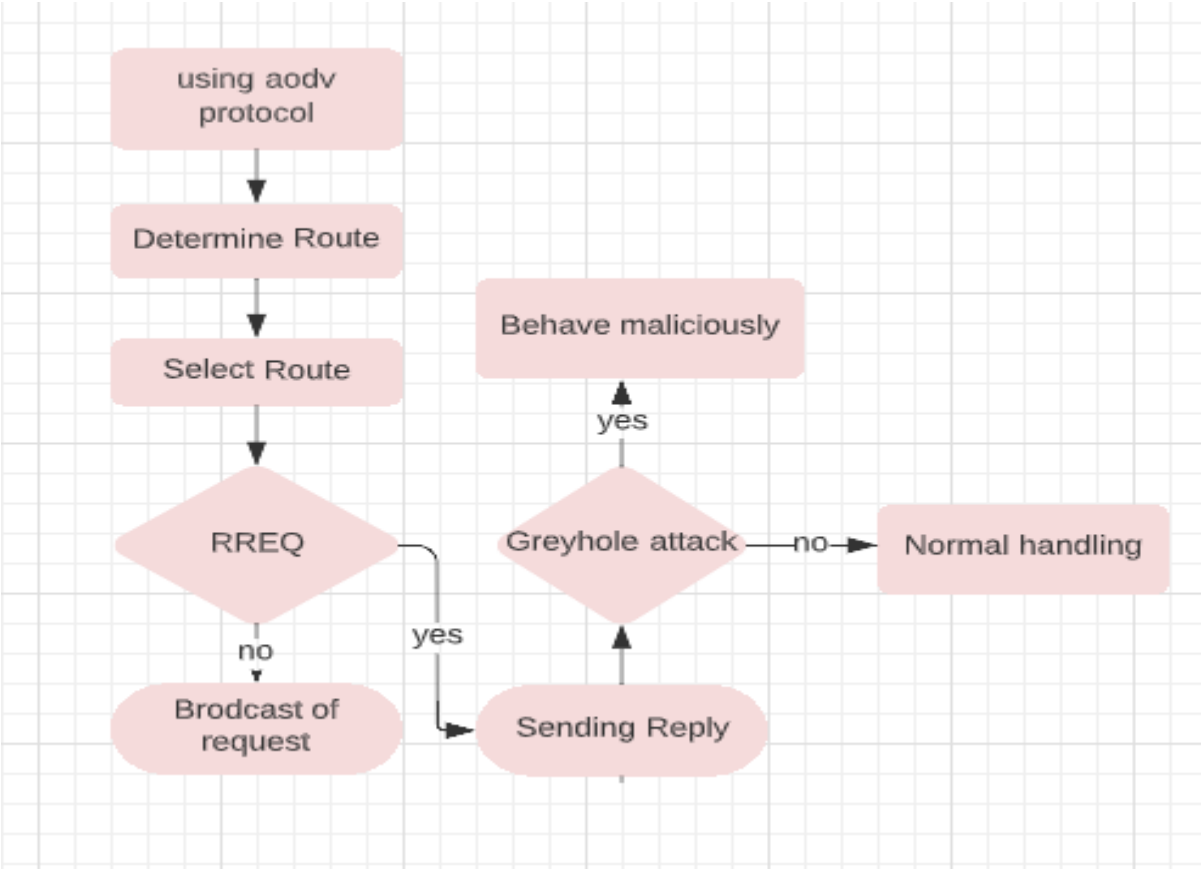

Figure 38 : Signal plane for greyhole attack

2. the second phase when the attacker node broadcast the RREQ packet knowing that the destination is by his side ,the honest node start establishing the connection between here and the destination through the malicious node so the attacker node will drop the packet randomly and with probability means some time will drop and sometimes will send the data .

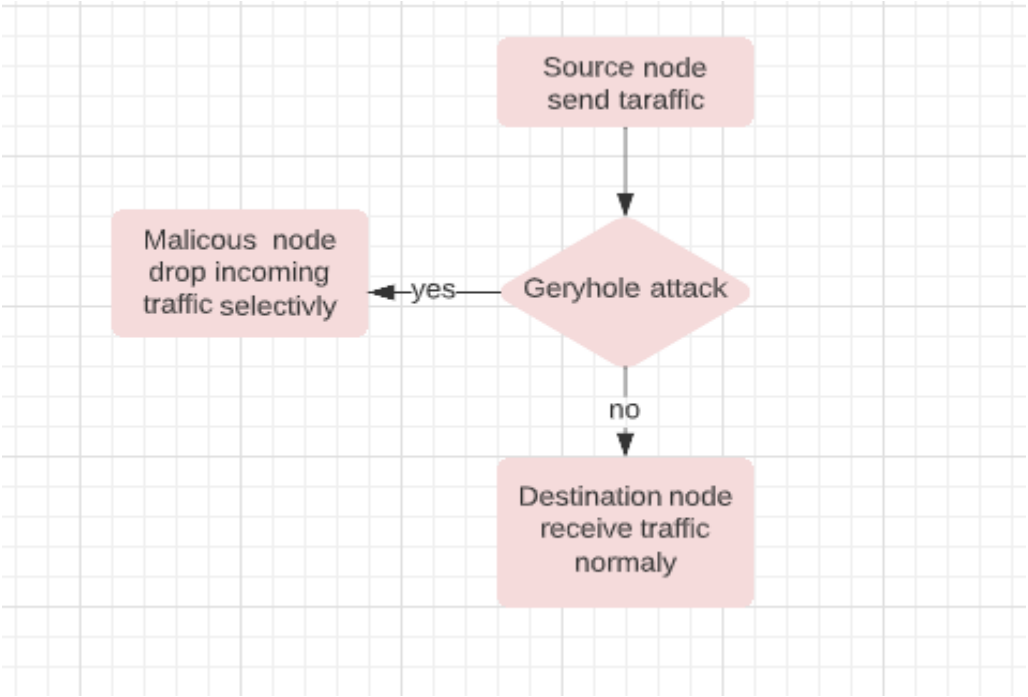

Figure 39: Data plane for greyhole attack

3.10 Proposed Approach for detection the blackhole

The proposed method for detecting and preventing blackhole attacks is designed with the constraints in account (battery power, storage and processing power) ,the primary characteristics of this suggested solution are that it does not change the function of either the intermediate or destination node, nor does it change the function of normal AODV, and the malicious node is recognized and quickly removed so that it cannot participate in the upcoming process but instead executes a function named checkReply.

The Black Hole attack will transmit a false RREP packet with the greatest destination sequence number and the fewest available hops, and the checkReply will continue accepting RREP packets while isolating fake RREP packets.

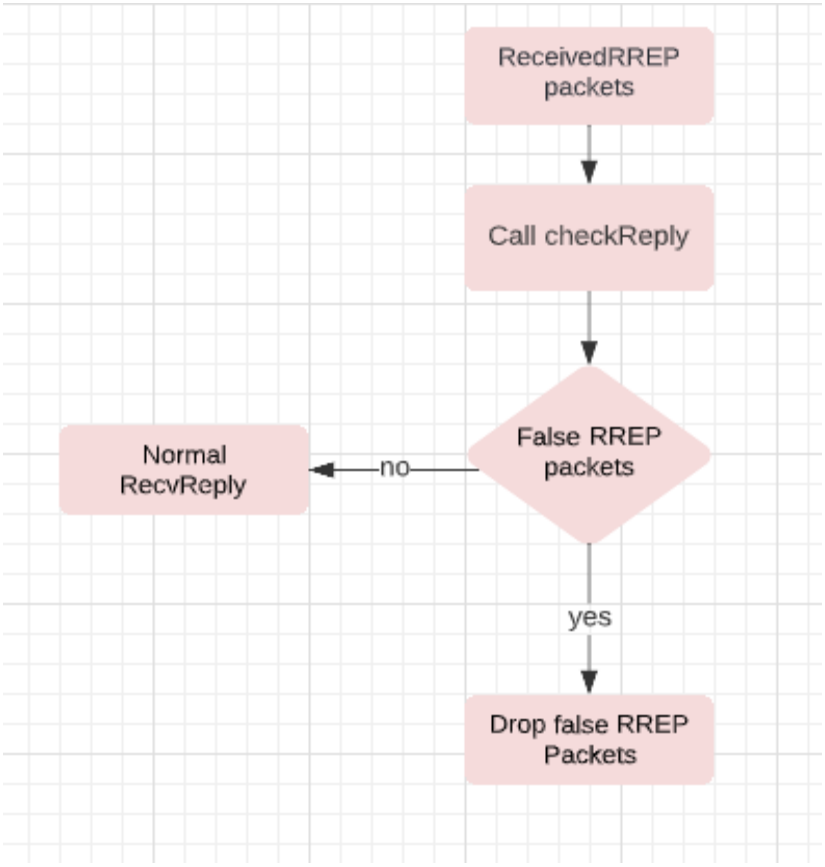

Figure 40: Architecture of detection approach

3.11 Performance metrics for evaluation

In order to check the performance of the detection method and the damage that can be happen by the grey hole attack and Sybil attack in the network we need to use different metrics which listed below:

- **Throughput**

The network Throughput is the quantity of data successfully transmitted from source to destination per unit time through a communication network. A larger Throughput value is more often an absolute decision in any network since it affects the ability of nodes to transmit packets from their origin to their intended destination. [35]

- **Packet delivery fraction (PDF)**

It is the ratio of the data packets received successfully by the destination to the data packets sent by the sources within the simulation period, Higher PDF implies that the packet loss rate is lower and protocol is more efficient from the perspective of data delivery

PDF analyzes protocol performance based on the loss ratio encountered at the network layer, which is influenced by factors such as packet size, network traffic, and the impact of mobility, which causes frequent topology changes. [35]

Conclusion

In this chapter, we have discussed key components of the AODV protocol. Furthermore, we detailed the proposed solution for the detection of blackhole, grey and Sybil attacks, and performance parameters.

Chapter 4 :

Implementation and Experimental Results

Introduction

After the analysis and design of the attacks, the next step is the implementation the attack and the proposed method of detection then, evaluating results are given. The main objective of this chapter is to present the damage that happen in routing process and evaluating the proposed method for detection which reduce the impact of the attacks.

4.1 Development Environment

4.1.1 NS2

NS2 is an event-driven simulator that has been beneficial for a while in networking research–field Thus, NS2 can be used to simulate both wired and wireless network services with various protocols. NS2 is made up of three programming languages [37]

- **C++ back-end**: creating new agents, protocols, links, and nodes.
- **front-end Otcl**: in order to use new agents, protocols, and links, we also use to create scenarios and topology.
- **SplitObcejt**: the main object is to connect C++ and Otcl. Means the object in octl linked with c++ object

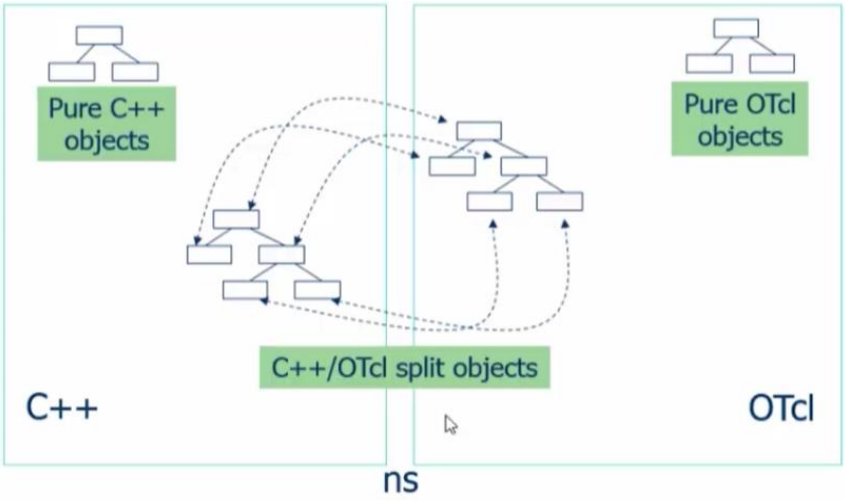

Figure 41: Component of ns2 [37]

4.1.2 Node structure

The structure of node is composed of two TCL object which are called address classifier and port classifier. Both objects are used to determine the destination address and the target agent.[37]

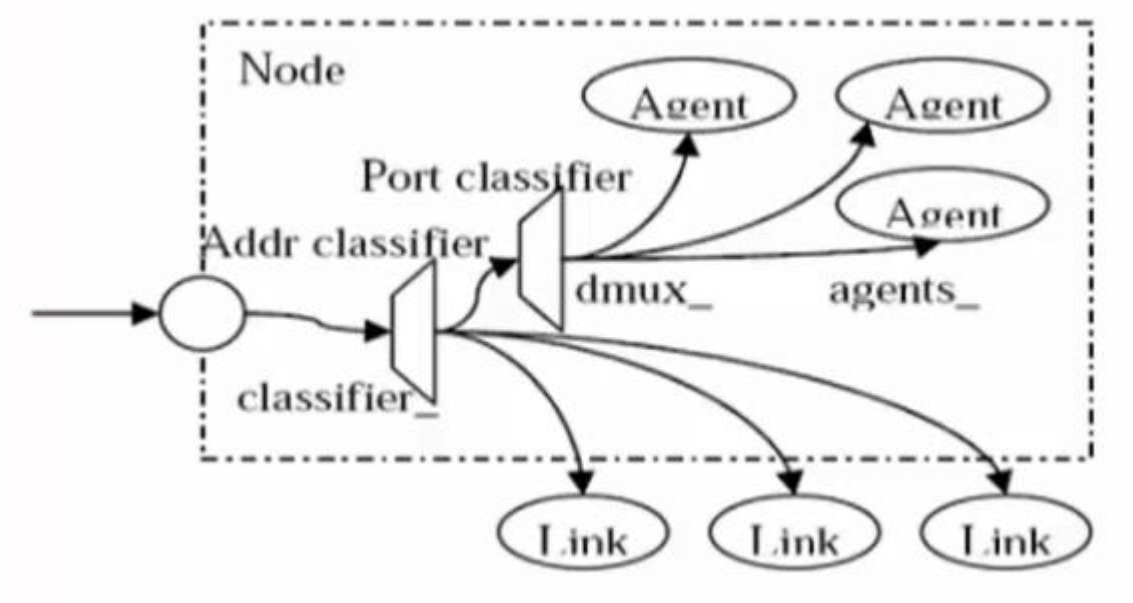

Figure 42: Node structure in ns2 [37]

4.1.3 Nam

NAM visualizes the network topology that has been established. The software was created as part of the VINT project. It has the following characteristics. The NAM application and its components are displayed; it is possible to run it straight from a tcl script. [35]

4.1.4 AWK

AWK is a tool used to read raw data of trace file (output from NS-2) to generate simulation metrics (packet delivery ratio (PDR), Average End-to-End delay (AED), Normalized Routing Load (NRL) and others for different routing protocols. AWK program is like parser, in the sense of reading each line of trace file and looks for keywords of packets' type such as 's' for send, 'f' for forward, 'd' dropped and so on, then use these data to calculate and compute PDR, AED.[35]

4.1.5 MannaSim

MannaSim is a framework made up of a collection of classes that enhance the capability of the Network Simulator 2 application (NS-2). MannaSim allows the user to create comprehensive simulation situations. Setting the network's compositional needs (number of nodes, node type, density, dissemination type) and organizational structure (flat or hierarchical).[36]

The "all-in-one package" NS-2 version 2.35 is used in this work. The ".tcl" files are created in a text editor, and the ".tr" file results are analyzed with "awk" commands. NS2 is installed on a personal computer with the following specifications

Table 3 : Personal computer characteristic

OS	Linux Lubuntu 16.04 LTS 64-bit
CPU	Intel R CoreTM i3-5200U CPU @ 2.20GHz 4
RAM	4.00 GiB

4.2 Implementing Blackhole Attack in AODV protocol

Due to the mechanism of the black hole attack, we must modify the "recvRequest" function in the aodv.cc file by sending a fake reply message indicating that the highest sequence number of the AODV protocol is 4294967295 and the hop count is equal to 1 , after that it drops all the packet in the network .

```
sendReply(rq->rq_src,           // IP Destination
          1,                    // Hop Count
          index,                // Dest IP Address
          429467295,                 // Dest Sequen
          MY_ROUTE_TIMEOUT,     // Lifetime
          rq->rq_timestamp);    // timestamp
```

Figure 43: The fake reply sending by blackhole node

4.3 Implementing Grey hole Attack in AODV protocol

To give a node the characteristics of a grey hole node, we must modify the aodv.cc and aodv.h files in the "ns-2.35" directory. To create a malicious node, we must include a drop function that drops packets selectively and randomly with probabilistic method it used for packet selection to ensure the other node does not recognize that it is a malicious node.

```
drop(p, DROP_RTR_MALICIOUS);
break;
```

Figure 44: Drop function for greyhole attack

4.4 Implementing Sybil Attack in aodv protocol

To make a Sybil attack function efficiently, if the request is sent to certain Sybil nodes, the malicious node will simply produce a fake reply, causing packets destined to them to be routed to the malicious node, where they will be dropped.

```
sendReply(rq->rq_src,           // IP Destination
          1,                    // Hop Count
          index,                // Dest IP Address
          429467295,                 // Dest Sequen
          MY_ROUTE_TIMEOUT,     // Lifetime
          rq->rq_timestamp);    // timestamp
```

Figure 45: Fake reply sending by malicious node

4.5 Testing the detection approach for black hole within reduced network

We have conducted an initial simulation over a small-scaled network to test black hole attack and the detection approach. Two simulations have been performed The first scenario (depicted in figure 46) contains a Black Hole Node (the malicious node that shows the Black Hole Attack would be referred to as "Blackhole"). A detection strategy for Black Holes was introduced in the second scenario (figure 47) along with the simulation results

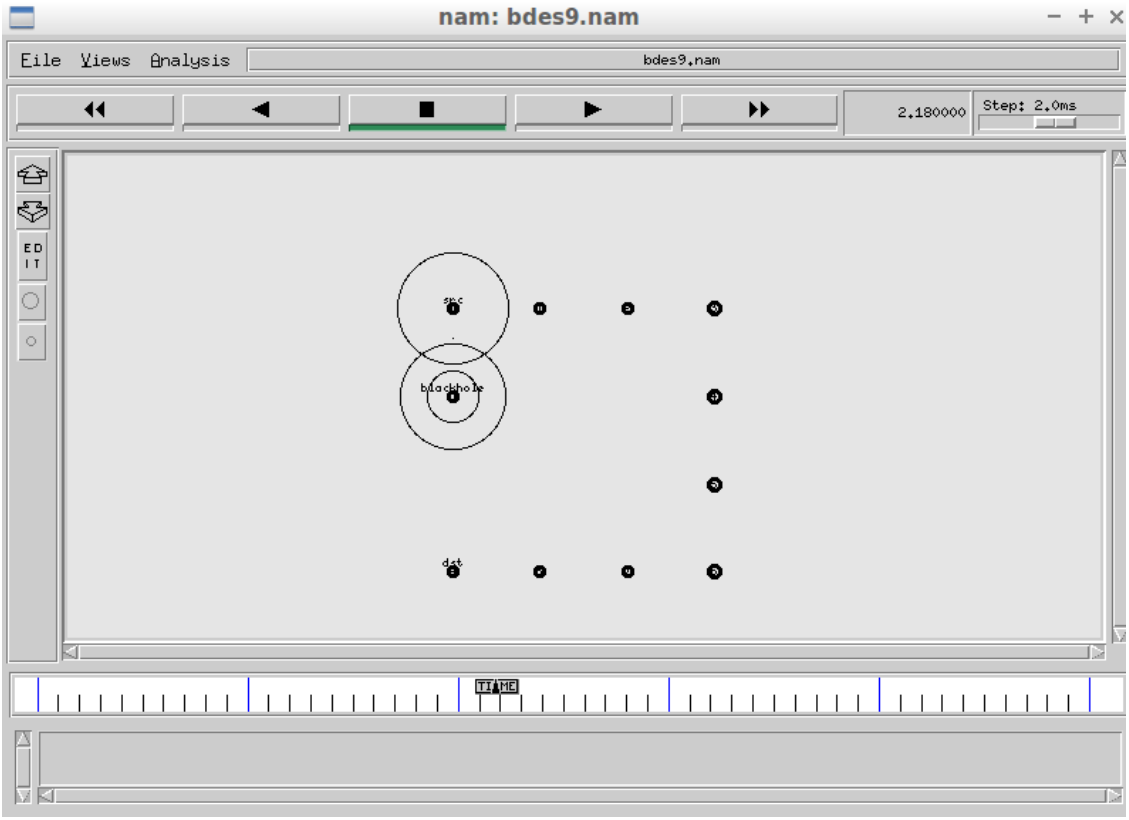

Figure 46: Flow data between source node and blackhole node

As it's shown in the figure 46 when the blackhole send fake reply the source node accept it the reply and start sending data to the blackhole node

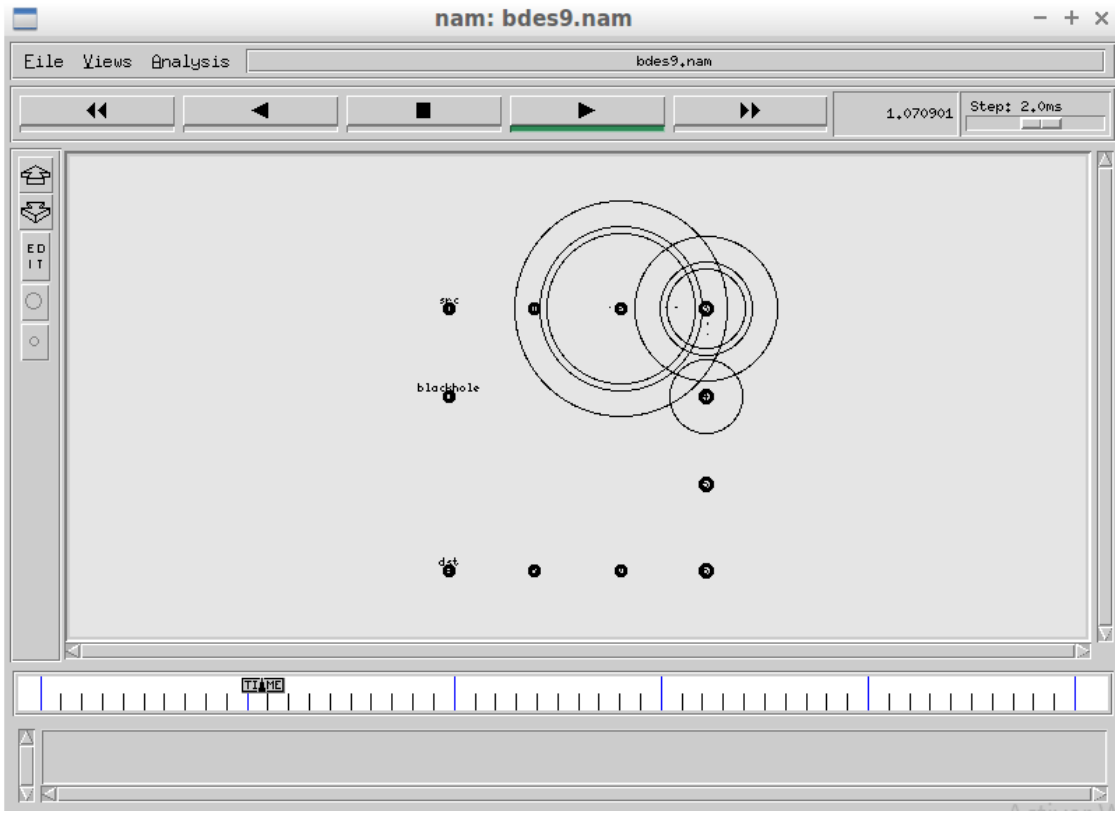

Figure 47: Flow data between source node and other node avoiding blackhole node

As it is shown in the above figure 47 when we apply the detection method, the source node avoids sending traffic to the blackhole node because the checkReply() function is dropping the reply of the blackhole node .For this simulation, we adopt the following parameters (showed in the table below).

Table 4: Parameters for first simulation

Simulator	NS2 network simulator
Total Number of nodes	11
Simulation Time	5s
Environment size	1000m×1000m
Packet size	256
Routing protocol	AODV
Traffic	Cbr
Number of Black Hole node	1

4.6 Evaluating Results of Blackhole attack and its detection

To determine whether the implemented approach for detecting the attack was effective, we present the impacts of malicious behaviors within the network.

Table 5: Result of performance metric

	packet sent	Received Packets	Dropped Packets	PDF	PDR	Throughput
Normal aodv	157	156	1	99.36 %	0.64 %	69.00 Kbps
With blackhole node	157	0	157	0.00 %	100.00 %	0.00 Kbps
With detection method	157	156	1	99.36%	0.64%	69.00 Kbps

4.7 Examining the attacks and detection in AODV Protocol

For the second experiment we evaluate the performance of the three attacks to determine whether they are performing properly. However, we used three different cases. The first scenario involved a black hole attack, the second a grey hole attack, and Sybil attack in the

third one. Thereafter, we compare the performance metrics with the three scenarios and the impact of the attacks then, will apply the detection method for blackhole and Sybil attacks.

For this simulation, we adopted a 600m × 600m space. In addition, we employed 49 temperature sensor nodes. All nodes deliver packets to the sink node in all cases. The simulation parameters are listed in the following table.

Table 6 : Parameters for second simulation

Parameter	Value
Routing protocol	AODV
Transport protocol	UDP
Node type	Mica2
Dissemination type	Continuous
Dissemination interval	60s
Initial energy for common node	10.0j
Initial energy for sink node	100.0j
Initial energy for malicious node	100.0j
Antenna Range of Common Nodes	100m
Antenna Range of sink Node	250m
Number of Common Nodes	50
Number of Malicious Nodes	Random
Number of sinks	1

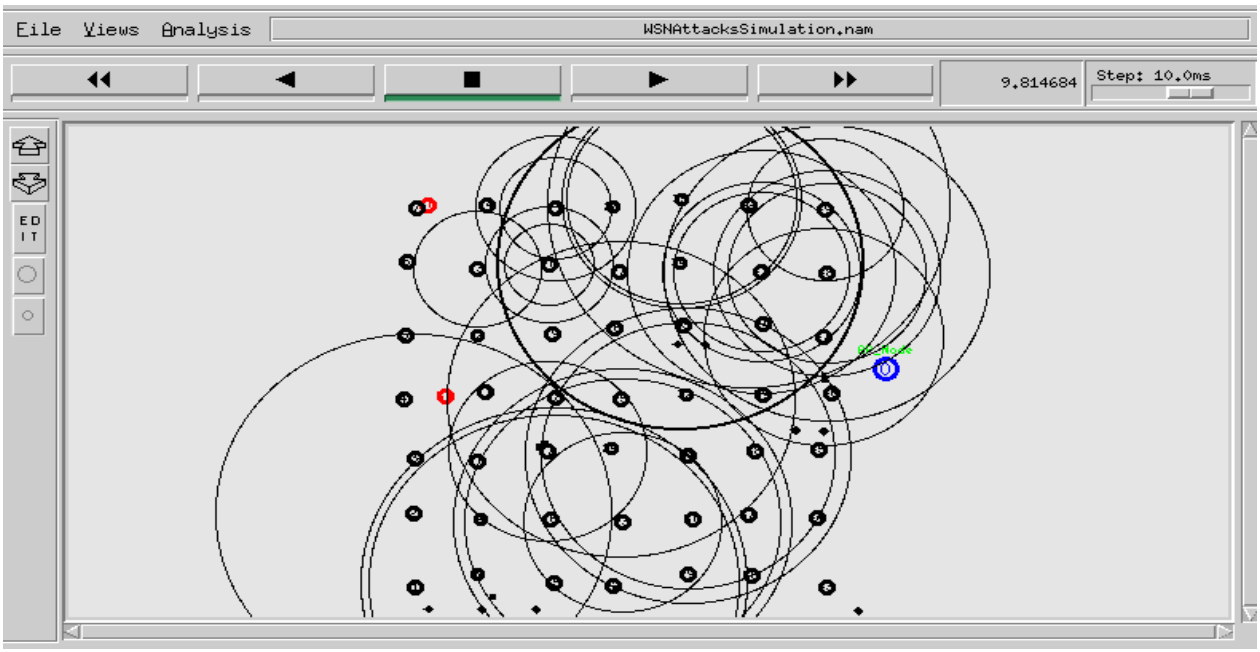

Figure 48: Simulation of attack with 2 malicious node

4.8 Evaluating Results of multiples attacks

In this section, we evaluated the scenarios and simulation parameters that were discussed earlier. We will see through the simulation results whether the proposed technique for implementing the attacks is successful and efficient and to show the effects of malicious attacks in the network.

A.Recieved Packets

Figure 49 shows that the presence of malicious nodes decreases the received packets to the sink with different attacks and reflects high packets drop in blackhole attack and Sybil attack

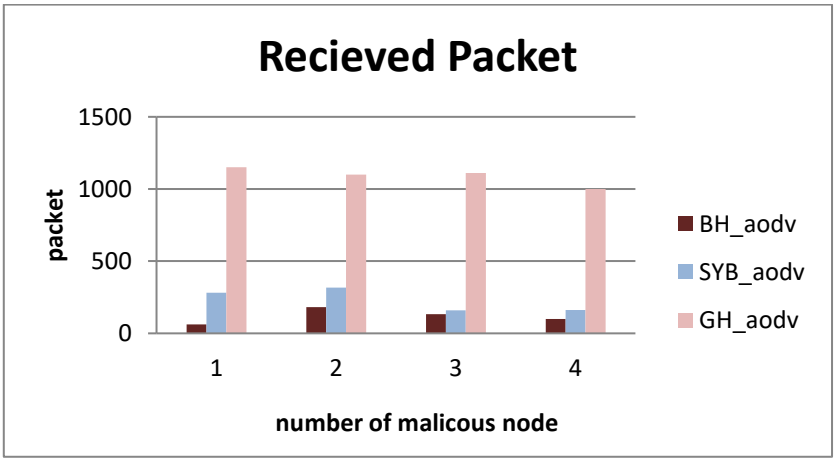

Figure49: Recieved Packet to sink node

B. The Throughput

Figure 50 shows the throughput which indicates a good performance with grey hole attack and the worst cases with black hole and Sybil attacks.

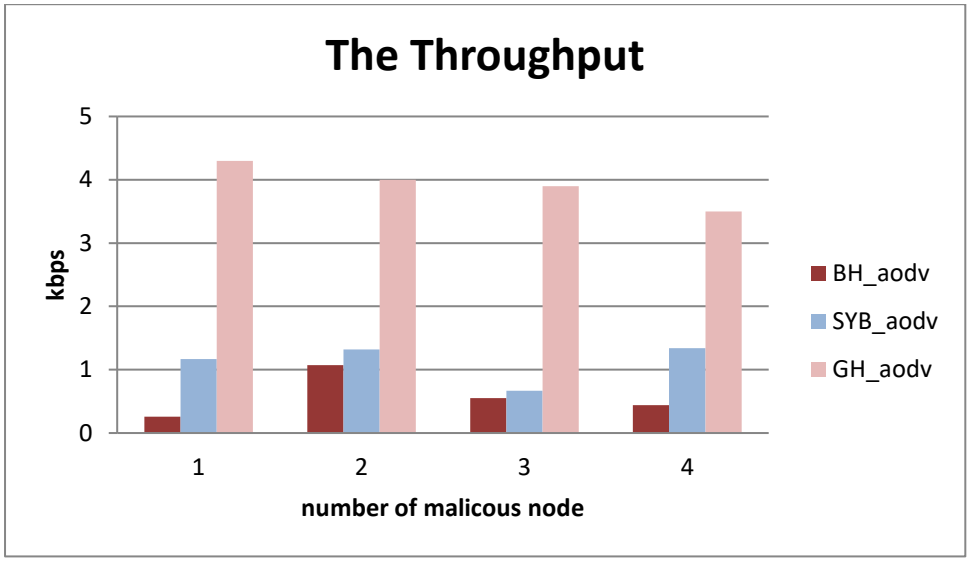

Figure 50: Throuput mesure with miltuples mlicous node

C. Packet Delivery fraction

Figure shows the highly rate of packet dropping is with black hole attack While in gray hole the dropping rate which the minimum comparing with the other attacks.

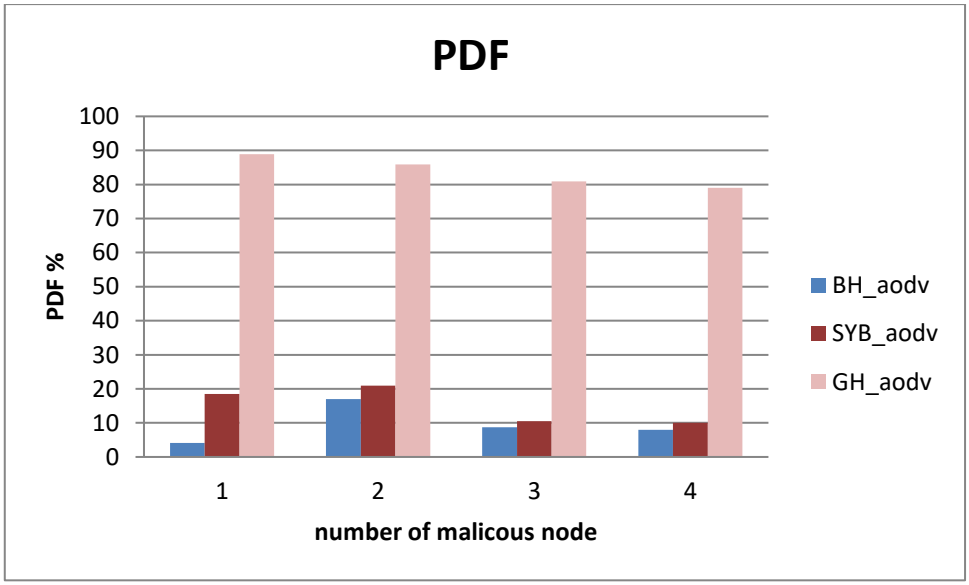

Figure 51: Packet delivery fraction mesure with miltuples mlicous node

4.9 Evaluating Results with the detection attack

For the third experiment after applying the detection, method for both black hole attack and the Sybil attack we need to evaluate the performance of the method in the environment that we create the total number of the packet sent is 1519 packets.

A. Received Packet

As it is shown in the figure 52 and figure53 below, the number of packets successfully received by the sink with the detection method for the black hole and Sybil attack is almost the same as the routing protocol in normal behaving

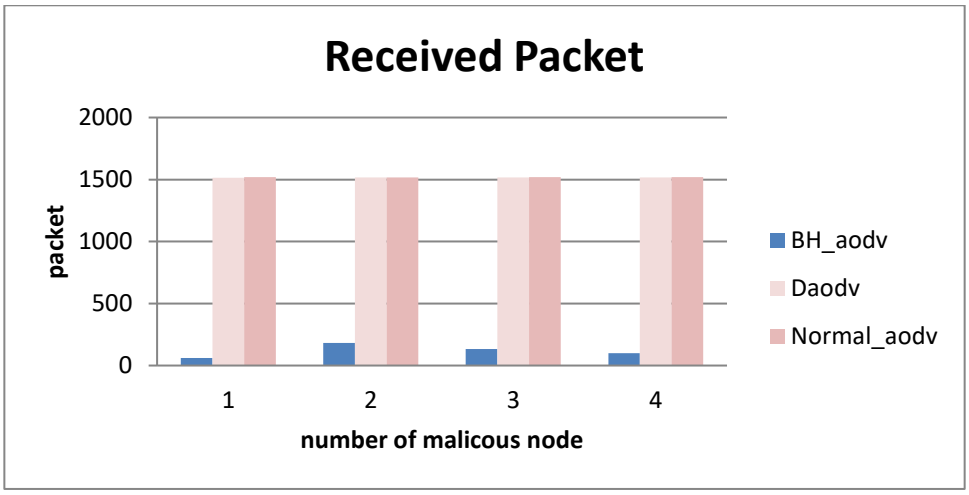

Figure 52: Received Packet to the sink with blackhole attack and with detection method

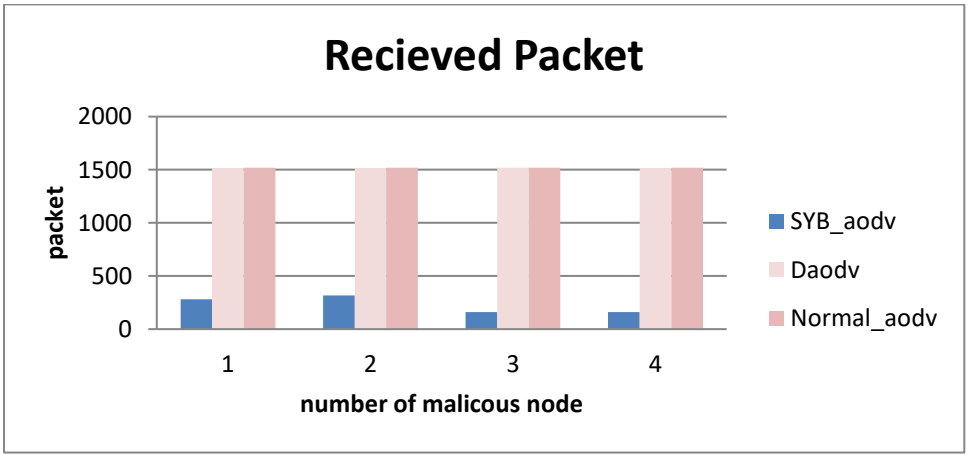

Figure 53 : Received Packet to the sink with Sybil attack and with detection method

B. The Throughput

As shown in the figure 54 and figure 55 below, the ability of the nodes to deliver the packets from source is more successful with the detection method with the both of the attack is similar to the AODV in normal behavior.

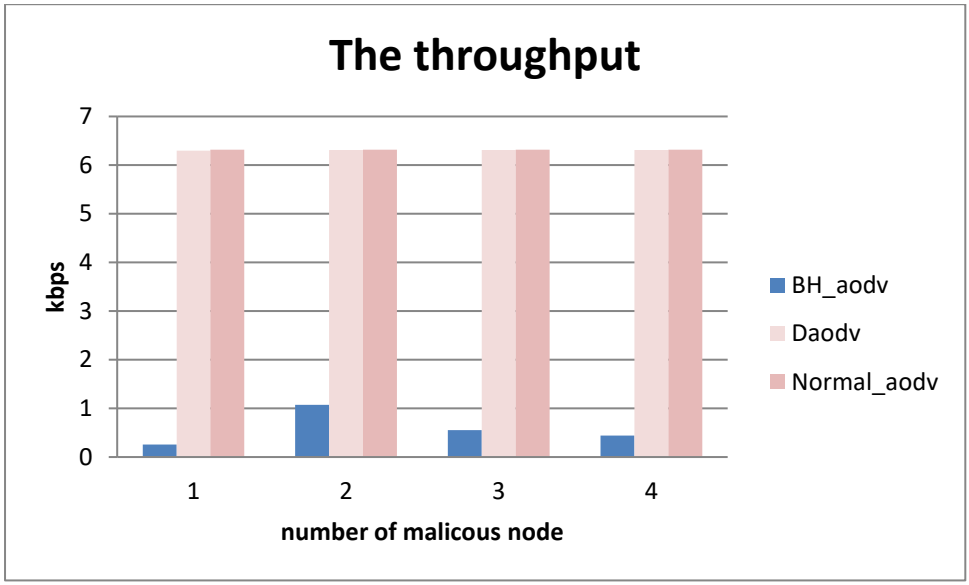

Figure 54 : Throuput mesure with detection method and blackhole attack

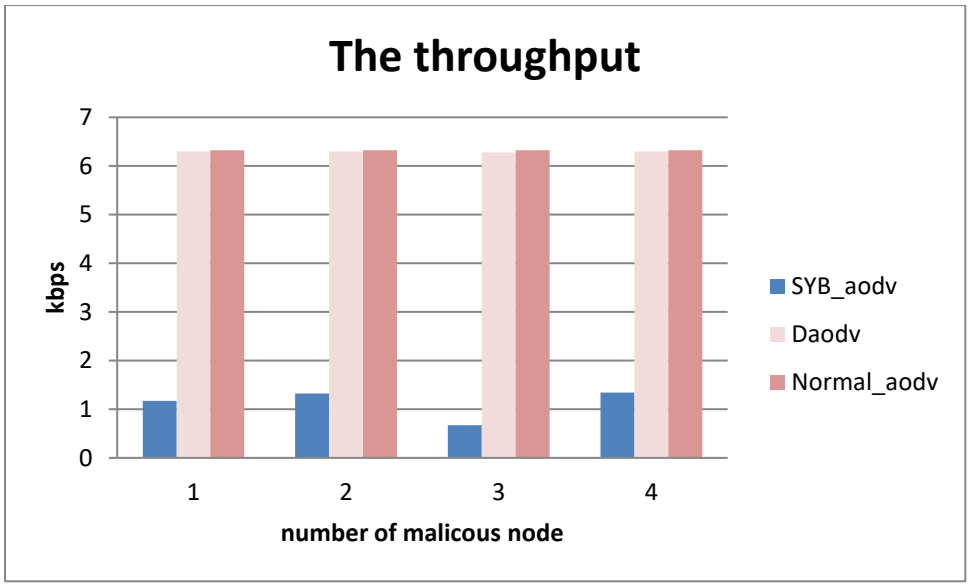

Figure 55: Throuput mesure with detection method and sybil attack

C.Packet Delivery fraction

As it shown in the figure 56 and figure 57 below the ratio of the data packets received successfully is higher with the detective solution, which means that the packet loss rate is lower and the D-AODV protocol is more efficient.

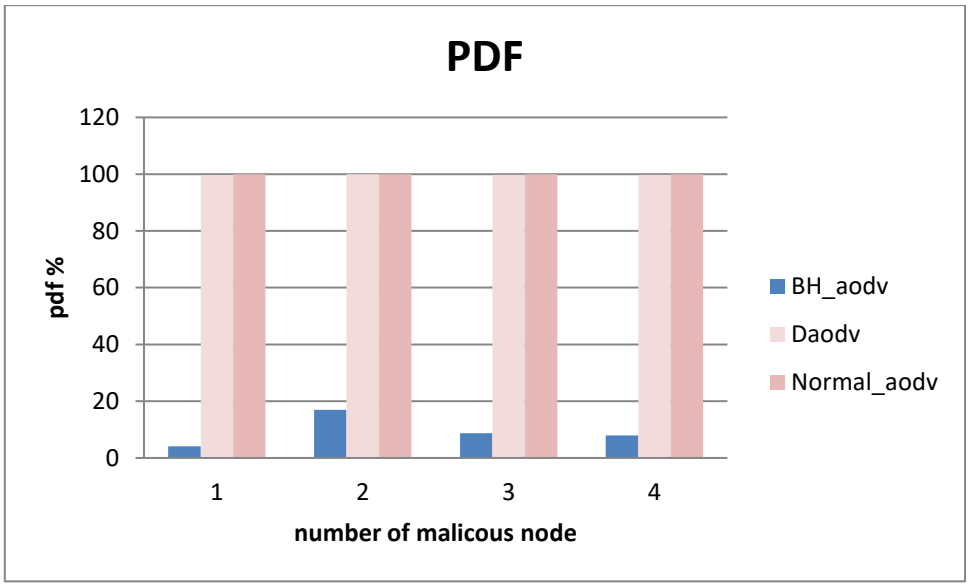

Figure56 : Packet delivery fraction mesure with detection methode and blackhole attack

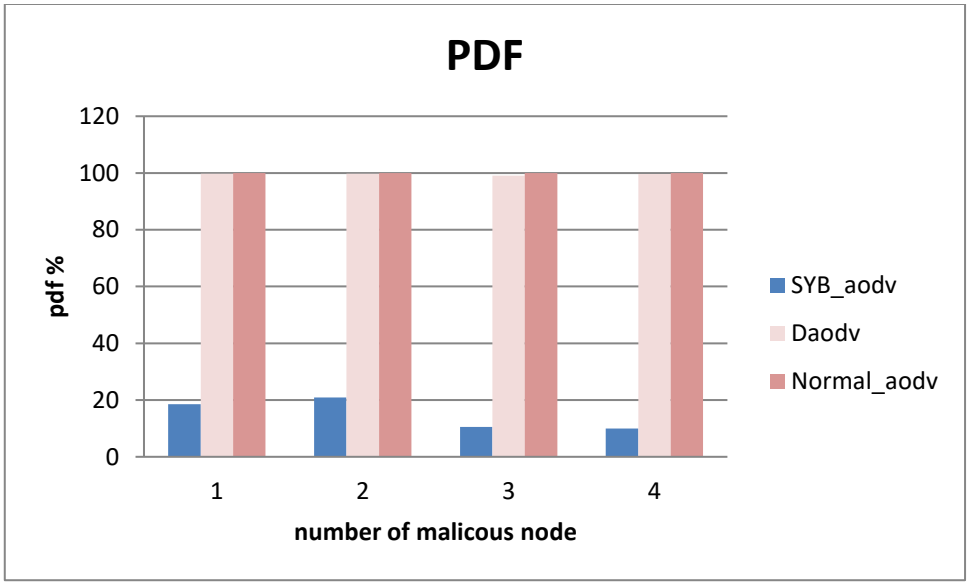

Figure57: Packet delivery fraction mesure with detection methode and sybil attack

Conclusion

In this chapter, we have first investigated the blackhole attack and the detection method in small scaled network after that, the simulation results show that the detection method is working correctly. After we have scaled-up the network size, we applied the Sybil, grey hole and blackhole attacks. Then, we have measured the impact of these attacks on the network and the routing process. In the last part of this chapter we presented the results of the detection policy and its accuracy against the studied attacks, in a larger network. The obtained results confirm that the solution named D-AODV (Detection with AODV) can

improve substantially the performance of AODV protocol against attacks causing packets unavailability in IoT-connected WSNs.

General Conclusion

General Conclusion

One of the most revolutionary technologies is the Internet of Things (IoT) which helps the human in their own life it's touched all fields one of its applications is wsn one of the most important topics in this century, the main purpose of wsn is to gather data from the environment, the weakness in routing protocol process and the morphology of the sensor make it more vulnerable to different attacks.

To point out the damage that may occur in WSNs as a result of routing assaults, we implemented different attacks (black hole, grey hole, Sybil attack) and studied the effect of each attack in the sensor network. We then offered ways to decrease the impact of those threats affecting packets unavailability. We proposed D-AODV by making modifications in the AODV protocol and taking the consideration the limits of WSN (battery power, storage, and processing power) so the solution is light weight means the main purpose is to isolate the fake RREP without any difficult process.

As future work, we can conduct extended evaluation context for the solution so that the effectiveness could be more accurate. We can also integrate other types of routing threats and their detection policies.

Bibliography

[1] S Sahraoui, Mécanismes de sécurité pour l'intégration des RCSFs à l'IoT (Internet of Things), thèse de doctorat, Université de Batna 2, 2016

[2] P. Suresh J. Vijay Daniel ,V.Parthasarathy R.H. Aswathy ‘’Things (IoT) history, technology and fields of deployment." 2014 International conference on science engineering and management research (ICSEMR). IEEE, 2014

[3] K. Patel, Sunil M Patel PG Scholar Assistant Professor, Internet of ThingsIOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges, Volume 6 Issue No. 5, International Journal of Engineering Science and Computing (IJESC)2016, pp2

[4] N. Sharma, M. Shamkuwar I. “The History, Present and Future with IoT” , © Springer Nature Switzerland AG in 2019

[5] Kavya Chandrashekhar, Internet of Things Characteristics, Business Analyst at Ellucian, published on September 19, 2016, Accessed 10 march on, [Online]. Available:https://www.linkedin.com/pulse/internet-things-iot-characteristicskavyashree-g-c

[6] Chen, W.: An IBE based security scheme of internet of things. Cloud Comput. Intell. Syst. (CCIS), pp. 1046, 1049 (2012)

[7] Suo, H., Wan, J., Zou, C., Liu, J.: Security in the internet of things: a review. Comput. Sci. Electron. Eng. (ICCSEE), pp. 648–651 (2012)

[8] Cheng, X., Zhang, M., Sun, F.: Architecture of internet of things and its key technology integration based-on RFID. In: Fifth International Symposium on Computational Intelligence and Design, pp. 294–297 (2012)

[9] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao, A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications, IEEE Internet of Things Journal,2017

[10] Sunil Cheruvu, Anil Kumar, Ned Smith, David M. Wheeler, Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment. Publishers :Apress, Berkeley, CA, 2020,pp374-395

[11] 6 Leading Types of IoT Wireless Tech and Their Best Use Cases, BehrTech Blog, Accessed on 10 march , [Online] Available: https://behrtech.com/blog/6- leading-types-of-iot-wireless-tech-and-their-best-use-cases/

[12] Lorenzo Vangelista, Michele Zorzi Marco Centenaro Andrea Zanella, LongRange Communications in Unlicensed Bands: the Rising Stars in the IoT and Smart City, IEEE wireless communication, 2016, ppt

[13] Naik, N. Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In 2017 IEEE international systems engineering symposium (ISSE) (pp. 1-7). IEEE.

[14] Musa G. Samaila, Miguel Neto, Diogo A. B. Fernandes, Mário M. Freire, Pedro R. M.Inácio, Challenges of securing Internet of Things devices: A survey, WILEY, 2018,pp9-15

[15] Keyur K Patel, Sunil M Patel PG Scholar Assistant Professor, Internet of ThingsIOT Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges, Volume 6 Issue No. 5, International Journal of Engineering Science and Computing IJESC 2016, pp2

[16] Zikria, Y. B., Kim, S. W., Hahm, O., Afzal, M. K., & Aalsalem, M. Y. (2019). Internet of Things (IoT) operating systems management: Opportunities, challenges, and solution

[17]R Gurunath , Mohit Agarwal, Abhrajeet Nandi, Debabrata Samanta, An Overview: Security Issue in IoT Network published in 2018

[18]IoT Security Issues, Threats, and Defenses Accessed on 12 march , [Online] Available :https:// IoT Security Issues, Threats, and Defenses - Security News (trendmicro.com)

[19] D. Nandal and V. Nandal, “Security Threats in Wireless Sensor Networks,” vol. 11, no. 01, pp. 59–63, 2011.

[20] M. Harun Yilmaz and H. Arslan, “A Survey : Spoofing Attacks in Physical Layer Security,” in 40th Annual IEEE Conference on Local Comp. Networks, IEEE, pp. 812–817, 2015

[21] Mukrimah Nawir, Amiza Amir, Naimah Yaakob,Ong Bi Lynn Internet of Things (IoT): Taxonomy of Security Attacks

[22] Parmar Amisha ,V.B.Vaghelab ‘’ Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol’’ 7th International Conference on Communication, Computing and Virtualization 2016

[23] U. Ahamed, S. Fernando “Simulation of Network Layer-Based Security Attacks in a Mobile Ad-hoc Network” Journal of Information Systems & Information Technology (JISIT) ISSN:2478-0677; Vol. 6 No.1 2021

[24] Salvatore D. Morgera Ismail Butun and Ravi Sankar. A survey of intrusion detection systems in wireless sensor networks. IEEE COMMUNICATIONS SURVEYS TUTORIALS, 16(1), first

[25] S. Khan Nabil Ali Alrajeh and Bilal Shams. ‘’Intrusion detection systems in wireless sensor networks: A review’’. International Journal of Distributed Sensor Networks, 16 April 2013.

[26] S. Halder A. Ghosal. ’’ Intrusion Detection in Wireless Sensor Networks: Issues, Challenges and Approaches’’. Springer-Verlag, 2013.

[27] J.Zhou A.Mitrokotsa, .A.Karygiannis mJ.Lopez. Wireless Sensor Network Security. 2008.

[28] S.Rajesh , M.Sangeetha. “Intrusion Detection In Wsn Using Modified AODV

Algorithm”. June 07-08

[29] Umashankar Ghugar, Jayaram Pradhan, Monalisa Biswal ‘’A Novel Intrusion Detection System for Detecting Black Hole Attacks in Wireless Sensor Network using AODV Protocol ’’ August 2016

[30] Saad Al-Ahmadi , Abdulrahman Alseqyani ‘’ SECURED AODV TO PROTECT WSN AGAINST MALICIOUS INTRUSION’’. International Journal of Network Security & Its Applications (IJNSA) Vol.12, No.5, September 2020

[31] A. Mohammed. ‘’A cross layer for detection and ignoring black hole attack in manet. I. J. Computer Network and Information Se- curity (IJCNIS), 2’’, September 2015.

[32] .D.N.Chaudhari A.P.Jadhao. Security aware adhoc on demand distance vector routing protocol in vehicular adhoc network. International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), 2, December 20

[33] C.K.Nagpal Bharat Bhushan, Shailender Gupta. Comparison of on demand routing protocols. I.J. Information Technology and Computer Science, 3:61–68, February 2013

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

[35] M.ALKHFAGY, “Countermeasure to Black Hole attack in Mobile Ad hoc networks(MANET),” 2013.

[36] 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.

[37] E. Hossain T. Issariyakul. An introduction to network simulator- NS2. Springer US, 2012.