Democratic and Popular Republic of Algeria
Ministry of Higher Education and Scientific Research
University of Mohamed Khider - BISKRA
Faculty of Exact Sciences, Natural Sciences and Life
Computer Science Department

Order N: RTIC6/M2/2019

Thesis

Presented to obtain the diploma of academic Master in

Computer Science

Option: **: Information and Communication Networks and Technologies**

Intrusion Detection for Wireless Sensor Networks by Game Theory

By:
GUESBAYA Nesrine

Defended the **/**/2020, in front of the jury composed of:

BOUKHLOUF Djemaa	MCA	Superviseur

University Year: 2019/2020

Abstract

Wireless Sensor Networks (WSNs) consist of a large number of tiny, spatially distributed, and autonomous devices, called sensor nodes. The latter are equipped with sensing, computation, and wireless communications capabilities. In view of the compelling applications in both military and civilian fields, WSNs have attracted an unprecedented focus on their easy configuration and low cost. Due to the openness of wireless media and constrained resources of WSNs, several attacks such as black hole attack may be easily applied on conventional routing protocols used in WSNs and compromise the security of networks. However, the security of these networks is critical. Especially secure routing is important given the fact that potential attackers aim to disrupt the appropriate operation of the routing protocol within a WSN.

In our project, we propose a game theoretic approach called AODV-GT (AODV-Game Theoretic) and we integrate this into the reactive Ad hoc On-demand Distance Vector (AODV) routing protocol to provide defense against blackhole attack. In our model, the interaction between potential attackers and defenders is formulated as a two-player non-cooperative non-zero sum game. Moreover, our simulation were implemented using the network simulator ns-2. Finally, AODV-GT outperforms AODV in terms of malicious dropped packets when blackhole node exists within the WSN.
Key words: WSN, security, IDS, AODV, blackhole attack, AODV-GT.

Résumé

Les réseaux de capteurs sans fil (RCSF) sont constitués d'un grand nombre de capteurs répartis dans l'espace et des dispositifs autonomes, appelés nœuds de capteurs. Ces derniers sont équipés des capacités : de détection, de calcul, et de communication sans fil. Compte tenu des applications convaincantes dans les domaines militaire et civil, les RCSF ont attiré un intérêt sans précédent pour leur facilité de configuration et leur faible coût. En raison de l'ouverture des médias sans fil et de ressources limitées des RCSF, plusieurs attaques telles que l'attaque du trou noir peut être facilement appliqué sur les protocoles de routage classiques utilisés dans les RCSF et compromettre la sécurité des réseaux. Par ailleurs, la sécurité de ces réseaux est essentielle. En particulier, le routage sécurisé et important étant donné le fait que les attaquants potentiels cherchent à perturber le fonctionnement approprié du protocole de routage au sein d'un RCSF.

Dans notre projet, nous proposons une approche de la théorie des jeux appelée AODV-GT (AODV-Game Theoretic) et nous l'intégrons dans le protocole de routage Ad hoc On-demand Distance Vector réactif pour fournir la défense contre l'attaque de trou noir. Dans notre modèle, l'interaction entre les attaquants et les défenseurs potentiels est formulée comme un jeu à deux joueurs, non coopératif et à non-somme nulle. De plus, notre simulation était mise en œuvre àl'aide du simulateur de réseau NS2. Enfin, AODV-GT surpasse AODV en termes de paquets supprimés malveillants lorsqu'un nœud de trou noir existe dans le RCSF.
Mots clés : RCSF, sécurité, IDS, AODV, attaque par trou noir, AODV-GT.

Contents

List of Tables

List of Figures

List of Algorithms

List of Acronyms

WSNs	Wireless Sensor Networks
DSR	Dynamic Source Routing
DSDV	Destination- Sequenced Distance-Vector
ADC	An analog-to-Digital Converter
OS	Operationg System
BLE	Bluetooth Low Energy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
MAC	Mesage Authentication Code
DoS	Denial of Service
IDS	Intrusion Detection System
UML	Unified Modeling Language
SOC	Self Organized Criticality

HMM	Hidden Markov Models
DR	Detection Rate
FAR	False Alarm Rate
NE	Nash Equilibrin
AODV	Ad ho On-demand Distand Vector
AODV-GT	Ad hoc On-demand Distance Vector-Game Theoritic
eMANETs	emergency Mobile Ad hoc NETworks
HIDS	Host Based Intrusion Detection System
VCG	Vickery-Clark-Grooves
RREQ	Route Request
RREP	Route Repley
RERR	Route Error
NetTT	Net Traversal Time
PDR	Packet Delivery Ratio

General Introduction

General Introduction

Technological and technical developments performed in the areas of wireless communication, micro- electronics and system integration have led to the advent of a new generation of large-scale sensor networks suitable for various applications. Consider a set of small electronic devices, autonomous, equipped with sensors and able to communicate with each other wirelessly. Together they form a Wireless Sensor Network (WSN) capable of monitoring a phenomenon of interest, and possibly react on the environment.

This technology promises to revolutionize our way of life, work and interact with the physical environment around us. Since the nodes communicate with each other, they provide the connectivity by forwarding packets over themselves.To support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination- Sequenced Distance-Vector). Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network.

Wireless sensor networks are usually deployed in distributed, hostile, remote, and insecure environments for monitoring and data gathering. However, despite their wide spread adaptation, WSNs are subjected to several constraints related to limited processing capabilities, narrow wireless bandwidths, finite battery powers, random sensor node deployment, limited storage spaces etc. All these constraints make WSNs vulnerable to various type of attacks. In addition, sensor nodes are usually low cost and tamper prone devices. Therefore, attackers can easily take control of them through physical alterations and introduce false information through compromised nodes to mislead the WSN and render it ineffective. Nevertheless, unlike the wired networks, where the intruder needs to bypass through several layers of defense at firewalls and gateways to gain a physical access to the network, attacks on WSNs can originate from all directions and target any sensor node.

All these factors make network security an indispensable aspect of the WSNs. However, it is well known that intrusion detection systems (IDSs) are an effective security mechanisms to protect the network against malicious attacks or unauthorized access, unlike other mechanisms such as cryptography, which remains ineffective when the attacker is within the network. Moreover, intrusion detection techniques must be light to adapt to the nature of WSN's limited resources.

In this thesis, a game theoretic approach called AODV-GT (AODV-Game Theoretic) is proposed. AODV-GT is integrated into the reactive Ad hoc On-demand Distance Vector (AODV) routing protocol to provide defense against blackhole attack. AODV-GT is an effective in terms of Intrusion Detection Systems' computational cost routing protocol.

This thesis starts with an introduction which presents the problematic and the project aim. The thesis is composed of two parts, the first part focuses on the theoretical aspect, and the second part shows our contribution in this work. Part I is divided into two chapters. Chapter 1 is devoted to the state of the art on wireless sensor networks. It presents a background of sensor technology, WSN applications, factors influencing WSN design, operating systems and wireless networking protocols used in this type of networks, etc. It also covers some concepts related to the WSNs security. Chapter 2 is about Intrusion Detection Systems, Game Theory and their application in the literature to secure WSNs. It is organized as two main sections. First section covers a look at Intrusion Detection System, its categories, architecture for WSN, etc. While in the second section an introduction to Game Theory and its use in WSN security alongside various accomplishments in this area is given.

Part II concentrates on the implementation of AODV-GT with the demonstration of its efficiency. It is composed of 2 chapters. Chapter 3 describes the analysis and design of our project in two main levels : global design and AODV-GT design along with the description of the AODV protocol and how black hole attack causes the protocol to misbehave. Chapter 4 shows the implementation of AODV-GT methodology with the illustration of its effectiveness using desired metrics. The thesis ends with a conclusion which evaluates the results, and discusses some perspectives.

Part I

Background

Chapter 1

Security of Wireless Sensor Networks

Chapter 1
Security of Wireless Sensor Networks

Introduction

Sensors link the physical with the digital world by capturing and revealing real-world phenomena and converting these into a form that can be processed, stored, and acted upon. There are, for example, sensors for position, speed, acceleration, pressure, movement, brightness, and temperature, to name a few among the simplest. More complex sensors, such as sound or image sensors are also widely used. Before the telecommunications revolution and the development of wireless technologies, the information collected by a sensor was carried by an expensive, cumbersome cabling system requiring relatively large human efforts. Now, the integration of sensors and wireless communications led to the birth of a new range of electronic devices opening the way for new applications based on wireless sensors equipped with "radio" circuits allowing them to send and receive information without the need for hard wired connections. In addition, these wireless sensors have storage capacity and computing power to route packets of information. As a result, many applications have been able to develop by taking advantage of this new sensor environment, and there will certainly be many more in the near future. These applications are grouped under the term Wireless Sensor Networks (WSNs). While many security concepts hold true for different kinds of computer networks, WSNs have certain properties that make them particularly susceptible to attack relative to the traditional computer networks. These properties do not only make possible a range of attacks not seen in regular computer networks, but also make a number of conventional defenses unsuitable for WSNs. The objective of this chapter is to provide an overview of Wireless Sensor Networks (WSNs) first. The starting point is the sensor itself which will then be integrated into a network in order to respond to a

given application. Then, we outline security constraints and requirements in WSNs, various possible attacks against these networks and major security issues

1.1 Wireless Sensor Networks

1.1.1 Sensor

A sensor is a device that measures a physical quantity and converts it into a signal which can be interpreted in a binary data exploitable and comprehensible by an information system [94][57].There are sensors for position, acceleration, heat, brightness, etc.

1.1.2 Structure of a Sensor Node

The architecture includes four elementary units for sensor operation: Sensing unit, processing unit, Transceiver unit, and Power unit.

Sensing Unit

This component is the unit that contains the onboard sensor(s) on the node. Typically, An analog-to-Digital Converter (adc) converts signals from sensors (analog signals) into signals that can be interpreted by the Processing Unit (digital signals).

Processing Unit

It is usually made up of a dedicated micro controller and memory. Micro controllers used in sensor networks are low energy consumers. Their frequencies are quite low, less than 10 MHz for a consumption of the order of 1 MW. Another feature is the size of their memory which is about 10 KB of RAM for data and 10 KB of ROM for programs [56]. In addition to data processing, the micro controller also controls all other units including the transmission system.

Transceiver Unit

The transmission unit is responsible for all data emissions and receipts via a radio communication medium. As in all wireless networks, we find the same problems: the amount of energy required for transmission increases with the distance. Motes are equipped with a low-rate (10- 100 kbps) and short-range

(less than 100m) wireless radio, e.g., IEEE 802.15.4 radio to communicate among themselves[87]. Since radio communication consumes most of the power, the radio must incorporate energy-efficient communication techniques to extend network lifetime. For example, the energy units can be supported by solar cells that convert light energy into electric current.

Power Unit

For WSN, power unit is a crucial component. Since it is desirable avoid any wired connection, the sensor must have its own source of energy, which is responsible for distributing the available energy to other modules and reducing the expenses by pausing the inactive components for example. The power source commonly used is rechargeable batteries.
Depending on the applications for which they are designed, wireless sensors could also have other modules, such as a location unit, to identify their geographical position, for example using a GPS receiver. Some applications may also require sensors with a mobilizer to move around.[75]

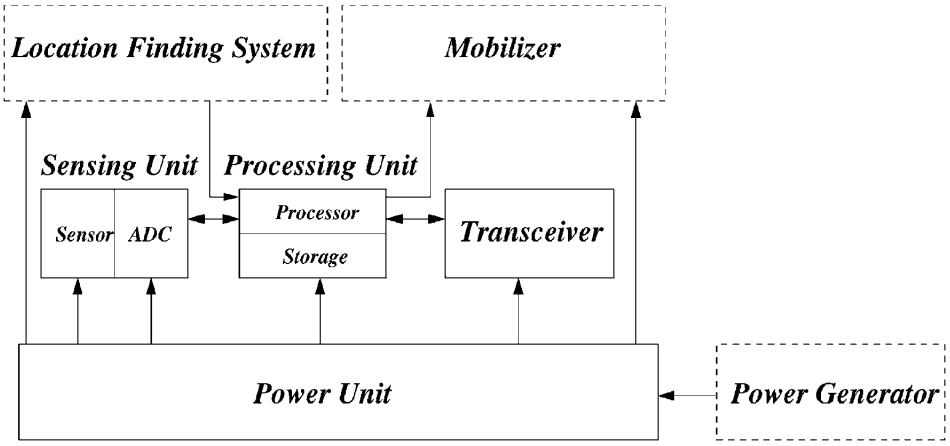

Figure 1.1: Components of a sensor node.[47]

1.1.3 Wireless Sensor Network Architecture

Wireless Sensor Network is a self-configured and infrastructureless wireless networks consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions, such as temperature, sound, humidity, pressure, motion, pollutants, etc, at different locations and to co-operatively pass their data through the network to a main location or sink where the data can be observed and analyzed [98]. The WSN is formed by

the "nodes" from a few to thousands of nodes. Each of the sensing devices in WSN network is called MOTE.[110]. Wireless sensor network consists of one or more base stations known as gateways, a number of sensor nodes and end user. The output generated by one node is wirelessly transmitted to the base station for data collection, analysis and logging. Each and every node in the Wireless Sensor Network acts as router for transmitting the information from source node to sink node [76] [77]. The end users are facilitated with the data from the sensor via some website or some application.

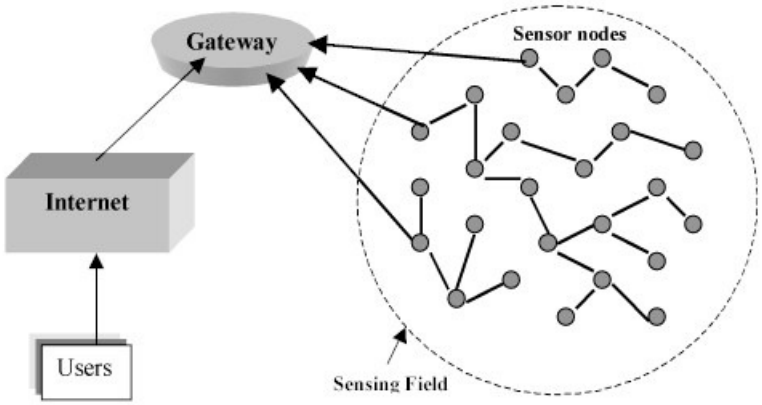

Figure 1.2: Wireless Sensor Network Model.[17]

1.1.4 Network Topologies

Previously we have described many applications of WSN for data collecting and processing. Such applications have a special feature: they have one data collecting point, namely sink. But there are also applications where sensor nodes have not only to send information to sink, but to exchange data between themselves. That is why there are different schemes of organization of interaction between sensor nodes within WSN. These schemes are called network topologies. The main types of network topologies for WSNs are: star, tree and mesh. Different WSN standards support different types of network topologies.

Star Network (Single Point-to-Multipoint)

A star network is a communications topology where a single base station can send and/or receive a message to a number of remote nodes. The remote nodes are not permitted to send messages to each other. The advantage of

this type of network for wireless sensor networks includes simplicity, ability to keep the remote node's power consumption to a minimum. It also allows low latency communications between the remote node and the base station. The disadvantage of such a network is that the base station must be within radio transmission range of all the individual nodes and is not as robust as other networks due to its dependency on a single node to manage the network.[51]

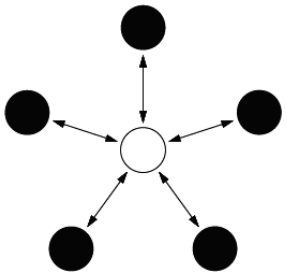

Figure 1.3: A Star network topology.[66]

Mesh Network

A mesh network allows transmitting data to one node to other node in the network that is within its radio transmission range. This allows for what is known as multi-hop communications, that is, if a node wants to send a message to another node that is out of radio communications range, it can use an intermediate node to forward the message to the desired node. This network topology has the advantage of redundancy and scalability. If an individual node fails, a remote node still can communicate to any other node in its range, which in turn, can forward the message to the desired location. In addition, the range of the network is not necessarily limited by the range in between single nodes; it can simply be extended by adding more nodes to the system. The disadvantage of this type of network is in power consumption for the nodes that implement the multi-hop communications are generally higher than for the nodes that don't have this capability, often limiting the battery life. Additionally, as the number of communication hops to a destination increases, the time to deliver the message also increases, especially if low power operation of the nodes is a requirement.[51]

Hybrid Star – Mesh Network

A hybrid between the star and mesh network provides a robust and versatile communications network, while maintaining the ability to keep the

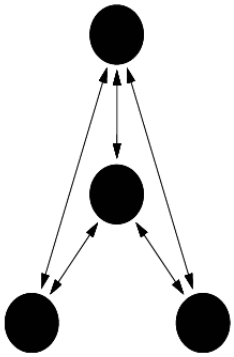

Figure 1.4: A Mesh network topology.[66]

wireless sensor nodes power consumption to a minimum. In this network topology, the sensor nodes with lowest power are not enabled with the ability to forward messages. This allows for minimal power consumption to be maintained. However, other nodes on the network are enabled with multi-hop capability, allowing them to forward messages from the low power nodes to other nodes on the network. Generally, the nodes with the multi-hop capability are higher power, and if possible, are often plugged into the electrical mains line.[51]

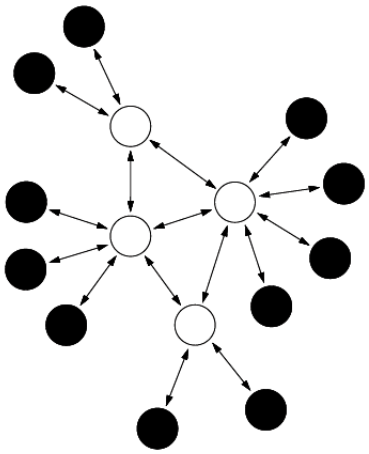

Figure 1.5: A Hybrid Star – Mesh network topology.[66]

1.2 WSN Applications

The main characteristics of WSN includes: energy harvesting, ability to cope with node failure, mobility of nodes, heterogeneity of nodes, scalability

to large scale deployment, ability to withstand harsh environmental conditions and ease of use. The mentioned features ensure a wide range of application of sensor networks. The application of wireless sensor network can be splited into four key domains: wearables, car and home automation, smart cities, and the industry as shown in figure 6 [69]. All these applications are encompassed by the concept of connected smart world.

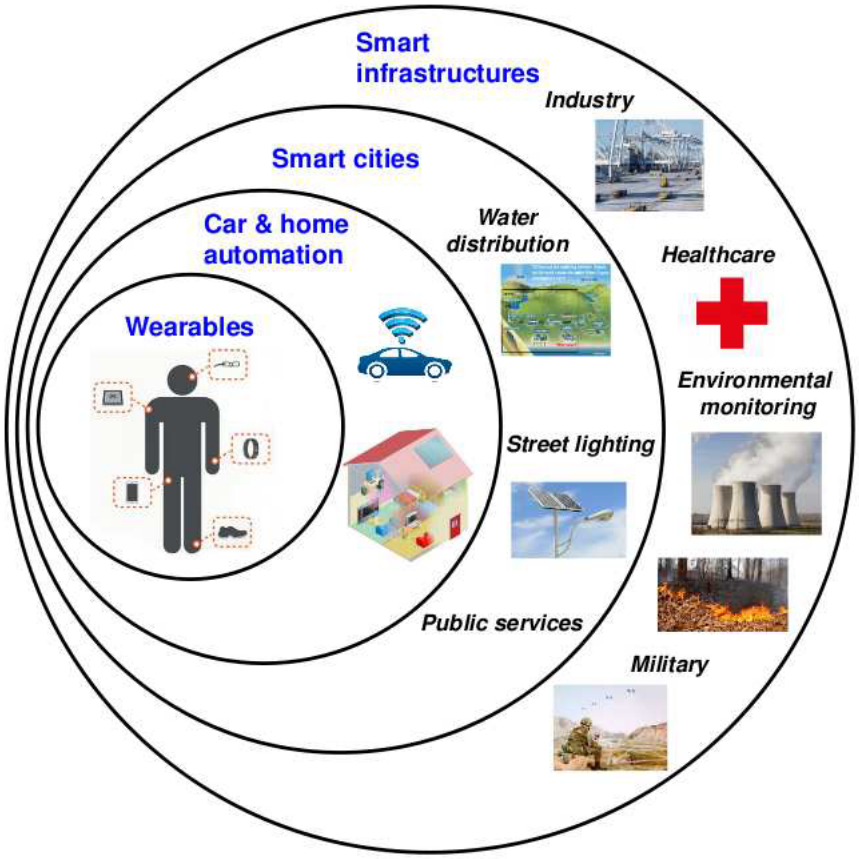

Figure 1.6: WSN application view.

1.2.1 Wearable Devices

Due to technological progress, intelligent sensor nodes may be integrated in devices such as wristwatch, chest strap monitors, glasses, shoes, or an ordinary .For example, glasses are used to know Overlays navigation directions and information about points of interest directly on to the wearer's field of vision jacket [69].Wearable devices can communicate with other WSNs deployed in a car or at home.

1.2.2 Car and Building Automation

A smart car is a car that is equipped with Internet access, and usually with a wireless local area network.[3] this allows the car to communicate with other devices both inside and outside it.special technologies are outfitted in Smart car. As an illustration, automatic notification of crashes, parking applications, engine controls and car diagnosis, etc [10] .This technologies ensure security and comfort to the driver. An intelligent building is a traditional one with sensors. Many techniques are employed in home automation such as: control of lighting, Heating, Ventilation and Air Conditioning , security lock of gates and doors and other systems, control of domestic activities, like house-plant and yard watering, pet feeding, and the use of domestic robots [69], to improve comfort, energy efficiency [79] and security [38].

1.2.3 Smart Cities

WSN technology has a main role in interconnecting such smart urban environments. Through various applications such as Smart Parking, Traffic Management, Noise and Pollution Monitoring, Smart Lightning [55], smart cities provide more efficient resource management and a better quality of life for the citizens.

1.2.4 Smart Infrastructures

There are other applications of WSN for smart infrastructure among which: industry, healthcare, environmental monitoring, and military.

Industry

several organizations, such as CISCO [4] are interested in the possibilities of using WSNs to monitor and enhance each step of a product including manufacture, delivery and consumption. Sensor nodes can offer real-time access to information about the equipment of plants, and prevent disruption of infrastructures[69].

Healthcare

193

Research on the use of intelligent sensors in the medical domain includes many health monitoring products such as SmartVest[85], AMON [104], and Wealthy[89]. These systems send wirelessly and continuously physiological

parameters about the patient's health, for example, they monitor vital signs, cancer detector [93].

Environmental Monitoring

WSNs can ease the measurement of environmental data[52][14] for a huge number of applications such as agriculture, meteorology, geology, etc. Today, WSNs are also used for the detection of forest fires[41] or floods and air pollution monitoring [54]. The advantage of using WSNs in such applications is mainly due to the need for acquiring large amounts of data in a region that would be costly to obtain using wired technologies.

Military

military applications have been the engines of research for sensor networks[65] [35]. For the military, a network of sensors offers very valuable advantages .WSN able to autonomously reorganize themselves [90] to form a network capable of routing measurements to the commanders. WSNs represent an important technology mandatory for maintaining soldiers safe in the battle-field [7].Moreover, WSN provides beneficial information such as enemy troop movement, coordinate resources and defense, monitor critical equipments, etc.

1.3 WSN Types

Current WSNs are deployed on land, underground, and underwater. There are five types of WSNs: terrestrial WSN, underground WSN, underwater WSN, multi-media WSN, and mobile WSN[53] .

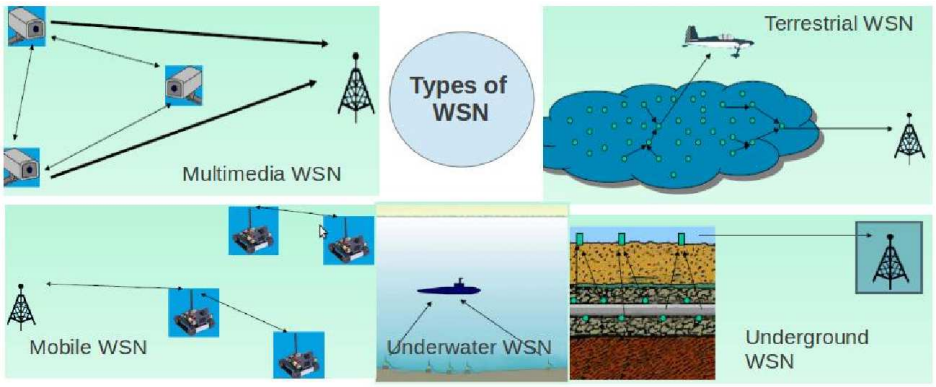

Figure 1.7: Types of WSN.[20]

1.3.1 Terrestrial WSN

consist of hundreds to thousands of inexpensive wireless sensor nodes deployed in a given area, usually in an ad-hoc manner .For example, dropped from a plane and randomly placed into the target area. [88]

1.3.2 Underground WSN

Underground WSNs are sensor nodes deployed in caves or mines or underground to monitor underground conditions.[45] [64] In order to relay information from the underground sensor nodes to the base station, additional sink nodes are located above ground [45]. An underground WSN is more expensive than a terrestrial WSN in terms of equipment, deployment, and maintenance.

1.3.3 Underwater WSN

consist of a number of sensor nodes and vehicles deployed underwater, for exploration or gathering of data to transmit acoustic waves [42]. The sensor nodes used here are fewer and more expensive than the terrestrial WSNs. Compared to a dense deployment of sensor nodes in a terrestrial WSN, a sparse deployment of sensor nodes is placed underwater.

1.3.4 Mobile WSN

A group of sensor nodes that move and interact with the physical environment is referred to as Mobile WSNs. Mobile nodes have the ability to sense, compute, and communicate measured or observed conditions like static nodes. After deployment, mobile nodes can reorganize and reposition themselves in the network to gather information. The information gathered can be distributed to other mobile nodes within their communication range. One of the key difference between mobile and static WSN is that in the latter data can be distributed using fixed routing or flooding while in the former dynamic routing is used[53].

1.3.5 Multi-Media WSN

The last type of WSN, multi-media WSN, has been proposed. These are low cost sensor nodes equipped with microphones and cameras to enable the tracking and monitoring of multi-media related events in the form of audio, video and imaging [46]. These sensor nodes interconnect with each

other over a wireless connection for data retrieval, process, correlation, and compression. Multi-media sensor nodes are deployed in a pre-planned manner into the environment to guarantee coverage.

1.4 Factors Influencing WSN Design

A set of metrics is used to determine the design of a WSN, which include fault tolerance, scalability, production costs, dynamic topology, environment, data aggregation, and power consumption. These factors influence the architecture of WSNs and the choice of protocols to implement.[75]

1.4.1 Fault Tolerance

Fault tolerance is the ability to maintain network functionality without interruption due to a failure of a sensor node. Indeed, the failure of a sensor node should not affect the overall operation of its network.[75]

1.4.2 Scalability

Unlike traditional wireless networks (personal, local or extended), a WSN can contain a very large number of sensor nodes (hundreds, thousands, etc.). To ensure the proper functioning of the network, deployment schemes must be able to work with this large number of nodes and deploy them in small areas using the high density property of sensor networks.[75]

1.4.3 Production Cost

As the WSN consists of a large number of sensor nodes, the cost of one sensor is very important to define the total cost of its network. If the latter is more expensive than deploying a set of ordinary sensors, then the cost of the WSN is not justified.[75]

1.4.4 Dynamic Topology

The dynamicity of the network comes from node failures, deployment of new sensors, or broken links between them. So, maintenance of a network is as important as changing its topology. Generally, there is three phases in the evolution of a network[75]:

•Deployment: The sensor nodes can be deployed in a random or deterministic manner.

•Post-Deployment – Operation: During the operating phase, the network topology may be subject to changes due to changes in node position or to breakdowns.

•Redeployment: Adding new sensors to a network also involves updating the topology.

1.4.5 Environment

In the majority of cases, sensor nodes are deployed in hostile areas or difficult to access. They are subject to different environmental conditions; they can work in a harsh environment such as the battlefield, under high pressure at the bottom of the ocean, etc. Therefore, they must be able to operate unattended in areas geographically distant or inaccessible.[75]

1.4.6 Data Aggregation

In WSNs, the data produced by sensor nodes is very linked, which involves the existence of data redundancies. A widespread approach is to aggregate data at intermediate nodes to reduce consumption energy when transmitting this data.[75]

1.4.7 Energy Consumption

Energy is a constraint in wireless sensor networks. Each sensor node works with a battery, generally, not rechargeable with limited capacity due to its small size. The sensors must therefore save as much energy as possible to be able to well functioning, especially in transmission time.[75]

1.5 Operating Systems for WSNs

An Operating Systems(OS) in a WSN is a thin software layer that logically resides between the node's hardware and the application and provides basic programming abstractions to application developers. Its main task is to: enable applications to interact with hardware resources, to schedule and prioritize tasks, and to arbitrate between contending applications and services

that try to use resources [103]. The following paragraphs describe Prototypes OF OSs for WSN in more detail.

1.5.1 TinyOS

TinyOS is s an event-based system. It is the most widely used, richly documented, and tool-assisted runtime environment in WSNs. Conceptually TinyOS's compact architecture consists of a scheduler and a set of components. Components are classified into configuration components and modules. A configuration component specifies how two or more modules are connected with each other (this is called "wiring"), whereas modules are the basic building blocks of a TinyOS program. TinyOS defines tasks, commands, and events as fundamental building blocks of a TinyOS runtime environment. TinyOS can support concurrent programs with very low memory requirements. In TinyOS, scheduled tasks are based on the FIFO principle. Resource allocation in TinyOS is optimized by adopting a static memory allocation.[106]

1.5.2 SOS

SOS is s an event-based system. The OS consists of a kernel and a set of modules that can be loaded and unloaded. It supports dynamic memory allocation. Moreover, in the same way that TinyOS components can be "wired" to build an application, a SOS application is composed of one or more interacting modules. Interaction with a module takes place through messages (asynchronous communication) and direct calls to registered functions (synchronous communication).[106]

1.5.3 Contiki

Contiki is a hybrid operating system. Predominantly is an event-based system but it provides optional multithreading. One of the interesting features of the Contiki OS is its support of dynamic loading and reconfiguration of services. This is achieved by defining services, service interfaces, service stubs, and a service layer. Services are to Contiki what modules are to TinyOS. It supports dynamic memory allocation.[106]

1.5.4 LiteOS

LiteOS is a thread-based operating system. It is based on the principle of a clean separation between the OS and the applications that run on top of it.

As far as LiteOS is concerned, developing building blocks and determining the way they interact with each other is entirely the task of application developers. Instead, LiteOS provides several system calls: a shell that isolates the system calls from a user; a hierarchical file management system; and a dynamic reprogramming technique.[106]

1.6 Protocol Stack for WSN

A protocol stack model is commonly used in communication theory to describe the processes taking place in a networked communication (between a supervisor, gateway(s) and all sensor nodes).[72] The protocol stack for WSNs comprises the Application, Transport, Network, Data Link and Physical layers. In addition, this stack has three management plans which include [47][103]:

1.6.1 Task Management Plane

It allows to well assign the tasks to nodes sensors.

1.6.2 Connection Management Plane

It keeps an image on the location of the nodes during the routing phase.

1.6.3 Power Management Plane

It preserves the maximum of energy.
Below is a brief description of each layer in the WSN model.

1.6.4 Application Layer

It interfaces with applications. It is therefore the layer closest to users, managed directly by software. Among the application protocols, we quote: SMP and TADAP.

1.6.5 Transport Layer

It checks the correct routing of the data and the quality of the transmission.

1.6.6 Network (or Routing) Layer

It allows the routing of data provided by the transport layer. It establishes the routes between the sensor nodes and the sink node, and selects the best path in terms of energy, transmission delay, throughput, etc. Among the routing protocols designed for WSNs we cite: LEACH and SAR.

1.6.7 Data Link Layer

She is responsible for accessing the physical media, detecting and correcting errors intervened on the physical layer. In addition, it establishes hop-by-hop communication between the nodes. Among the data link protocols, we cite: SMACS (Self-organizing Medium Access Control for Sensor networks) and EAR (Eavesdrop And Register).

1.6.8 Physical Layer

This layer allows the modulation of the data and conveys it in the physical media while choosing the right frequencies.

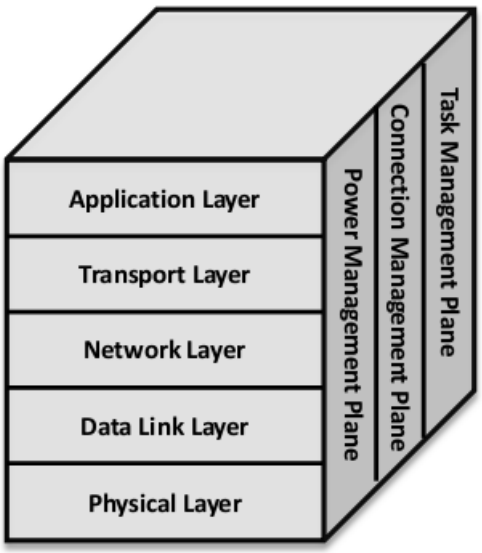

Figure 1.8: WSN protocol stack.[69]

1.7 Communication Standards for WSN

Wireless sensor standards have been developed with the key design requirement for low power consumption. The standard defines the functions and protocols necessary for sensor nodes to interface with a variety of networks. There are several WSN standards and technologies the most widely used are: ZigBee, Bluetooth and Bluetooth Low Energy (ble) and Wireless Fidelity (Wi-Fi). The following paragraphs describe these standards in more detail.

1.7.1 ZigBee

It defines the higher layer communication protocols built on the IEEE 802.15.4 standards for LR-PANs. ZigBee is a simple, low cost, and low power wireless communication technology used in embedded applications. It is maintained by ZigBee Alliance.[1] ZigBee uses the 2.4 GHz frequency band for higher bandwidth, and a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) transmission system, based on the IEEE 802.15.4 MAC layer. ZigBee supports a data rate of 250kbps.[95] ZigBee devices can form mesh networks connecting hundreds to thousands of devices together. ZigBee devices use very little power and can operate on a cell battery for many years. There are three types of ZigBee devices: ZigBee coordinator, ZigBee router, and ZigBee end device. ZigBee coordinator initiates network formation, stores information, and can bridge networks together. ZigBee routers link groups of devices together and provide multi-hop communication across devices. ZigBee end device consists of the sensors, actuators, and controllers that collects data and communicates only with the router or the coordinator.[2]

1.7.2 Bluetooth and Bluetooth Low Energy

Bluetooth is a wireless technology for short-range and cheap devices intended to replace the cables in WPANs. It operates in the 2.45 GHz ISM band (Industrial, Scientific and Medical radio band) and uses frequency hopping to combat interference and fading. Bluetooth can cover a communication range of 10-100 m and allows data rate up to 3 Mbps. It was standardized as IEEE 802.15.1, but the standard is no longer maintained. Currently, Bluetooth is managed by the Bluetooth Special Interest Group, which adopted Bluetooth Core Specification Version 4.0 in 2010. Bluetooth v4.0 is the most recent version. It introduced Bluetooth Low Energy (BLE) technology that enables new low-cost Bluetooth Smart devices to operate for months or years on tiny, coin-cell batteries. BLE operates in the same 2.45 GHz ISM band as classic

Bluetooth, but uses a different set of channels. Instead of Bluetooth's 1-MHz wide 79 channels, BLE has 2-MHz wide 40 channels. As compared to classic Bluetooth, BLE is intended to provide considerably reduced power consumption and lower cost, with enhanced communication range. BLE allows 1 Mbps data rates with 200 m range and has two implementation alternatives; single-mode and dual-mode. Single-mode BLE devices support only new BLE connections, whereas dual-mode devices support both classic Bluetooth as well as new BLE connections and have backward-compatibility.[20][24]

1.7.3 Wireless Local Area Network (WLAN)

Wireless Fidelity (Wi-Fi) technology is established on the basis of IEEE 802.11 standard. WLANs are prevalent for LAN applications with peak data rates of around 150 Mbps and extreme coverage range of 250 m. Wi-Fi (IEEE 802.11b) operating on 2.4 GHz band achieves maximum data rates of 11 Mbps. The main advantages of Wi-Fi are high data throughput, wide spread availability, IP support and network scalability[63]

1.8 Security in WSNs

1.8.1 Security Constraints in WSN

A wireless sensor network is a special network that has many constraints, compared to the traditional computer network. Because of these constraints, it is difficult to directly use existing security approaches for the field of wireless sensor networks. Therefore, develop effective security mechanisms while borrowing ideas from current security techniques. It is however essential to know and understand these constraints. Some of a WSN's major constraints are listed below.[97]

Energy Constraints

Energy consumption in sensor nodes is probably the biggest constraint for a WSN. The biggest challenge in the field of WSN remains to design security protocols, which minimize energy in order to maximize the lifetime of the network. Most security solutions that exist today cannot be used because they are often too costly in terms of resources. New security algorithms and protocols are needed. [75]

Memory Limitations

The sensor nodes are provided with a very limited memory and storage space for code. The total space available in the code for TinyOS, the operating system for wireless sensors, is approximately 4K, and the basic scheduler occupies only 178 bytes[102] . In order to build a very effective security mechanism, it is necessary to limit the size of the code of the security algorithm. [75]

Unreliable Communication

It is another serious threat to sensor security. Ordinarily, the packet-based routing of sensor networks is based on connectionless protocols and so unreliable. Packets may get damaged due to channel errors or may get removed at very congested nodes. Moreover, the unreliable wireless communication channel may also lead to damaged or corrupted packets. In certain situation even if the channel is reliable, the communication may not be so. This is due to the broadcast nature of wireless communication.[97]

Higher Latency in Communication

In a WSN, multi-hop routing, network congestion and processing in the intermediate nodes may lead to higher latency in packet transmission. This makes synchronization very difficult to achieve. The synchronization problems may at times be very critical in security as some security mechanisms may depend on critical event reports and cryptographic key distribution.[97]

Unattended Operation of Networks

In most situations, the nodes in a WSN are deployed in distant regions and are left unguarded. The probability that a sensor encounters a physical attack in such an environment is as a result, very high. This makes security in WSNs an especially hard task.[97]

1.8.2 Security Requirements in WSN

Sensor networks share some of the characteristics of a typical computer network but also have specific ones. Therefore the security requirements include those of the traditional networks and the requirements caused by the WSNs' constraints. Key security requirements include.[75]

Authentication

It allows cooperating within the WSN without risk by ensuring that the communicating node is the one that it claims to be. If authentication is mismanaged, an attacker can join the network and inject wrong messages. For that reason, it is essential for a receiver to have a mechanism to verify that the received packets have really come from the actual sender node. Data authentication can be achieved through the use of Mesage Authentication Code (MAC) . [75][97]

Confidentiality

The security system should assure that no message in the network is understood by anyone except the intended recipient. In WSNs, confidentiality applies to the following elements[58] [97]:

•A sensor network must preserve the secrecy of messages exchanged and not display them to opponents.

•Key distribution mechanism should be extremely robust.

•Public sensor information, such as sensor identities and public keys, should also be encrypted to protect against traffic analysis attacks. One standard security method of providing data confidentiality is to encrypt data and use of shared key so that only intended receivers can get the sensitive data.

Integrity

It ensures that the data received have not been changed during their transit through the network intentionally or accidentally. It can be ensured by the use of cryptographic hash functions which make it possible to obtain a digital fingerprint for each message.[75]

Availability

It means the capacity of the network to ensure its services to maintain its proper functioning by guaranteeing the presence and use of the information for the communicating parties at the desired time even in presence of an internal or external attack such as a Denial of Service (DOS) attack . Various approaches have been proposed to achieve this goal. While some of them make use of additional communication among nodes, others propose

the use of a central access control system to ensure successful delivery of every message to its receiver. [58] [97]

Freshness

This service ensures that the data exchanged on the network are current and are not a reinjection of previous exchanges intercepted by an attacker. To achieve freshness, security protocols must be designed in such a way that they can identify duplicate packets and discard them preventing replay attack.[75][97]

1.8.3 Attacks Against WSNs

WSNs are prone to numerous attacks or hackers, each one can perform a variety of attacks not necessarily having the same objective or motivation. There are several approaches to the categorization of attacks on WSNs. One of these approaches categorizes attacks based on whether they disrupt the functionality of the network or not. Attacks which disrupt network functionality are known as active attacks (i.e. network jamming attacks), while those which do not disrupt network functionality are referred to as passive attacks (i.e. packet eavesdropping attacks). Another common way to categorize WSN attacks is to classify them into two main categories: internal (i.e. launched by nodes which are part of a WSN) and external (i.e. launched by nodes or devices that are not part of the network). The most prominently used approach to categorize WSN attacks in the literature classifies them based on the layer of the communication architecture which the attack targets. The most known attacks in WSNs are presented below.[27][112]

Jamming Attack

The intruder floods the radio frequencies used by the network, with noise so as to prevent transmission and / or reception of messages. This type of attack can impact all or part of the network depending on the radio range of the adversary.

Tempering Attack

As WSNs are generally deployed in areas without protection, they are exposed to several physical attacks. One is related to the equipment that is not tamper-proof. The other physical attack would be to remove the sensor from the network by destroying or stealing it.

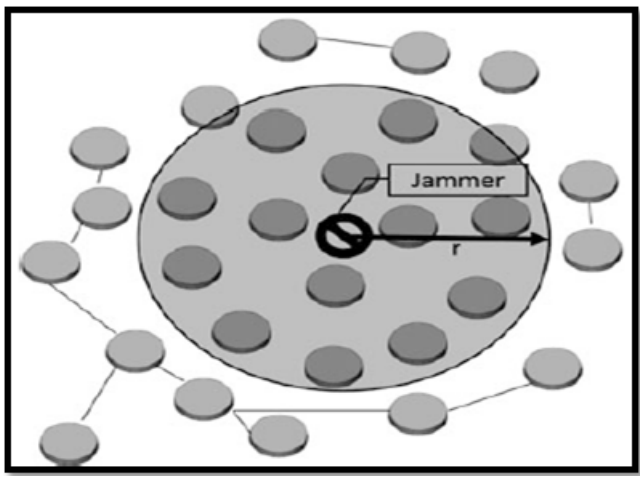

Figure 1.9: A jamming Attack disrupting all communications between nodes within a radius r of the jamming node.[96]

Eavesdropping Attack

Because of the transmissions are broadcast by radio waves, the network access control is not possible, especially that the network can be deployed in an open environment. It is therefore very easy to intercept data altered on a sensor network and access their content if no privacy service is provided.

Sybil Attack

In many situations sensors in WSN need to work together to perform a task so they can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes (Figure 1.10). This type of attack where a node forges the identities of more than one node is the Sybil attack. It aims to disrupt cooperation between other nodes. Authentication techniques and encryption can prevent an intruder from launching a Sybil attack on the sensor network.[80]

Selective Forwarding Attack

Selective Forwarding attack is one of the network layer attacks. As we know in multi-hop technique all the nodes in the network will forward received messages to the sink or sensor nodes .An attacker may create corrupt nodes in the network that drops some important messages intentionally while selectively forwards few of them. Defense mechanism against this attack is

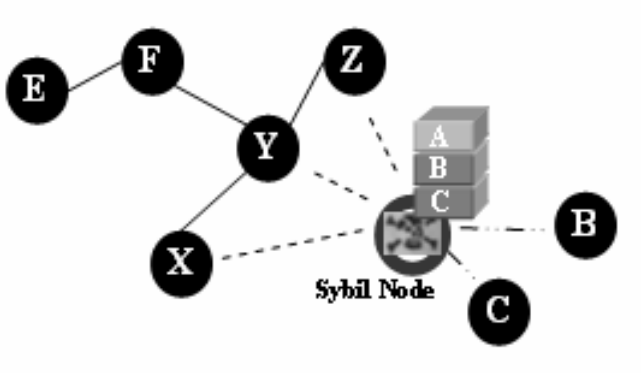

Figure 1.10: Sybil Attack.[109]

to use multiple paths to route data in the network.[111]

Sinkhole Attack

In a sinkhole attack, an attacker comes to an agreement with a node or introduces a fake node inside the network and uses it to occur an attack. The attacker listens route requests of nodes and tries to persuade that it has the shortest path for the base station [60] [30]. When the agreed node or fake node achieves to attract network traffic itself, it will create an attack.[80]

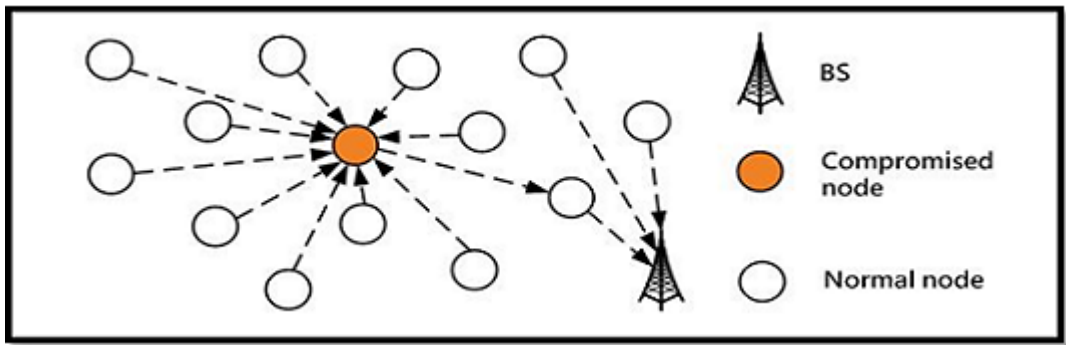

Figure 1.11: The model of Sinkhole Attack.[109]

Wormhole Attack

Wormhole attack is considered as a network layer attack and it can affect the network without the knowledge of cryptographic techniques implemented in the WSN. In this critical attack, an attacker records the packets (or bits) at

one location in the network and tunnels those to another location. The tunneling or retransmitting of bits could be done selectively. It has a significant influence on network routing.[80]

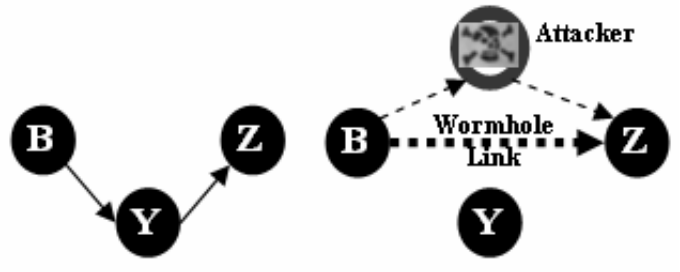

Figure 1.12: Wormhole Attack.[109]

HELLO Flood Attack

In network structures, routing protocols need some packets called "HELLO Packets" to find neighbors. The simplest attack for an attacker is to send a flood of such messages to flood the network and prevent other messages from being exchanged. A sensor which gets packets can assume that intruder is a normal node.[80]

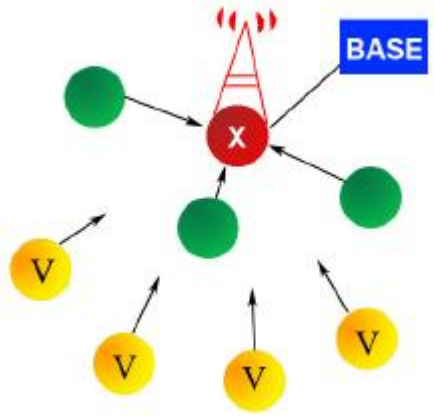

Figure 1.13: HELLO Flood Attack.[109]

1.9 Major Security Issues

Security is a wide field and represents a scientific challenge because of the specific characteristics of sensor networks. Among several areas of research in this problem, we mention [75]:

1.9.1 Routing Security

The problem of routing is to find an optimal routing for packets through the network taken into consideration a certain performance criterion such as energy consumption. En présence des attaques telles que déni de service, L'attaque du trou de ver,...etc. Les nœuds du réseau mis à jour leur table de routage pour continuer d'assurer la fiabilité de leur service. It is required to secure the routing protocols originally designed or even to design new robust algorithms in order to perform the data routing even in the presence of malicious nodes.

1.9.2 Security of Data Aggregation

A current approach to overcoming the limitations of sensor networks is aggregating the data at intermediate nodes level. Ensuring security in conjunction with aggregation techniques is difficult because a captured node poses a double problem. It compromises the confidentiality of the data and their availability. Moreover, an aggregation node endangers all measures that are part of the aggregate for which the node is responsible. This leads to false alarms or even masking exceptional events. This can have a negative impact in critical applications.

1.9.3 Location Security

Knowledge of sensor positions in the monitored environment is often essential for majority of applications. Localization can be used in geographic routing protocols in large-scale networks, forwarding data only in the direction of the recipient. Therefore, we need to locate all the nodes of the network. However, most sensors cannot be equipped with a GPS receiver and depend on a sensor named anchor to estimate their position. Hence, the security of Localization protocols is needed to protect the network from malicious anchors and attackers who try to disrupt the localization process.

1.9.4 Key Management

To provide security services such as confidentiality, authentication, integrity, etc. sensors need to share/establish secret cryptographic keys. This can be done with key management that provides efficient, secure and stable mechanisms. So, key management is a vital service for the safety of any which communication-based system. As sensor nodes are potentially exposed to attacks, an attacker can extract all secret keys from a node and trigger any type of attack without being identified. Consequently, the protocols for key management must be resistant to attacks against sensors. As a result, a secure key distribution strategy is required to ensure a certain level of security.

Conclusion

In recent years there has been a world-wide interest in Wireless Sensor Networks (WSNs).They are a new step in the evolution of information and communication technologies. It will not be an exaggeration to consider WSNs as one of the most researched areas. This new technology is attracting increasing interest given the diversity of these applications: health, environment, industry and even in the military field. In this chapter we have studied wireless sensor networks. We laid the basic bricks and federated some general concepts of WSN security necessary to understanding our problem in the rest of this paper.

Several research works have been done to solve WSN's security problems, such as intrusion detection systems which will be detailed in the next chapter.

Chapter 2

Intrusion Detection Systems and Game Theory for WSNs

Chapter 2
Intrusion Detection Systems and Game Theory for WSNs

Introduction

Many researchers are currently focusing on the security of wireless sensor networks (WSNs) because the features of both the wireless infrastructure and these sensors can cause potential attacks which can be either inside or outside on this type of network. It is very difficult for a single security technique to thwart these types of attacks in sensor networks. Therefore, intrusion detection which is an important aspect of network security came to be used in wireless sensor networks.

Recently game theory which is an advanced branch of intelligent optimization has been used extensively to model network security problems.

This chapter is composed of two parts; the first part presents a holistic view of intrusion detection systems in wireless sensor networks. The second part is focused on game theory and its application in wireless sensor networks security. We thus begin by presenting this theory. We provide a brief overview about game theory; that includes some definitions such as: a game, a player, a strategy, a pay-off, Nash equilibrium, etc and we cite a famous game known by Prisoner's Dilemma. Then, motivation to use game theory in intrusion detection is given. Afterward, we introduce a brief interpretation of the different game techniques presented in the literature to address WSN security. Finally, we present some of the related studies on existing solutions using game theory toward intrusion detection systems for WSNs. These studies were found useful and have provided a focus for our study.

2.1 Intrusion Detection Systems (IDSs) for WSNs

2.1.1 Intrusion Detection System

Security mechanisms are capable of ensuring security at some level; however they cannot eliminate most of the security attacks. An Intrusion Detection System (IDS) is one possible solution to address a wide range of security attacks in WSNs.[97] In a network or a system, any kind of unauthorized or unapproved activities are called intrusions. An IDS is a set of the tools, methods, and resources to help identify, assess, and report intrusions. IDSs are always considered as a second wall of defense from the security view. [50]. The following figure presents the four main components of IDS. [74]

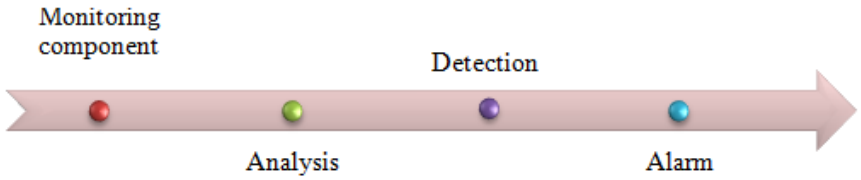

Figure 2.1: IDS Components

2.1.2 Motivation of Intrusion Detection in WSNs

The implementation of sensor networks in inaccessible areas coupled with the nature of their communicating medium and resource constraints pose difficulties for existing classical security techniques such as steganography to prevent all kinds of intrusions. One of the security method used is cryptography that is used for ensuring authentication and integrity by verifying the data source and its contents. The cryptographic operations can secure WSN from outside attacks. But these cryptographic techniques are incapable to detect internal attacks when the attacker knows the keys and uses them to perform encryption/decryption. This technique is the first line of defense. For that reason, it is often necessary to establish a second line of defense: An IDS that can detect an attack (known or unknown) and notify the sensors about it. This system allows detecting abnormal or suspicious activities on the analyzed target and triggers an alarm when an intrusion occurs.[8]

2.1.3 Detection Methodologies

Researchers in WSNs are working on three broad categories of IDSs; that is, signature-based detection, anomaly based detection, and Hybrid detection.

Signature-based detection

Signature based IDS, also known as rule-based IDS, has predefined rules of different security attacks. When the network's behavior shows any deviation from the predefined rules, it is classified as an attack. The advantage of this type of detection is that it can exactly and efficiently detect known attacks; hence they have a low false-positive rate. The disadvantage of this detection type is that it cannot detect new security attacks or those attacks having no predefined rules.[50]

Anomaly-Based Detection

Anomaly based IDS monitors network activities and classifies them as either normal or malicious using statistical behavior modeling. Normal operations of the members are profiled and a certain amount of deviation from the normal behavior is flagged as an anomaly. The main advantage of anomaly-based IDS is its capability to detect new and unknown attacks. The disadvantage of this detection type is that the normal profiles must be updated regularly, since the network behavior may change quickly.[50]

Corresponding to the nature of the processing implicated in the behavioral model considered, anomaly-based IDSs are divided into three categories. [84]These categories are modified and the final categorization is illustrated in Figure 2.2.

Statistical Based

In this category, the network traffic is captured and then a profile representing its stochastic behavior is created. When the network operates in normal conditions, a reference profile is generated. Then, the network is monitored and profiles are generated periodically and an anomaly score is generated by comparing it to the reference profile. If the score passes a certain threshold, the IDS will indicate an appearance of the anomaly.[50]

•Univariate: Parameters are modeled as independent Gaussian random variables.

•Multivariate: Correlations between two or more metrics are also considered here.

•Time series model: an interval timer is used along with an event counter that takes into consideration the order and inter-arrival times of the observations and also their values.

Knowledge Based

Here, IDSs rely on the prior knowledge of the network parameters in normal operating conditions and the one under certain attacks.

•Expert Systems: It is based on rules classification of audit data.

•Description languages: Diagrams (such as Unified Modeling Language (UML) diagrams are created based on the data specifications.

•Finite State Machine: States and transitions are defined according to the available data set.

•Data clustering and outlier detection: data are grouped into clusters according to a specified similarity or distance measure. Points that do not join to any cluster are considered as the outliers.[50]

Machine Learning Based

In machine learning based anomaly IDSs, the system generates an explicit or implicit model of the analyzed patterns. To enhance the intrusion detection performance based on the previous results, these models are updated periodically.

•Bayesian networks: It is based on probabilistic relationships between the variables of interest.

•Markov models: It is based on stochastic Markov theory where the topology and capabilities of the system are modeled as states. These laters are interconnected via certain transition probabilities.

•Fuzzy logic: It is based on approximation and uncertainty.

•Genetic algorithms: It is inspired by the evolutionary theory of biology.

•Neural networks: It is based on the human brain foundations.

•Principal Component Analysis (PCA): It is based on a dimensionality reduction method.[50]

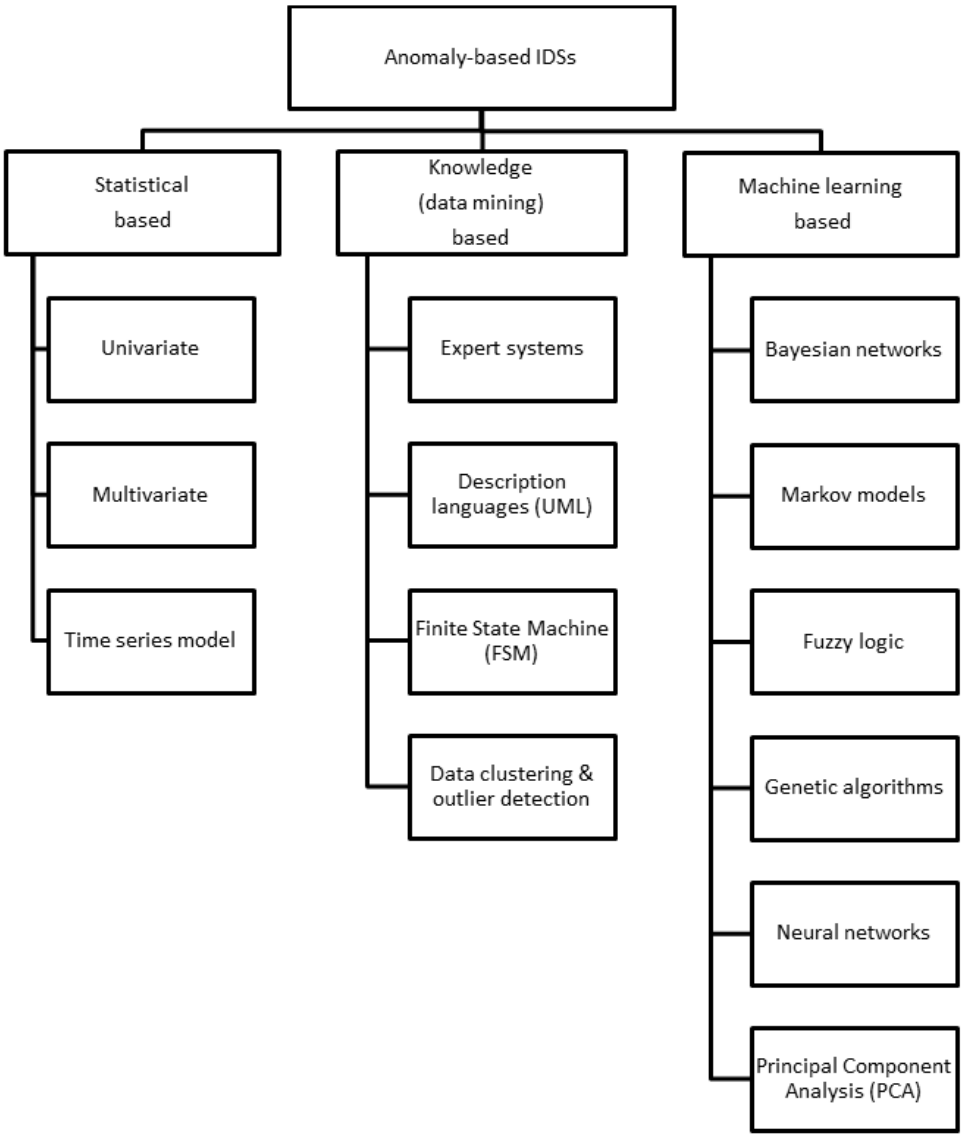

Figure 2.2: Classification of anomaly based IDSs according to their detection algorithms.[50]

Hybrid Detection

Hybrid IDSs are a combination of both anomaly-based and signature-based technique. Hybrid mechanisms generally contain two detection modules; that is, one module detects well-known attacks using signatures, while the other detects and learns normal and malicious patterns or monitors network behavior deviation from the normal profile. They are more accurate in terms

of attack detection with fewer false positives. Though, these mechanisms consume more energy and more resources. Hybrid IDSs are generally not advisable for resource limitation networks like a WSN; nevertheless, they are still an active research field.[73]

2.1.4 IDS Architectures

IDS architectures are classified into two basic categories depending on the data collection mechanism: host-based and network-based.[100]

Host-Based Systems HIDS

Host-based IDS check several types of log files such as kernel, system, application, etc. and compare the logs versus an internal database of usual signatures for known attacks. They determine if an attempted attack was indeed successful, and can detect local attacks, privilege escalation attacks, and encrypted attacks. Even so, such systems can be difficult to deploy and manage, especially in large scale networks. Furthermore, these systems are unable to detect attacks against multiple targets within the network.[8][37]

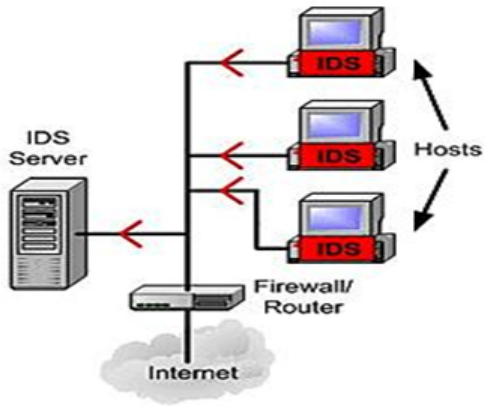

Figure 2.3: Example of HIDS.[8]

Network-Based Systems NIDS

The tasks of network-based IDS consist of scanning network packets, auditing packet information, and logging any suspicious packet, and are usually run on a separate machine termed a sensor. Network-based systems monitor a large number of hosts with little deployment costs and identify attacks to

and from multiple hosts. However, they are unable to detect that an attempted attack was indeed successful, and are unable to deal with local or encrypted attacks.[8] [37]

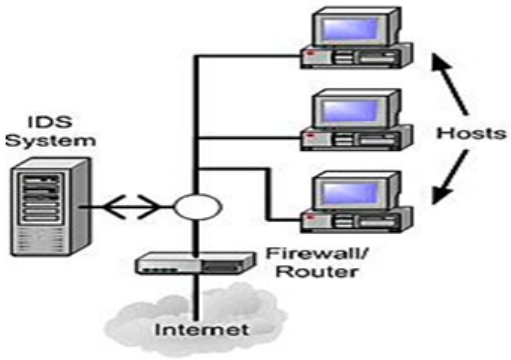

Figure 2.4: Example of NIDS.[8]

Hybrid systems, which contain Host- and Network-based elements, can offer the best protective capabilities.[37]

2.1.5 IDS Architectures for WSN

Furthermore, in [22] authors have also partitioned ad-hoc network IDS architectures into three categories and these categories can be adjusted according to the needs of WSN IDS.

Stand-Alone

In this case each node operates as an independent IDS and it is responsible for detecting attacks only for itself; that is, all the nodes of the network are capable of running an IDS. The IDS does not share any information or cooperate with other systems.[8]

Distributed and Cooperative

Here, all nodes still are running their own IDS, but the IDSs of all nodes cooperate in order to create a global intrusion detection mechanism.[8]

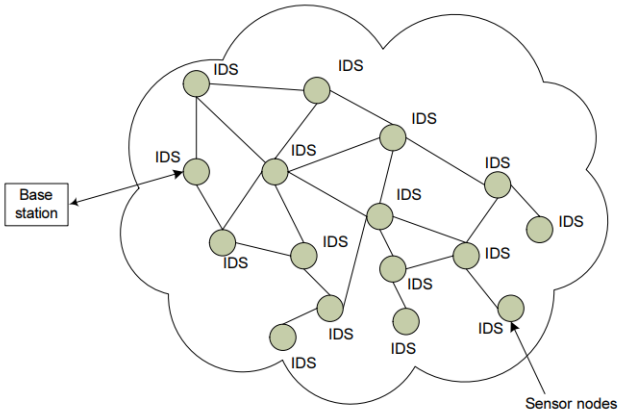

Figure 2.5: Distributed IDS Architecture.[16]

Hierarchical

In this category the network is divided into clusters with cluster-head nodes. These nodes are responsible for routing within the cluster and accept all the accusation messages from the other cluster members indicating something malicious. Furthermore, the cluster-head nodes may also detect attacks against the other cluster-head nodes of the network, as they represent the backbone of the routing infrastructure.[8]

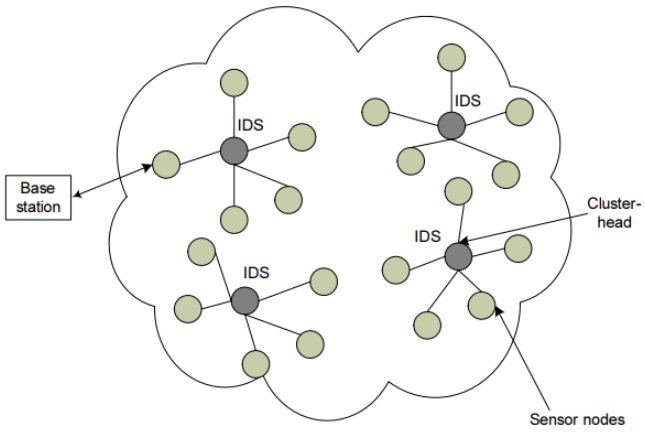

Figure 2.6: Cluster-based IDS Architecture.[16]

2.1.6 Literature Review Based on WSNs

IDS Approaches IDS approaches proposed for safeguarding sensor networks can be classified into four distinct categories [16][8][12]:

IDS Using Routing Protocols

In this category the attacker, either being insider or outsider, aims to manipulate user data directly or try to affect the underlying routing protocol. Diverse routing protocols are available for WSN applications, some focus on energy saving, others on resource awareness or in-built security mechanisms. However, there is no optimal routing protocol yet which is robust against all attacks e.g. flooding, selective forwarding, etc. Several intrusion detection systems have been proposed to detect routing attacks in WSNs. Loo et al. [23] and Bhuse and Gupta[105] describe two intrusion detection techniques for routing attacks in sensor networks. However, both proposed approaches are based on the assumption that routing protocols for ad hoc networks can also be applied to sensor networks.[48] The Ad ho On-demand Distand Vector (AODV) routing protocol is used by Loo et al.[23] , while DSDV and DSR (Dynamic Source Routing) protocols are used by Bhuse and Gupta.[105] Bhuse et al. [105] propose lightweight methods in order to perform intrusion detection in sensor networks. The proposed methods use existing system information such as neighbor lists, routing tables, sleep and wake up schedules etc., and attempt to detect the malicious behavior at multiple layers.

IDS Based on Neighbor Monitoring

Here, with the goal of detecting malicious nodes or attackers, nodes behave cooperatively. Usually in WSNs nodes which are close to each other have similar behavior. If a node's behavior significantly differs from its neighbors, it is considered as a malicious node. Various works have been proposed for intrusion detection in WSNs based on neighbor monitoring. Da Silva et al. [9], Onat and Miri [49], Krontiris et al. [48] and Hsin et al [25] propose intrusion detection approaches that present some similarities to each other. In all these approaches some sensor nodes monitor their neighbors in order to detect possible intrusions. According to the proposed methods, the monitoring nodes select data from messages transmitted in their radio range and select related information including message fields. This data is used as input to the corresponding IDS.

IDS Based on Innovative Techniques

In this type of IDS, different innovative techniques have been proposed for detecting intrusion in WSNs. Few works in this section that are based on certain innovation techniques are mentioned. Agah et al. [5], [6] suggest that game theory can be applied to intrusion detection in sensor networks. They propose an approach for the prevention of DoS attacks in sensor networks based on a game theory approach. The prevention approach is formulated as a repeated game between an intrusion detector and the nodes of a sensor network. Doumit et al. [29] propose a light-weight intrusion detection technique for wireless sensor nodes based on naturally occurring events and the analysis of fluctuations in sensor readings. Based on the Self Organized Criticality Self Organized Criticality (SOC) of the deployment region they acquire some knowledge, on which they deploy Hidden Markov Models (HMM) .

IDS Based on Fault Tolerance

Several fault tolerant techniques have been proposed related to intrusion detection in WSNs. we have cited some of the intrusion detection works based on fault tolerance. The first work towards an intrusion fault tolerant protocol for WSNs is INSENS.[28] The INSENS protocol is more capable of tolerating the intrusions than detecting the intrusions. Y. Challala et al. [26]proposed an intrusion-fault tolerant protocol for WSNs based on total in-network verification. In contrast to other solutions, the proposed protocol provides an efficient and secure method to build node disjoint paths in a totally distributed manner without referring to the base station.

2.1.7 IDS Assessment Metrics

In order to assess the effectiveness of an IDS, a set of metrics should be adopted to quantify security's level and make the best use of resources like energy consumption and storage space. These performance measurements will allow a network administrator to choose the best intrusion detection system. The following metrics are considered as major features for the effective design of IDSs in the WSN: [44]

Detection Rate(DR)

It is defined as the ratio of the actual number of attacks detected by the IDS to the total number of attacks in the network.

False-positive Rate (False Alarms)

It is defined as the ratio of the number of normal connections classified as an anomaly to the total number of normal connections.

False Alarm Rate (FAR)

It is defined as the ratio of number of normal data incorrectly classified as attacks to the total number of attacks detected by the IDS.

2.2 Game Theory for WSN Security

At the beginning of the 20th century, the first work on strategy games with Zermelo (1912), Borel (1921), and Von Neumann (1928) appeared. However, the theory of games was concretely born in 1944 with the book: Theory of Games and Economic Behavior by Von Neumann and Morgenstern. [34] Over a few decades, game theory has marks the development of many disciplines, such as science economics, management, operational research, engineering, political science, computer science and biology.etc. The study of theory games has become a need for anyone interested in these disciplines. [36] Game theory is a very effective mathematical tool for analyzing conflictual situations that carry interactions between their decision-making elements. Two or more players, with different interests, make decisions, act and participate in the outcome of each game. Each player intervenes to bring the game back to his favor. Players are considered to be rational and each one acts by taking into account the possible actions of others.[83]

2.2.1 Basics of Game Theory

A game in game theory is represented as: a game between player groups that choose to behave cooperatively or non-cooperatively and try to promote their benefits (payoffs) through the used strategy (ies) executed through the cumulative players actions. A game can be modeled as:[107][92][39][67][61]:
1. $P = \{p_1, p_2, p_3, \ldots, p_n\}$, a set of n players;
2. $A = \{a_1, a_2, a_3, \ldots, a_m\}$, a set of m actions;
3. $S = \{s_1, s_2, s_3, \ldots, s_k\}$, a set of k strategies;
4. $U =$ pay-off function to calculate the pay-off.

The fundamental definitions of game parameters are summarized below:

Game

A game is a formal description of the strategic interaction between opposing or collaborating, interests where the constraints and payoff for actions are taken into account.

Player

A player is a basic entity in a game, which is implicated in the game with a finite set of players denoted by N that is responsible for taking rational actions denoted by A_i, for each player i. A player can represent a person, machine, or group of people within a game, depending on the field in which the game is played.

Rationality

We said that a player is rational if he plays such that his own pay-off is maximized. It is often assumed that the rationality of all the players is common knowledge.

Strategy (Pure and Mixte)

A strategy is a plan of action within the game that a given player can adopt during game play denoted by a strategic game $\langle N, (A), (\mu_i)\rangle$. There are pure strategies which are actions or action plans chosen with certainty by each player. While, we interfere a random mechanism that assigns a weight to each pure strategy to obtain mixed strategies.

Dominant Strategy

A strategy is called dominant when it is better than any other strategy for one player, no matter how that player's opponents could play. In terms of mathematics, for any player i, a strategy $s^* \in S_i$ dominates another strategy $s' \in S_i$ if $\forall\ s_{-i} \in S'_i : U_i\ (s\ ,s_{-i}\ ) \geq U_i\ (s'\ ,\ s_{-i}\ )$

Utility

The Utility/Payoff is the positive or negative reward to a player for a given action within the game denoted by $\mu_i : A \to \mathbb{R}$, which measures the outcome for player i determined by the actions of all players $A = \times_{i\in\mathbb{N}} A_i$, where the symbol $\times$ denotes Cartesian product. The utility of a player can depend not only on his decisions but also on those of all other players.

Action Profile

An action profile is a list of actions, one for each player in the game.

Nash Equilibrin (NE)

Theorist John Nash has demonstrated that it is possible to any conflict situation under certain conditions to be in balance that leads to stability, where all players will be satisfied with their utilities and none of them is trying to change its situation. Players in Nash equilibrium are always non-cooperative.

Nash equilibrium is a profile of optimal actions $a^* \in A$, where any player pi cannot perform better by choosing an action different from a^* . This can be translated in terms of the utility function such as, $\mu_i(a_i^*, a_{-i}^*) \geq \mu_i(a_i, a_{-i}^*)$ for all $a_i \in A$. That is the utility of player i when he chooses s_i^* and everyone else makes a choice different of s^*, is greater than the utility of the same player i when he deviates from s^* and selects another strategy.[61]

Generally, Nash equilibrium (NE) is the intelligent solution for the social problems that has become a promising concept for wireless networks and more specifically for WSN security.

Prisoner's Dilemma

The prisoner's dilemma is the best-known example in game theory. It is presented as follows; "Police arrest two suspects of a criminal gang and question them separately. To each of them we present the following bargain: "if your accomplice confesses (A) and you shut up (T), you will bail out the ten years and he will get away with a reprieve. If it's the other way around, you can get a reprieve while he languishes in prison. Otherwise, if you both confess, the penalty will be shared (five years fixed)". If both keep silent, the penalty will be three years for each one".

The possible choices of the two prisoners ($P1$ and $P2$) can be represented in the figure below.

The Nash Equilibrium of this game is when both prisoners confess (confess, confess).

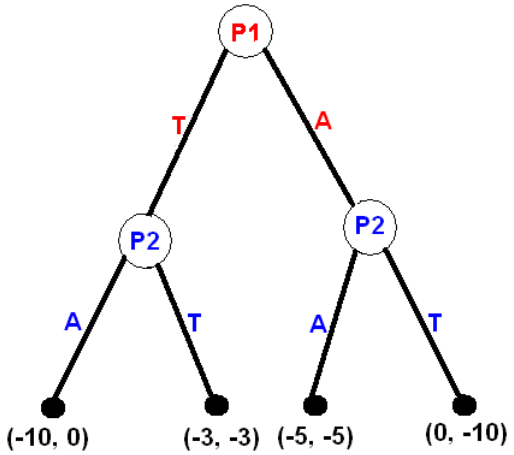

Figure 2.7: Payments of prisoners. [61]

2.2.2 Motivation to Use Game Theory in Intrusion Detection

Due to the increasing development of network technology, network security problems are receiving more and more awareness. The Intrusion Detection System (IDS) is the firewall for data encryption and other traditional security measures that ensures the security of the new generation of technology. Since the invasion and the scale of the network are constantly burgeoning, IDSs based on the traditional pattern matching is no longer useful. The game-theory-based intrusion detection systems will effectively fix this issue; it is the third-generation intrusion detection pattern matching technology that can meet the needs of the new IDSs.[33]

Most of the existing IDSs are subject to many problems: they need supplement resources, they are subject to tampering, etc. Therefore, there have been increased interests and efforts devoted recently to analytical methods for researching security problems. As a first reason for using a game model is that it will respond to minimize the loss of the system after the IDS detects an attack. Moreover, we can get an optimal choice if the right game model is established; we can analyze the Nash equilibrium via the process of the game and get the optimal strategy of the game, which is not achievable by other IDSs. Finally, the game's process is bidirectional; we can use the payoffs of both offensive and defensive to judge whether the defense is successful or not.[33]

2.2.3 Game Theory Types for WSNs Security

Game Theory types that are commonly used to mitigate WSNs security threats are divided to cooperative games and non-cooperative games as Figure 3.1 shows. In Cooperative games, cooperating nodes aiming at maximizing the whole network's security against different security threats. While in the non-cooperative games every node aims at maximizing its own payoff that opposes the others' outcomes by conflicting individual actions. A brief description of the different categories of game theory for WSNs security is provided.[67]

Cooperative Games

•Bargaining Game Bargaining game or Nash bargaining game is modeled based on the bargaining interaction concept between two players, who request a fraction of the same benefits. In this game, both requests are discarded if the total requests by the two players exceed the available resources. In contrast, if their requests are less than the available resources, both requests are realized.

•Repeated Game Is also known as iterated game which is considered as two players interact with each other repeatedly. It includes some repetitive stages and each one has two players at which the current action is taken into account in the actions of the other players. The repeated games can be divided into two categories: finitely repeated games and infinitely repeated games.[81] Finitely games are played in known and fixed Time period. Even as, in the most famous notion infinitely repeated game, the game is possibly played for limitless time. According to the players' interactions, the reputation is calculated.

•Coalition Game In this game a set of player act cooperatively as one player against the others in order to maximizing the mutual payoff which is called coalition value. There are two forms of this game: strategic and partition. In strategic partition, the number of participant players in the coalition effect on the coalition value regardless of their network establishment. On the other hand, in partition form, the coalition value depends on the establishment.[13]

Non-cooperative Games

•Zero-Sum Game Zero-Sum Game is a Non-cooperative Game between two players. One player strives to maximize its gain though the other, minimizing

its losses is his goal. [11][91] Hence, it can be regarded as a two-sides conflict game or a one-side win game, where the total payoff of two players stills fix during the game,$\sum_i^2 = 1\mu_i(s) = 0 \; \forall$ s $\in S$, where s is a strategy profile.[40]

•Nonzero-Sum Game This game, during which the sum of players' outcomes is not constant, is played between two or more players that are maximizers or minimizers. In the contrary of zero-sum games, players have no constraints on the total utility.[107][32] However, they can gain or lose together.[40]

•Stackelberg Game The Stackelberg game is utilized in the modelization of two competitive players.[40][82] The first is considered as a game leader who chooses an action from a set A1 where the second chooses an action from a set A2 after he traces the leader's action. This scenario is used broadly for different WSNs securing issues where the defender acts as a leader and the attacker is the follower [62]

•Jamming Game It is a game between the WSN defender that is player 1 and the jamming attack which his goal is disrupting the transmitted data stream. [15][108] Jamming Game is inspired basically from the zero-sum game. Interestingly, biomedical sensor and underwater sensor networks are booming applications which use the concept of jamming game.[108][70]

•Stochastic Game The stochastic game is a dynamic game which is played in a sequence of stages which are modeled on the basis of probabilistic transitions by one or more players. The new state of the game is random which depends on the previous players' actions.[40][99]

•Bayesian Game In the Bayesian game which is included in the non-cooperative game category, players have some information shortage while executing their actions. Accordingly, a player can estimate the other players' payoffs.[107][40]

•Evolutionary Game Evolutionary Game is fundamentally utilized in biological networks where players in order to enhance some population characteristics, combine pure and mixed strategies with rational behavior.[40]

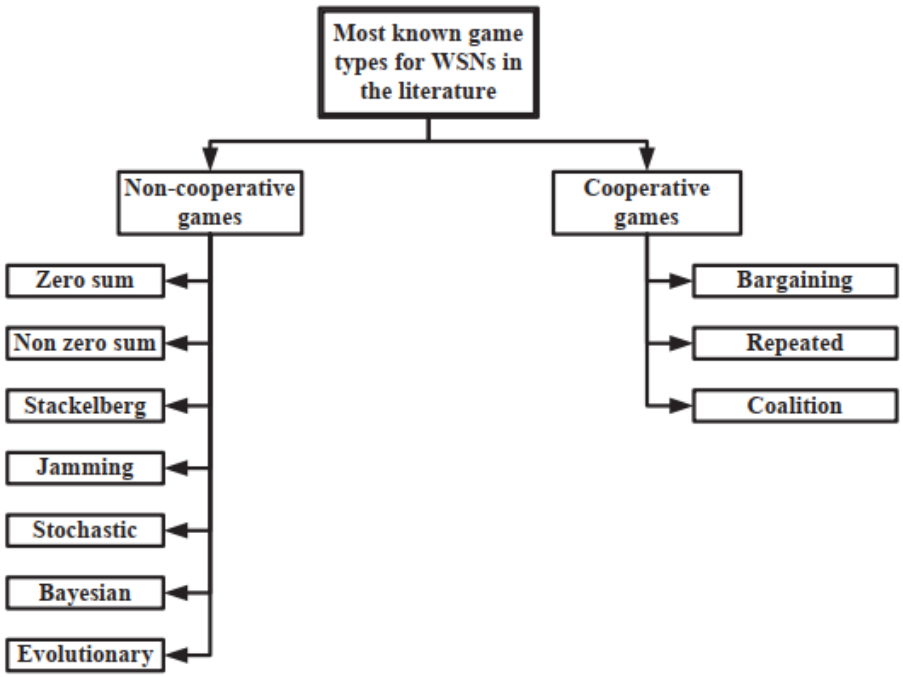

Figure 2.8: Game Theory Classification for Addressing WSN Security Issues.[67]

2.2.4 Related Work

In the literature, game theory has been widely used in IDSs for safeguarding wireless network security. Some of the existing related studies are explored below.

In paper [35], authors engage in providing an intrusion detection mechanism relying on a novel multi-criteria game. Bearing in mind the contradiction among information security, reputation and energy consumption, they formulated a two-player multi-criteria game based intrusion detection mechanism for WSNs, followed by a concrete analysis of its Pareto equilibrium. Moreover, they proposed a light weighting strategy for constructing the payoff vector, which was a feasible solution for their proposed multi-criteria game. In their model, the interaction between potential attackers and defenders is formulated as a two-player non-zero-sum multi-criteria game, where multiple objectives, i.e. the information security, reputation and energy consump-

tion, are considered when searching for the Pareto equilibrium. Although the analytical solution of the game model remains an open challenge, they deduced the reasonable mixed Pareto equilibrium strategies relying on their preference-based weighting mechanism.

In paper[31], they proposed a game theoretic approach called Ad hoc On-demand Distance Vector-Game Theoritic (AODV-GT) and they integrated it into the reactive Ad hoc On-demand Distance Vector (AODV) routing protocol to provide defense against blackhole attacks. They defined the emerging non-cooperative game between the (eMANT) and potential blackhole nodes. They found the NE and they showed that the most effective route to forward the packets according to AODV-GT is the one with the lowest cost, the least possible route to be attacked, and it introduces the lowest Host Based Intrusion Detection System (HIDS) computational cost. The simulation results show that AODV-GT outperforms AODV in terms of dropped per received packets for different number of blackhole nodes within an eMANET.

In paper [19], a game theory based multi layered intrusion detection framework for WSNs was proposed. A hierarchical intrusion detection framework for WSN, wherein intrusion detection is carried out at three different levels namely, the sensor node level (L1), the cluster head level (L2) and the base station level (L3) was designed. Authors used a combination of specification rules and a lightweight neural network based anomaly detection module to identify the malicious sensor nodes. Additionally, the framework modeled the interaction between the IDS and the sensor node being monitored as a two player non-cooperative Bayesian game. This allowed the IDS to adopt probabilistic monitoring strategies based on the Bayesian Nash Equilibrium of the game. The framework also proposed two different reputation update and expulsion mechanisms to enforce cooperation and discourage malicious behavior among monitoring nodes. These mechanisms were based on two different methodologies namely, Shapley Value and Vickery-Clark-Grooves (VCG) mechanism. Simulation results showed that the proposed framework achieved higher accuracy and detection rate across wide range of attacks, while at the same time minimized the overall energy consumption and volume of IDS traffic in the WSN.

In this work, we chose one of the most known network layer attacks which is the Black hole attack in an Ad-hoc On-Demand Distance Vector (AODV) network. A solution named AODV-GT (AODV- Game Theory) against this attack was then proposed.

Conclusion

WSNs are generally deployed in hostile and insecure environments. Such sensors are vulnerable to various threats. Hence, game-theory-based intrusion detection systems came to be used for protecting the network toward these threats.

The first section of this chapter gives an idea of a major part of intrusion detection systems for wireless sensor networks. It includes a discussion on methods of intrusion detection, IDS architectures for WSNs, a review based on WSNs IDS approaches is also given, and finally IDS assessment metrics are explained. In the second section, we have presented theoretical key concepts required to understand game theory. At the same time, game theory classifications, addresses the different game types that are involved in WSN security are outlined. Alongside some of the recent studies using game theory approach for intrusion detection in different wireless networks. These studies give us the inspiration to construct an intrusion detection game for WSNs that will be conceived in the next chapter

Part II

A Game Theoretic Approach for Securing AODV in WSN

Chapter 3

Analysis and Design

Chapter 3
Analysis and Design

Introduction

After having learned the necessary theoretical points in the two previous chapters, this chapter is dedicated primarily to review fundamental concepts related with the field under study. Accordingly, it will explain the Ad-hoc on Demand Distance Vector (AODV) routing protocol and will present in detail the black hole attack. Thereafter, it will describe the abstract model of the proposed work. Later on, the proposed methodology will be detailed.

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

AODV is a reactive routing algorithm designed by Charles E. Perkins and Elizabeth M. Royer. It is engineered for Mobile infrastructure-less networks and is based on the distance vector routing philosophy. Owing to node mobility, network topology changes frequently which make the active route out of service and new route should be discovered. AODV uses a sequence number as route freshness indicator.[68]

Routes in AODV are discovered on demand. When a node needs a route to a destination, it broadcasts a route request (RREQ) within the network. Each neighboring node that receives the broadcasted packet must check the freshness of the routing information through sequence number to update its routing table. This request will be forwarded to either the destination node or a node with an active route to the destination. A destination will unicast a response packet RREP to the source trough the preceding node choosing the shortest path with a sequence number greater than or equal to that which

was received in the RREQ. After receiving a RREP, a source node begins transmitting data packets to the destination.[68]

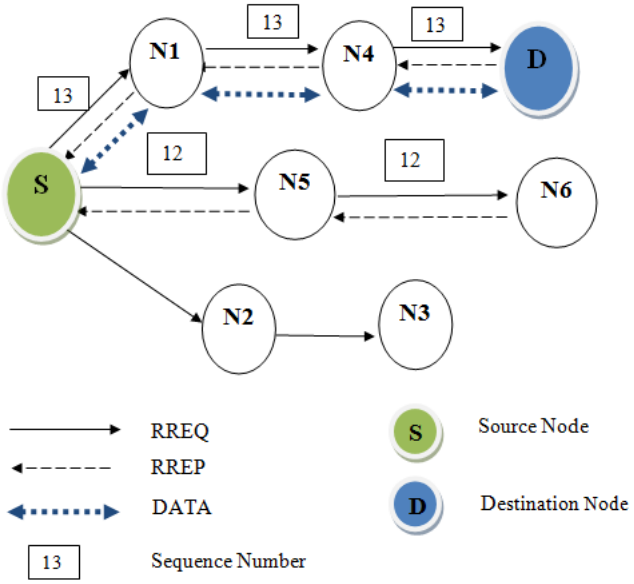

Figure 3.1: Process of AODV.[68]

3.1.1 Control Messages in AODV

AODV employs three kinds of control messages to discover a route to the destination node in the network.

Route Request Message (RREQ)

When a node determines that it needs a route to a destination and does not have one available, it disseminates a RREQ. AODV floods RREQ message, using expanding ring search technique.[18]

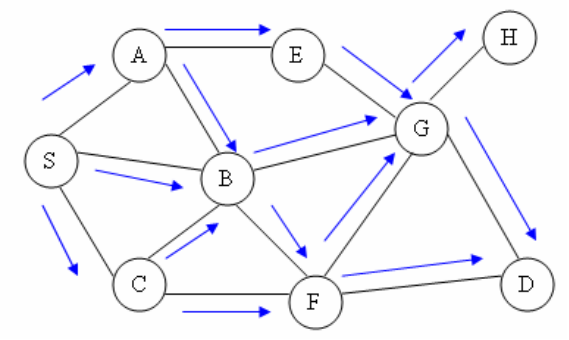

Figure 3.2: Flooding RREQ in AODV.[21]

Route Reply Message (RREP)

When the destination node or a node that has a route to the destination, it generates a Route reply message (RREP) message back to the originator node.[18]

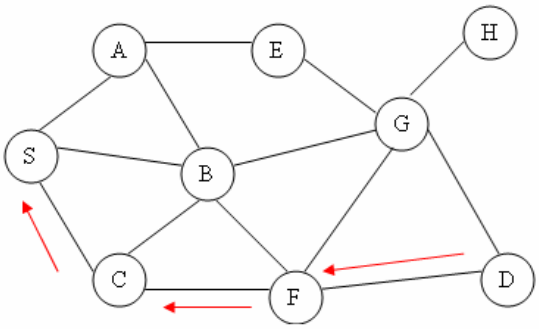

Figure 3.3: Route Reply in AODV. [21]

Route Error Message (RERR)

Every node in the network keeps monitoring the link status to its neighbor's nodes in an active route. If a link fails is detected within an active route , the node launches a route repair process by sending a Route error message (RERR) message in order to notify other nodes that the link is down.[18]

3.1.2 Route Discovery Mechanism in AODV

When a node "A" wants to communicate with another node "G", it first checks its own routing table if an entry for this destination node exists. If this is not the case, the source node create a RREQ message. This message is

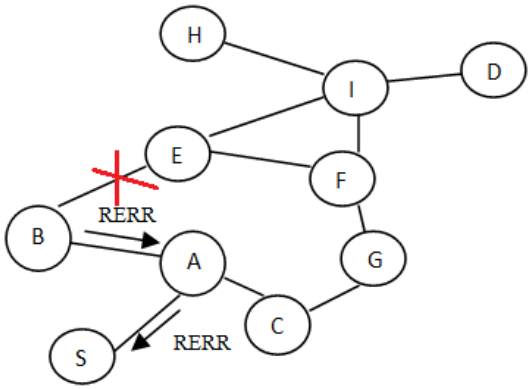

Figure 3.4: Route Error in AODV.[43]

broadcasted through a limited flooding to the neighbors whose also forward it to their neighbors nodes. This process goes on until it finds the destination node or a node that has a fresh enough route to the destination. Then they create a RREP message and unicast it to the source node. When the source node receives RREP, a route is set up between the source node "A" and destination node "G". Once the route is established, node “A” and “G” can communicate with each other. Figure 3.5 shows exchanging of control messages among the source node and the destination node. [18]

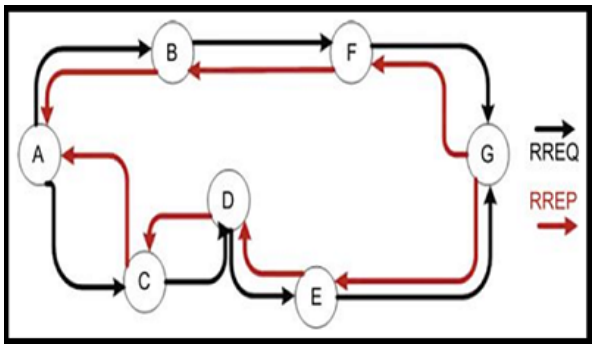

Figure 3.5: AODV route discovery.[18]

3.1.3 Route Maintenance in AODV

Whether there is a link down or a link between destinations is broken that causes one or more than one links unreachable from the source node or neighbors nodes, a RERR message is sent to the source node. When RREQ message is broadcasted for locating destination node i.e. from node “A” to

the neighbors nodes, at node "E" the link is broken between "E" and "G", hence a route error RERR message is generated at node "E" and transmitted to the source node informing the source node a route error.[18]

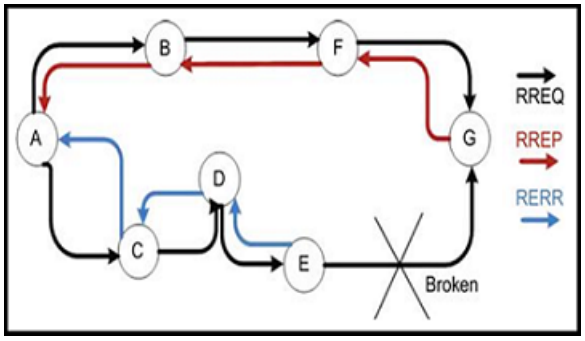

Figure 3.6: AODV Route Error Message.[18]

3.2 Black Hole Attack

The black hole attack is well known, active, and dangerous network attack, in which the attacker injects false routing information in received routing packets to behave as having the best path to destination. When the malicious node receives a RREQ packet broadcasted by the source node for any destination it immediately responds with a false RREP packet in which the sequence number field is set to a higher value i.e 2^{32} , 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 than drop them. [68]

Figure 3.7 presents of the black hole attack process summary. We assume that the node S wants to send data packets to node D, and M is a malicious node that does not have a valid route to D. The node M responds immediately to the RREQ sent to D with a fake RREP message, claiming that it has an active route to the destination. However, the attacker node performs a black hole attack in the network. It can easily drop any data traffic rather than forwarding it on and conduct a crisis at the network.[68]

3.3 Motivation

Routing is an important function of any WSN given the fact that the nodes play the role of routers. Therefore, the implementation of routing protocols

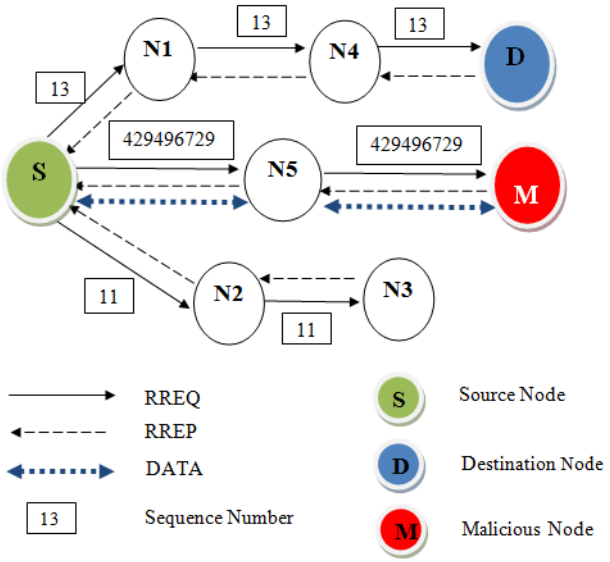

Figure 3.7: Black hole attack.[68]

is essential requirement whilst we need to guarantee that these protocols are secure. Ad-hoc On-demand Distance Vector (AODV) is one of the most familiar routing protocol of reactive routing protocol. The disadvantage of the most ratified routing protocols for WSNs is the fact that they have been developed without considering security mechanisms in advance. The case becomes more crucial in critical application sectors of WSNs sush as battlefield reconnaissance, health care surveillance, and emergency Mobile Ad hoc NETworks (eMANETs) which are deployed in emergency situations (like forest fires). In these cases adversaries could launch different kind of attacks such the blackhole one to damage the quality of the applications. In light of securing the AODV routing protocol, we have proposed a methodology, called AODV-GT (AODV- Game Theoretic) to provide defense against blackhole attack.

3.4 Proposed Approach

In this work we proposed a new routing protocol, for securing the AODV protocol against black hole attack and to reduce its adverse effects in WSN, called AODV-GT (AODV- Game Theoretic). The methodology is an effective in terms of Intrusion Detection Systems' (IDS) computational cost routing protocol. It is effective due to the fact that implements routing in

a way that the utility function of the WSN is maximized. In addition, we proved that the emerging two-player game between the WSN and the black-hole node converges to a Nash Equilibrium point when AODV-GT is applied. Moreover, we created another protocol to simulate the black hole behavior, called blackholeAODV.

Before entering in the process of development or programming, it is necessary to present our proposed work as an abstract architecture. Figure 3.8 shows to us the structure of the whole study.

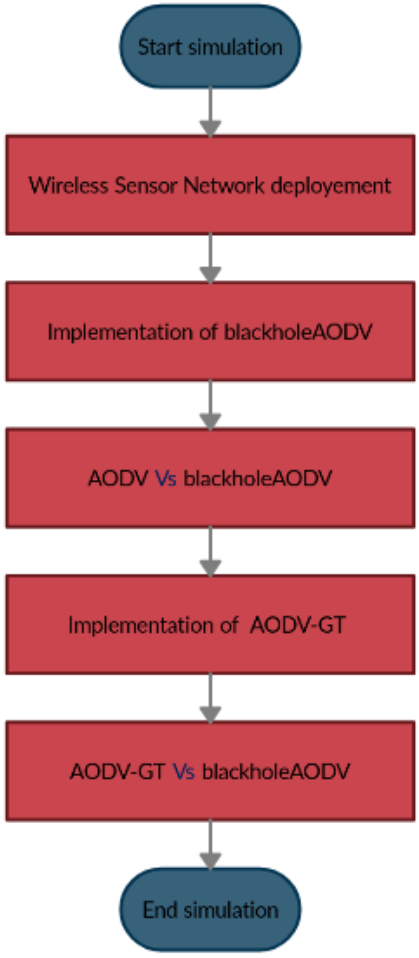

Figure 3.8: Global architecture design of the proposed study

According to our global architecture it is clear now that our study is divided into five phases which are described below:

• Phase 1: Deploy the WSN nodes in two different networks with different node numbers.

• Phase 2: Implement the blackholeAODV routing protocol to simulate the black hole attack behavior.

•Phase 3: Analysis and compare results carried out in previous phase to evaluate the WSN performance with and without black hole.

•Phase 4: Implement the proposed game theoretic approach AODV-GT and integrate it into the AODV protocol.

•Phase 5: Analysis and compare results carried out in previous phase to determine the success of the proposed solution against blackhole attack in WSN.

3.4.1 AODV-GameTheoretic Approach

We proposed a two-player non-cooperative non-zero sum route selection game, called AODV-GT between the WSN and the blackhole node in order to forward the packets of the legitimate nodes across the WSN.

We considered the HIDS approach. Once the data are collected by the HIDS sensors, they have to be analyzed in order to detect malicious activities. Thereafter, actions will be taken automatically in order to stop the attack.

We assumed that in a WSN, a malicious nodes M_1 is trying to launch blackhole attack. Specifically, the adversary has the potential to advertise shorter route to a destination node. As a result the source node believes that its packets should be passed through the node M_1. In this case, the function of the routing protocol has been disrupted. Later on, the malicious node succeeds in dropping a significant number of packets.

In accordance with our methodology, we formulated the described situation using a game theoretic framework. The players of the game were i the WSN

and *ii* a blackhole node. Thus, a two-player game was emerging. The game reached a NE as we will show later on.

Game Model

In our work we examined especially the case of a non-cooperative game where the WSN tries to defend the most critical route among all the routes that are delivered to the source node by the AODV protocol [86]. On the other hand, malicious node tries to launch blackhole attack on these routes. Towards the formulation of our game we defined the strategy space for each player.

• strategy space of the WSN:
– d $_i$: the WSN defends a route i
– d $_i$: the WSN defends any other route $-i$.
• strategy space of a blackhole node:
– m$_i$: the blackhole node attacks a route i
– m $_0$: the blackhole node does not attack WSN
– m$_h$: the blackhole node attacks a route h.
Therefore, the WSN has the potential to play:

$$\mathrm{D} = (\ \mathrm{d}_i\ \mathrm{d}_i\ \mathrm{d}_{-i}\ )$$

and each malicious node:

$$M = \begin{pmatrix} m_i \\ m_0 \\ m_h \end{pmatrix}$$

The payoff matrices of the WSN and the malicious node are detailedly described in Table 3.1, Table 3.2, and in Table 3.3.

s.t	m$_i$	m$_0$	m$_h$
d$_i$	PD(t) − DC$_i$	PD(t) − DC$_i$	PD(t) − DC$_i$ − FC$_h$, for $h \neq$i
d$_{-i}$	PD(t)− DC$_{-i}$ − FC$_i$	PD(t) − DC$_{-i}$	PD(t) − DC$_{-i}$ − FC$_h$, for $h \neq$i,-i

Table 3.1: Payoff Matrix of WSN

s.t	m_i	m_0	m_h
d_i	PA(t) − CA_i	0	PA(t) − CA_h, for $h \neq$i
d_{-i}	PA(t) − CA_i	0	PA(t) − CA_h, for $h \neq$i

Table 3.2: Payoff Matrix of Malicious Node

Symbol	Meaning
s.t.	Strategy tuples
PD(t)	Utility of the WSN at time t
DC_i	Cost for defending a route i
FC_i	Cost of failing to protect the route j
nn_j	Number of one-hop neighbors of a node j
n_i	Number of nodes which constitute the route i
R_j	Radio transmission range of the node j
N	number of nodes within the transmission range of node j at time t
A	size of the region of the WSN
PA(t)	Profit of each successful attack at time t
CA_i	Cost of any attack against a route i

Table 3.3: Parameter Description for the Payoff Matrices

DC_i depends on the values of $nn_j \; \forall \; j \in i$ and it is equal to:

$$DC_i = \frac{\sum_{j \in i} nn_j}{n_i} \quad (1)$$

More precisely, the cost of defending a route against a malicious node is actually the cost of operating the HIDS sensors in the nodes which constitute this route as well as in the one-hop neighbors of these nodes. The latter could hear the transmissions and they could participate in the intrusion detection. Obviously, when a packet is forwarded through a route which has higher DC_i value than another route, the cost for defending the former route is higher due to the participation of more HIDS sensors. At the same time, according to equation (1) when DC_i is minimized the number of nodes that a blackhole node has the potential to damage is minimized too.

FC_i changes as a function of the density of the nodes that constitute a route. The cost of failing to protect a route i is equal to the utility value that the attacker gains by dropping packets on this route. When a route is

comprised of nodes with low density, the blackhole node is less interested to place itself on this route due to the fact that it cannot damage so many nodes as it would have done if it was on a route of higher density. So it has lower possibility to gain better utility value. We defined the metric of density for each node j, according to [71], as follows:

$$dens_j(R) = \frac{NR_j^2\pi}{A} \quad (2)$$

Therefore, we defined:

$$FC_i = \frac{\sum_{j\in i} dens_j}{n_i} \quad (3)$$

Nash Equilibrium Analysis

It is worth mentioning why our game is a non-zero sum game. From the payoff matrices of the players we observe that even if the attacker does not attack the WSN is defending. The payoff of the latter therefore decreases while the payoff of the malicious node is steady. The above assumption contradicts with the zero-sum assumption which means that our game is a non-zero sum game.

Theorem 1 (Nash-Theorem): Every game that has a finite strategic form, with finite numbers of players and finite number of pure strategies for each player, has at least one NE involving pure or mixed strategies. [31]

The game we examined satisfies the assumptions of the Nash theorem which means that a NE exists in that game. In a non-zero sum games the NE has to be found considering the concept of the dominant strategy. [31] In order to find the NE of our game, first, we set the values d_1 , d_2, d_3 in the array D for the WSN as follows:

$$D^* = (d_1 d_2 d_3)$$

and we did the same in the array M:

$$M^* = \begin{pmatrix} m_1 \\ m_2 \\ m_3 \end{pmatrix}$$

In our game, at the NE, the WSN chooses to defend the route with the highest value $U(t)-DC_i$. While, the blackhole node prefers to attack the WSN in order not to receive utility equal to 0. As we have discussed, for

the maximization of $U(t)-DC_i$ we needed to minimize the value of DC_i . Therefore, what we needed first is to find the NE of the non-cooperative non-zero sum game and then to define a utility function which will be the criterion of AODV-GT for the selection of the most secure and cost effective, in terms of IDS computational cost, route. In order to find the NE, we needed to find the dominant strategy of the game. The payoff matrices of the WSN and the blackhole node are : D = $[d_{xy}]_{2\times3}$ and M = $[m_{xy}]_{\ 2\times3}$, respectively. According to the table 3.1. we had that:

$$d_{11}, d_{12} \geq d_{13} \ (4)$$

Obviously, for the WSN we had that:
(i) if $DC_i > DC_{-i}$ then $U(t)-DC_i < U(t)-DC_{-i} \Rightarrow d_{12} > d_{11}$ and (ii) if $DC_i < DC_{-i}$ then U (t) − $DC_i > U(t) - DC_{-i} \Rightarrow d_{11} > d_{12}$.
In accordance with the table 3.2:

$$m_{11} = m_{13} \geq m_{12} \ (5)$$

From the above and from the definition of the dominant strategy, the strategy pair (d_1 , m_1) is the NE of our game.

Applying AODV-GT in the AODV Protocol

In this part, we describe how AODV-GT is integrated into the AODV protocol. We assumed that a node S wants to find out a route to a node D. According to AODV, if S does not have a route to D, it has to send a RREQ message to its one-hop neighbors. Every node A which receives a RREQ derives the utility value $_A = \frac{1}{nn_A}$. A has to add the value of μ_A to the current utility value of the AODV packet. If A does not have a route to D it forwards the packet according to AODV. On the other hand, if A has a route to D, first it has to add its utility value μ_A to the utility value of the route A, ..., D in order to derive the utility μ_{AD} .

Second, A adds the value of μ_{AD} to the current utility value of the AODV packet. Then, it sends a RREP to S through the reverse route according to AODV. Finally, if A is the destination node D, it has only to add its utility value to the current utility value of the AODV packet and to send back to S a RREP including itself as the destination node.

According to AODV, S sends its packets to D using the route which it receives first. In other words, S saves only one route to D. According to AODV-GT, S has to save all the routes which it receives. For this purpose, S is waiting for a timeout to receive all the potential routes. We set the value of timeout equal to Net Traversal Time (NetTT). According to [86], this is the maximum time in milliseconds waiting for the receiving of a RREP after the sending of a RREQ. In the next step, S derives the average value $\bar{\mu}_i$ of each route $_i$ which has cached using the following equation:

$$\bar{\mu}_i = \frac{nhops_i+1}{\sum_{j\in i} nn_j} \quad (6)$$

The nhops i value indicates the number of hops which is included in the AODV packet [86]. Every node which is included in the route i has to increase the hop count by 1 during the traversing of the message from D to S.
Obviously, $n_i = nhops_i + 1$ where n_i is the number of nodes on a route i. After the computation of the average utility value of each received route, S has to send its packets to D through the route which has the maximum average utility value. This route is the most secure and cost effective route in terms of HIDS sensors computational cost among all the available routes to D due to the fact that it maximizes the utility of the WSN when the game reaches the NE. Additionally, it is worth mentioning that in case only one route is received by S, the latter sends its packets to D using this unique route.
Specifically, the utility of the WSN at the NE is equal to:

$$U(t)-DC_i = U(t)-\frac{\sum_{j\in i} nn_j}{n_i} = U(t)-\frac{\sum_{j\in i} nn_j}{nhops_i+1} \quad (10)$$

We integrated within the AODV protocol our proposed methodology as we show in Figure 3.9 and Figure 3.10.

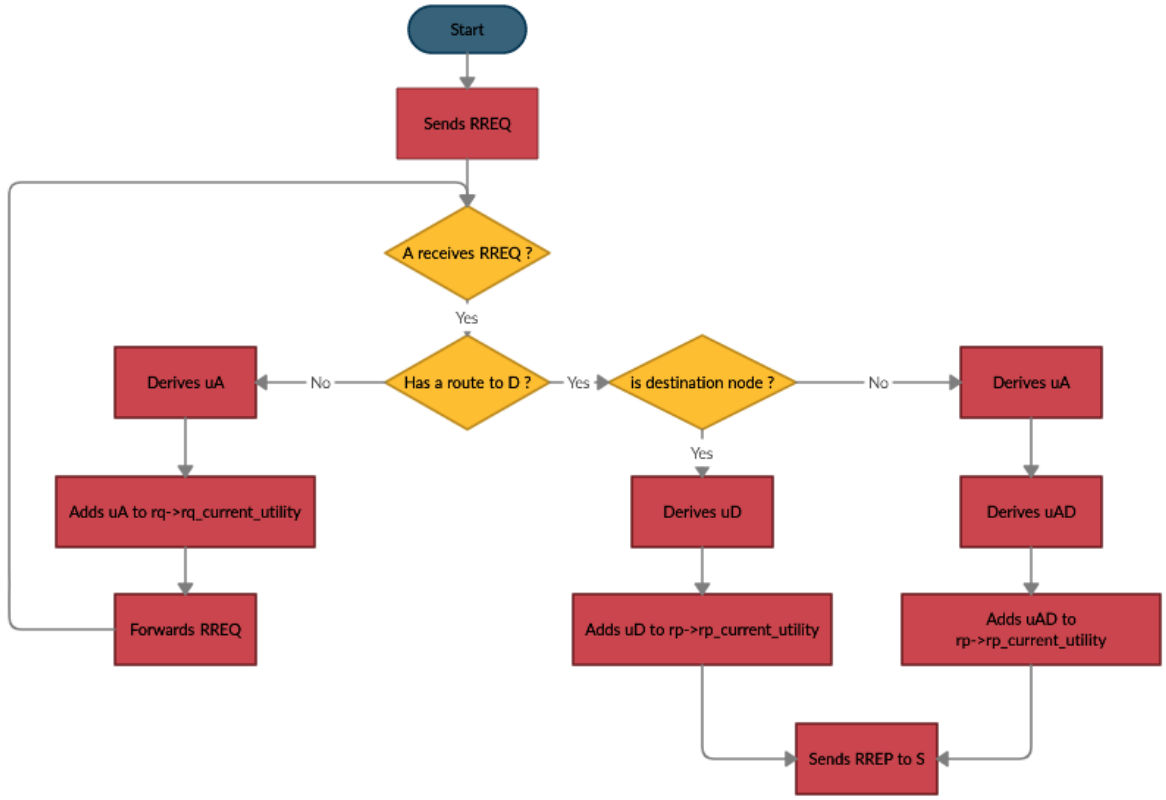

Figure 3.9: Flowchart of AODV-GT (node S sends a RREQ)

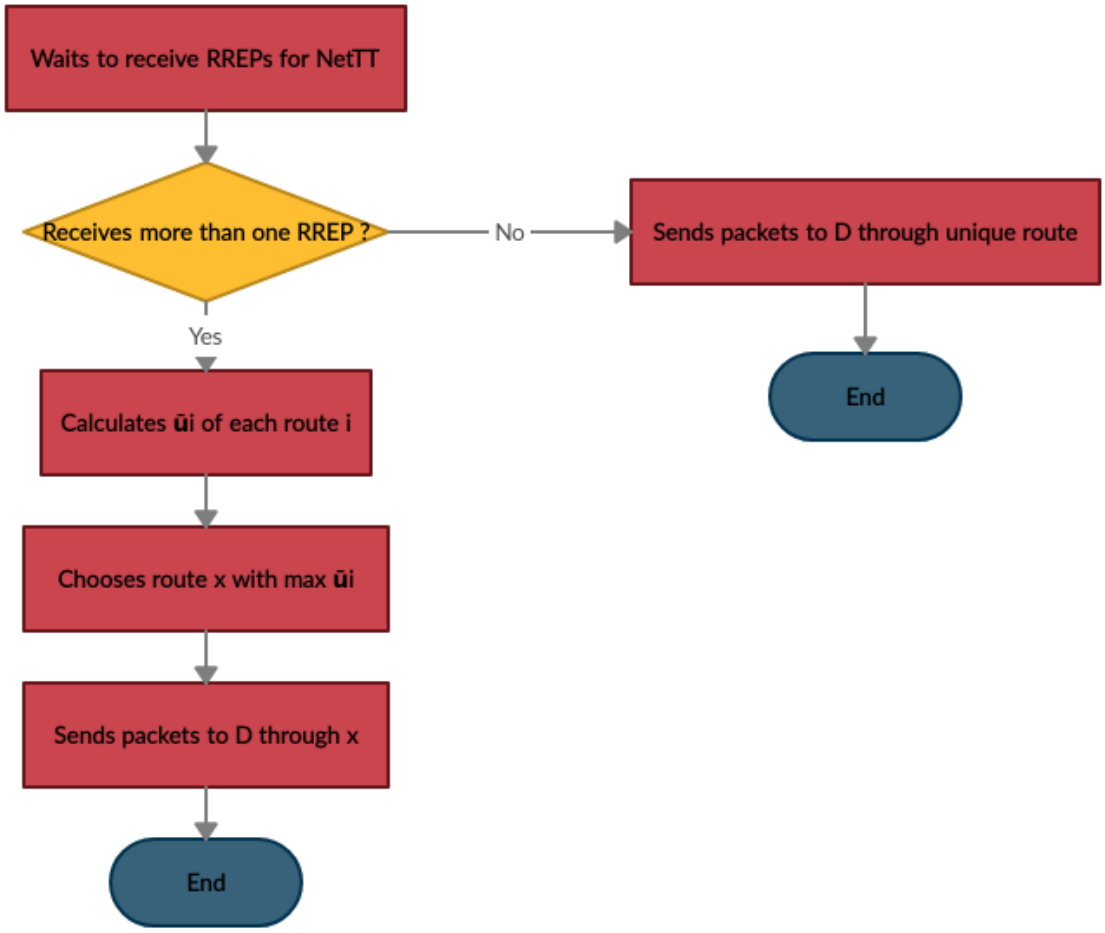

Figure 3.10: Flowchart of AODV-GT (node S receives RREP)

Figure 3.11 shows that the source node sends its data through the route with the highest utility. The HIDS sensors monitor the route in order to collect information and detect malicious activities.

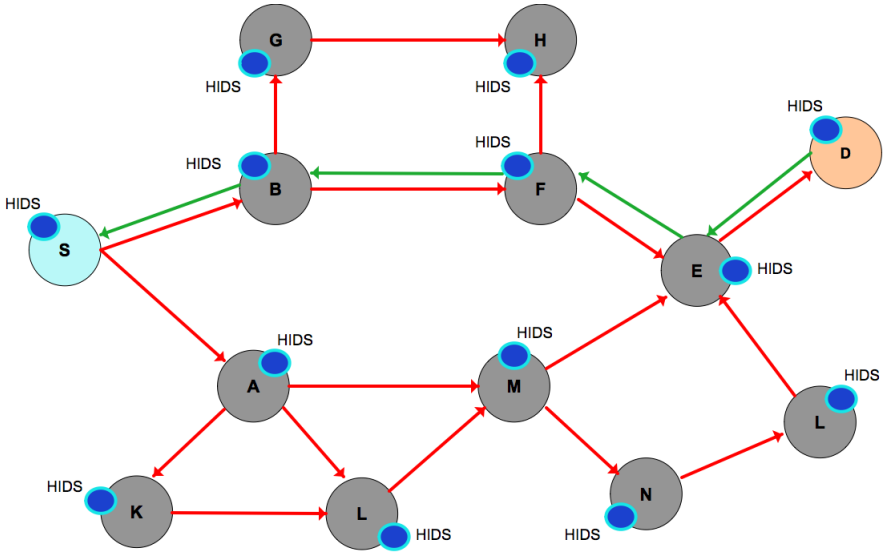

Figure 3.11: The routing procedure according to AODV-GT.

3.4.2 Performance Parameters

Metrics are routing protocol test parameters that allow performance measurement. In our study, we took into account the following metrics:

Packet Delivery Ratio (PDR)

Packet delivery ratio is the ratio of total number of data packet received by the destination node to the total data packet sent by the source node[78].

$$PDR = \frac{Number\ \ of\ \ received\ \ packets}{Number\ \ of\ \ sent\ \ packets}$$

Throughput

Throughput is the ratio of the number of packets sent by the source to the time taken to send those packets[78].

$$Throughput = \frac{Number\ \ of\ \ sent\ \ packets}{Time\ \ to\ \ send\ \ packets}$$

End-to-End Delay

Latency or end-to-end delay is the amount of time taken by a packet to reach its destination. [78]

Conclusion

In this chapter, we have presented our contribution. We have presented important aspects of the used routing protocol AODV and the effect of the black hole attack to the whole network. Moreover, we have described the proposed approach and have discussed used performance parameters. We move on to the next stage where we implement this project. The next steps of the project are an implementation of the proposed design, testing and discussing some experimental results. These steps will be the aim of the next and last chapter.

Chapter 4

Implementation and Experimental Results

Chapter 4
Implementation and Experimental Results

Introduction

After the analysis and design of the hole study, The next step is the implementation of the black hole attack protocol and the proposed solution for securing AODV protocol from the blackhole attack. Then, evaluating results are given. The objective in this chapter is to present the performance of the proposed approach.

4.1 Development Environment

4.1.1 Simulation

Simulation is the process of designing a model of a real system and conducting experiments with this model for the purpose of understanding the behavior of the system and/or evaluating various strategies for the operation of the system.[101]

4.1.2 Network Simulator 2

Network Simulator (Version 2), widely known as NS2, is simply an event-driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols can be done using NS2. Practically, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors.[101]

Figure 4.1 shows the basic architecture of NS2. NS2 provides users with an executable command ns which takes on input argument, the name of a Tcl simulation scripting file. In most cases, a simulation trace file is created, and is used to plot graph and/or to create animation. NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). While the C++ defines the internal mechanism of the simulation objects, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events. The C++ and the OTcl are linked together using TclCL. After simulation, NS2 outputs either text-based or animation-based simulation results. To interpret these results graphically and interactively, tools such as NAM (Network AniMator) and XGraph are used.

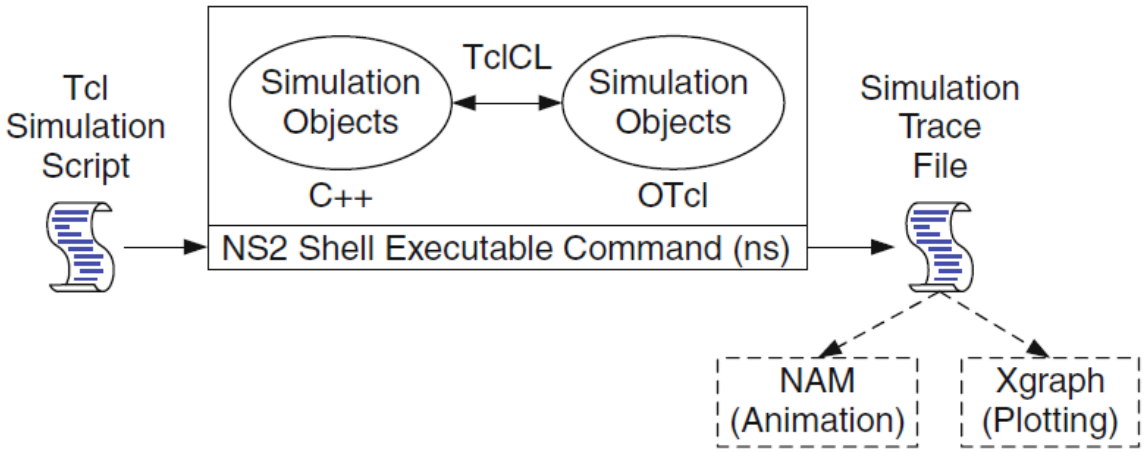

Figure 4.1: Basic architecture of NS2 [101]

In this work, NS-2 version 2.35 of "all-in-one package" is used. The ".tcl" files are written in text editor and the results of the ".tr" file are analyzed using "awk" commands. NS2 is installed on a personal computer Lenovo which has the following characteristics:

OS	Ubuntu 16.04 LTS 64-bit
CPU	Intel® Core™ i5-5200U CPU @ 2.20GHz 4
RAM	4.00 GiB

Table 4.1: Physical machine specifications

4.2 Implementing a New Routing Protocol to Simulate Black Hole Attack

To give a node the characteristics of blackhole node we need to implement a new routing protocol in NS2. Implementation of this protocol is detailed below. All routing protocols in NS2 are installed in the directory of "ns-2.35". We first duplicate the AODV protocol in the ns-2.35 directory and change the name of this directory as "blackholeaodv". In this blackholeaodv directory the name of all files that are labeled as "aodv" are changed to "blackholeaodv" such as blackholeaodv.cc, blackholeaodv.h, blackholeaodv.tcl etc. All classes, functions, variables, and constants names in blackholeaodv directory have changed but struct names that belong to AODV packet.h file have not changed. To integrate the new blackholeaodv protocol in NS-2.35 simulator, we have changed two files that are used globally in this simulator. In " tcl lib ns-lib.tcl" file we first add the lines shown in Code 1, for the agent procedure for blackholeaodv.

Code 1: Adding the "blackholeaodv" protocol agent in the " tcl lib ns-lib.tcl" file.

```
1:  blackholeAODV {
2:          set ragent [self create − blackholeaodv − agent node]
3:  }
4:  Simulator instproc creat-blackholeaodv-agent  node  {
5:          # Create blackholeAODV routing agent
6:          set ragent [new Agent/blackholeAODV [$node node-addr]]
7:          $self at 0.0 "$ragent start"
8:          $node set ragent_$ragent
9:          return $ragent
10: }
```

Second file which is in the ns-2.35 directory named " makefile" where we add the lines shown in Code 2.

Code 2: Addition in the " makefile" at the ns-2.35 directory

```
1:  blackholeaodv/blackholeaodv_ logs.o blackholeaodv/blackholeaodv.o
2:  blackholeaodv/blackholeaodv_rtable.oblackholeaodv/blackholeaodv_
rqueue.o
```

In aodv.cc, the "recv" function process the packet based on the type of the packet. If packet type is AODV route conducting packet such as RREQ, RREP, RERR, it sends the packet to the "recvAODV" function. When the received packet type is data packet type then AODV protocol sends it to the destination address. In Code 3, the first "if" condition provides the node to receive data packets if it is the destination and the "else" condition consume all remaining packets as a Black Hole node.

Code 3:"If" statement for accepting the packets by destination or dropping packets by malicious node.

```
1:  // If destination address is itsself
2:  if ( (u_int32_t)ih->saddr() == index)
3:      forward((blackholeaodv_rt_entry) 0, p, NO_DELAY);
4:  else
5:  //Node drops all packets
6:      drop(p, DROP_RTR_ROUTE_LOOP);
```

To generate the black hole behavior we need to make change in blackholeaodv.cc file by adding the false RREP. The false RREP message show that it has the highest sequence number and the hop count is set to 1. The Highest sequence number of AODV protocol is 4294967295, 32 bit unsigned integer value [59]. The lines in Code 4 are added to aodv.cc file to generate the characteristics of black hole node.

Code 4: The false RREP of blackhole or malicious node.

```
1:  sendReply(rq->rq_src,          // IP Destination
2:      1,                         // Hop Count
3:      index,                     // Dest IP Address
4:      4294967295,                // Highest Dest Sequence Num
5:      MY_ROUTE_TIMEOUT,          // Lifetime
6:      rq->rq_timestamp);         // timestamp
7:  Packet::free(p);
```

After all changes are finished, we have to recompile all NS-2 files to create object files. For recompiling, we have to run ./configure, make clean, make, and make install commands, respectively in ns2.35 directory.

4.3 Examining the Blackhole AODV Protocol

The implementation of the black hole is tested to see whether it is correctly working or not using the NAM application of NS2. However, we used two scenarios. The first scenario was without black hole attack. Where in the second one, we added a black hole node to the simulation. Conceptually, the malicious node that exhibits the black hole attack is called "black hole node". Then, we compared the performance metrics of the two scenarios.

4.3.1 Simulation Parameters

We simulated an area which is equal to 1000m x 1000m for 10 seconds. We also generated a UDP traffic and we examined the cases of 8, and 16 nodes. In all scenarios, the sending node is node 0 and the receiving node is node 7. Additionally the appropriate positions of the nodes are manually designed to show the data flow. The parameters used in simulation are shown in table 4.2.

Type	**Value**
Simulator	Network Simulator (Version 2.35)
Simulation Time	10 secondes
Simulation Area	1000 x 500
Number of Nodes	8 and 16 nodes
Number of Blackhole	Nodes 1 node
Radio Propagation Model	Propagation/Tworayground
MAC Protocol	$Mac_8$02.11
Data Packet Size	512 bytes
Antenna	Antenna/Omniantenna
Link Layer	LL
Routing Protocol	AODV, blackholeAODV and AODV-GT
Traffic	CBR

Table 4.2: Simulation parameters.

The statement: "$ns_node - config - adhocRouting$val(brp)" changes the routing protocol of the selected node to "blackholeAODV" which is declared in the parameter setup to the value "brp" as shown in Code 5 and Code 6, so we can easily add the blackholeAODV behavior with writing the number of node we wish to be blackhole.

Code 5: Creation of black hole node.

```
1:    blackhole node creation
2:    $ns node-config -adhocRouting $val(brp)
3:    set node_(2) [$ns node]
```

Code 6: Black hole protocol in the parameters setup.

```
1:    set val(brp) blackholeAODV ;    # blackhole aodv protocol mentioned here..
```

4.3.2 Simulation Evaluation

In both scenarios where there is not a black hole node, connection between source node and destination node is correct. Figures 4.2 and 4.3 illustrate the data flow from node 0 to node 7

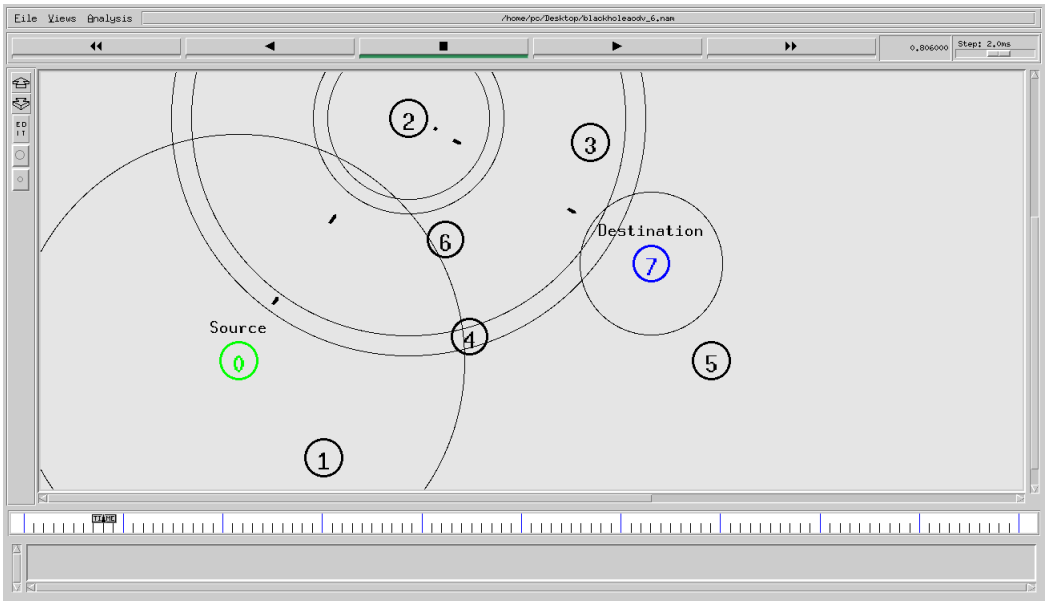

Figure 4.2: Data flow between node 0 and node 7 via node 2.

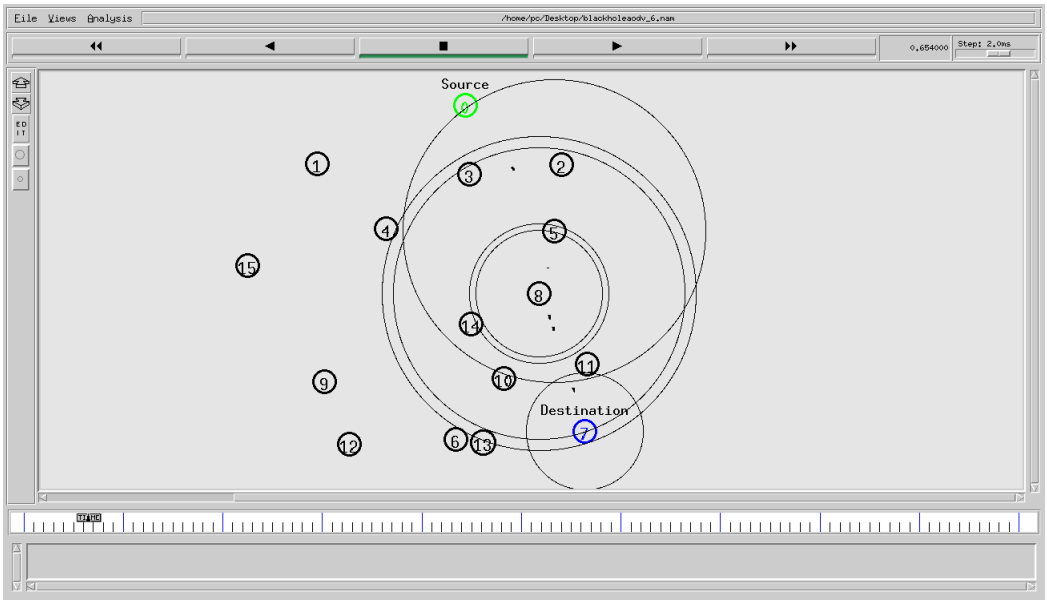

Figure 4.3: Data flow between node 0 and node 7 via nodes 5 and 8 .

The black hole node absorbs the packets in the path from the source node to the receiving one. Figures 4.4, and 4.5 show how the black hole node attracts the traffic. In figure 4.4 node 8 is black hole node, node 0 is sending node, and node 7 is destination node. Node 8 sends RREP to sending node's RREQ and after receiving data packets it will drop them.

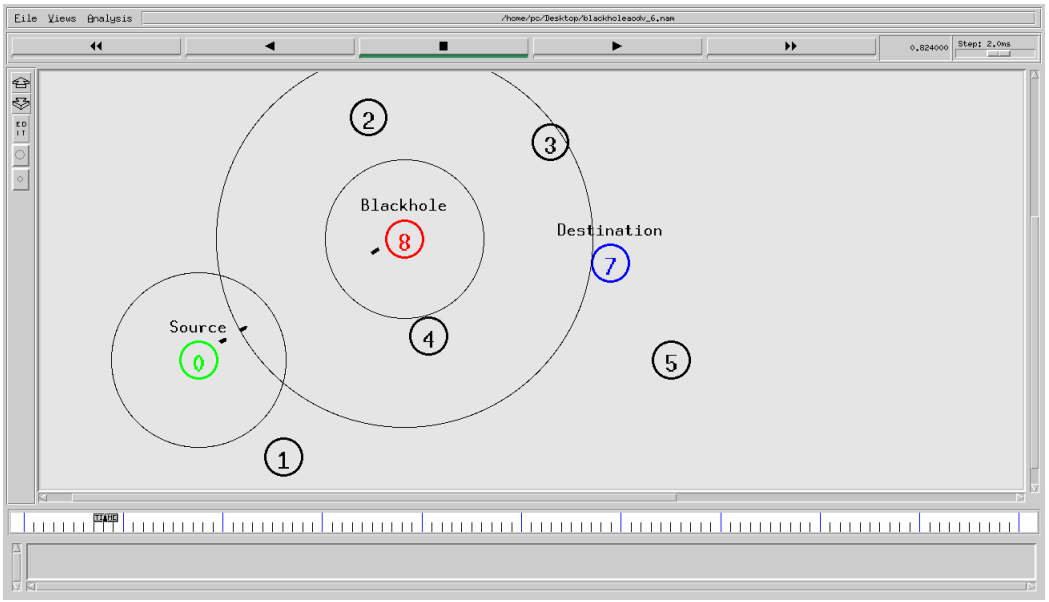

Figure 4.4: Node 8 attracts the connection between nodes 0 and 7.

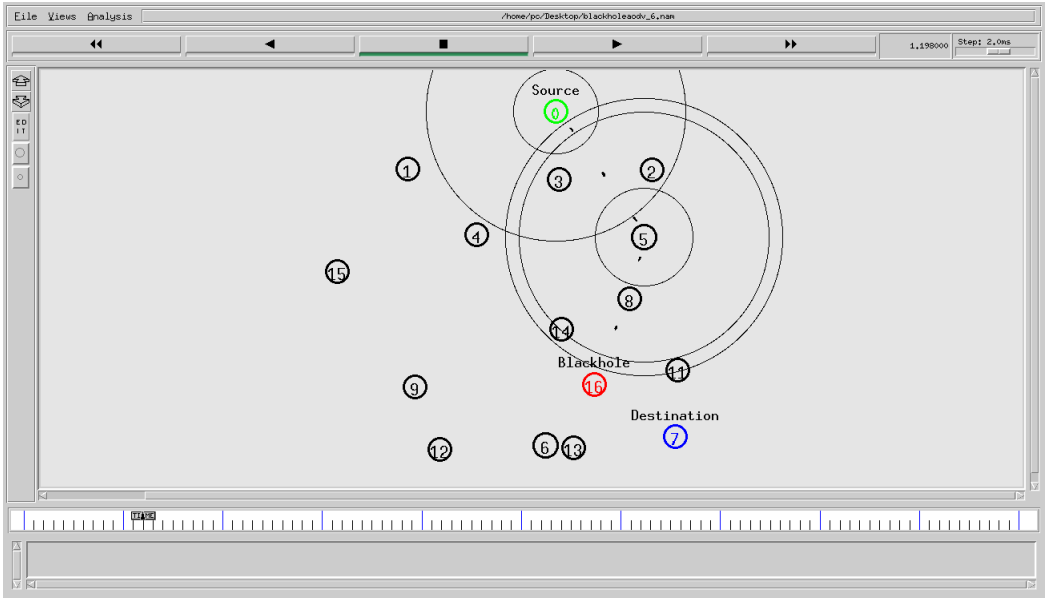

Figure 4.5: Node 16 attracts the connection between nodes 0 and 7.

4.3.3 Testing Trace File and Evaluating Results

We get the simulation results from output trace file of the Tcl scripts, which has .tr extension. Trace files include all events in the simulation such

as when the packets are sent, which node generated them, which node has received, which type of packet is sent, if it is dropped why it is dropped etc.

The two previous scenarios have been examined. Afterward, the results of these scenarios are compared to understand the network and node behaviors.

As we can see from Figure 4.6 , PDR is almost 75 % for the 8 nodes network and 50% for the 16 nodes networks without black hole attack. That means almost total packets sent by sender node are received by receiver node, but for network with black hole node PDR reduces to 0%, that means the whole packets sent by sender node are dropped by black hole nodes.

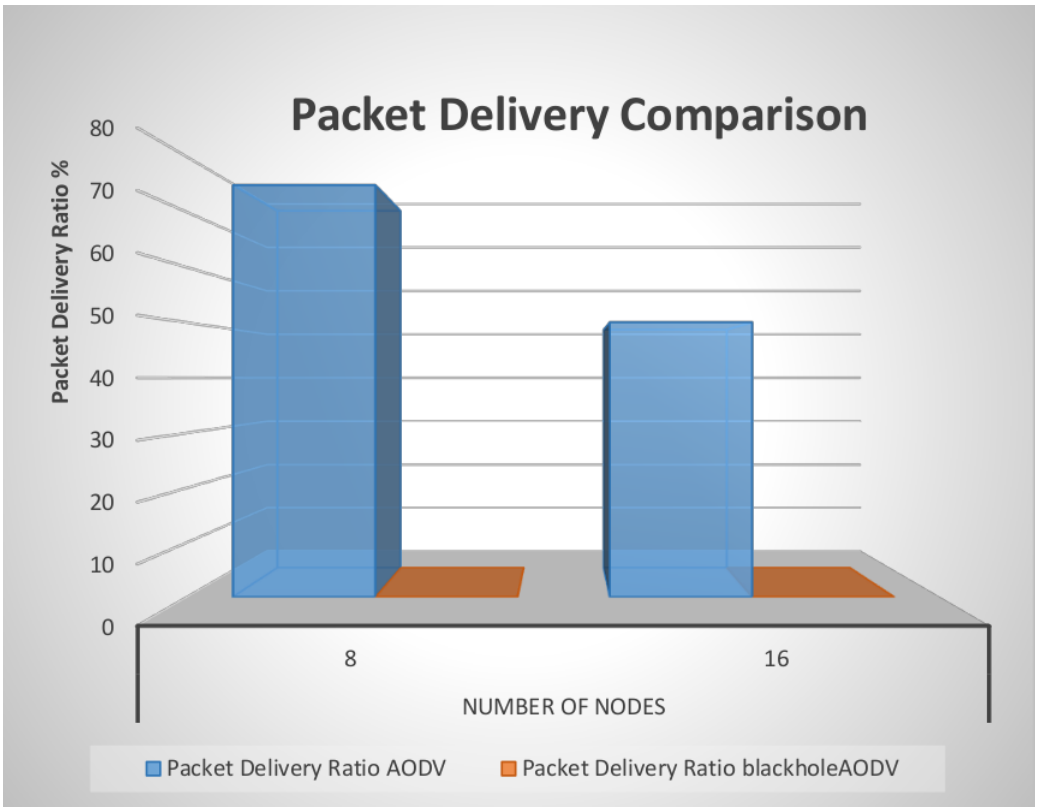

Figure 4.6: Packet Delivery Ratio comparison

Figure 4.7 shows that The throughput equals to 336 (ms) for the 8 nodes scenario and to 224 (ms) for the 16 scenario, when the AODV protocol is applied. Where for the blackholeAODV protocol, it tends towards 0. Because of the effect of malicious nodes.

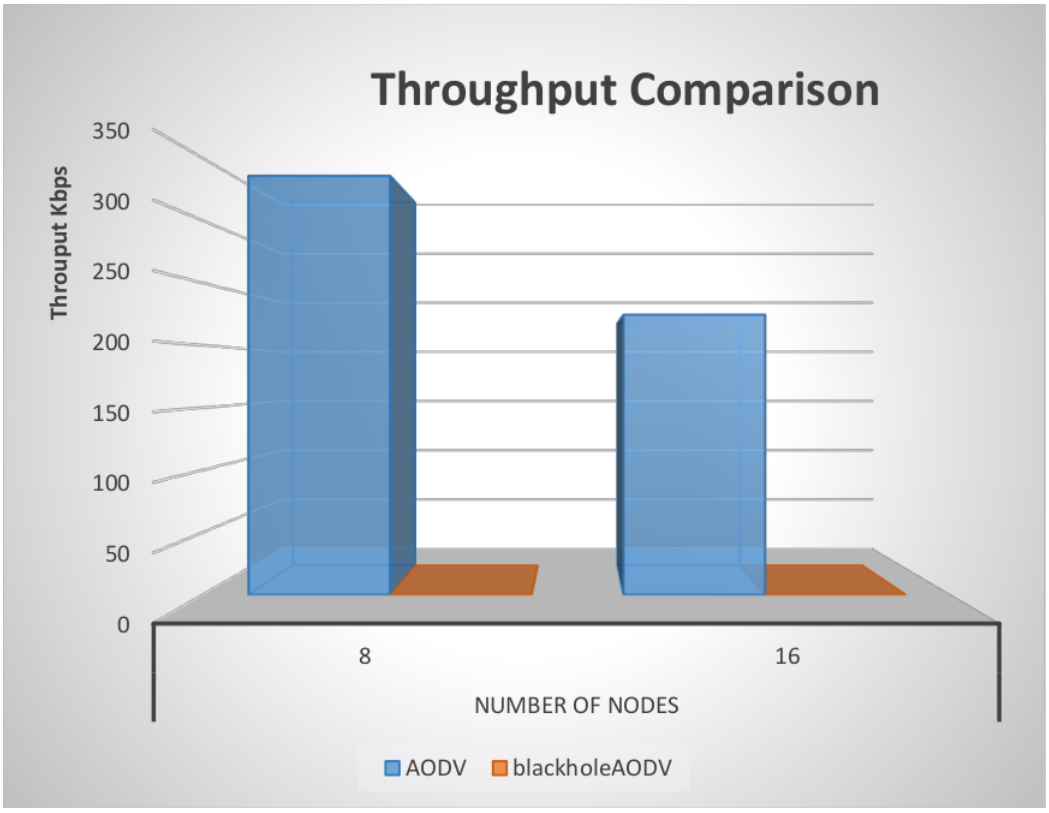

Figure 4.7: Throughput comparison

From Figure 4.8 illustration, the value of delay in AODV is higher when the network did not have any blackhole nodes present. It dropped down upon the introduction of blackhole nodes in the network to 0.

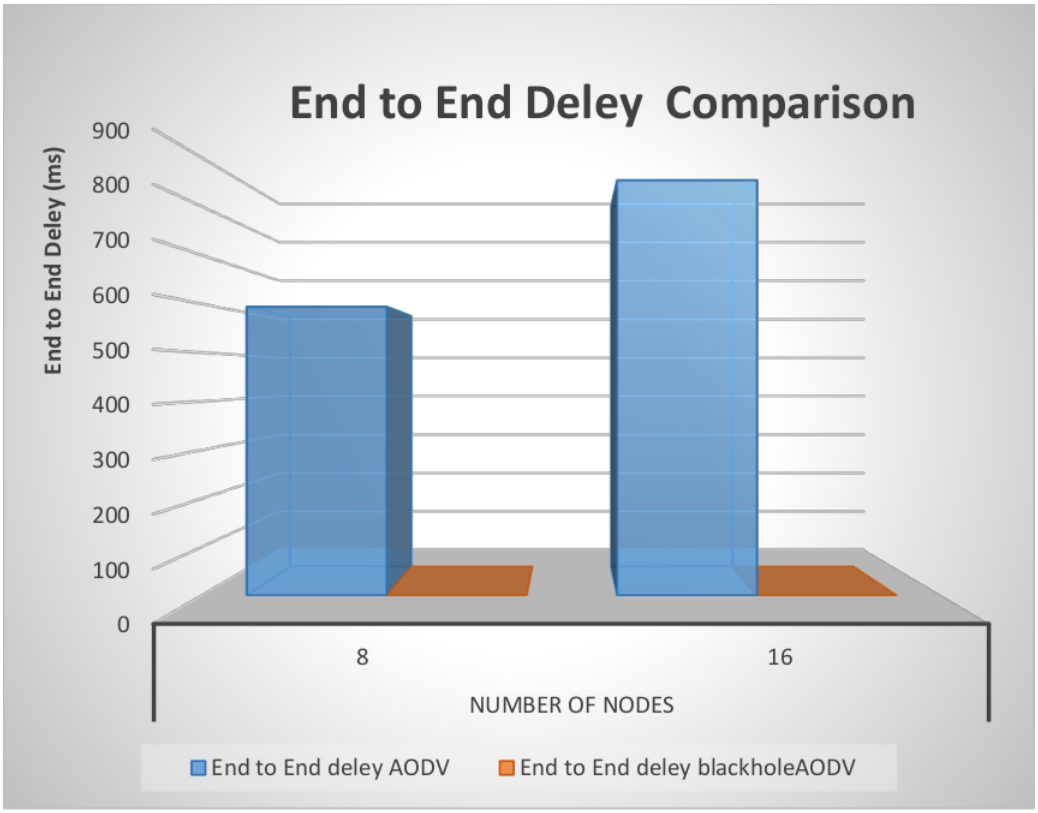

Figure 4.8: Average End-to-End Delay comparison

4.4 Implementing AODV-GT Protocol Against Blackhole Attack

To implement the proposed solution against Blackhole, we duplicated the "AODV" protocol, changing it to "AODV-GT" as we did in "blackholeaodv". At first, we have changed all files name in the cloned "aodv" directory to "AODV-GT". To integrate the new AODV-GT protocol in NS-2.35 simulator, at First the file " tcl lib ns-lib.tcl" is modified where protocol agents are coded that is presented in Code 7.

Code 7 : Adding the "proposed" protocol agent in the " tcl lib ns-lib.tcl" file

```
1:  GTAODV {
2:  set ragent [$self create-GTaodv-agent $node]
3:
4:  }
5:  Simulator instproc create-GTaodv-agent { node } {
6:    # Create GTAODV routing agent
7:  set ragent [new Agent/GTAODV [$node node-addr]]
8:  $self at 0.0 "$ragent start"
9:  $node set ragent_ $ragent
10: return $ragent
11:   }
```

Second file which is in the ns-2.35 directory named " makefile" where we added the lines that are in Code 8.

Code 8 : Addition in the " makefile" at the ns-2.35 directory.

```
1:  GTaodv/GTaodv_logs.oGTaodv/GTaodv.o
2:  GTaodv/GTaodv_rtable.oGTaodv/GTaodv_rqueue.o
```

To provide defense against blackhole attack, we integrated within the AODV protocol our proposed methodology as we show in algorithms 1 and 2.

Algorithm 1 AODV-GT (node S sends a RREQ)

If a node A receives a RREQ **Then**
  If A does not have a route to the destination node D **Then**
    derives u A
    adds u A to the current utility value in the AODV packet
    forwards the RREQ according to AODV
  ELSE
    If A has a route to D **Then**
      derives u A
      adds its utility value u A to the utility value of the route A, .., D in order to compute a final
      utility u AD
      adds u AD to the current utility value in the AODV packet
      sends a RREP to S according to AODV
    ELSE
      // A is the destination node D
      derives u D
      adds u D to the current utility value in the AODV packet
      sends a RREP to S according to AODV
    EndIf
  EndIf
EndIf

Algorithm 2 AODV-GT (node S receives RREP)

S is waiting for RREP for a timeout NetTT
If S receives more than one RREP **Then**
  S calculates the average average utility $\bar{u}_i$ of each route$i$
  S chooses the route x with the maximum average utility max$\bar{u}$ x
  S sends its packets to D through x
ELSE
// S receives only one RREP
  S sends its packets to D through the route which it received by the unique RREP
EndIf

4.5 Examining The AODV-GT Protocol

To validate the AODV-GT protocol, we tried it in the previous two simulations (8 and 16 nodes) with the same simulation parameters. In the scenarios

of the simulation, idsAODV protocol is used instead of AODV for all nodes except the black hole node.

Figure 4.9 and 4.10 illustrate that the sender node is sending packets to the appropriate receiver node as expected.

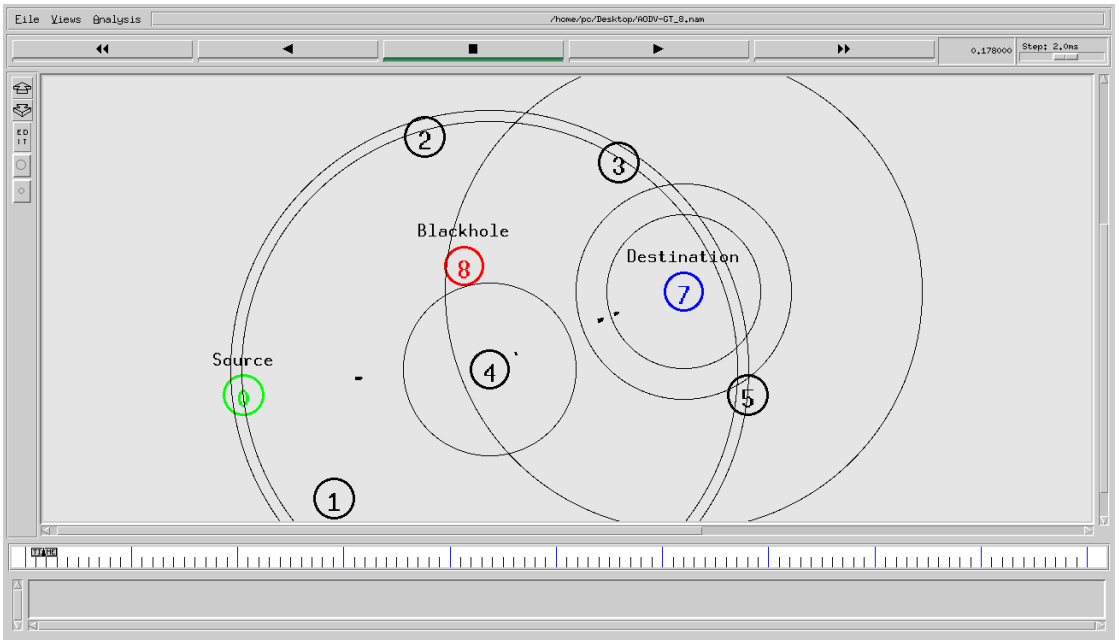

Figure 4.9: Packets are reaching the destination node properly through node 4.

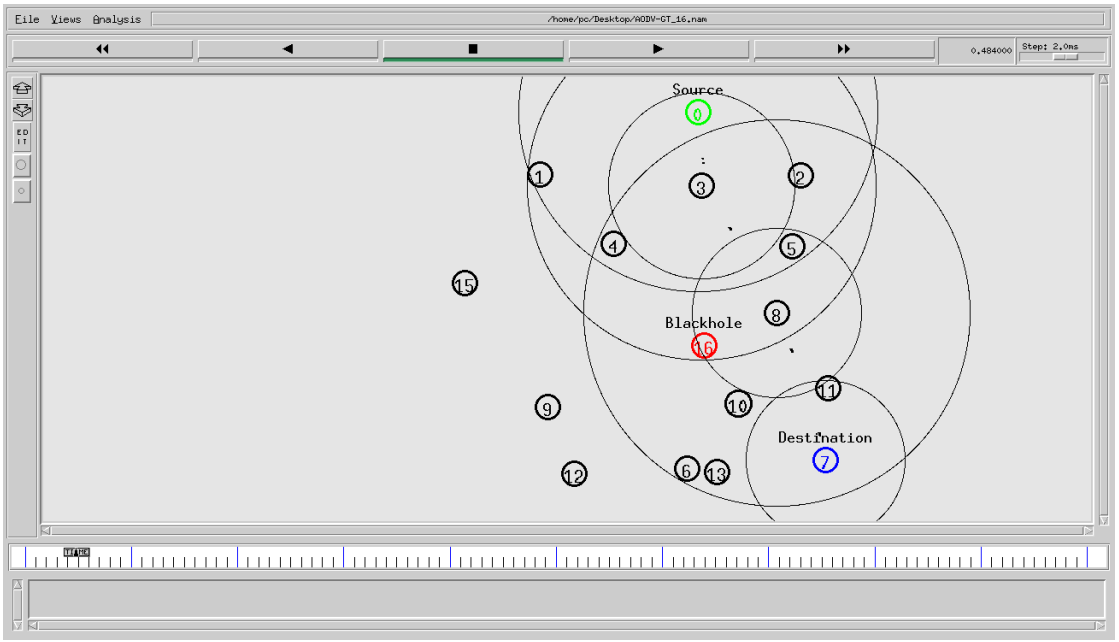

Figure 4.10: Packets are reaching the destination node properly through nodes 3 and 8.

4.5.1 Evaluating Results

To be able to evaluate if the proposed approach has been successful, we used same scenarios and simulation parameters as described before.

In Figure 4.11 we observe that with existence of malicious node, PDR reduces to 0 % , which means the whole packets sent by sender node are dropped by malicious nodes. While for the network using AODV-GT the PDR increases almost as the normal network without black hole attack.

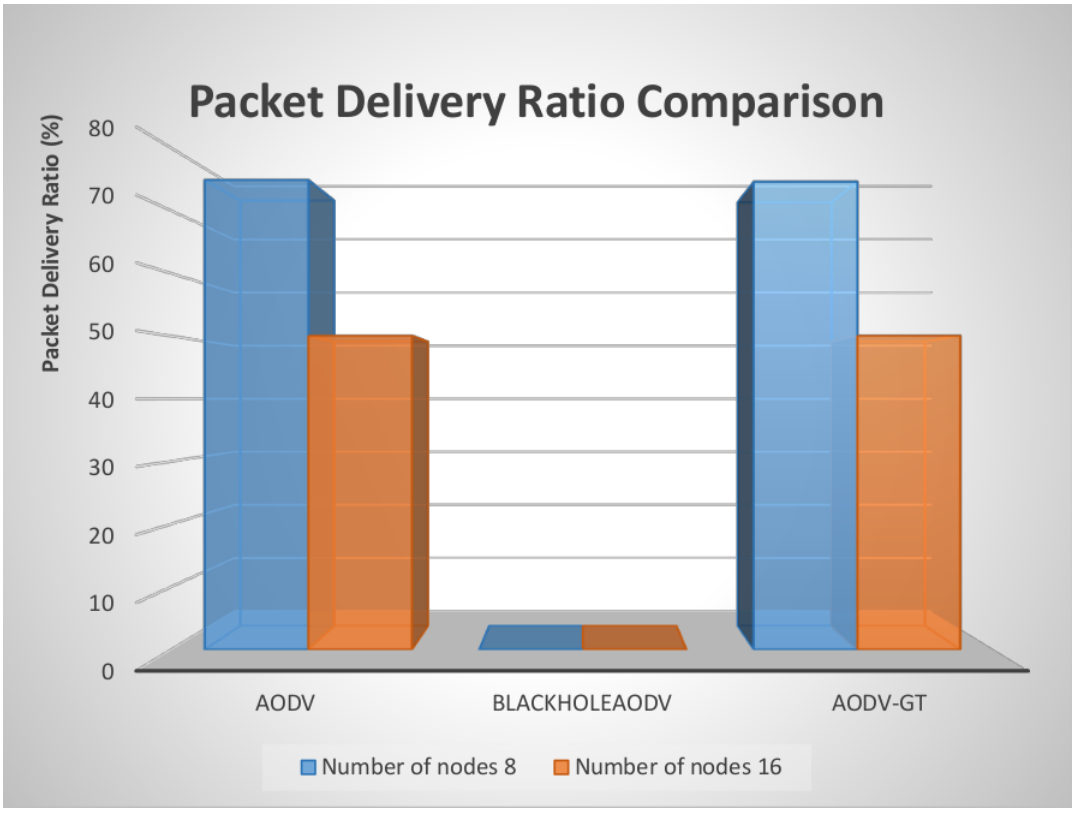

Figure 4.11: Packet Delivery Ratio comparison

Figure 4.12 shows the comparison of throughput values before black hole attack, after black hole attack and after using AODV-GT. Throughput is approximate 336 (ms) for 8 nodes normal network. When there is a blackhole attack in the network, it decreases to 0. As the AODV-GT is applied, this value increases to 335 (ms).

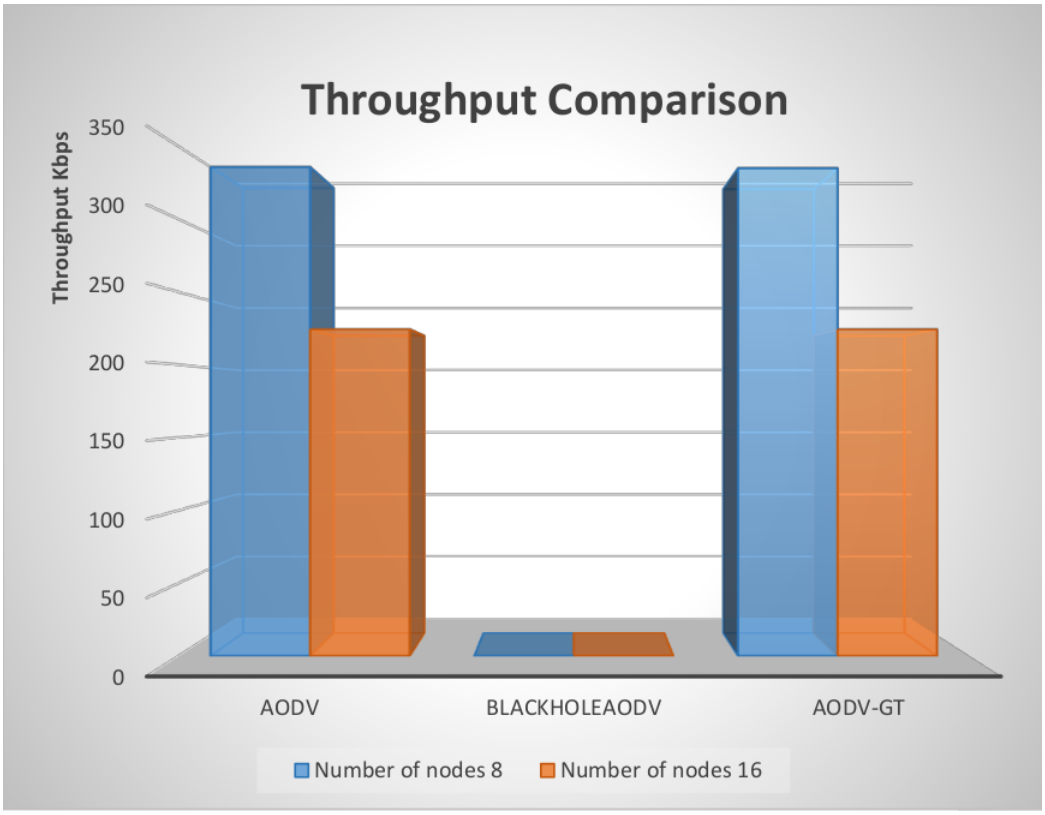

Figure 4.12: Throughput comparison

The lower value of average end-to-end delay means the better performance of the protocol. We can see from Figure 4.13 that the average end-to-end delay was little higher when the WSN did not have any blackhole node. It became lower upon the application of AODV-GT solution to 549 (ms). But it reaches the 0 upon the introduction of blackhole nodes in the network.

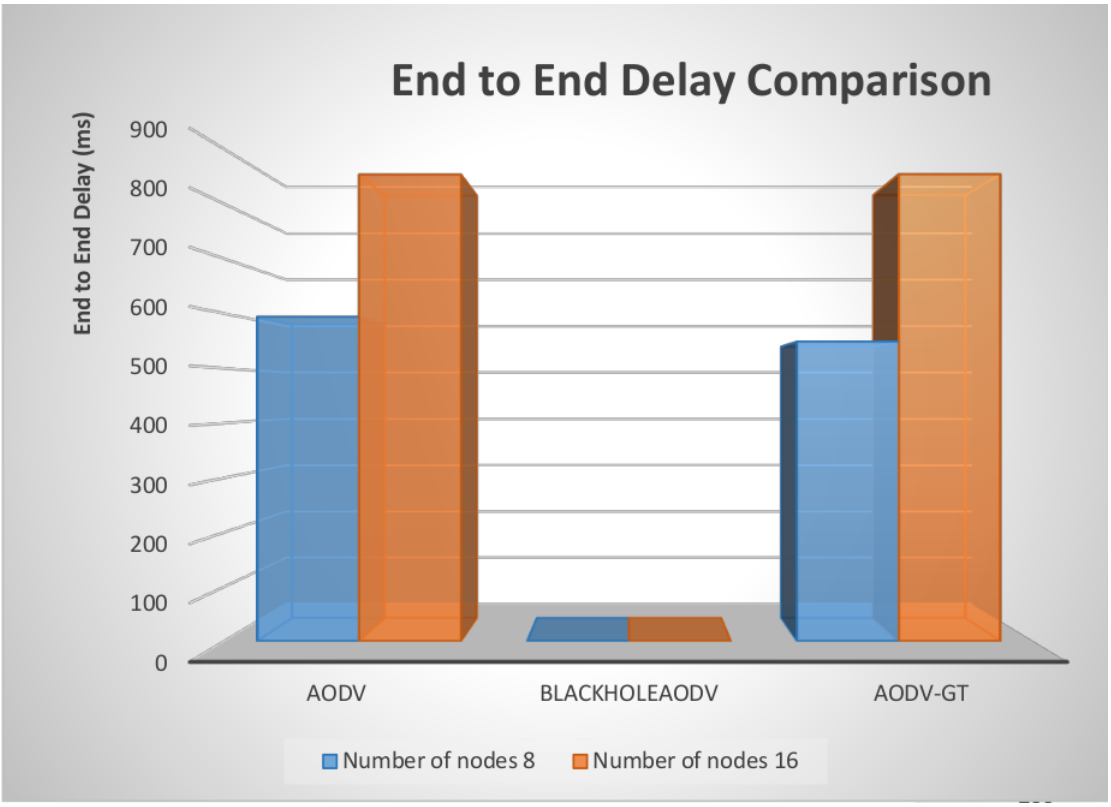

Figure 4.13: Average End-to-End Delay comparison

Conclusion

In this chapter, first we investigated the performance of network before black hole attack and after black hole attack. The results obtained show that the blackholeAODV protocol is working and the attack is correctly simulated. Also the performance of the network is examined under this attack. The last part of this chapter shows the proposed solution to this attack and it is correctly simulated. According the results, AODV-GT can improve performance of AODV in Wireless Sensor Network under a blackhole attack.

General Conclusion

General Conclusion

Wireless Sensor Networks consist of sensor nodes deployed in a manner to collect information about surrounding environment. Their distributed nature, multihop data forwarding, and open wireless medium are the factors that make WSNs highly vulnerable to security attacks at various levels. Intrusion Detection Systems (IDSs) can play an important role in detecting and preventing security attacks.

We have analyzed effect of the Black Hole in an AODV sensor Network. For this purpose, we implemented an AODV protocol that behaves as Black Hole in NS-2. After that, we proposed a game theoretic approach called AODV-GT and we integrated it into the AODV protocol for securing AODV in Wireless Sensor Networks against blackhole attacks. To this end, we formulated a game between the WSN and the potential blackhole node. We found the NE and we showed that the most effective route to forward the packets according to AODV-GT is the one with the lowest cost DC i . This route is the least possible route to be attacked and it introduces the lowest HIDS computational cost. This makes sense due to the fact that malicious nodes prefer to damage parts of WSN which have high number of legitimate nodes achieving high utility. The simulation results show that AODV-GT outperforms AODV in terms of dropped per received packets when blackhole node exists within our WSN.

Our future work involves experimenting with different areas, mobile networks (MANETs), multiple black hole attacks and other type attacks such as wormhole attack.

Bibliography

[1] Zigbee alliance. http://www.zigbee.org/, 30 Dec 2019.

[2] Zigbee standards overview. http://www.freescale.com/webapp/sps/site/overview.jsp?nodeId=01J4Fs25657725, 30 Dec 2019.

[3] Definition of connected car - what is the connected car? defined. https://www.autoconnectedcar.com/, 6 January 2020.

[4] Industrial networking and iot. https://www.cisco.com/, 06 January 2020.

[5] K. Basu A. Agah, S. K. Das and M. Asadi. Intrusion detection in sensor networks: A non-cooperative game approach. *In Proceedings Third IEEE International Symposium on Network Computing and Applications*, page 343–346, NCA 2004, Aug 30-Sep 1 2004.

[6] S. K. Das A. Agah. Preventing dos attacks in wireless sensor networks: A repeated game theory approach. *International Journal of Network Security*, 5(2):145–153, Sept. 2007.

[7] M. Durresi A. Durresi and L. Barolli. Security of mobile and heterogeneous wireless networks in battlefields. 2008.

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

[9] B. P.S. Rocha A. A.F. Loureiro L. B. Ruiz-H. C. Wong A. P. R. da Silva, M.H.T. Martins. Decentralized intrusion detection in wireless sensor networks. 2005.

[10] R.Chaki A. Sharma and U. Bhattacharyac. Applications of wireless sensor network in intelligent traffic system: A review. in 3rd international conference on electronics computer technology. *In 3rd International Conference on Electronics Computer Technology*, 5:53–57, 2011.

[11] Scalabrin M. Guglielmi A.V. Badia L adori, V. Jamming in underwater sensor networks as a bayesian zero-sum game with position uncertainty. 20015.

[12] A. Karygiannism J. Lopez Aikaterini Mitrokotsa and J. Zhou (Eds.). *Wireless Sensor Network Security.* All rights reserved, 2008.

[13] K. Akkarajitsakul, E. Hossain, D. Niyato, and D. I. Kim. Game theoretic approaches for multiple access in wireless networks: A survey. *IEEE Communications Surveys Tutorials*, 13(3):372–395, 2011.

[14] I. F Akyildiz and E. P. Stuntebeck. Wireless underground sensor networks: Research challenges. *Ad Hoc Networks*, (4(6)):669–686, 2006.

[15] Avrachenkov K. Garnaev A Altman, E. A jamming game in wireless networks with transmission cos. *Network Control and Optimization, Springer: Berlin, Germany, 2007*, pages 1–12, 2007.

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

[17] Rajeshwar Singh Anand Nayyar. A comprehensive review of simulation tools for wireless sensor networks (wsns). *Journal of Wireless Networking and Communications*, (5[1]):19–47, 2015.

[18] Dr.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 2014.

[19] Sushanta Karmakar Basant Subba, Santosh Biswas. A game theory based multi layered intrusion detection framework for wireless sensor networks. *International Journal of Wireless Information Networks*, 25:399–421, 2018.

[20] Kostas Berberidis and Dimitris Ampeliotis. Signal processing communication issues in sensor networks. *Computer Engineering and Informatics Department University of Patras*, 2009.

[21] 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.

[22] Ko C. Brutch, P. Challenges in intrusion detection for wireless ad-hoc networks. 2003.

[23] C. Leckie C. E. Loo, M. Y. Ng and M. Palaniswami. Intrusion detection for sensor networks. *International Journal of Distributed Sensor Networks*, 2005.

[24] J. Oller C. Gomez and J. Paradells. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors*, 12(9):11734–11753, 2012.

[25] M. Liu C.F. Hsin. A distributed monitoring mechanism for wireless sensor networks. 2006.

[26] Ouadjaoutb A. Laslab N. Bagaab M. Hadjidj A. Challala, Y. Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks. *Journal of Network and Computer Applications 34(4)*, (34(4)):1380–1397, 2011.

[27] Wood A D and Stankovic J A. Denial of service in sensor networks. *IEEE Computer*, pages 48–56, 2002.

[28] Han R. Mishra S Deng, J. Insens:intrusion-tolerant routing for wireless sensor network. *Computer Communications*, (29(2)):216–230, 2006.

[29] S. S. Doumit and D. P. Agrawal. Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks. 2003.

[30] J. Liu E. C. Ngai and M. R. Lyu. An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. *Computer Communications*, 30(11):2353–2364, 2007.

[31] Panaousis Emmanouil A and Christos Politi. A game theoretic approach for securing aodv in emergency mobile ad hoc networks. 2009.

[32] Khademzadeh A Estiri, M. A game-theoretical model for intrusion detection in wireless sensor networks. 2010.

[33] KUN WANG et .al. Game-theory-based active defense for intrusion detection in cyber-physical embedded systems. *ACM Transactions on Embedded Computing Systems*, 16(1), October 2016.

[34] N. Berlin et al. *Théorie des jeux : Introduction à la théorie des jeux répétés*. 2007.

[35] Sanghai Guan et al. Intrusion detection for wireless sensor networks: A multi-criteria game approach. *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2018.

[36] Auteur ; K.bouibed F. kacker. La théorie des jeux : Cours , exercices corrigés , sujets d'examens. `Alger;PagesBleues`, 2012. Bibliogr.

[37] Jelena Mi•si¶c Yang Xiao Fereshteh Amini, Vojislav B. Mi•si¶c. *Security in Distributed, Grid, Mobile, and Pervasive Computing", Auerbach Publications*. 2006.

[38] C. Gomez and J. Paradells. Wireless home automation networks: A survey of architectures and technologies. *IEEE Communications Magazine*, (48(6)):92–101, 2010.

[39] Md Arafat Habib and Sangman Moh. Game theory-based routing for wireless sensor networks: A comparative survey. *applied sciences*, 19 July 2019.

[40] Z Han. *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*. 2012.

[41] M. Hefeeda and M. Bagheri. Wireless sensor networks for early detection of forest fires. *In IEEE International Conference on Mobile Adhoc and Sensor Systems*, pages 1–6, 2007.

[42] J. Heidemann, Wei Ye, J. Wills, A. Syed, and Yuan Li. Research challenges and applications for underwater sensor networking. In *IEEE Wireless Communications and Networking Conference, 2006. WCNC 2006.*, volume 1, pages 228–235, 2006.

[43] Rachid Latif Noureddine. Idboufker Youssef. Elmourabit Hicham Zougagh, Ahmed Toumanari. A performance comparison of routing protocols for ad hoc networks. *I.J. of Engineering Research and Applications*, 4:124–131, September 2014.

[44] Mr SEDJELMACI Sid Ahmed Hichem. *MISE EN ŒUVRE DE MECANISMES DE SECURITE BASES SUR LES IDS POUR LES RESEAUX DE CAPTEURS SANS FIL*. PhD thesis, 2013.

[45] E. Stuntebeck I. Akyildiz. Wireless underground sensor networks: Research challenges. *Ad Hoc Networks*, (4(6)):669–686, 2006.

[46] T. Melodia I. F. Akyildiz and K. R. Chowdhury. A survey on wireless multimedia sensor networks. *Computer Networks*, 51(4):921–960, Mar 2007.

[47] Y. Sankarasubramaniam I. F. Akyildiz, W. Su and E. Cayirci. Wireless sensor networks: a survey. *Computer networks*, (38(4):393422, pages=8,10,14, year=2002,).

[48] F. C. Freiling I. Krontiris, T. Dimitriou. Towards intrusion detection in wireless sensor networks. 2007.

[49] I.Onat and A. Miri. An intrusion detection system for wireless sensor networks. 2005.

[50] 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 quarter 2014.

[51] Wilson. J. Sensor technology handbook. *Elsevier/Newnes: Burlington, MA, USA*, 2005.

[52] H.-W. Braun P. Bryant S. Gage T. Hansen P. Hanson C.-C. Lin F.-P. Lin T. Kratz et al J. Porter, P. Arzberger. Wireless sensor networks for ecology. *BioScience*, (55(7)):561–572, 2005.

[53] B. Mukherjee J. Yick and D. Ghosal. Wireless sensor network survey. *Comput. Netw*, 52(12):2292–2330, Aug2008.

[54] A. Mungur et al K. K. Khedo, R. Perseedoss. A wireless sensor network air pollution monitoring system. *arXiv preprint arXiv:1005.1737*, page 6, 2010.

[55] J. Li K. Su and H.Fu. Smart city and the applications. 2011.

[56] Holger Karl and Willig Andreas. *Protocols and architectures for wireless sensor networks*. 2005.

[57] F. Khedim. *Détection des attaques par réplication dans un réseau de capteurs sans fil*. PhD thesis, University, 2013.

[58] Benahmed Khelifa. *Surveillance Distribuée pour la sécurité d'un réseau de capteurs sans fils*. PhD thesis, 2011.

[59] Ashok Koujalagi. Considerable detection of black hole attack and analyzing its performance on aodv routing protocol in manet (mobile ad hoc network). *American Journal of Computer Science and Information Technology*, 6, 22/06 2018.

[60] Ioannis Krontiris, Tassos Dimitriou, Thanassis Giannetsos, and Marios Mpasoukos. Intrusion detection of sinkhole attacks in wireless sensor networks. In *Proceedings of the 3rd International Conference on Algorithmic Aspects of Wireless Sensor Networks*, page 150–161, Berlin, Heidelberg, 2008. Springer-Verlag.

[61] BOUCENNA Mohamed Lamine. *Coopération dans les réseaux ad hoc par application de la théorie des jeux.* PhD thesis, 2014.

[62] Ghinita G. Bertino E. Kantarcioglu M Lim, H.S. A game-theoretic approach for high-assurance of data trustworthiness in sensor networks. 2012.

[63] Govind Bhagwatikar Lipi Chhaya, Paawan Sharma and Adesh Kumar. Wireless sensor network based smart grid communications: Cyber attacks, intrusion detection system and topology contro. *Electronics*, pages 6–5, 2017.

[64] Y. Liu M. Li. Underground structure monitoring with wireless sensor networks. 2007.

[65] G. Dimic M. P. Durisic, Z. Tafa and V. Milutinovic. A survey of military applications of wireless sensor networks. 2012.

[66] M.A. Matin. Wireless sensor networks technology and protocols. *Janeeza Tradine 9.51000 Rijeka, Croatia*, 2012.

[67] Maha Elsabrouty Osamu Muta Hiroshi Furukawa Mohamed S. Abdalzaher, Karim Seddik and Adel Abdel-Rahman. Game theory meets wireless sensor networks security requirements and threats mitigation: A survey. *Sensors*, 29 June 2016.

[68] 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.

[69] Olesia MOKRENKO. *Energy management of a Wireless Sensor Network at application level.* PhD thesis, 2015.

[70] Byun S.S. Balasingham I Moussavinik, H. On the steady state in multiuser multiband ir-uwb without nbi detection. *In Proceedings of the 6th International Symposium on Wireless Communication Systems (ISWCS), Siena, Italy*, pages 522–525, 7–10 September 2009.

[71] L. Girod N. Bulusu, D. Estrin and J. Heidemann. Scalable coordination for wireless sensor networks: Self-configuring localization systems. 2001.

[72] C. C. De Wit N. C. De Castro and K. H. Johansson. On energy-aware communication and control co-design in wireless networked control systems. *In 2nd IFAC Workshop on Distributed Estimation and Control in Networked Systems*, pages 49–54, 2010.

[73] 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.

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

[75] Mrs LABRAOUI Nabila. *LA SÉCURITÉ DANS LES RÉSEAUX SANS FIL AD HOC*. PhD thesis, University, 2012.

[76] Gupta A Nayyar, A. A comprehensive review of cluster-based energy efficient routing protocols in wireless sensor networks. *IJRCCT*, 42(3[1]):104–110, 2014.

[77] Sharma S Nayyar, A. A survey on coverage and connectivity issues surrounding wireless sensor network. *IJRCC*, (3[1]):111–118, 2014.

[78] Raghav Yadav Nidhi Tiwari. Detection of black hole attack using control packets in aodv protocol for manet. *International Journal of Computer Applications*, 118:23–29, 05 2015.

[79] S.D.T. Kelly N.K. Suryadevara, S.C. Mukhopadhyay and S.P.S. Gill. Wsnbased. smart sensors and actuator for power management in intelligent buildings. *IEEE/ASME Transactions on Mechatronics*, (20(2)):564–571, 2015.

[80] Ozgur Koray SAHINGOZ Okan CAN. A survey of intrusion detection systems in wireless sensor network. *IEEE*, 2015.

[81] Rubinstein A Osborne, M.J. *A Course in Game Theory.* MIT Press: Cambridge, 1994.

[82] Rubinstein A Osborne, M.J. *A Course in Game Theory.* MIT, 1994.

[83] Madjid Ouharoun. *Modelisation de detection d'intrusion par des jeux probabilistes.* PhD thesis, 2010.

[84] G. Macia-Fernandez P. Garcia-Teodoro, J. Diaz-Verdejo and E. Vazquez. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Elsevier J. Computers and Security*, 28(1-2):18–28, 2009.

[85] K. P. Safeer-T. M. Kotresh D. T. Shakunthala P. Gopal P. S. Pandian, K. Mohanavelu and V. C. Padaki. Smart vest: Wearable multi-parameter remote physiological monitoring system. *Medical engineering physics*, (30(4)):466–477, 2008.

[86] C. Perkins and E. Royer. Ad-hoc on-demand distance vector routing. 1997.

[87] Hakima Chaouchi Jean Marie Bonnin Priyanka Rawat, Kamal Deep Singh. Wireless sensor networks: A survey on recent developments and potential synergies. *The Journal of Supercomputing*, pages 1–48, April 2014.

[88] Hakima Chaouchi Jean Marie Bonnin Priyanka Rawat, Kamal Deep Singh. Wireless sensor networks: recent developments and potential synergies. *The Journal of Supercomputing*, April2013.

[89] G. Loriga R. Paradiso and N. Taccini. A wearable health care system based on knitted integrated sensors. *IEEE Transactions on Information Technology in Biomedicine*, (9(3)):337–344, 2005.

[90] R. Rahul. Swarm robotics: a developing field. `ieeesbcet.org/swarm-robotics-adeveloping-field`, 2013.

[91] Srivathsan S Reddy, Y.B. Game theory model for selective forward attacks in wireless sensor networks. 2009.

[92] Ellis C. Shiva S. Dasgupta D. Shandilya V. Wu Q Roy, S. A survey of game theory as applied to network security. 5–8 January 2010.

[93] A.-S. K. Pathan S. Khan and N. A. Alrajeh. *Wireless Sensor Networks: Current Status and Future Trends.* 2012.

[94] S. Ouadah S. Maarouf. Implémentation et évaluation des schémas de routage sur une plateforme réelle de réseau de capteur sans fil. Master's thesis, University, 2014.

[95] A.M.; El-Hag A.H.; Salama M.M.A Sallabi, F.M.; Gaouda. Evaluation of zigbee wireless sensor networks under high power disturbances. *IEEE Trans. Power Deliv*, 2011.

[96] Phoha Vir V. Serwadda Abdul Selmic, Rastko R. Wireless sensor networks. *Springer International Published*, 2016.

[97] Jaydip Sen. *Security in Wireless Sensor Networks*, pages 407–460. 11 2012.

[98] Ricardo Severino. An introduction to wireless sensor networks. *CISTER Summer Internship*, pages 227–232, 2017.

[99] L.S Shapley. Stochastic games. *Proc. Natl. Acad. Sci. USA*, (39(10)):1095–1100, 1953.

[100] Andreas Strikos. A full approach for intrusion detection in wireless sensor networks. 04 2007.

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

[102] S. Shankar Sastry Tanya Roosta, Shiuhpyng Winston Shieh. Taxonomy of security attacks in sensor networks and countermeasures. 2006.

[103] Dr. Labib TERRISSA. Réseaux de capteurs sans fil (wsn). course : « Futur Networks », Biskra University , 2015/2016.

[104] P. Lukowicz G. Troster F. Dolveck M. Baer F. Keita E. B. Schenker F. Catarsi L. Coluccini A. Belardinelli D. Shklarski M. Alon E. Hirt R. Schmid U. Anliker, J. A. Ward and M. Vuskovic. Amon: a wearable multiparameter medical monitoring and alert system. *IEEE Transactions on Information Technology in Biomedicine*, (8(4)):415–427, 2004.

[105] A. Gupta V. Bhuse. Anomaly intrusion detection in wireless sensor networks source. *Journal of High Speed Networks*, 15(1):33–51, January 2006.

[106] C. Poellabauer W. Dargie. Fundamentals of wireless sensor networks theory and practice, 2010.

[107] Wu Y. Liu K.R Wang, B. Game theory for cognitive radio networks: An overview. *Comput. Netw*, (54):2537–2561, 2010.

[108] Li Q. Chen T. Cheng E. Dai H Xiao, L. Jamming games in underwater sensor networks with reinforcement learning. *In Proceedings of the Global Communications Conference (GLOBECOM), San Diego, CA, USA*, pages 1–6, 6-10 December 2015.

[109] Maleh Yassine and Abdellah Ezzati. A review of security attacks and intrusion detection schemes in wireless sensor network. *International Journal of Wireless Mobile Networks*, 5, 01 2014.

[110] Mukherjee B Ghosal D Yick, J. Wireless sensor network survey. *Computer networks*, pages 2292–2330, 2008.

[111] Garhan Attebury Yong Wang and Byrav Ramamurthy. A survey of securituy issues in wireless sensor networks. *IEEE Communications Surveys Tutorials*, 2nd Quarter 2006.

[112] Z. Yanchao Z. Yun, F. Yuguang. *Securing wireless sensor networks: a survey*, volume 10. IEEE Communications Surveys and tutorials, 2008.