N°d'ordre: .....

People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
University Djillali Liabes of Sidi Bel Abbes
Exact Sciences Faculty
Computer Science Department
EEDIS Laboratory

Doctorate Thesis
Sciences

Field : Computer science
Specialty : Computer Systems Networks

By

Mrs AISSAOUI Sihem

Security in Wireless Networks

Defense on 10-02-2022 in front of the jury :

Pr.	ADJOUDJ Réda	UDL-SBA	Jury chairman
Pr.	KESKES Nabil	ESI-SBA	Jury member
Pr.	BOUCHIHA Djelloul	University Center of Naama	Jury member
Pr.	BOUKLI-HACENE Sofiane	UDL-SBA	Thesis supervisor

Academic Year : 2021 - 2022

Acknowledgement

I am truly indebted to my supervisor, Pr. BOUKLI-HACENE Sofiane, for giving me the opportunity to work with him, for his guidance, support in crucial moments, and constant encouragement during these years. I am grateful to Pr ADJOUDJ R., Pr KESKES N. and Pr BOUCHIHA D. for serving in my committee; and for their precious time and invaluable suggestions.

Words are not enough to express deepest gratitude to my parents, my husband, my sisters, my aunt for their relentless support, encouragement and supplications throughout my life.

In the end, the ultimate reality is that this would not be possible without the Will of ALLAH. I pray to ALLAH to pave our way to ultimate knowledge and help us use it for the real benefit of mankind.

Dedication

I dedicate this modest work to:

My dearest parents for all their sacrifices and thanks to you I've lacked nothing, "MAY GOD BLESS YOU WITH GOOD HEALTH AND LONG LIFE"

My Husband, I would not find enough courage to finish my thesis without your moral support, " THANK YOU "

My lovely children Abdelillah, Nada and Lilya, " I LOVE YOU "

My sisters Hanane, Ikram and Imène, my dear only brother Mohamed Hachem and my dear nephews Mehdi and Younes.

My dear aunt Djemaa and my dear uncle Ali.

Finally to my family AISSAOUI and my step family BEGHDADI.

Contents

List of Figures

List of Tables

Introduction

The communication patterns in Wireless networks use Radio Waves to transmit and receive data between nodes rather than wires. Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. However, the broadcast nature of radio propagation in wireless communications yields the wireless air interface open and accessible to both authorized and illegitimate users.

This completely differs from a wired network, where communicating devices are physically connected through cables and a node without direct association unable to access the network for illicit activities. The open communication environment makes wireless transmissions more vulnerable than wired communications to malicious attacks, including both the passive eavesdropping for data interception and the active jamming for disrupting legitimate transmissions (Zou *et al.* 2016).

The security requirements of wireless networks are specified for the sake of protecting the wireless transmissions against wireless attacks, such as eavesdropping attack, DoS attack, data falsification attack, node compromise attack, and so on (Chen *et al.* 2021). In this thesis we will be interested in security issues in a particular type of wireless networks which are Wireless Sensor Networks.

Wireless Sensor Networks (WSNs) (Akyildiz *et al.* 2002) are an advanced wireless networks with lightweight platforms called sensors or motes, deployed arbitrarily in hostile environment with limited computing power, limited energy reserve and unreliable wireless transmission medium. Under these restricted conditions, sensor nodes can easily be physically captured by the adversaries and be an easy target of a variety of attacks that causes Denial of Service (DoS) and affects the network's lifetime. Thus defending these networks from security attacks has become a great challenge for the researchers (Ring *et al.* 2019) (Gnanapriya & Ramya 2020) (Gavel *et al.* 2021) (Waoo & Tiwari 2021).

The layered architecture of WSN is divided into five layers, which are physical layer, data link layer, network layer, transport layer and application layer. The most destructive attacks are those of the network layer as they disrupt the entire functionality of the network, especially routing procedure that further causes denial of service (DoS) attack in the network. Some of the DOS network layer attacks or DOS routing attacks are

blackhole attack, wormhole attack, selective forwarding, Sinkhole attack, etc.

In Sinkhole attack, the malicious node tries to attract network traffic to itself by advertising a fake routing information about its high link quality. After routing table update, the victim nodes send data to the attacker node rather than sending it to the node it was formerly using, the attacker node become thus a sinkhole. The sinkhole attack can be used as a springboard to perform more severe attacks, namely Selective Forwarding attack, Wormhole attack, Flooding attack, Sybil attack and Black hole (Anand & Vasuki 2021) (Zawaideh & Salamah 2019) (Raghav *et al.* 2020) (Hasan *et al.* 2021).

Cryptography, Key management, data aggregation, secure routing, intrusion detection are the most studied solutions related to the security threats (Iqbal & Shafi 2019) (Gunathilake *et al.* 2020) (Albakri *et al.* 2019) (Thahniyath & Jayaprasad 2020) (Saeedi & Al-Qurabat 2021). However, most of the security techniques, including Intrusion Detection Systems, devised for traditional wired/wireless networks are not directly applicable to a WSN environment due to the restricted operating conditions of WSNs. Designing an effective and efficient intrusion detection technique that is applicable to WSNs is a very big challenge, which motivated us to work on this research area.

The Intrusion Detection System (IDS) (Anderson 1980), as its name implies, is to detect any suspicious activity occurring in the network by analyzing information collected from the network or a host, in order to effectively protect the privacy and property safety. IDS have several applications in WSNs; security routing is one of them.

Motivation and objective of the work

Many detection techniques for IDSs in WSNs have been proposed in the last decade. Designing an efficient IDS that ensure a trade-off between high detection rate and energy saving is the big challenge. The first objective of our work is to discuss about Sinkhole attack, its vulnerabilities and different Sinkhole attack detection techniques. Then, to propose a new detection scheme for Sinkhole attack detection based on SVM machine learning technique. Finally, to evaluate the designed systems with respect to common metrics (detection accuracy, energy saving).

Contributions

The contributions we have made aligned to our research goals can be summarized as follows:

1. The first task of any research is to conduct an extensive literature review, which led us to the preparation of this survey as the first outcome of our research.

2. We propose a new detection technique for Sinkhole attack detection based SVM. SVM is a supervised classification method which requires a labeled dataset for training and test. In the present work, the dataset generated in (Garofalo *et al.* 2013) is used to train and test our different SVM classifiers on four kernel functions (linear, polynomial, radial basis function and sigmoid). The obtained classification model based SVM is used in the different experimentations, on NS3 simulation tool, to investigate AODV protocol data for detecting suspect behavior of a node in network. Our proposed technique uses only two extracted features (HopCount and Destination Sequence Number) from AODV packets for detecting sinkhole nodes, with no computational parameters or additional messages. The results show that our system is able to detect attack with 100% accuracy and energy saving.

3. HIDS vs. NIDS. The IDSs running on the network can be divided into two categories: 1) HIDSs that autonomously decide about neighboring sensor nodes based only on own observations; and 2) NIDS that monitors all sensor nodes and decides based on the hole traffic. We show the difference in results of the two IDS architecture on our proposed detection techniques.

Organization of the thesis

The organization of the thesis is as follows.

- Chapter 1 *"Introduction to Wireless Sensor networks"*, presents a detailed introduction to Wireless Sensor Networks.
- Chapter 2 *"Security in Wireless Sensor Networks"*, discusses security challenges and requirements in WSNs, describes various types of attacks especially DOS Routing attacks and highlights known security approaches of detection and defensive mechanisms in WSNs.
- Chapter 3 *"Intrusion Detection in Wireless Sensors Networks"*, outlines the requirements that an IDS for sensor networks should satisfy, gives a detailed review on the existing schemes of intrusion detection in WSN and discusses future research directions on IDS in WSN.
- Chapter 4 *"Review of Related Works"*, reviews related work on Sinkhole attack detection and highlights open challenges in dealing with such attack.
- Chapter 5 *"Contribution"*, proposes a new technique for Sinkhole attack detection in WSNs based Support Vector Machines (SVM) and discusses the obtained results.
- *"General Conclusion"* gives the conclusion to this thesis, summarizing our contribution and suggesting directions for possible future work.

Introduction to Wireless Sensor Networks

1

Contents

The integration of sensors into everyday objects is in full development. Our daily live are being transformed, enriched with applications that were previously unthinkable. Wireless sensor networks (WSNs) are part of the technological revolution in measuring instruments, stemming from the convergence of wireless communication systems and miniaturized electronic systems.

WSNs are widely used in many areas and have become a cheap and viable solution for a variety of applications, especially in wildlife habitat monitoring, industrial quality control, disaster recovery situations, military command applications and much more.

In this chapter, we are interested in the presentation of Wireless Sensor Networks where we describe their functioning, architectures, constraints and characteristics as well as the used communication models.

1.1 Wireless Sensor Networks

Wireless sensor networks are spontaneous networks consisting of tens to several hundreds and sometimes thou-sands of nodes called sensors or motes. These nodes are dispersed in an environment called a collector field in order to perform autonomously three complementary tasks: to collect data (generally measurements of temperature, humidity, vibrations, radiation, etc.), to process them and finally to transmit theses data to the base station via a radio circuit. The following figure illustrates a WSN architecture.

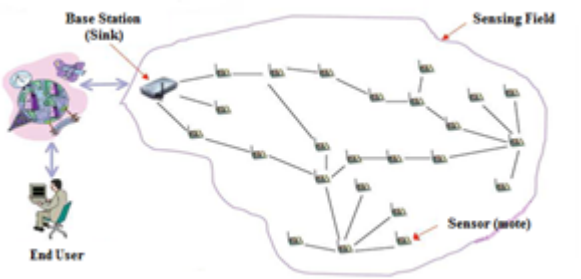

Figure 1.1 – *Example of WSN*

The base station or sink is a specific node responsible for receiving, storing and processing data from the sensor nodes and then transmitting them by internet or satellite to end users for analysis and decision-making.

1.2 Components of a wireless sensor node

Sensor node is a very tiny device that has the ability to sense its immediate environment (temperature, humidity, pressure, presence, etc.). The collected data are sent to a base station or other sensor via wireless radio communication and transformed into measures that can be used by end users. These tiny devices are illustrated in Figure 1.2.

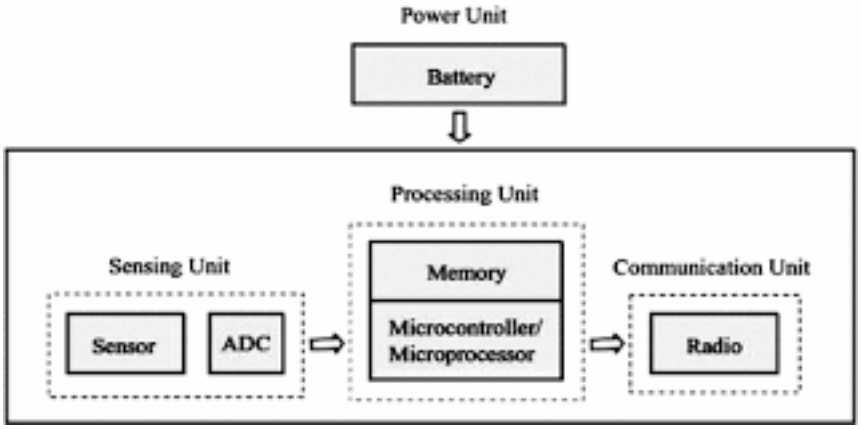

Figure 1.2 – *Components of a wireless sensor node*

1.2.1 Sensing Unit

Sensing unit is usually composed of two subunits: sensors and an ADC (Analogue to Digital Converter) (Akyildiz *et al.* 2002). Sensors measure physical data of the parameter to be monitored and have specific characteristics, such as accuracy, sensitivity etc. The analogue signals produced by the sensors are digitized by the ADC and then fed into the processing unit.

1.2.2 Processing Unit

The processing unit is usually a microprocessor or a microcontroller, most frequently programmed in C and generally associated with a small storage unit (Memory), can perform an intelligent data processing and control the functionality of other components in the sensor node to carry out the assigned sensing tasks.

1.2.3 Communication Unit

This Unit is in charge of transmitting and receiving the data produced by the processing unit, thus giving the sensors the ability to communicate with the other components of the network. The communication is carried out via a wireless medium which can be of optical, ultrasonic or radio-frequency type.

1.2.4 Power Unit

Power is stored either in small batteries or capacitors. Batteries, both rechargeable and non-rechargeable, are used to power the entire system. Due to their small size, energy is quite limited which directly affects the lifetime of the sensors and therefore of the entire network.

Changing the energy source of sensor node is not an applicable solution. So, the current sensors are able to renew their energy from solar sources, Radio Frequency(RF), temperature differences, or vibration.

The sensors can also have application dependent additional components, such as a location finding system, a power generator and a mobilizer.

1.3 WSN Topologies

Since a wireless sensor network may consist of tens, hundreds or thousands of devices, network topologies must be considered in its design. Structure of a Wireless Sensor Network includes different topologies for radio communications networks like the ones given below.

1.3.1 Star Topology

A Star topology is a Single-hop network architecture in which all wireless sensor nodes communicate bidirectionally with a base station (sink). Nodes do not transmit data or commands to each other, directly. They use the base station as a coordination point where all data fl ow is concentrated. This allows low-latency communications between the remote node and the sink. Addition of further nodes is easy and can be done without interrupting network operation. The star topology is the lowest in overall power consumption but for long distance transmission, the energy consumption for communication will be a Mesh topology (see Figure 1.4).

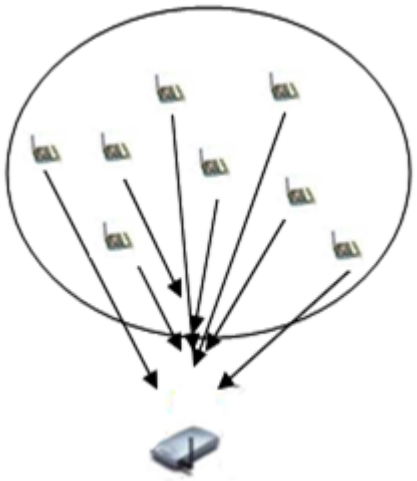

Figure 1.3 – *A Star network topology*

1.3.2 Mesh Topology

A Mesh topology is a Multi-hop network architecture where each sensor node is connected to all the nodes within its radio transmission range. The data is transmitted through one or more intermediate node. This network topology can be highly fault tolerant, because when an individual node fails, a remote node still can communicate to any other node in its range to forward the message to the desired location. For power consumption, the nodes that implement the multi-hop communications are generally higher than for the nodes that don't have this capability. Multi-hop nodes are always waked up, because they can be part of the path between any other

node and the base station. In Addition, as the number of communication hops to a destination increases, the time to deliver the message also increases. The multi-hop system allows for a much longer range than a star topology.

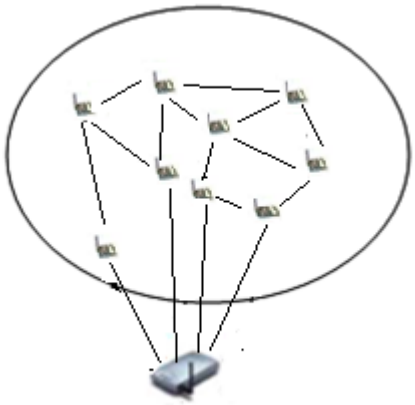

Figure 1.4 – *A Mesh network topology*

A Mesh topology can be implemented in two ways : Flat network architecture or Hierarchical network architecture. In flat architecture, the network is consisting of homogeneous sensor nodes of the same capabilities and functionalities. In such networks, the sink node generally send a query message to the sensor node which respond sink in multi-hop basis.

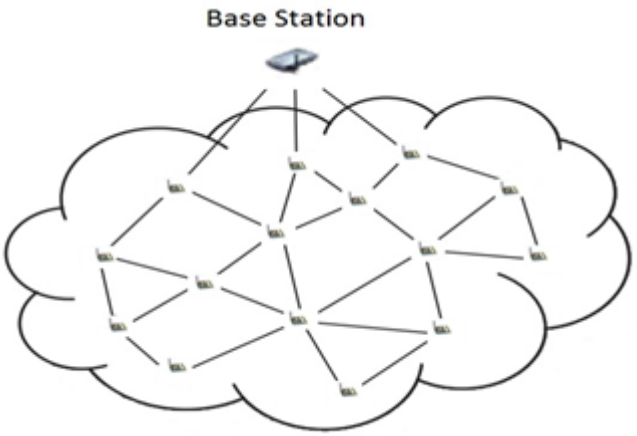

Figure 1.5 – *Flat network architecture*

On the other hand, In hierarchical architecture (or cluster-based architecture), the network is divided into clusters in which heterogeneous sensor nodes are deployed. In each cluster, there is a cluster head and cluster members. The cluster head has as role to collect data from all the sensors in its cluster and transmits them to the sink. The cluster head can be connected with the sink either directly or through other cluster heads in multi-hop way.

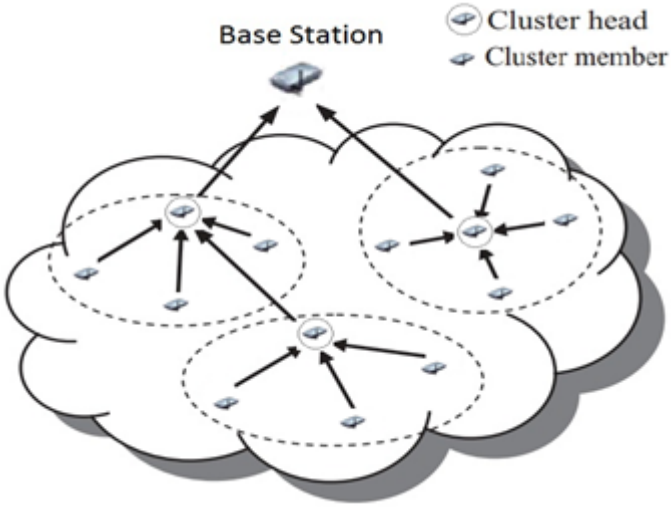

Figure 1.6 – *Hierarchical network architecture*

1.3.3 Hybrid Topology

Generally, in large networks, consisting of hundreds, even thousands of nodes, a hybrid combination of the star and mesh topologies is used to take advantages of the star topology in keeping the wireless sensor nodes power consumption to a minimum, where just the nodes with the multi-hop capability are enabled to forward messages from the low power nodes to other nodes on the network, as well as the fault tolerance and the extended range, the advantages of a mesh network topology.

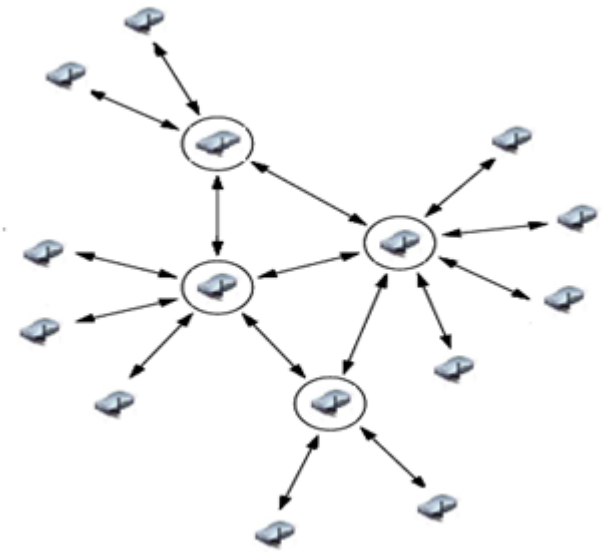

Figure 1.7 – *Hybrid Star-Mesh network architecture*

A detailed study on network topologies in Wireless Sensor Networks is given in (Sharma *et al.* 2013).

A comparison between the performances of the topologies of Wireless Sensor Network in terms of path, node failure, radio rang, energy consumption and network life time is shown in Table 1.1.

Topology	Path	Node Failure	Power Usage	Communication Range	Network Life Time
Star	Single	More	High	Short	Less
Mesh	Multiple	Less	Low	Long	More
Hybrid	Multiple	Less	Low	Long	More

Table 1.1 – *Network topologies*

1.4 Types of Sensor Networks

WSNs may deploy numerous types of sensors, depending on requirements of the application, like seismic, magnetic, thermal, visual, infrared, radar, acoustic and so on. Sensor nodes can be classified according to several criteria: environment, Mobility, nodes capacities, data communication modes and collected data.

1.4.1 Environment

Terrestrial WSNs

Terrestrial WSNs (Yick *et al.* 2008) are made up of hundreds and sometimes thousands of sensor nodes, able to communicate efficaciously data to the base station, distributed randomly or in prefixed manner in sensing field. In this WSN, The energy-constrained sensor nodes can have a secondary source energy as solar cells and the power conservation can be achieved by using low duty cycle operations, minimizing delays, and optimal routing, and so on.

Underground WSNs

Underground WSNs (Akyildiz & and 2006; Li & and 2007) comprise several entombed nodes to monitor underground situations. An aboveground sink nodes are used to communicate data from the buried sensor nodes to the base station. Due to the underground conditions as soil, rocks, water and other mineral contents and contrary to Terrestrial WSNs, the underground WSN are more expensive in terms of deployment, maintenance, and equipment cost considerations. However the two networks are similar in term of energy constraints where sensor nodes have a limited source power and in order to conserve it, an efficient communication protocols have to be implemented.

Underwater WSNs

Underwater WSNs (Akyildiz *et al.* 2004; Heidemann *et al.* 2006) are composed of several sensor nodes and vehicles deployed under-water. The used vehicles serve to gather data and to transmit them to the base station. The big communication challenges in underwater WSN Sensor are failure, bandwidth and long propagation delay. As all the WSNs, the sensor nodes are equipped with a limited battery that cannot be recharged or replaced. Developing efficient underwater communication and networking techniques involves energy conservation issue for underwater WSNs.

1.4.2 Mobility

Static WSNs

In static sensor networks, the sensor nodes and the base station are stationary; they keep their initial positions throughout their life time. This type of network is characterized by a static topology, easy localization of the nodes in the network and simple routing techniques.

Mobile WSNs

In Mobile WSNs(Yick *et al.* 2008), sensors and / or the base station have the ability to move and organize themselves in the network . The mobility of the sensor occurs either when the sensor is glued to a mobile object, or when the sensor self-moves (in the case of a sensor equipped with a motor). Mobile sensor networks are intended much more for tracking applications where mobility is indispensable and is also advantageous in investment cost instead of deploying multiple static nodes, a minimal number of mobile devices is sufficient. However, when mobility is too frequent, the change in topology complicates the routing and location mechanisms.

1.4.3 Nodes Capacities

Homogeneous WSNs

In a homogeneous sensor network, all the nodes of the network have the same energy, computation and storage capacities (Limited resources and short live-time). This is the type often found in the majority of sensor network applications, because they address the need for autonomy.

Heterogeneous WSNs

Whereas, in a heterogeneous sensor network there are some sophisticated nodes which have more processing and communication capacity than normal nodes. This improves energy efficiency and extends the life of the network. The advantage of such network is that it can be used to carry out more complex tasks such co-computers, cluster heads, etc. The disadvantage is that is difficult to position these nodes randomly. In addition, the cost of these nodes is high.

1.4.4 Data communication modes

Event-driven

In the event-driven mode, sensors report the sensing data to the sink once a specified event (e.g., fire) has been detected. Target or event detection and tracking is a typical example of applications in event-driven reporting. Its purpose is to detect, classify, and locate specific targets or events, as well as track the targets or events over a specified region. Once there is an event or a target emerging in the area, the sensor nodes around the target or event gather the required information and report back to the sink.

Time-driven

In the periodic reporting (or time-driven) mode, sensor nodes gather information from the environment at predetermined times and periodically send the data to the sink.

Query-driven

In the on-demand (or query-driven) mode, users decide when to gather data. They send instructions to the WSN indicating that they wish to receive data and then wait for the required type of data to be sent in the requested format. Users may even specify the future reporting periods; subsequent reports would then be sent in periodic reporting mode.

1.4.5 Collected Data

Scalar-based sensor network

Scalar-based sensor network or Wireless Sensor Networks, can be defined as a self-configured and infrastructure-less wireless networks to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location or sink.

Multimedia-based sensor networks

Multimedia-based sensor networks or Wireless Multimedia Sensor Network (WMSN) is a distributed wireless system that interacts with the physical environment by monitoring it through embedded devices equipped with audio and visual information collection modules. The embedded devices has as role retrieving video and audio streams, still images, and scalar sensor data from their region. In addition to the ability to retrieve multimedia data, WMSNs are able to store, process in real-time, correlate, and fuse multimedia data originated from heterogeneous sources.

Multimodal-based sensor networks

Multimodal Sensor networks (M2WSNs) are special WSNs in which Sensor Nodes can perform two data communication modes. First, a time-driven data-reporting mode for periodic monitoring situations in a target environment. Second, an event-driven reporting mode for keeping track of critical events upon their occurrence, with the aim of energy consumption reduction in sensor nodes (Aranda† *et al.* 2020).

In the next section, we will present different fields of application of WSNs which require the use of the various types of sensors exposed in the section above.

1.5 Applications of wireless sensor network

Due to their flexibility in solving problems in different application domains and having the potential to change daily lives in many different ways, the Wireless Sensor Networks (WSNs) have become an emerging technology with a wide range of potential applications. Theoretically speaking, the possible applications of Wireless Sensor Networks are unlimited. WSNs are mostly used in, low bandwidth and delay tolerant, applications ranging from civil (Qurishee *et al.* 2020) (Salehi *et al.* 2021) and military (Lim *et al.* 2010) (Naz *et al.* 2012)(Usha & Muzzammil 2020) to environmental (Muduli *et al.* 2018) (Tripathy *et al.* 2021) and healthcare monitoring (Kakria *et al.* 2015), (Kashyap 2020) and in other commercial areas (Baldovino *et al.* 2018) (Zeng *et al.* 2021). Despite their powerful capabilities, the successful development of WSN is still a challenging task. The figure 1.8 shows the categories of WSN applications.

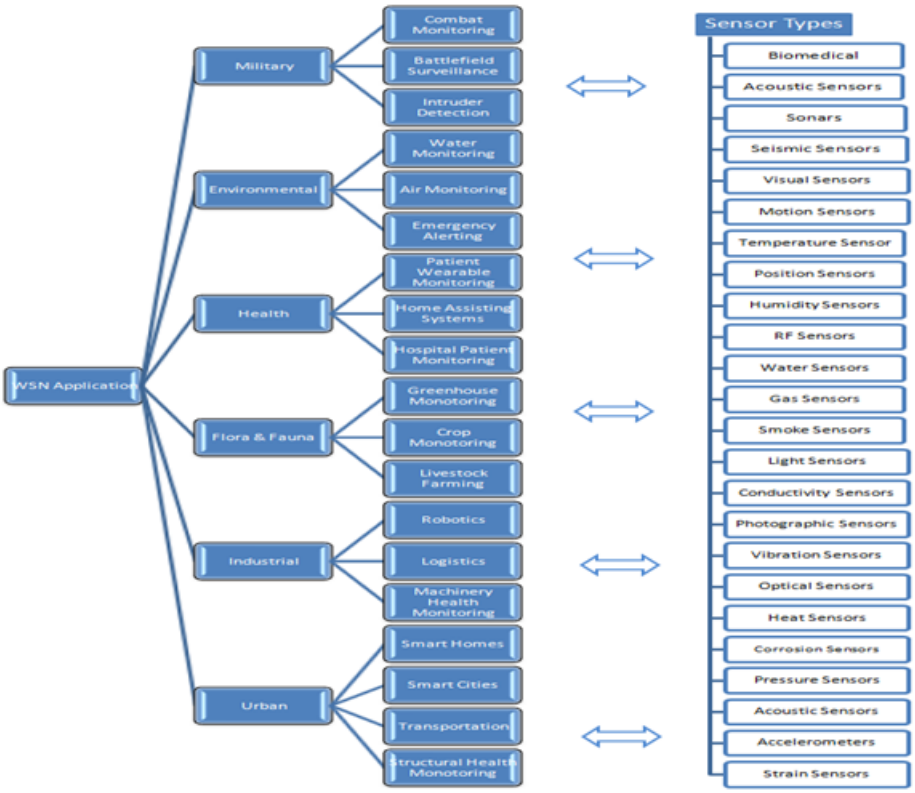

Figure 1.8 – *WSN Applications and different used Sensor types*

For more details on recent applications of WSN, (Kandris *et al.* 2020) provide an up-to-date presentation of both traditional and most recent applications of Wireless Sensor Networks. The main categories of applications of WSNs are identified, and characteristic examples of them are studied. Their particular characteristics are explained, while their pros and cons are denoted.

Required specifications of Wireless Sensor Networks (WSNs) per type of application are synoptically presented in Table 1.2 (Kandris *et al.* 2020).

Type of Application		Required Specifications						
		Node Weight and Dimensions	**Node Robustness**	**Communication Range**	**Communication Throughput**	**Communication Reliability**	**Communication Security**	**Network Tolerance**
Military		Application dependent	Very High	Wide	Very High	Very High	Very High	Very High
Health		Small	High	Small	Very High	Very High	High	High
Flora and Fauna		Application dependent	High	Wide	Medium	Medium	Low	High
Environmental		Of minor importance	Very High	Wide	Very High	High	High	Very High
Industrial		Application dependent	Very High	Application dependent	Very High	Very High	High	Very High
Urban	**Indoor**	Small	Medium	Small	Medium	Very High	Very High	High
	Outdoor	Of minor importance	Very High	Wide	Very High	Very High	Very High	Very High

Table 1.2 – *Required specifications of WSNs per type of application (Kandris et al. 2020).*

1.6 Unique Properties of WSN

The properties of WSN are illustrated below (Sandhu *et al.* 2018):

- Tree-Structured Routing: It is the basis of most current sensor networks. In such networks, the sink node or the base station is at the root. This forms a hierarchical arrangement of sensor nodes.
- Agglomeration: It is used not only to monitor conditions across the wide area of coverage, but also to compensate for unreliability, miscalibration of sensor devices, and intermittent connectivity.
- Tolerable Failures: Sensors are low-cost devices, and the loss or corruption of a sensor can either be mitigated by redundant sensors or be tolerated by the network. The redundancy of sensors and tolerance for a limited quantity of malicious data makes individual sensor nodes less critical and further enhances the ability to cope up with node failure.
- In-Network Filtering and Computation: It allows agglomeration and computation to be "pushed" as close as possible to the devices that originate specific sensor readings. This thus enables greater efficiency as fewer data packets must be transmitted.
- Sensors as Routers: There is no distinction between the sensing nodes, computing nodes, and the routing nodes. This, combined with the above properties, reduces network traffic significantly.
- Phased Transmission Periods: Within a sensor network, each node has a phase in which it senses, a phase in which it receives messages from its subordinate nodes and a phase in which it forwards data to its parent. Thus, the radio link can be kept active for this duration of time.

1.7 Communication architectures of WSNs

Communication architecture of WSNs is broadly categorized as layered architecture, cross-layer architecture, and unified layered architecture.

1.7.1 Layered architecture

The layered communication architecture is also known as the Open Systems Interconnection (OSI) model. Most common architecture of WSNs follows the OSI model. In layered communication architecture, both sink and source nodes transmit the data. The communication architecture consists of five layers: application layer, transport layer, network layer, data link layer, and physical layer; and three cross-planes: power management plane, mobility management plane, and task management plane (see figure 1.9.

- Physical layer: The physical layer provides the interface to transmit a stream of bits over the physical channel. The main task is frequency

selection, carrier frequency generation, signal detection, Modulation and data encryption. The standard IEEE 802.15.4 is proposed as standard for low rate personal area and WSN with low cost, complexity, power consumption, range of communication to maximize battery life.

- Data link layer: Responsible for Channel access policies, scheduling, buffer management and error control. In WSN we need a MAC protocol to consider energy efficiency, reliability, low access delay and high throughput as a major priorities.
- Network layer: The major function of this layer is routing. In WSNs, this layer has a lot of challenges depending on the application but apparently, the major challenges are in the power saving. To save power, this layer follows various routing mechanisms, such as minimum energy route, minimum hop route, maximum power available route, and maximum–minimum power available route. It is also responsible to connect the external network.
- Transport layer: Since WSN is application-specific network and different applications can have different needs, the transport layer should be application specific. The designing of the transport layer protocol is a challenging task because of inherent constraints like limited power and memory.
- Application layer: This layer provides the management level functionality as per the requirement of user and application. Responsible for traffic management and provide software for different applications that translate the data in an understandable form or send queries to obtain certain information. Sensor networks deployed in various applications in different fields, for example, military, medical, environment, agriculture fields

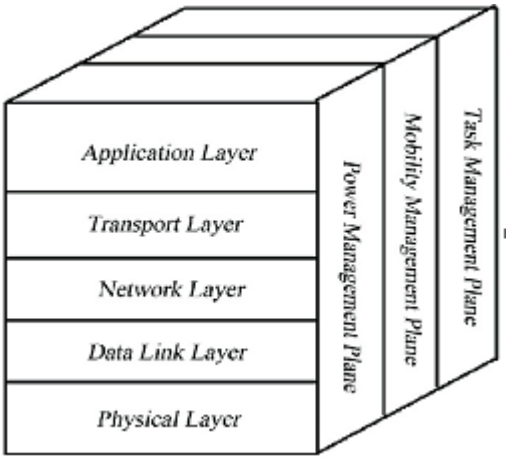

Figure 1.9 – *Layered communication architecture in WSNs*

The three cross planes or layers are used to manage the network and make the sensors work together in order to increase the overall efficiency of the network.

- Power management plane: deals with the power consumption of the node.
- Mobility management plane: detects the movement of node and maintains the information of neighboring nodes
- Task management plane: is used to schedule the sensing task in the given area. It determines which nodes are off and which ones are on.

1.7.2 Cross layered communication architecture

In the layered architecture all the protocol is proposed for a single layer and each layer cannot communicate directly with the non-adjacent layer. And this characteristic is opposite to energy limitation, node mobility, and the dynamic nature of wireless sensor networks. By violating the rules, the designer can give solutions for direct communication between non-adjacent layers using shared variables. Such violation of traditional architecture is Cross Layer Design (CLD). The basic idea of a CL is to use the close interaction between different layers for improving the performance of the entire network. For many domains, this technique has been widely used (see figure 1.10.

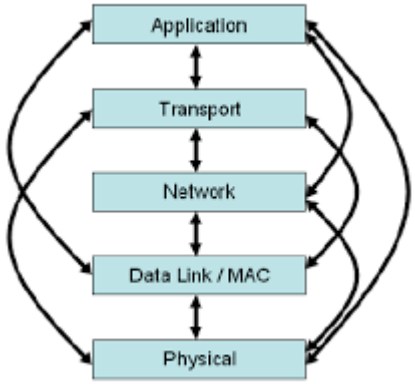

Figure 1.10 – *Cross layered communication architecture in WSNs*

Need of CLD Approach in WSN

Cross-layered approach is used to minimize the transfer overhead, caused by the traditional layered approach, by having data and information shared among different layers. The development of various protocols and services are optimized and improved as a whole system. Some of the parameters which can be optimized by CLD are (Ranjan & Varma 2016) (Sah & Amgoth 2018):

1. Throughput Many cross-layer approaches are introduced to maximize the network throughput [5–7]. The "many-to-one" communication pattern in WSN which consist of routing all the sensed data to the Base Station, called Sink node, causes high congestion in a large scale network. The relay-traffic close to the sink node is very high, and the area is heavily loaded, which causes significant collisions and packets lost.

2. QoS The main issue to achieve desirable QoS in WSNs is due to resource constrains (like energy, bandwidth, etc.), data redundancy, node heterogeneity, distributed network and topology of the network which also affects the QoS. In addition, the applicability of WSNs in nowadays are widely in real time application which seeks restrict QoS to provide desired latency, reliability, energy consumption, throughput and fairness etc. (Rani *et al.* 2020)

3. Network Lifetime Cross-layer is a technique for minimizing energy consumption by many ways as it reduces message passing overhead and increase data availability to all layer. Literature (Chen *et al.* 2017) (Singh & Verma 2017) (Sun *et al.* 2019) (Saini *et al.* 2021) points out that CLD techniques help in improving energy conservation in WSN at physical layer, routing layer and MAC layer.

4. Security Different attacks are possible at different layers. For example, Interference attack at the physical layer, Denial of Sleep at the data link layer and DOS routing protocol at the network layer. In addition, the use of WSN in surveillance, intelligence, protection and real-time target tracking,etc are some of the possible security concerns which need an CLD solution (Arya & Binu 2017) (Parween & Hussain 2020) (Ambika 2021).

5. Other Issues Many other issues are approached by CLD, like delay and fairness, mobility in nodes, heterogeneity, hidden terminal problem, health care applications, multimedia application, underground and underwater sensor application, and so on.

(Parween & Hussain 2020) present different types of cross layer design techniques in Wireless Sensor Network (WSN) and discuss several cross-layer proposals given by researchers.

1.7.3 Unified layered architecture

By taking into consideration the constraints of WSNs (such as network lifetime, energy, transmission range), the authors have proposed unified layered architecture for WSNs. Unified layered approach is a layer-less technique that allows the integration of different services which are developed for different tasks in different environments by different research communities. The unified layered architecture is useful from the perspective of technology development in WSNs. Various researchers have given the approaches for different applications using the unified layer (see figure 1.11).

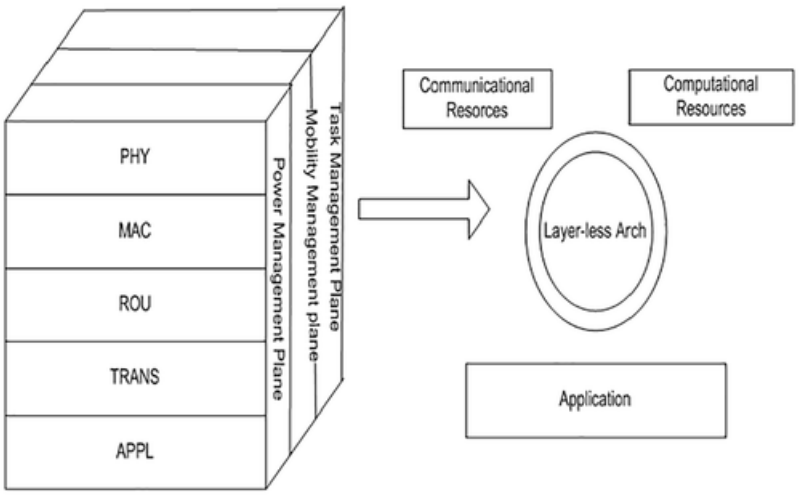

Figure 1.11 – *Unified communication architecture in WSNs*

For more details on the different communication architectures presented above, the paper (Singh *et al.* 2020a) gives a detailed review of existing communication architectural developments and their adaptability.

Conclusion

Sensor networks have been deployed massively in recent last years for a variety of applications. They have become an integral part of military Command, Control, Communications, Computing, Intelligence, Surveillance, Reconnaissance and Targeting systems due to their rapid deployment, self-organization and fault tolerance characteristics for sensing, all these characteristics make them a very promising sensing technique.

We have presented in this chapter the Wireless Sensor Networks and their topologies. The application areas of WSNs with different types of sensor nodes is defines. The unique properties and the different communication architecture in WSNs have discussed. In the next chapter, we will be interested to security issues in WSNs.

Security in Wireless Sensor Networks

2

Contents

The sensor network security has attracted extensive attention, and it has also become an hot topic in the research field of computer science. In this chapter, we focus on security in WSNs including security Challenges of WSN, security requirements in WSNs and the most common DOS routing attacks. Also, this chapter reviews the last approaches of detection and defensive mechanisms against the security attacks.

2.1 Security Challenges of WSN

WSNs have many characteristics that make them very vulnerable to a variety of attacks. Below, some of security challenges are mentioned.

- Wireless Medium: as the wireless channel is open to everyone, the adversary can very easily monitor or participate in communication when desired, or launch attacks like eavesdropping.
- Ad-Hoc Deployment: node failure, mobility or addition of new one make topology dynamic. the security solutions must facilitate the uninterrupted operation of sensor nodes and have the potential to support self-configuration.
- Hostile Environment: the sensor nodes of WSN are usually deployed in unattended and hostile environment without any fixed infrastructure. So, An adversary may physically capture some sensors to compromise their stored sensitive secret data
- Constrained resources: with low computing power, limited energy and only small amount of programmable memory, implementing strong security algorithms with energy saving on a sensor platform become very difficult. Moreover, caused by resource restriction, some of WSN applications work without security which decreased Quality of Service (QoS).
- Immense Scale Deployment: the node number in WSN can range from few dozens to thousands. Thus the security protocols have to be designed thoughtfully, the model must be simple, flexible, and scalable in order to achieve high computation and communication efficiency in WSN.

2.2 General security requirements of WSN

Like traditional networks, WSNs demand certain security considerations. However, the limitations of sensor nodes of the WSN discussed in the previous Section make it particularly challenging task to provide the following security requirements (Wazid 2017):

1. **Authentication**: ensuring the identity of the sending origin of the received message and also its reliability (Stallings 2000). A message authentication code (MAC) can be used to authenticate the origin of the message.

2. **Integrity**: checking that the send message has not been altered. The contents of the message can be deleted or modified by an attacker or intermediate nodes.

3. **Confidentiality**: maintaining the secrecy of the data transmitted between the sensor nodes. however, ensuring data confidentiality in WSN is much more difficult than a wired network since neighbouring nodes can easily accomplish eavesdropping on the information being routed.

4. **Availability**: providing all network services under any critical situation like DoS attacks. A denial of service attack can be launched by sending radio interference, disrupting network protocols, or depleting the power of nodes through various methods.

5. **Non-repudiation**: referring to condition in which both sending and receiving parties must not deny that they have not sent/received the data message/control message in order to preventing malicious nodes to hide their activities. Owing to the lack of centralized controlling infrastructure, WSNs are the most vulnerable networks to these types of attacks.

6. **Authorization**: ensuring that only the sensor nodes, those who are authorized, can be involved in providing information to network services.

Apart from these general security requirements, WSNs have precise security objects:

1. **Forward secrecy**: preventing a node from reading any future secret messages after it leaves the network.

2. **Backward secrecy**: preventing a new deployed node in the WSN, from reading any previously transmitted secret message.

3. **Freshness**: ensuring that the data is recent, and no adversary can replay old messages.

4. **Scalability**: sustaining a large number of nodes.

5. **Efficiency**: storage, processing and communication boundaries on sensor nodes must be measured.

2.3 Energy for security

Lifetime node is generally limited by the lifetime of a tiny battery, so energy is the fundamental resource constraint. The additional power consumed by nodes of sensor due to security is dependent on(Messai 2014):

- Calculation necessary for the functions of security, such as ciphering, deciphering, verification of the signature.

- Energy necessary for the transmission and management of security material (keys, etc).

- Energy necessary for the storage of the keys.

  The challenge is to minimize the consumption of the energy with maximizing the performances of security. Energy is an important factor to consider when designing security measures for WSNs. Conserving node energy to extend his lifetime, and prolong network functionalities.

2.4 Attack categorization in WSN

A variety of security attacks against WSNs is documented in the literature. To face these attacks, various attack classification criteria were proposed in order to find the appropriate against measurements. The following figure (2.1) summarizes the main categories of attacks in WSN.

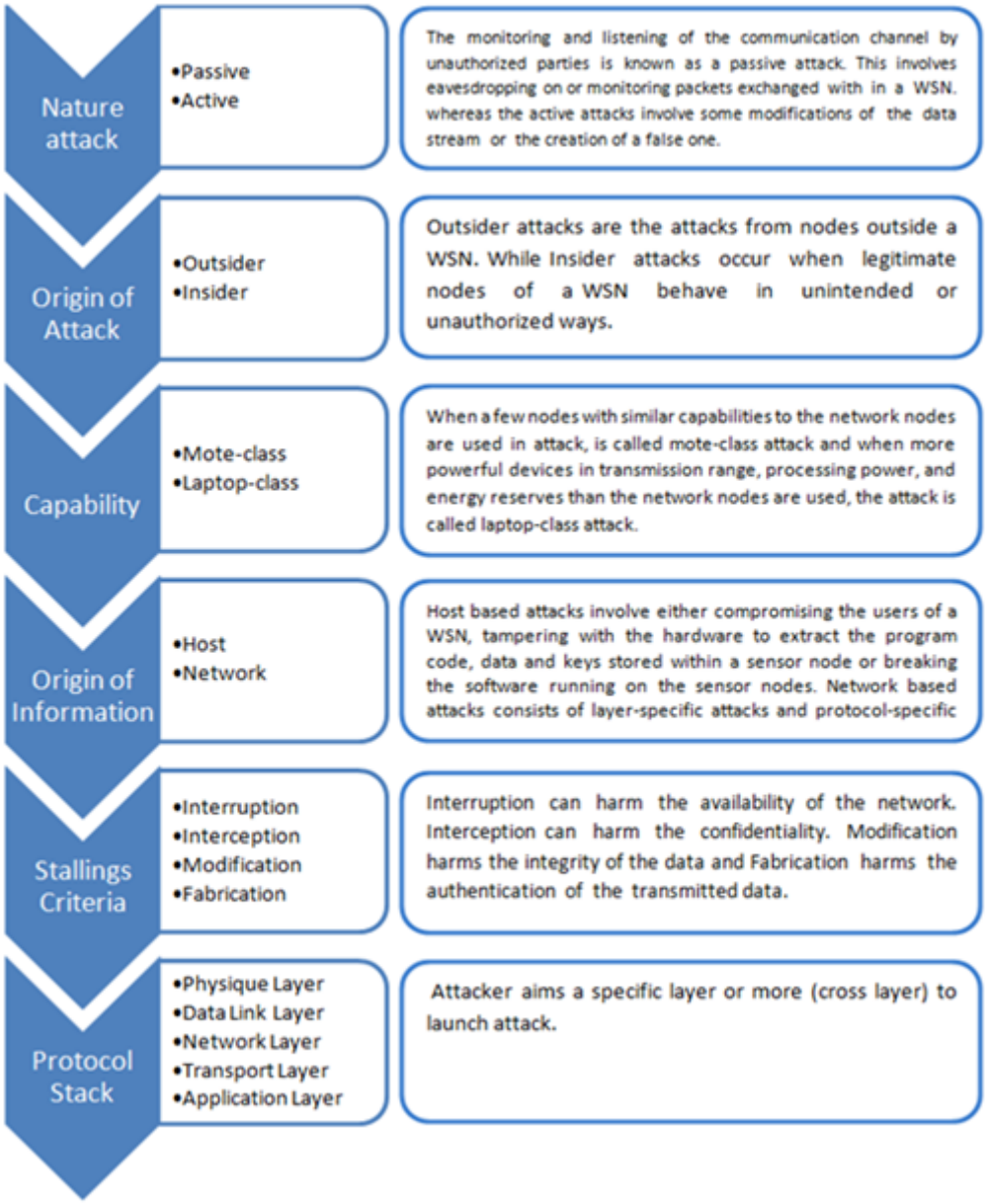

Figure 2.1 – *WSNs Attack Categorization*

The authors in (Kardi & Zagrouba 2019) propose a new classification model distinguishing four classes of attacks in WSNs and provide a survey of the security techniques which will facilitate the design of WSNs for researchers and routing protocol programmers.

2.5 Attacks in WSN

WSNs have a layered architecture which makes these networks susceptible to many kinds of attacks. (Riaz *et al.* 2018) covers majority (fifty two) of the WSN attacks and presents a detailed taxonomy of WSN attacks based on different layers of communication protocol stack. In the table 2.1 is listed most of these attacks.

Layer	Attacks
Physical	Jamming Attack, Physical Attack, Node Subversion, Passive Information Gathering, Device Tampering Attack, Message Corruption
Data Link	Manipulation of Protocol Parameters of 802.11, Selfish Nodes' Refusal to Forward Packets, Back-off Interval Manipulation, Jellyfish Attack, Intelligent Cheater Attack, Link Layer Jamming Attack, Packet-tracing, Collisions
Network	Flooding Attack, Blackhole Attack, Greyhole Attack, Wormhole Attack, Rushing Attack, Link Withholding Attack, Link Spoofing Attack, Byzantine Attack, Colluding Misrelay Attack, Replay Attack, Location Disclosure Attack, Resource Consumption Attack, IP Spoofing Attack, State Pollution Attack, Neighbor Attack, Packet Dropping Attack, Sleep Deprivation Torture, Sinkhole Attack, Sybil Attack, False Node Attack, Acknowledgement Spoofing Attack, Desynchronization Attack, Hello Flood Attack, Selective Forwarding Attack, Routing Table Overflow Attack, Routing Table Poisoning Attack, Packet Replication Attack, Route Cache Poisoning Attack, Monitoring & Eavesdropping, Traffic Analysis, Camouflaged Adversaries
Transport	SYN Flooding Attack, Session Hijacking Attack
Application	Malicious Code Attack, Repudiation Attack, False Data Filtering Attack, Clock Synchronization Attack, False Data Injection Attack

Table 2.1 – *WSNs Attacks (Riaz et al. 2018)*

The most frequent attacks against WSN are the Denials of service attacks (DOS)(Ahmad *et al.* 2019) (Gavrić & Simić 2018). This class of attacks which leads to WSNs' unavailability, aims to degrade the WSNs'

performance or broken it.

DoS attacks are possible on all layers especially the network layer, which is responsible for neighbor discovery, link recovery and routing packets between sensors and the base stations. Thus, the collaboration between sensors, for routing, is vulnerable to a number of attacks including probing, monitoring, injection of false routing information, etc.

The attacks which act in the network layer are called routing attacks (Narayanan *et al.* 2021). In this thesis, we focus mainly on the DOS routing attacks in the WSN and which are discussed in detail below.

2.5.1 DOS Routing Attacks in WSNs

The network layer attacks are malignant as they perturb the entire functionality of the WSN, especially routing procedure that further causes denial of service (DoS) attack in the network. (Mohammadi *et al.* 2011) (Solapure *et al.* 2018) present an overview of different routing attacks on WSNs and compare them to each other based on their goals, results, strategies, detection and defensive mechanisms. We present in the continuation the Some of DOS routing attacks in WSN.

Blackhole Attack

The blackhole attack is one of the simplest attacks in network layer where the attacker swallows (i.e. receives but does not forward) all the messages he receives. Consequently, all packets that enter in the blackhole area are compromised by an attacker and nothing reach the base station. Hence, the throughput and end-to-end delay of the subset of nodes surrounding attacker is dramatically decreased (Kalkha *et al.* 2019) (Saputra *et al.* 2020) (Zala *et al.* 2021) (Bensaid *et al.* 2016) (Tami *et al.* 2021).

Wormhole attack

Wormhole attack is an attack on the routing protocol where a captured data at one location are tunnelled to another one. In this attack usually two malicious nodes are involved. These nodes strategically placed at different ends of network create an illusion that the two distant locations are close to each other and directly connected (Aliady & Al-Ahmadi 2019) (Ahutu & El-Ocla 2020) (Singh *et al.* 2021).

Sybil attack

Sybil attack is defined by "malevolent device, taking multiple identities in an illegitimate way" (Newsome *et al.* 2004), the malicious node present multiple identities to other nodes in the network in order to take part in multiple routes through it. This attack appears to be in multiple locations or multiple times in a single network at once (Jamshidi *et al.* 2019) (Dong *et al.* 2020) (Giri *et al.* 2021).

Selective forwarding

In selective forwarding attack, malicious nodes may refuse to forward certain messages or simply drop them according to certain criteria. To launch this attack, the attacker should be on the route of packet transfer in a multi-hop network. Otherwise, the attacker needs to position himself in the routing path using other attacks, such as the Sybil attack or sinkhole attack. When all the packets are dropped and any of them is forwarded, selective forwarding attack is called blackhole (Zhang & Zhang 2019) (Li & Wu 2020) (Liu & Wu 2021).

Hello flooding

Hello flooding is the simplest routing attack which consists to broadcast Hello message to flood the network and to prevent other messages from being exchanged, using equipment which has strong emission power. Hello packet is usually used in many routing protocols to discover neighboring nodes and establishing network topology. The attacker declares itself as a neighbor node and the nodes whose receive its Hello messages assume that the sending node is in communication range and start communicating to that node, and make entry into its routing table as a neighbor. Hence,the attacker can easily control the network (Gill & Sachdeva 2018) (Srinivas & S. S. Manivannan 2020) (Banga *et al.* 2021).

Sinkhole Attack

In a sinkhole attack, the intruder aims to compromise a node in the network to attract all the traffic from neighbor nodes based on the routing metrics used in the routing protocol (Zhang *et al.* 2019) (Babaeer & Al-Ahmadi 2020) (Ansar *et al.* 2021) (Aissaoui & Boukli-Hacene 2021). Sinkhole attack is discussed in detail in the following section.

Figure 2.2 illustrates the principal DOS routing attacks in WSN.

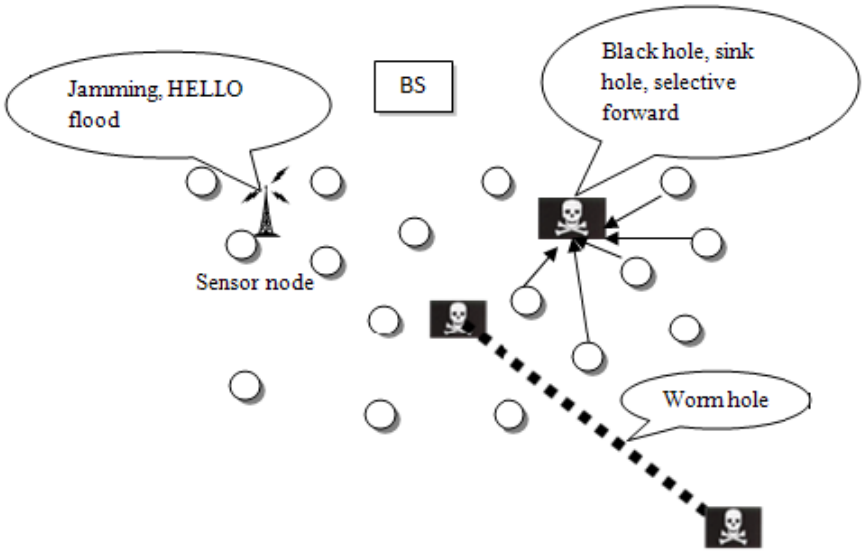

Figure 2.2 – *DOS routing attacks in WSN (Messai 2014)*

2.6 Sinkhole Attack

Sinkhole attacks are a form of network layer attack where an intruder tries to compromise an existing node or to introduce a counterfeit node inside the network to launch the attack. The attacker node tries to attract network traffic to itself by advertising a fake routing information, about its link quality which is used by the routing protocol, to neighboring nodes for un-authorized/illegitimate routing updates. Once routing tables are updated, the victim nodes send data to the attacker node rather than sending it to the node it was formerly using, the attacker node become thus a sinkhole.

The sinkhole attack can be used as a springboard to perform more severe attacks namely, Selective Forwarding attack, Wormhole attack, Flooding attack, Sybil attack and Black hole attack. To be more destructive and to prevent the base station from obtaining complete and correct sensing data, the sinkhole node needs to position itself relatively close to the base station to attract the packets to its destination, hence its name.

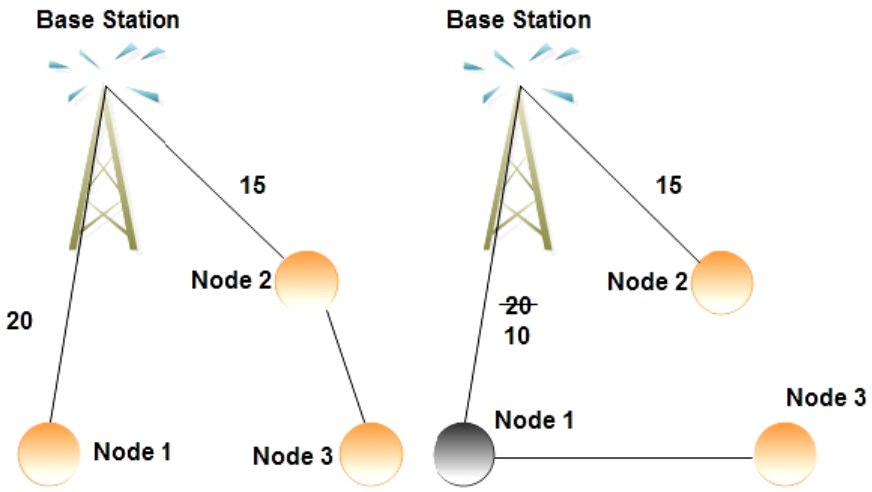

Figure 2.3 – *Sinkhole Attack in WSNs*

For example, as shown in Figure 2.3, the comprised Node 1 advertises a high-quality single-hop link to the Base Station. As a result, Node 3 select Node 1 to relay their data.

Many researchers have proposed several techniques for detecting sinkhole attacks in WSNs. These works will be discussed in the chapter 4.

2.6.1 Sinkhole Attack Analyze

We consider two points, in this analysis of sinkhole attack : Analyse based on the capabilities of attacker node and Analyse based on the location of attacker node.

Based on the capabilities of attacker

The attacker node have higher or similar capabilities to the network nodes in terms of communication and computational power. The intruder pretends to have the shortest path to base station since is the basic routing metric for attracting data to itself. In the first case, the attacker will be able to attract all neighboring nodes by forwarding the packets intended to the base station through the intruder. Whereas in the second case, the intruder will be only able to cause a routing update for the close nodes.

The sinkhole node can be easily detected if it performs as blackhole where the attacker node would capture all the relay nodes nearby the base station and prevent them from communicating with it.

Based on the location of attacker

In a sinkhole attack, the goal of an adversary is to lure nearly all the traffic from a particular area through a captured node. Different locations of the sinkhole attacker don't induce different influences on the network closely the same. Area 1: If the attacker is located close to the base station, the compromised node surrounds the base station, it can easily attract all the

traffic by telling its neighbors that it has shortest route, by advertising an artificial high quality route, to reach to the base station (see Figure 2.4). Area 2: if the sinkhole attacking node is at the edge of the WSN (far from the base station), the sinkhole attack remains effective and can be launched in conjunction with a wormhole attack (Xu *et al.* 2007). This attack involves two compromised nodes linked via a tunnel (see Figure 2.5). The adversary creates, thus, a sinkhole by tunneling messages attracted in its part of the network and replays them in a different part with another malicious node to reach to the base station. In this attack, the surrounding nodes are convinced that they are only one or two hops from base station while they are at multiple hop distance away.

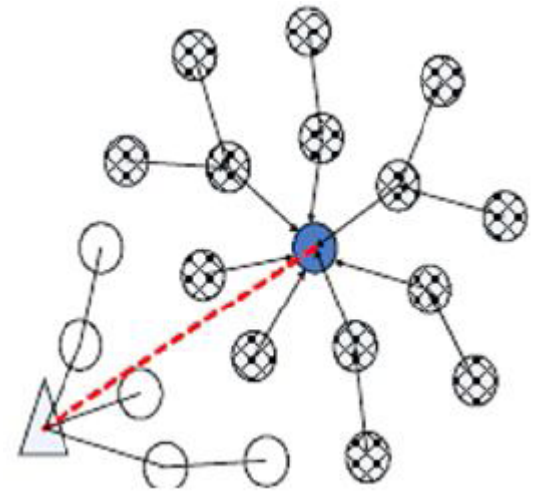

Figure 2.4 – *Wormhole Attack under Sinkhole Attack "A"*

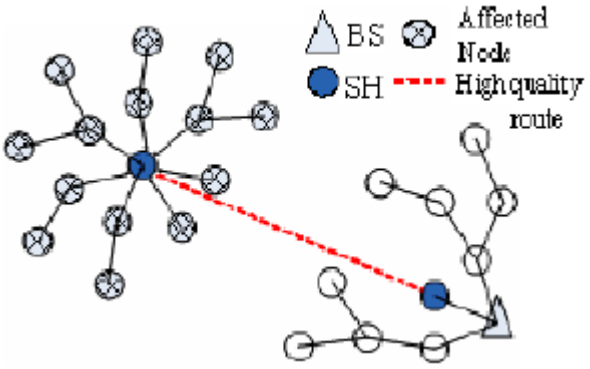

Figure 2.5 – *Wormhole Attack under Sinkhole Attack "B"*

Since we use Ad hoc On Demand Distance Vector (AODV) as our routing protocol, how a sinkhole attack is launched in AODV is explained in the section below.

2.6.2 Sinkhole Attack in AODV Protocol

The AODV routing protocol

The Ad hoc On Demand Distance Vector (AODV) algorithm (Perkins *et al.* 2000) is a reactif routing protocol designed for use by

mobile nodes in an ad hoc network. AODV creates and maintains routes only if these are needed, on demand. Routes remain active only as long as data packets are traveling along the paths from the source to the destination. When the source stops sending packets, the path will time outed and will be deleted.

At each node, AODV maintains a routing table. The routing table entry for a destination contains three essential fields: a next hop node: used to send all packets destined to the destination, a sequence number: acts as a form of time-stamping, and it indicates the freshness of a route, and a hop count: represents the current distance to the destination node.

AODV makes use of four message types: RREQ (Route REQuest): is broadcasted by a node requiring a route to a given destination, RREP (Route REPly): is unicasted back to the source of RREQ message by providing information about the requested route, RERR (Route ERRor): is sent to notify e.g. that a route has to be deleted and RREP-ACK (Route REPly ACKnowledgement): returns an acknowledgment when a RREP message is received (Boukli-Hacene *et al.* 2006).

The figure 2.6 illustrates a route search initiated by node A and in the direction of node J and the various routing tables created. The RREQ message from A is broadcast to all of its neighbors. When J receives the message it unicasts an RREP message to A by passing by H, G and D.

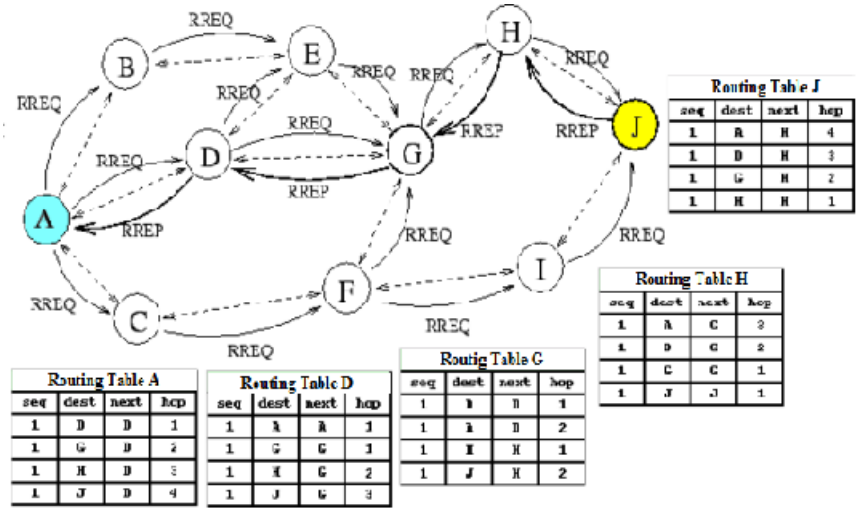

Figure 2.6 – *Route Detection in AODV Protocol*

How To

AODV protocol uses the number of hops and High sequence number as metrics to choose the best route to send packet to the Base Station. Generally the route from source to destination is created when one of the nodes sends a request. So to launch sinkhole attack in AODV protocol, the attacker sends a not necessary but required to launch the attack a routing request for a path to the WSN base station according to RREQ message

format.

After, the attacker replies itself by sending a route response through a RREP message. This RREP packet is tampered with low number of hops which indicates close proximity to the base station and a high sequence number which indicates fresh message. Any neighboring nodes receiving this tampered message, believe that it is the recent fresh route with less number of hops to destination. They update, thus, their old route with the new one and decide to forward packet to sinkhole node and the attack is successful. The following flowchart (see figure 2.7) illustrates how to launch Sinkhole Attack in AODV protocol.

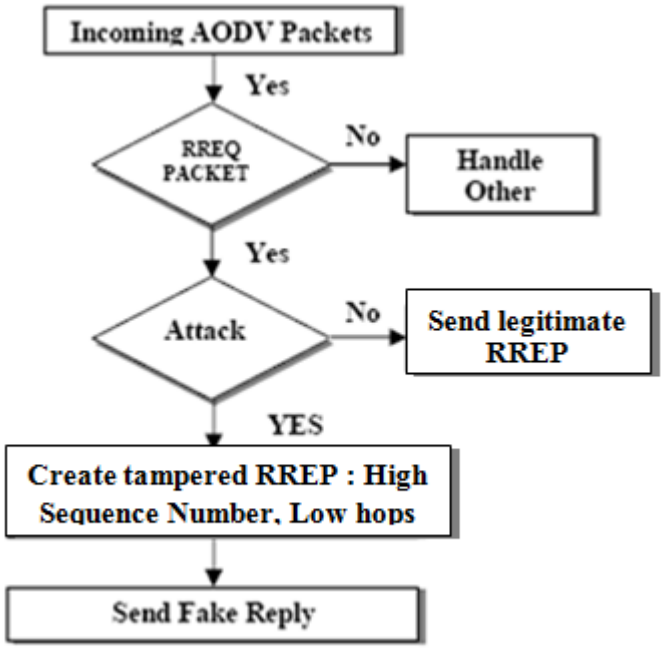

Figure 2.7 – *Sinkhole Attack in AODV protocol*

Sinkhole attack in other protocols can be found in (Kibirige & Sanga 2015) (Rehman *et al.* 2019). We describe in following the security mechanisms against attacks in WSNs.

2.7 Security Mechanisms in WSNs

Wireless Sensor networks are much more vulnerable than wired networks by their nature. The security attacks in WSNs range from passive eavesdropping to active interfering.Security in WSNs has various difficulties, discussed above, which make application of existent solutions inappropriate to WSNs. The security mechanisms for WSNs are actually used to detect, prevent and recover from the security attacks. Numerous analysts proposed so many threats handling models and diverse security protocols to counter malicious attacks and these can be categorized in various kinds, which are shown in a taxonomy form in Figure 2.8. The cryptography, key management, secure routing, secure data aggregation and intrusion

detection and prevention are the main security issues in WSNs.

In this section, we first provide a taxonomy of various security mechanisms proposed in wireless sensor networks (WSNs). We then provide brief literature survey on cryptography, key management, secure routing, secure data aggregation and intrusion detection in WSNs.

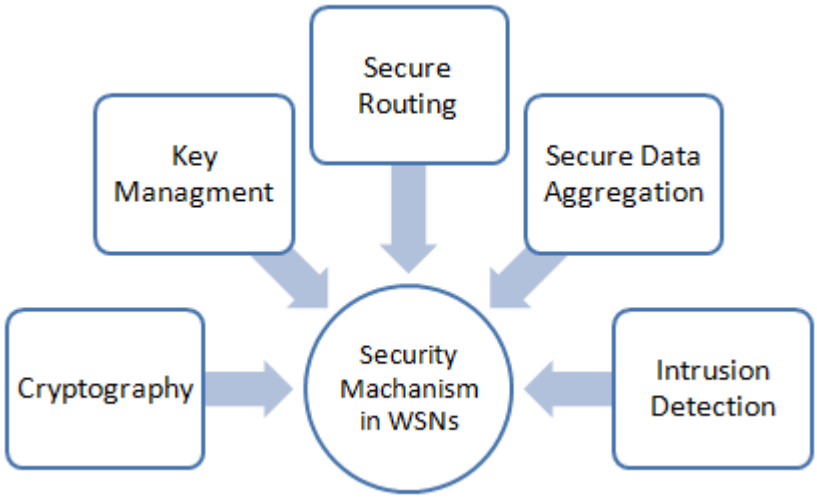

Figure 2.8 – *Taxonomy of security protocols in WSNs*

2.7.1 Cryptography

Cryptography provides the mathematical foundations for the construction of secure protocols which response to the basic security requirements of confidentiality, integrity and identities authentication in networks. But as the sensor nodes are limited in their computational and memory capabilities,the most of traditional cryptographic techniques cannot be simply applied to WSNs without adapting them. Thus, many works in recent years have proposed cryptographic security mechanisms for WSNs, to secure the communication between sensor nodes and the base station, by addressing the different particularities of those networks. Based on the existing cryptographic techniques, we can classify them into three classes: symmetric, asymmetric and hybrid cryptographic techniques as shown in Figure 2.9. Some of the most relevant works in this area are surveyed and summarized in this section.

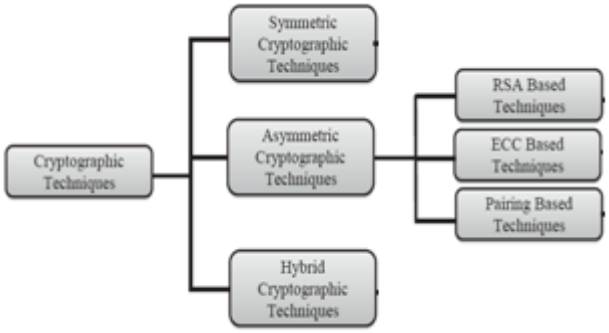

Figure 2.9 – *Cryptographic Techniques in WSNs*

Selecting the most appropriate cryptographic method is crucial in WSNs and it is based on code size, data size, processing time, and power consumption criteria.

Symmetric Cryptography

In symmetric cryptography, a single key is used for both encryption and decryption of the data. The symmetric encryption is also called secret key cryptography. It is the oldest technique of encryption and it is reliable and fast, and consumes less energy and memory. However, the most disadvantages of this technique are how to exchange the key securely between communicating nodes and compromising of the entire WSNs through compromised pre-loaded key nodes.

Asymmetric Cryptography

Contrary to symmetric encryption, in the Asymmetric Cryptography or Public Key Cryptography (PKC) two different keys are used, a published public key used for encryption and a secret private key used for decryption. This encryption mechanism is much secure than symmetric but the generation of pair of keys causes high time, energy, and memory consumption. So in general, PKC is a costly security mechanism for WSNs. The well-known PKC techniques are RSA (Rivest, Shamir and Adleman) and ECC (Elliptic Curve Cryptography). The most favorable for implementation in restricted devices as WSNs, according to the literature are the alternatives relied on elliptic curves because the main advantage of ECC is that shorter keys (less-memory requirements and faster field arithmetic operations) can be used if compared with other cryptosystems like RSA. For the same security, it is often stated that the security of a 160-bit key for ECC is equivalent to 1024-bit key of RSA.

Hybrid Cryptography

Hybrid cryptography is the combination of symmetric and asymmetric cryptography. It benefits the advantages of both techniques where asymmetric encryption is used only to exchange a secret key and symmetric encryption is used afterwards (Iqbal & Shafi 2019).

To achieving high level of security in WSNs and after examining their constraints and limitations in sections above, we conclude that these kinds of environment need Light Weight Cryptography (Tawalbeh & Tawalbeh 2017) (Biryukov & Perrin 2017) (Gunathilake *et al.* 2020).

Light Weight Cryptography

The Light Weight Cryptography (LWC) is a developing field that combines Computer Science, Cryptography, and Electrical Engineering aiming to provide the required level of protection for environments with limited power and computational capacities (Manifavas *et al.* 2014). Lightweights in cryptography can be achieved on both the hardware and software levels

and must address the three tradeoffs: security-performance, security-cost and performance-cost (Tawalbeh *et al.* 2017).

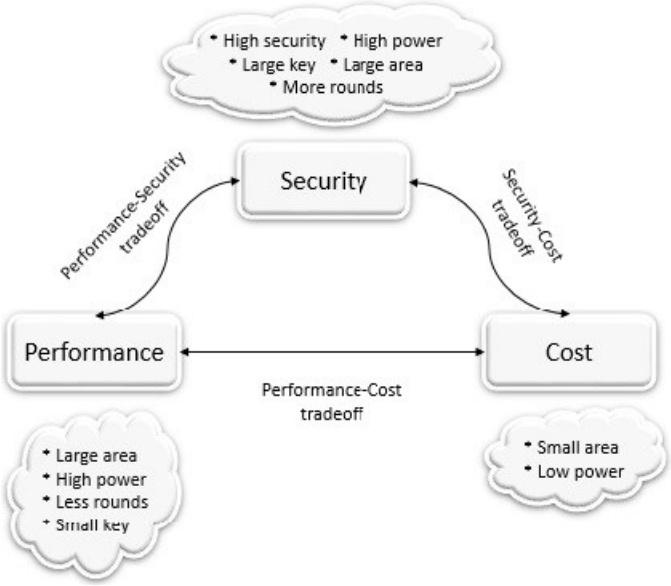

Figure 2.10 – *Lightweight Cryptographic Algorithm Design Tradeoff (Luhach 2016)*

As Symmetric Lightweight Cryptographic Approaches for WSNs we find AES (Advanced Encryption Standard). AES is a strong symmetric key encryption widely used with good performance. AES has a well-balanced tradeoff between implementation size and performance but without energy saving. Recently, due to rapid development in the hardware industry, we can find lower cost and less power consuming AES implementations. In (Thangarajana & Bhaaskaran 2018) an architecture to optimize the power dissipation of the circuit is proposed by trading off the throughput and area of the system. The power is minimized by the method of parallel processing and this structure was implemented using Verilog HDL and synthesized using Cadence RTL Compiler and Cadence Encounter SoC. From the results, the power dissipation of the proposed structure is 2.04 times less than the existing parallel processing structures. The paper (Acla & Gerardo 2019) presented an enhancement to the existing AES algorithm by introducing a bitwise permutation in place of MixColumns function to lessen the computational complexity of the algorithm and in order to reduce the resource utilization of the WSN node and thus develop a lightweight version of AES, LAES. Results have shown that LAES have lesser device utilization as compared to recent implementation of traditional AES. To test the security, both LAES and AES were implemented on the same ten sets of data to obtain the avalanche effect. The results conclude that replacing MixColumns function of AES with 128-bit permutation improved the security of the cipher in terms of avalanche effect. Furthermore, The time security was computed and it would take 7.2563x1013 years to break the LAES using brute force attack.

In (Ali *et al.* 2020b), a secure light data encryption approach is proposed. This approach is less computational and response times based on

a modified version of Diffie–Hellman technique. The modification is by generating a hash of each value that is transmitted over the network. The proposed approach has been analyzed in terms of encryption/decryption time, computation time, and key generation time for different sizes of data and on various attacks. The comparative analysis with the existing approaches shows that the proposed approach performs better in most of the cases.

For Asymmetric Lightweight Cryptographic Approaches, the well-known RSA algorithm is a bad candidate for lightweight optimization since it depends on two factors which are large prime numbers between 1024 and 4096 bits to generate the pair of keys. However, ECC is considered the most suitable because it requires less power consumption, a smaller area, and fewer clock cycles (Tawalbeh *et al.* 2017) (Gulen & Baktir 2020). Several optimized implementations were proposed for lightweight ECC. (Ajaykumar *et al.* 2020) designed and implemented a highly robust and efficient Symmetrical Elliptic Curve Cryptosystem with Rabin Technique for WSN routing protocol. The proposed algorithm uses double binding hash code technique. It supports sensor nodes with bio hash code for identification of authorization network to share the data. The simulation results show that the proposed Rabin ECC-L (Elliptic Curve Cryptosystem-Linear) algorithm performs optimally better than the existing ECC algorithm because it is taking initially fixed key sizes and later varying it randomly, thus ensuring better energy efficiency and enhanced security. The security technique proposed for WSN in (Naresh *et al.* 2018) is a discrete logarithm problem-based lightweight secure communication system using HEC (Hyper Elliptic Curve). A full scale study of the adaptability of different genus curves over varied prime fields on various types of constrained networks is made. It is shown that the proposed scheme is proficient as the timings of various operations, such as signature generation/verification, key generation, message encryption, and decryption compares favorably with the timings of ECC (Elliptic Curve Cryptography) Systems available in existing literature. From the results of the comparative analysis with ECC-based cryptosystems, HEC cryptosystems are more appropriate for implementation in the constrained platforms in wireless network.

In paper (Lara-Nino *et al.* 2018), the authors presented a survey of ECC in the context of lightweight cryptography to identify the criteria that make an ECC-based system lightweight and a viable solution for using in practical constrained applications. A methodology to create ECLC (Elliptic Curve Lightweight Cryptography) systems is designed and described and the open challenges that must be addressed by these systems is also discussed. The authors provided, for the first time and as a result of the work, the concept and requirements for Elliptic Curve Lightweight Cryptography.

The authors in (Shankar & Elhoseny 2019) proposed a Lightweight Cryptography (LWC) based hash function for image security in WSN. The hash value of encryption was developed upon the optimal secret

key and it was recognized by the Enhanced Cuckoo Search (ECS) optimization. The proposed model exchanges the images securely through WSN and makes it conceivable to encrypt the information in real-time applications because of its low computational expense. For performance examination, impressive measurements, such as PSNR (Peak Signal to Noise Ratio), MAE (Mean Absolute Error), Entropy, NPCR (Number of Pixels Change Rate), and throughput were considered. The results show that the proposed system provided expanded security and adequately utilized the algorithm when compared with ordinary encryption and optimization strategies.

Whereas for hybrid approaches, the proposed scheme in (Tiberti *et al.* 2020) , called topology-authenticated key scheme 2 (TAKS2), presented the evolution of a hybrid cryptography scheme, based on the generation of topology-authenticated keys, specifically designed for WSN platforms. TAKS2 is, by design, a lightweight scheme where only partial components of symmetric keys are predistributed (and not the whole keys). The N-secure TAKS 2 scheme was developed in two implementations based on two state-of-art IEEE 802.15.4 MAC layers for validation. The results shown that the scheme provides security with a performance loss which is negligible in common environmental monitoring applications, and when the performance overhead is introduced on the WSN nodes TAKS2 become less effective in those situations when an highframe throughput (along security) is required.

According to (Dhanda *et al.* 2020) and based on their findings, AES and ECC are the most suitable for used lightweight cryptographic primitives. Hence we can conclude that the Light Weight Cryptographic approaches (symmetric and asymmetric) are the most appropriate solution for the security-performance tradeoff in Wireless Sensor Networks. An analyse of lightweight cryptographic approaches for WSN can be found in (Tawalbeh *et al.* 2017) (Sadkhan & Salman 2018) (Shah & Engineer 2019) (Aslan *et al.* 2020).

2.7.2 Key Management

In cryptography, keys are used for encryption and signcryption in order to maintain the integrity and authentication of messages. So, efficient key management protocols are needed in resources-constrained WSNs to exploit cryptography mechanisms. Key management, by definition, is a set of protocols, which support generation and process of updating the keys among authorized nodes following the security policy. Numerous scientific categorizations for Key Management Schema (KMS) have been proposed, as shown in the Figure 2.11. A classification according to:

- The network structure
- The encryption mechanism (symmetric, asymmetric and hybrid).
- The key pre-distribution: is characterized into area free key Predistribution and area subordinate key pre-distribution.

- The ability to update the keys in the sensor nodes, rekeying (static, dynamic).
- The Network model: depending upon the network mode, it is ordered into homogeneous or heterogeneous WSNs.
- The probability of key sharing between a pair of sensor nodes (probabilistic and deterministic).
- The attacker model: the authors of (Lee *et al.* 2007) characterize four assailant models.

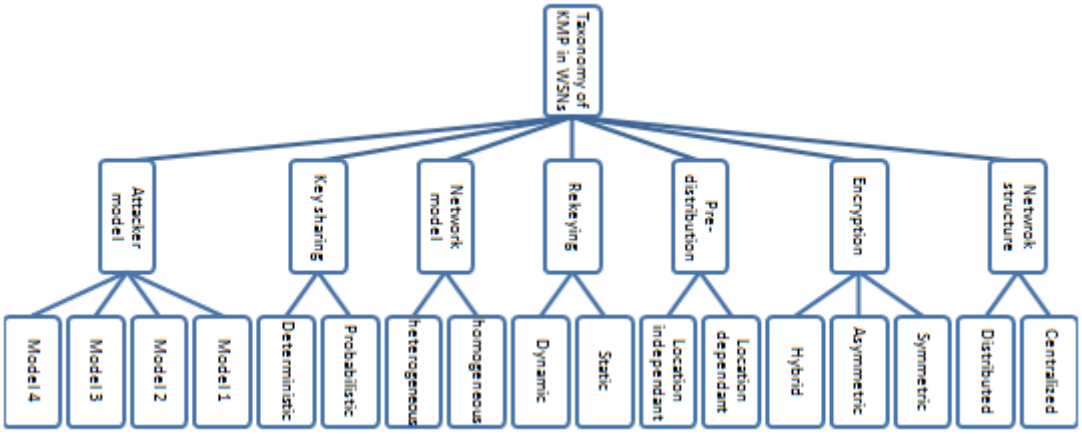

Figure 2.11 – *Classifications for KMSs (Elqusy et al. 2017)*

Key management involves three processes namely, key establishment, rekeying and revocation. In (Lara-Nino *et al.* 2018), key establishment is defined as "a process or protocol through which a shared secret is made available for two or more participants, for its subsequent use in cryptography. The key establishment can be divided into key transport and key agreement".

The efficiency of key management techniques is examined and evaluated by means of the following scales (Yousefpoor & Barati 2018):

- Node revocation: an efficient key management protocol should have the ability to revoke cryptanalyzed nodes in an efficient way in order to prevent more node compromises and secure network safety.
- Forward and backward secrecy: it should be guaranteed through methods of key management so as to defeat the node capture attacks.
- Collusion resistance: a proper dynamic key management technique should be able to resist against compromised nodes.
- Resilience. This measure indicates resistance to node capture. If capturing only one node results in the cryptanalysis of the whole network, then the resilience level of key management system is low.
- Mobility : the key management protocol should have the ability to distribute keys to the mobile nodes and provide them with the ability to communicate with their new neighbours.

- Scalability: the key management protocols should be compatible with networks of different dimensions and sizes.
- Key connectivity: this scale is used for evaluating the ability of the nodes of the network in key formation after rekeying. There are two types of connectivity: local connectivity and global connectivity.

In the paper (Albakri *et al.* 2019), the authors proposed a novel polynomial-based key management scheme with a probabilistic security. Polynomial-based key distribution schemes have been proposed in WSNs to provide a lightweight solution for resource-constraint devices. A deterministic key distribution is guaranteed on hierarchical structure in which a pairwise key is shared between any two arbitrary sensor nodes in a cluster, between a sensor node and its CH, and between the sink and each CH. One problem associated with all polynomial-based approaches in WSNs is that they are vulnerable to sensor capture attacks. However, the probabilistic security feature in the proposed scheme reduces the security risk of sensor-captured attacks and requires minimal memory, communication and computation overhead.

Hamsha and Nagaraja in (Hamsha & Nagaraja 2019) proposed a Light Weight Threshold Key Management Scheme (LWKMS) in WSNs. In the proposed schema, each sensor stores three keys: a preloaded network key that is used to secure communication between sensors; a cluster key that is used to secure communication between a sensor and its cluster head; and a share of a secret that is assumed to be utilized for group communication based on Shamir's secret key sharing scheme. In addition, the base station is responsible for selecting a polynomial, secret keys, generating shares, and updating thresholds. The presented scheme seems lightweight in terms of storage since it reduces the size of the secret key to be communicated and provides less overhead along with less energy consumption and an efficient security even when the keys are compromised by an attacker node.

In (Mesmoudi *et al.* 2019), a smart and dynamic key management scheme for hierarchical wireless sensor networks (SKWN) is proposed. SKWN relies on three subschemes: key establishment, key renewal, and new sensor node integration which allows to guarantee scalability and flexibility of the network. The proposed approach enables to make dynamic decisions in real time based on an ISA component that implements some machine learning rules, to decide the appropriate security level. The authors shown that the ISA component allows consequently to provide efficient energy consumption and the non-redundant use of security operations. With respect to existing scheme, SKWN optimizes energy consumption and overheads related to communication and memory use.

2.7.3 Secure Routing

Routing is one of the most important operations in wireless sensor networks (WSNs) as it deals with data delivery to base stations. Routing attacks can cripple it easily and degrade the operation of WSNs significantly.

Traditional security mechanisms, such as cryptography and authentication alone cannot cope with some of the routing attacks as they come from compromised nodes mostly. Many routing protocols exist with-no efficiency in security. To build secure and efficient routing model for WSNs the following challenges have to be considered:

- Balancing trade-off between performance and security, a prerequisite for heterogeneous WSNs (Zeng *et al.* 2019).
- To detect oscillating devices that sways from good to bad state and vice versa and evaluates the credibility of feedback given by sensor devices.
- In clustered-WSNs, load balancing among cluster head devices is challenging as the existing routing model always routes packet to node with highest trust parameter causing overhead among cluster heads.

Many secure routing protocols are proposed to secure routing, in which different routing attacks are considered and the most recent are trust-based models. In routing, trust mechanism avoids/includes nodes in routing operation based on the estimated trust value. In this section, we present some of proposed schemes.

(Thahniyath & Jayaprasad 2020) presented a Secure and Load Balanced Routing (SLBR) scheme for heterogeneous clustered based WSNs. SLBR presents a better trust-based security metric, via Biased and fluctuating trust evaluation that overcomes the problem when sensors keep oscillating from good to bad state and vice versa, and also SLBR balances load among CH. Thus, aids in achieving better security, packet transmission, and energy efficiency performance. The proposed protocol is compared over existing trust-based routing model namely Exponential Cat Swarm Optimization (ECSO). The obtained result showed SLBR model attains better performance than ECSO in terms of energy efficiency, communication overhead, throughput, packet processing latency, malicious sensor device misclassification rate and identification.

In (Zhao *et al.* 2019), authors presented Exponential-based Trust and Reputation Evaluation Scheme (ETRES) for provisioning security for wireless sensor networks. For measuring Direct Trust (DT), entropy method is used. Furthermore, for strengthening communication and bringing in more reliability, Indirect Trust (IDT) is used. The model can dynamically adjust the trust weight for reducing impact caused due to compromised sensor devices.

The Base Station Controlled Secure Routing Protocol (BSCSRP) is introduced in (Sajan & Jasper 2021) to protect the Base Station (BS) from taking erroneous decisions that affects the network's lifetime. The proposed work aims to detect the anti-nodes from safe nodes by a trust-based mechanism that secures the network from false data injection as well as provides an efficient route that is free from carousal and stretch attack.

The effectiveness of the proposed protocol (BSCSRP) is evaluated by comparing its performance with the existing AF-TNS, BTEM, RSA, and ERF methods.

In (Ishmanov & Bin-Zikria 2017), the authors attempted to demonstrate a research state of the trust-based routing from routing attack perspective and surveyed proposed schemes. The existing methods were discussed and presented based on the attack which they were proposed against and to analyze their efficiently, they discussed based on the proposed framework dividing schemes into three components: learning, trust estimation, and routing. Moreover, the proposed schemes were evaluated based on two important factors, which are energy consumption and attack resiliency/detection. Finally, the researchers identified open research issues in the proposed schemes and research field in general and pointed out several recommendations to solve these issues.

2.7.4 Secure data aggregation

Currently, the data aggregation protocols (Saeedi & Al-Qurabat 2021) mainly focus on improving the efficiency of data transmitting and aggregating, alternately, the aim at enhancing the security of data. The performances of the secure data aggregation protocols are the trade-off of several metrics, which involves the transmission/fusion, the energy efficiency and the security in Wireless Sensor Network (WSN). In this section, we give an overview of the most recent secure data aggregation protocols in WSNs.

(Song *et al.* 2020) proposed a secure data aggregation solution based on AutoRegressive Integrated Moving Average model (ARIMA), a technique for time series analysis, in WSNs. For prediction, the proposed solution requires a cluster head to store the prediction model of all nodes in the cluster and all nodes to make predictions synchronously during data aggregation. To update model on nodes, new data and a new ARIMA model are sent to the cluster head in the form of the prediction error plus a private random number. The experimental results showed that the ARIMA model provided accurate predictions and outperformed a few competing methods in terms of accuracy, computation cost, and communication cost and also achieved desirable data privacy, which was not provided by any of the competing methods.

An energy-efficient Adaptive Slice-based Security Data Aggregation scheme (ASSDA) is presented in (Hua *et al.* 2018). The proposed scheme consists of five steps: (1) Construction of aggregation tree; (2) Determination of slicing numbers; (3) Determination of the size of each slicing; (4) Mixing and assembling; (5) Aggregation. For data aggregation, an additive aggregation function is used and the adaptive mechanism in the model decreases the energy consumption of sending data as low as possible. The author demonstrated that the presented solution reduced the traffic, prolonged the lifetime and improved the security level of WSN,

nearly the same with Slice-Mix-AggRegaTe (SMART) scheme.

A recent review on secure data aggregation scheme in WSN can be found in (Abood *et al.* 2021).

2.7.5 Intrusion detection

Because of their resource constraints, sensor nodes usually cannot deal with strong cryptographic strategies. So what is needed is a second line of defense: An Intrusion Detection System (IDS) that can detect a third party's attempts of exploiting the insecurities of the network. IDSs already represent a key tool for ensuring cyber security in traditional computer based systems and they became an active research topic for wireless sensor networks.

The following Chapter gives a detailed introduction on IDSs in WSNs and surveys the most recent works in this field.

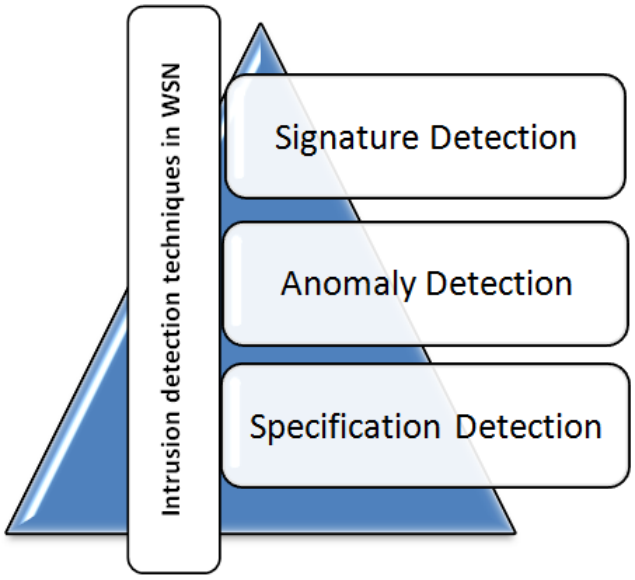

Figure 2.12 – *Intrusion detection techniques in WSN*

2.8 Holistic Security

The holistic approach (layered approach, cross-layer approach) of security (Olariu *et al.* 2005) (Parween & Hussain 2020) aims at involving all the stack layers for ensuring overall security in a network under changing environmental conditions. For WSNs, a holistic approach is required to tackle security challenges in the network as single security solutions for a single layer might not provide the desired result in terms of security efficiency, for example; if a sensor is somehow captured or jammed in the physical layer, the security for the overall network breaks despite the fact that, there are some efficient security mechanisms working in other layers, hence by using a holistic approach, protection could be established for the overall network with a high level of efficiency.

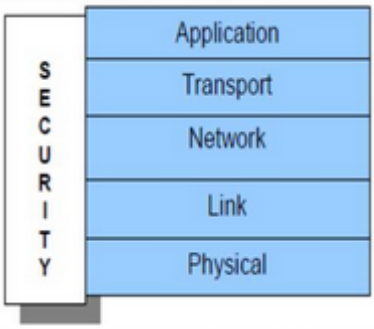

Figure 2.13 – *Holistic view of Security in wireless sensor networks*

The paper (Olariu *et al.* 2005) is viewed as an initial contribution towards developing a holistic solution for securing sensor networks. The proposed solution provides security not only for the various individual layers of the system but also for the entire system in an integrated fashion based on a set of the following four guiding principles: **Security of a network is determined by the security over all layers, in a massively distributed network, security measures should be amenable to dynamic reconfiguration and decentralized management, in a given network, at any given time, the cost incurred due to the security measures should not exceed the cost assessed due to the security risks at that time** and finally **if the physical security of nodes in a network is not guaranteed, the security measures must be resilient to physical tampering with nodes in the field of operation**.The solution in the context of these principles supports a differential security service that can be dynamically configured to cope with changing network state and can potentially minimize the energy cost of security over the network lifetime.

Pathanet et al (Pathan *et al.* 2006) proposed the methods to identify the security related issues and challenges in wireless sensor networks with the holistic view of security for ensuring layered and robust security levels for WSN.

The authors in (Parween & Hussain 2020) presented different types of cross-layer design techniques in Wireless Sensor Network (WSN) and discuss several cross-layer proposals given by researchers and at the end, the paper highlights some challenges faced in implementing CLD (Cross-Layer Design) in Wireless Sensor Networks.

The security challenges in WSNs have continually been a source of great concern to many scientific researchers, their applicability, their nature and their complexity makes them very vulnerable to many security attacks. Up till this moment, there is no well-defined holistic security approach in solving these issues. Combining all the today proposed security mechanisms together for making them work in collaboration with each other will incur a hard research challenge. Providing a clear-cut holistic approach that has the capacity to detect all the possible entry points for attacks within the entire network calls for further research and more the cost-effectiveness and energy efficiency to employ such mechanisms could

still pose great research challenge in the coming days. Ensuring the holistic security in wireless sensor network hence is a major research issue.

Conclusion

In this chapter, we have highlighted various security attacks, especially DOS attacks, and their effect on the WSN. The countermeasures and defensive mechanisms proposed in literature against attacks has been explored to understand them better and to defend them effectively. Thus, providing a secure sensor network remains a challenge.

In the next chapter we focus on the intrusion detection mechanism in WSNs.

Intrusion Detection In Wireless Sensor Networks

3

Contents

After having outlined the threats that Wireless Sensor Networks are exposed to and motivating the need for IDSs to detect attacks. In this chapter, we outline the requirements that an IDS for sensor networks should satisfy. Then, we give a detailed review on the existing schemes of intrusion detection in WSN. Finally, we conclude, the chapter, with future research directions on IDS in WSN.

3.1 Intrusion Detection System (IDS)

In network security, Intrusion Detection Systems are considered as a second line of defense since attacks cannot be always avoided or prevented. IDSs already represent a key tool for ensuring cyber security in traditional computer based systems and they became an active research topic for wireless sensor networks.

3.1.1 Definitions

(Anderson 1980) introduced the concept of intrusion detection in 1980 and defined intrusion as "The potential possibility of a deliberate unauthorized attempt to:

1. Access information;
2. manipulate information;
3. render a system unreliable or unusable."

In other words, an intrusion is an intentional activity that tries to interrupt the confidentiality, integrity and availability of systems.

In the other hand, (Scarfone & Mell 2007) comprehensively defined IDS as "IDS is a complete system that monitors events in a stand-alone computer system or networks; make analysis to find out the conflicting incidents which are against the system's security policy, and identify them as an unauthorized activity from malicious or authorized entity". So, the fundamental goal of IDS is thus to automate the intrusion detection (Khan *et al.* 2020).

3.1.2 Key Challenges of Intrusion Detection in WSNs

View the difference between wired and wireless sensor networks, developing an IDS for WSN should meet the special features of sensor network. In the following, we present the main challenges that should be considered when designing IDS for WSN (Rassam *et al.* 2012):

1. Resource constraints: Unlike wired networks, the IDSs are not installed on powerful computers to operation efficiently in WSN. The sensor nodes have limited physical resources: power, storage capacity, memory, power processing capability and limited signal bandwidth. These constraints make design of an efficient IDS very difficult.

2. Dynamic topology change: The mobility of sensor nodes make difficult for IDS, especially IDS based position map of nodes, to fit with this dynamic change in topology.

3. Continuous data streaming: Setting up an online IDS is very critical mainly with data streaming application where detection task can not be deferred

4. Different types of routing protocols: The different types of WSN applications need a variety of routing protocols.Thus, a developed IDS for a specific routing protocol can not be suitable for an other one or easily adapted.

5. Difficulty in building intelligent IDS models: The wired networks has standard sets of labeled data including both normal and abnormal behaviour, such as KDD99 dataset [1]. Unfortunately, there no such standard for WSN. The use of classification techniques that demand training dataset to build an intrusion detection model seems difficult or if impossible.

6. Lack of standards: Because of the lack of intrusion detection model and standard for WSN, the evaluation of the new proposed IDS compared to other is not feasible.

In addition to challenges, an IDS solution should fulfill some requirements.

3.1.3 Requirements of IDS for WSN

According to (Krontiris 2008) a good IDS for sensor networks must satisfy the following properties:

1. Localize auditing: Apart from the base station, there is no centralized point that can collect the entire audit data in WSN. Thus the IDS must use a localized and partial audit data with considering the problem of high false alarm rate.

2. Minimize the use of resources: WSN is a set of constrained resources sensors which make designing a lightweight and efficient IDS a difficult task. In addition, the available limited bandwidth should be considered when managing the communication between nodes in attacks detection.

3. Trust no single node: IDS using a cooperative algorithms must not fully trust the sensor nodes since they can be easily compromised.

4. Be truly distributed: The gathering of audit data, analysis, detection execution and alert correlation processes should be distributed in order to load balance the intrusion detection charge over the sensor nodes.

[1] https://www.unb.ca/cic/datasets/nsl.html

5. Support addition of new nodes: Adding new nodes due to damage of some nodes or for need, the IDS must support this procedure with the ability to differentiate it from an attack.

6. Be secure: An IDS should be able to resist attacks against itself and have the ability to avoid revocation of a legitimate node from the network or no detection of another intruder node when a monitoring IDS agent is compromised.

Figure 3.1 below summarizes requirements of designing IDS for WSN.

Figure 3.1 – *Requirements of designing IDS for WSN*

The key challenge of designing IDS for WSNs is to detect with high accuracy any security attacks including unknown ones with maximum energy saving so that network life time is prolonged.

3.1.4 IDS components

The basic function of the IDS is to monitor the network and user's behaviour at different levels. Broadly speaking, IDS has three main components: monitoring component, analysis and detection component and alarm component, as shown in Figure 3.2.

1. Monitoring component: controls and monitors traffic, local events and resource utilization on node as well as its neighbours.

2. Analysis and detection component is the key module in which network operations, behavior and activities of nodes are analyzed. Also, it is responsible to classify the network nodes as suspicious or not.

3. Alarm component is responsible to generate an alert when abnormal activities are detected. The following action(s) would be taken according to the system specifications (Butun 2013):

- An audit record should be generated.
- All the network members, the system administrator (if it exists) and the base station (if it exists) should be alerted about the intrusion. If possible, location and identity of the intruder should be provided in the alert message.
- If it exists, a mitigation method should be induced in order to stop the intrusion. For example, an automated corrective action should be generated through a collaborative action of the network members (especially the neighboring members to the incident).

Figure 3.2 – *IDS components in WSN*

3.2 IDS Taxonomy

As showed in the Figure 3.4, IDS can be classified in various groups as follow.

3.2.1 Detection techniques

The IDSs can be grouped into three major categories based on technique they used for intrusions detection: signature or misuse based detection, anomaly based detection and specification based detection. Later on, a new technique arose by combining two or all the three mechanisms namely hybrid based detection.

Signature based detection

Signature based IDS, also known as misuse based or rule based IDS, try to find a match between the analyzed traffic and the pre-known attacks traces or signature. This technique gives a low false positive rate but it only detects known attacks and does not perform well for unknown attacks. According to (Sobh 2006), signature based IDS are very much like the anti-virus systems that could detect known patterns efficiently but fails to detect new ones. Signature detection in WSN is based on stored attack patterns in sensor nodes memory to detected threat. Since sensor nodes have limited storage capacity, signature based IDS are not suitable for WSN (Mitchell & Chen 2014).

In (daSilva *et al.* 2005), the authors present the following rules in order to monitor the network anomalies:

- Interval rule: delay between the arrivals of two consecutive messages must be within certain limits.
- Retransmission rule: the transit messages should be forwarded by the intermediate nodes.
- Integrity rule: the original message from the sender must not deviate when it arrives to the receiver.
- Delay rule: the retransmission of a message must occur after a certain wait time.
- Repetition rule: same message can only be transmitted from the same node in certain number of counts.
- Radio transmission range: the messages should be originated from the neighboring nodes only.
- Jamming rule: the number of collisions for a packet transmission must be lower than a threshold.

Anomaly based detection

Anomaly based IDS also called behavior based IDS, models and predicts the normal behavior of systems named profile by learning phase in which reference cases representing the normal profile are constructed. An alarm is triggered when an excessive deviation of this profile is observed. In this type of detection, unknown attacks can be detected but with high false positive rate.

Anomaly based IDS consists of two phases: training phase and testing phase (or detection). In the training phase, the IDS must learn normal and abnormal behaviors through normal traffic and attack traffic datasets given as input to the IDS. In testing phases, test set of new traffic flows is given to IDS model for classification as normal or attack.

According to (Butun 2013) , anomaly based IDSs are divided into three main categories: statistical based, data mining (knowledge) based and machine learning based:

- **Statistical based**: In statistical based anomaly detection, profiles of normal and abnormal behaviors are created based on the captured network traffic and some scores are generated to calculate the threshold value of the normal behavior. IDS detects attacks when an abnormal activity increases the threshold value. Statistical based methods are also divided into three subcategories which are listed below (Wazid 2017):
  - *Univariate*: In this method, various parameters are modeled as independent Gaussian random variables.

  - *Multivariate*: In multivariate method, the correlations between two or more metrics is considered.
  - *Time series model*: Here, an interval timer is used along with an event counter that takes into account the order and inter-arrival times of the observations, and also their values.

- **Data mining based**: In knowledge based anomaly detection, a prior knowledge (data) of the network parameters in normal and under attack conditions is required. Thus IDS can detects attacks by comparing the values of the parameters under attack with the ones of normal flow. This technique is consists of the following subcategories (Wazid 2017):

  - *Expert systems*: The IDS performs on a set of rules classification of audit data.
  - *Description languages*: Some diagrams are generated (such as Unified Modeling Language diagrams) on the basis of data specifications.
  - *Finite state machine (FSM)*: based on the available dataset, a FSM is generated on the defined states and transitions in the dataset.
  - *Data clustering and outlier detection* : The monitored data are grouped into clusters using clustering techniques, such as K-means. The outliers points (points that do not belong to any cluster) predicts an attack.

- **Machine learning based**: In machine learning based anomaly detection, a machine learning algorithms are used to generate an explicit or implicit classification model of the analyzed network. However, the generated models should be updated periodically in order to improve the performances of IDS. In this technique, we can find the following subcategories (Wazid 2017):

  - *Bayesian networks*: In Bayesian networks, the probabilistic relation-ships among the variables of interest are formed, and further they are used for detection of an attack.
  - *Markov models*: Markov models are used in intrusion detection. They work on the basis of stochastic Markov theory in which the capabilities of the system are modeled, and they are inter connected through transition probabilities.
  - *Fuzzy logic*: This type of detection is based on approximation and uncertainty.
  - *Genetic algorithms*: In these techniques, the genetic algorithms are used in intrusion detection process.
  - *Neural networks*: Neural networks work on the basis of human brain foundations. Neural networks can also be used for intrusion detection process.
  - *SVM*: The goal of SVM is to produce a model (based on the training data) which predicts the target values of the test data

given only the test data attributes by finding a linear separating hyperplane with the maximal margin in a higher dimensional space of data.

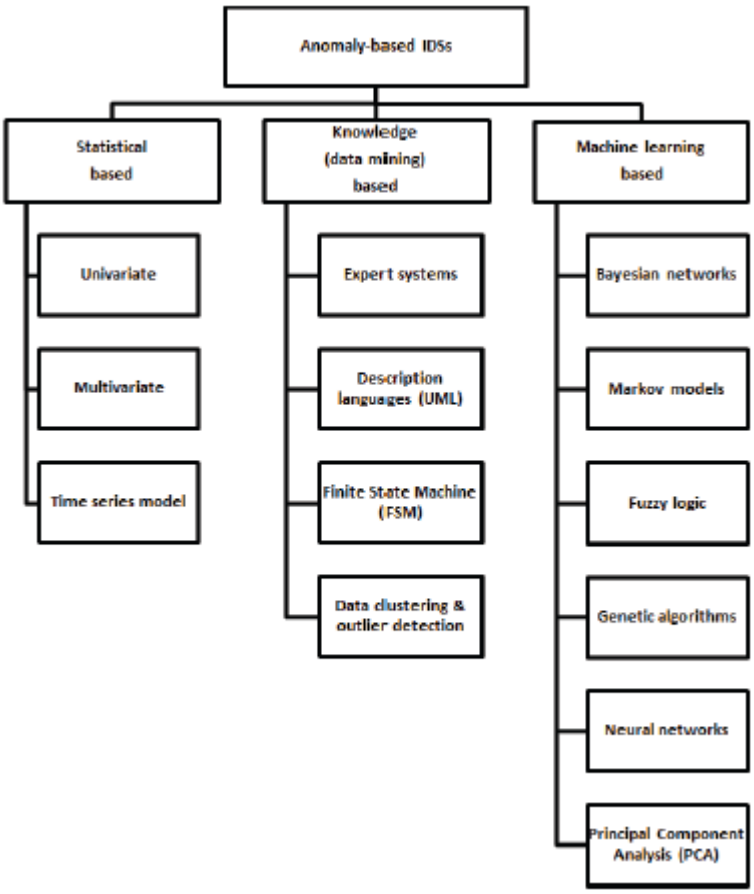

Figure 3.3 – *Classification of anomaly based IDSs (Butun 2013)*

Specification based detection

In Specification based detection a set of manually developed specifications and constraints to characterize legitimate system behavior and to recognize the abnormal behavior of the network, is defined. Specification means set of rules and thresholds defined for predictable behavior of network modules, such as protocols, nodes and routing tables (Khan *et al.* 2020).Thus, this mechanism combines the advantages of both misuse and anomaly based detection techniques. Specification and anomaly based detection work in the same way as attacks detection is based in both of them on deviation from normal profile. This technique can thus detect unknown attacks and gives low false alarm rate compared to anomaly detection. However, to achieve this low false alarm, developing a detailed specifications is a very time consuming task.

Hybrid based detection

Hybrid based IDS uses a combination of signature, anomaly and specification based technique in order to improve the IDS. A hybrid approach

requires use of at least two approaches in one system of the three IDS detection mechanism. Hybrid IDS is developed to overcome the disadvantages of the existing approaches and to design a more powerful system.

3.2.2 Audit Data Source

Based on the location of the data to be analyzed, IDSs can be divided into three groups: Host based Intrusion Detection System (HIDS), Network based Intrusion Detection System (NIDS) and Hybrid based Intrusion Detection System (HyIDS). These types are described one by one.

Host based IDS

HIDS is used to monitor a single host for suspicious activities by either monitoring the real-time system usage of the host or by examining the log files on the host. Such an intrusion detection system has benefit of high protection strategy: it can detect the changes to critical system files on the host, repeated failure access attempts to the host, unusual process memory allocations, unusual CPU activity or I/O activity which makes difficult for attacker to penetrate the system directly. However, due to the installation cost, especially in large networks, and use of resources of each host, HIDS is unattractive solution for resource constrained networks as WSNs.

Network based IDS

NIDS is used to listen to the network traffic passively or actively in order to monitor the entire network or sub-network for the detection of various network threats by doing the analysis of protocol activity. NIDS can analyze packets, their payloads, IP addresses or ports. To find out intrusion, NIDS compares the audit data with threats already stored in its database, in case of match an alarm will be generated. Compared to HIDS, NIDS is less expensive in installation cost but monitoring the whole network traffic results degradation in performances with communication delays.

Hybrid based IDS

HyIDS is used to overcome the drawbacks of HIDS and NIDS above mentioned. It works by combining components and features of both the IDSs using mobile and central agent. the agents play the role of communication between HIDS and NIDS. Mobile agents perform system log file checks on every host. Whereas, central agents check the overall network traffic to detect anomalies.

3.2.3 Detection architecture

IDS can be categorized into four types based on its operational structure (detection architecture), including standalone IDS, distributed and cooperative IDS, hierarchical IDS and Mobile agent IDS (Bruth & Ko 2003):

Standalone

A standalone IDS operates on each individual node to identify abnormal activities and to detect intruders against his node. In this system, there is no interaction between nodes or sharing of information. This deployment requires that each node is able to ensure the functionality of an IDS. The common limitations of this architecture are:

- Coordinated attacks can not be detected.
- May cause collision due to independent IDS in every node.
- Detection accuracy is small as compared to distributed IDS.

Distributed and Cooperative

Here each node runs its own IDS for its local intrusion detection and for a global detection all nodes cooperate to create a unique IDS. This detection architecture is suitable for the flat WSNs. Distributed and cooperative architecture has improved detection accuracy and is able to detect the coordinated attacks. However, it suffers from the following limitations:

- Complex architecture due to the Maintaining of local and global detection mechanism.
- Cooperation increases communication overhead.
- Susceptible to attacks.

Hierarchical

In this case, the WSN is composed of a set of clusters with cluster-head and members. The member nodes are responsible for monitoring its neighbours activities and indicating any suspicious activity to cluster-head. In addition, the cluster-head should detect intrusion against other cluster-heads and all the cluster-heads can cooperate with base station for global detection. Some well-known limitations are:

- Longer delays are reported.
- Susceptible to attacks.
- Vulnerable to cluster damage because it could affect the entire cluster member.
- Selection of cluster-head mechanism each time cause an extra communication in the network.

Mobile Agent

In this detection architecture, the mobile agents can freely move in the network to perform a specialized software on selected node or each node. These agents can cooperate their action to detect the eventual suspicious activities in monitored node. This architecture supports insertion of new nodes in order to increase network lifetime, enable tolerance to faults and/or efficacy of IDS. Limitations

- Correlation issue between high detection and reporting delays.
- Decrease in IDS performances due to the agent portability in heterogeneous environments.
- Compromising of Agents.

3.2.4 Network Architecture

Based on network architecture, (Anantvalee & Wu 2007) divided IDSs into two groups: flat and hierarchical. Designing of an effective and efficient IDS mechanism for WSNs is strongly related to the network architecture.

Flat Architecture

In flat architecture, all nodes are considered as equal in capabilities, contribute equally in any internal functions and participate in routing. Therefore, a lightweight IDSs are required and the most workable detection pattern will be rule-based techniques and statistical techniques.

Hierarchical

In a hierarchical architecture, all the nodes are grouped into clusters and in each cluster they elect a node as cluster head (CH). A distributed detection patterns are implemented in which energy consumption is dispatched over the network and communication cost is low. CH is used to organize and coordinate the sub-computation tasks throughout a cluster while nodes member participate in data processing procedure resulting thus in conserving the communication overhead.

3.2.5 Detection Mode

Based on mode of detection, IDSs can be divided in two sub groups, such as Online IDS and Offline IDS. The difference between them is stated as below.

Online IDS

In this class, the IDS analyze the network traffic (incoming and outgoing) continuously in order to detect in real time intrusions using the detection pattern. Online IDS is the most widely used IDS and is also called Real Time IDS.

Offline IDS

On the other hand, offline IDS requires gathering enough historical data stored in large independent date repositories and detects intrusions from time to time.

3.2.6 Detection Response

When as intrusion is detected, IDSs can be categorized, based on its response, into two classes namely Active IDS and Passive IDS.

Active IDS

Since the IDS works in a reactive way, when an attack is happened in the network, it actively responds to the detected threats by taking the following actions in accordance with system specifications:

- Generation of an audit record.
- An alert message should be sent to all the member entities of the network (nodes, base station and administrator) including, if possible, the location and the identity of the intruder.
- Induction of a mitigation method to stop the intrusion.

Active IDS is also called Intrusion Detection and Prevention System (IDPS) as it prevents the intrusion after detection without external help. IDSP systems are widely used to protect real time systems but Unfortunately, they suffer from resource issues (huge memory and computational resources).

Passive IDS

In passive IDS, the system or the network is only monitored silently with no prevention react to any detected intrusions. It is computerized to notify the system manager or administrator to block the attack.

3.2.7 Usage Frequency

Based on the analysis way, IDSs can be categorized in two types, such as Continuous IDS and Periodic IDS.

Continuous IDS

Here, The IDS monitors the network continuously. It detects and blocks any security threats occurring in the network. Continuous IDS is very effective however it consumes resource of the network continuously resulting to computing and energy issues.

Periodic IDS

The IDS monitors the network in certain periods of time to perform a period wise detection strategy. Periodic IDS is efficient in terms of energy and computation. However in security side, the network can be harmed during waiting period of the IDS if an intrusion appears until its mitigation.

3.3 Decision Making in the IDS

Due to the wireless communications between nodes in the WSN, the following features need to be considered in the decision making model of IDS (Butun 2013):

- Collisions
- Packet drops
- Limited transmission power
- Fading battery power

There are two types of decision making mechanisms for IDSs: collaborative and independent decision making.

3.3.1 Collaborative decision making

In collaborative mechanism, all or designated sensor nodes collaborate with each other and work together to make decision concerning events that happened in the network. As example, the voting mechanism where the event occurred is an intrusion or it is not an intrusion according to the final decision of the majority of the member nodes.

3.3.2 Independent decision making

In independent mechanism, each sensor concludes a decision of its own over the surrounding events in the network. The produced decision is one out of the four decision mentioned below (Ghosal & Halder 2017).

- *Intrusive but not anomalous (false-negative)*: An intrusion manifests in the network but it is not detected by the IDS. The IDS classifies the event as non-anomalous one.
- *Not intrusive but anomalous (false-positive)*: No intrusion appears in the network but a normal event is classified mistakenly as an anomalous one by the IDS
- *Not intrusive and not anomalous (true-negative)*: No intrusion in the network, and the event is correctly classified as non-anomalous one by the IDS.
- *Intrusive and anomalous (true-positive)*: An intrusion occurs in the system, and it is correctly classified as an anomalous event by the IDS.

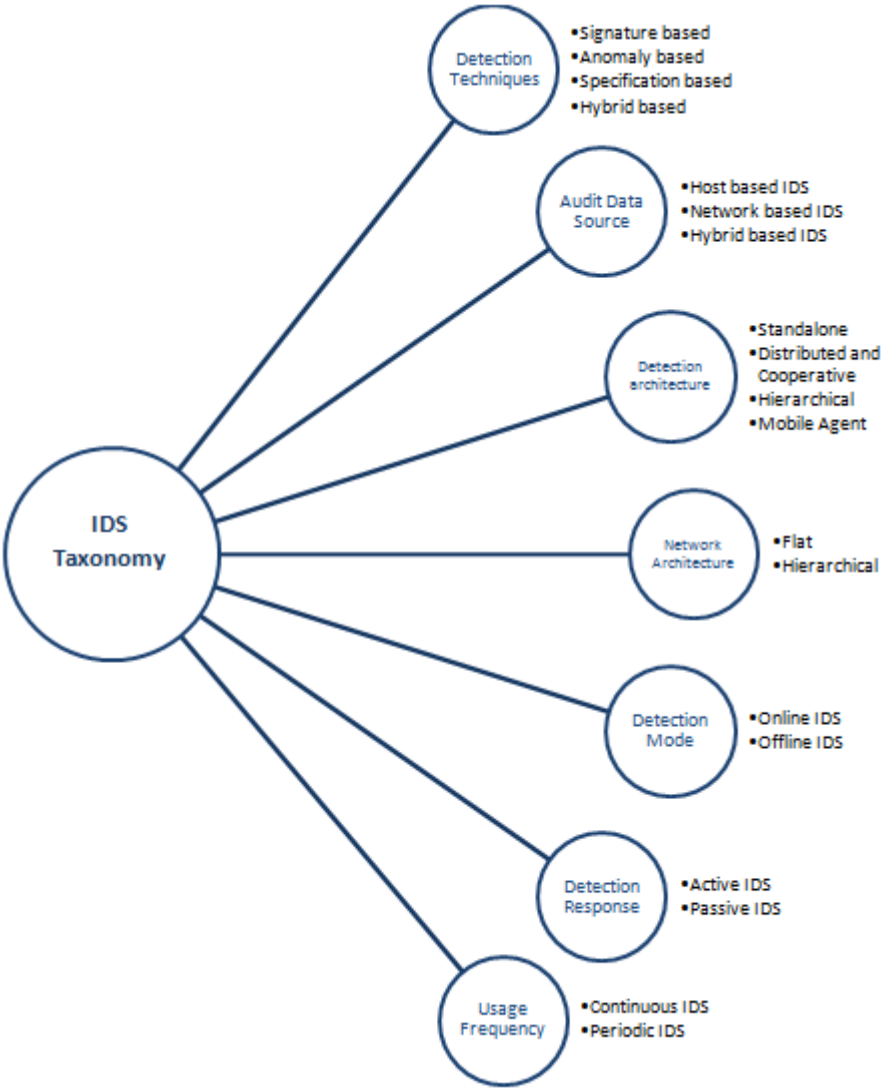

Figure 3.4 – *IDSs taxonomy in WSNs*

3.4 IDSs proposed for WSNs

Various intrusion detection systems have been proposed recently in literature for detecting malicious node(s) in WSNs. Many survey papers are thus published on IDS (Kaur & Rattan 2021) (Ali *et al.* 2020a) (Godala & Vaddella 2020) (Mehta *et al.* 2018). The most relevant survey was presented in (Godala & Vaddella 2020). So we try in this section to complete the presented survey by adding two new categorises: Trust approach and bio-inspired approach.

In the following, a detailed review on most recent IDS for WSN is presented with the respect of the categorisation presented in figure 3.5.

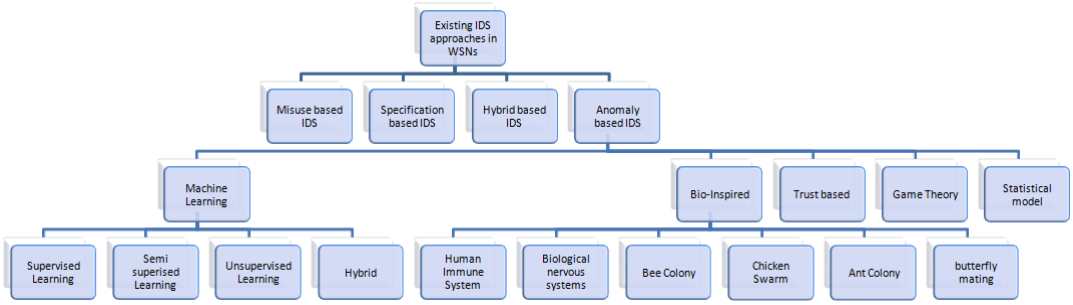

Figure 3.5 – *Existing approaches in WSNs*

3.4.1 Anomaly based IDS

Machine Learning Algorithms

1. Supervised Learning

   Deep Learning (DL) is a subset of Machine Learning (ML) that uses many hidden layers to attain the characteristics of a deep network. DL methods could be more efficient than machine learning because of their deep structure and capacity to learn important characteristics from a dataset on their own and give an output. In the work presented in (Otoum *et al.* 2019), authors give a comprehensive analysis of the use of machine learning and deep learning solutions for IDS systems in Wireless Sensor Networks (WSNs). The Restricted Boltzmann-based Clustered-Intrusion Detection System (RBC-IDS) is compared to an adaptive machine learning approach : The Adaptively Supervised and Clustered Hybrid IDS (ASCH-IDS). The RBC-IDS is based on the RBM (Restricted Boltzmann Machine) which is a neural, energetic network with two layers: visible (V) and hidden (H) where the learning procedure is managed by an unsupervised fashion. In the proposed RBC-IDS, each CH totals the sensed data from the other sensors in its consistent cluster, and sends this to the IDS, which is installed in a central server, by performing the data aggregation procedure. The procedure computes the aggregator trust score based on other sensor trust scores and the trust evaluation between the sensors and the aggregator. To evaluate the performance of the two IDSs, the Network Simulator-3 (NS-3) was used with regards to Accuracy Rate (AR%), False Negative Rate (FNR%) and Detection Rate (DR%) metrics. Simulation Numerical results showed that RBC-IDS performs at the same rate as ASCH-IDS, However, training and detection times of ASCH-IDS are approximately half that of ASCH-IDS. Based on their findings, the authors proposed that an ML-based IDS system is preferable to a DL-based IDS system under the circumstances for an exemplary case of WSN-based critical infrastructure monitoring.

   (Zhang *et al.* 2020) proposed an intrusion detection system based on multi-kernel extreme learning machine(MK-ELM) for clustered WSN environments. The KELM is an excellent classification algorithm in artificial neural networks (ANNs) which combines the advantages of extreme learning machine and the generalization

performance of the support vector machine method. The proposed WSN network model consists of three heterogeneous in energy parts: sensor nodes, sink nodes and management node where the later has the infinite energy resource. Sensor nodes collect, aggregate and transmit collected date to cluster-head which in turn transfers them to the sink node for data preprocessing, so that in the end, the management node ensures anomaly detection based on the MK-ELM classifier which predicts and classifies the incoming data. The proposed MKELM algorithm achieve the highest performance compared to ELM and SVM in detection rate, low false positive rate and network energy saving with fast learning speed.

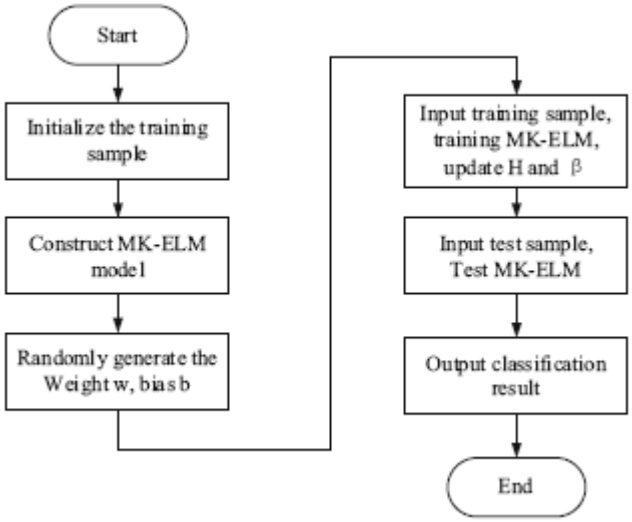

Figure 3.6 – *Flowchart of MK-ELM algorithm (Zhang et al. 2020)*

In (Zhang *et al.* 2021), the authors proposed a WSN intrusion detection system based on Time-Varying Parameter Improved Particle Swarm Optimization with Principal Component Analysis (PCA) and Support Vector Machine (SVM), reffered as TVP-IPSO-SVM. In this system, the PCA technique is applied first to reduce data dimension in the aim to optimize the amount of transmitted data and reducing thus energy consumption. Next the intrusion detection algorithm based SVM is used. Since the learning ability and generalization ability of SVM depend on the choice of its parameters, the TVP-IPSO algorithm is introduced optimize the parameters of SVM. The performance of the proposed model is evaluated on the public dataset KDD Cup99.

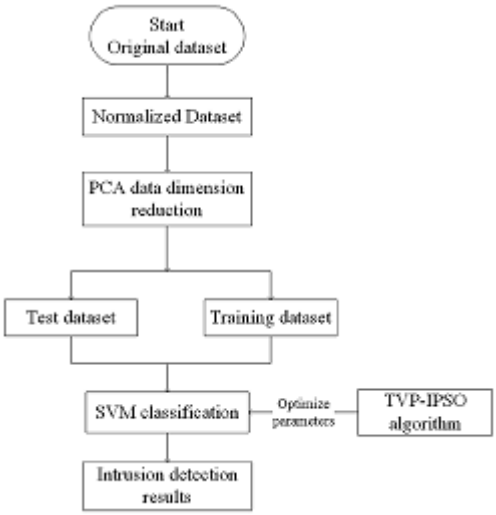

Figure 3.7 – *(Zhang et al. 2021)'s intrusion detection model framework*

2. Semi-Supervised Learning

   (Li *et al.* 2018) proposed an improved K-means clustering Algorithm based on particle swarm optimization (PSO-KM) for intrusion detection. The proposed system use particle swarm optimization to guide K-means clustering algorithm to select initial cluster centers, it makes cluster easily converge to overall optimization. In order to evaluate application effect of PSO-KM algorithm in intrusion detection, the KDD Cup 1999 data set is used. The PSO-KM algorithm uses data set which contains only the normal data as training data, then detects data set which contains intrusion data. The intrusion detection mechanism in the proposed IDS is based on the distance (denoted d) between Xi (Input samples) and cluster center, when d is less than threshold, Xi is considered normal data, otherwise it is considered as intrusion data. Experimental results showed that detection rate of PSO-KM is improved for detecting known attacks and unknown attacks, and false detection rate is greatly reduces compared to traditional K-mean algorithm.

3. Unsupervised Learning

   A knowledge-based intrusion detection strategy (KBIDS) is proposed and developed in (Qu *et al.* 2018). To detect various unknown attacks against WSN, the authors used the Mean Shift Clustering Algorithm (MSCA), an unsupervised learning scheme to distinguish undefined abnormal features reflecting the behavior of a WSN under attacks from the normal context. An excellent balance between high detection rate and less false alarms was achieved by using a weight support vector machine that can maximize the margin between abnormal and normal features which in turn can effectively enhance the detection accuracy. In addition, by using a feature updating strategy, KBIDS can co-evolve with the network structural dynamics and perform constantly well when network architecture or topology changes. To validate the proposed system, KBIDS was implemented in both QualNet network emulator and real 6LoWPAN

wireless sensor network application. Simulation and real application results showed that KBIDS had the highest detection rate and the lowest false alarm rate compared to several common intrusion models.

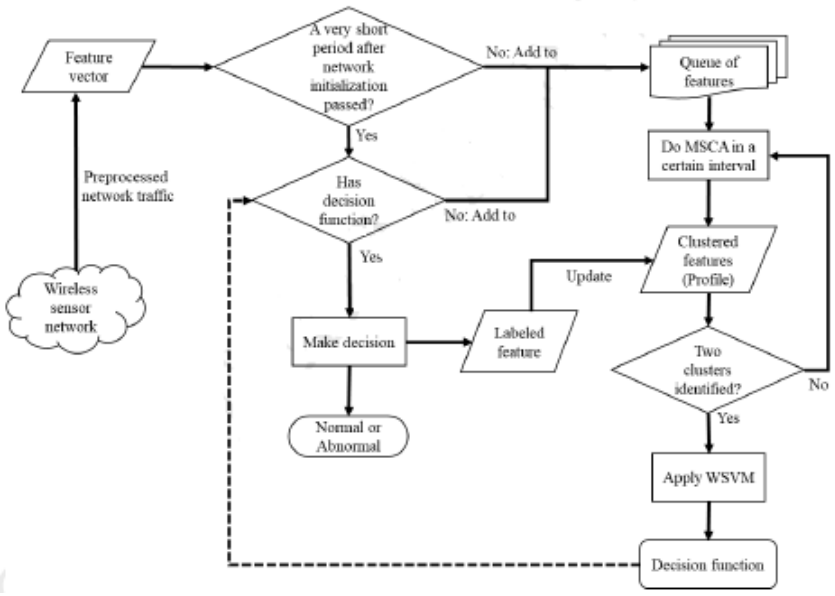

Figure 3.8 – *The schematic diagram of (Qu et al. 2018)'s IDS model*

4. Hybrid

(Nivaashini & Thangaraj 2018) presented an intrusion detection system based on hybrid machine learning technique, by combining K-means clustering and Support Vector Machine (SVM) classification. K-means clustering was implemented as a part of unsupervised learning and SVM algorithm was implemented to perform supervised learning. In grouping phase, a binary clusters one for normal traffic flow and other for abnormal traffic flow were quantified and generated. Attacks of various kinds were clustered into one group depending upon their characteristics. In classification phase, Support Vector Machine (SVM) is utilized to categorize dataset to normal traffic flow or abnormal traffic flow. In the proposed system, a specified WSN dataset is built to describe different types of attacks using temperature sensors. To assess the proposed IDS efficiency, three evaluation metrics was considered: False Positive Rate (FPR), Detection Rate (DTR) and Accuracy (ACC). The results showed that Hybrid (SVM + K-mean) algorithm performs well with high DTR and low FPR in the classification of normal and abnormal WSN traffic compared to common K-mean and SVM.

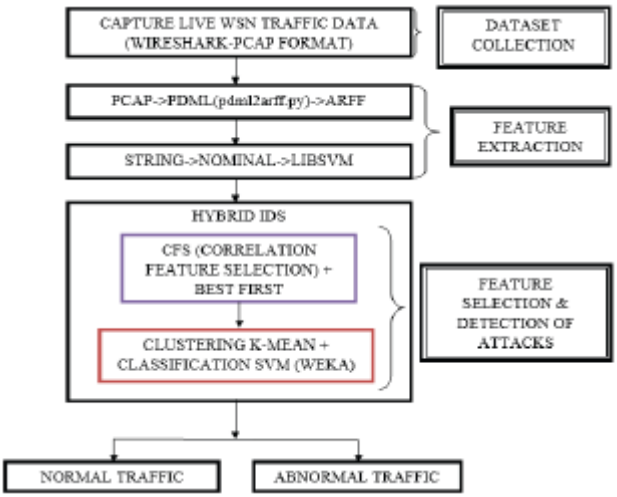

Figure 3.9 – *Systematic Workflow of (Nivaashini & Thangaraj 2018)'s Proposed System*

Bio-Inspired

1. **Human Immune System**

   (Alaparthy & Morgera 2019) designed a cooperative intrusion detection system (IDS) based on human immune concept called danger theory. The proposed approach unifies various monitoring parameters, such as energy, data transmitted and frequency of data transfer to counter the attacks. The danger theory in the presented system, emits four different quantified signals as a function of network performance. These signals include Danger, PAMP (pathogen associated molecular patterns), Safe and Cytokine signals. A threshold value is calculated after the detection process and it is used to determine the state of the network and the countermeasures to be taken. To validate the proposed approach, four different types of attacks, such as Blackhole, DDOS, Wormhole and Selective forwarding were introduced into the network simulated on Cooja simulator and the results concluded that the designed IDS can be used to test a wide range of attacks with a decent detection rate.

2. **Biological nervous systems**

   In (Hasan *et al.* 2021), the authors presented energy optimization based intrusion detection technique using the biological nervous systems. The biological system is implemented using Artificial Neural Network (ANN). The proposed method operates in three sequential phases: Gathering data, training phase and ANN classification. In gathering data phase, the IDS collects data and measure the energy consumption and packet loss between two nodes. During the second phase, the ANN is trained on the collected data to detect the suspicious behavior. The last phase, the ANN will be able to classify the network activities based the energy consumption and Packet Delivery Ratio (PDR). The evaluation of the proposed system is performed using Qualnet simulator. The authors concluded that the ANN based-PDR is faster than ANN-based-energy consumption, but both of them detects the unsecured nodes.

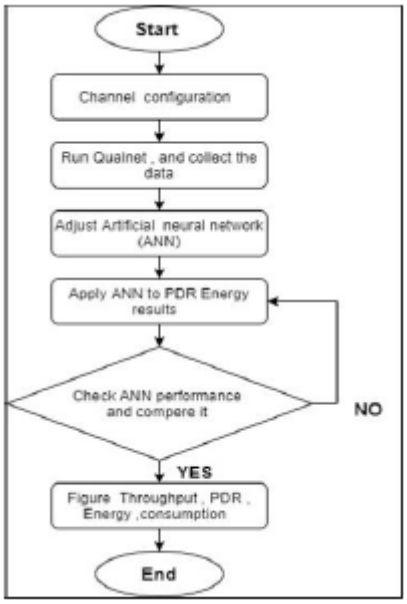

Figure 3.10 – *Secured node detection based ANN (Hasan et al. 2021)*

3. **Bee Colony**

   In (Raghav *et al.* 2020), the authors proposed a bio-inspired based secure routing protocol using Bee Algorithms, named The BEEWARE algorithm. The proposed routing mechanism consists of two important metrics known as primary scout bee and secondary scout bee for carrying routing and security mechanism. The considered attacks are mainly concentrating in network layer, such as flooding attack, Spoofed attack and Sybil attack. The BEEWARE algorithm was compared with the famous routing protocol, such as RLEACH, SECLEACH and CASER. The performance assessment of the proposed IDS was carried in MATLAB with the following factors: End to end delay, Efficiency of path, Routing overhead, Data forwarding efficiency, Packet loss and Packet delivery ratio. The obtained result showed that the proposed Beeware routing scheme provides a better result compared to other mechanism.

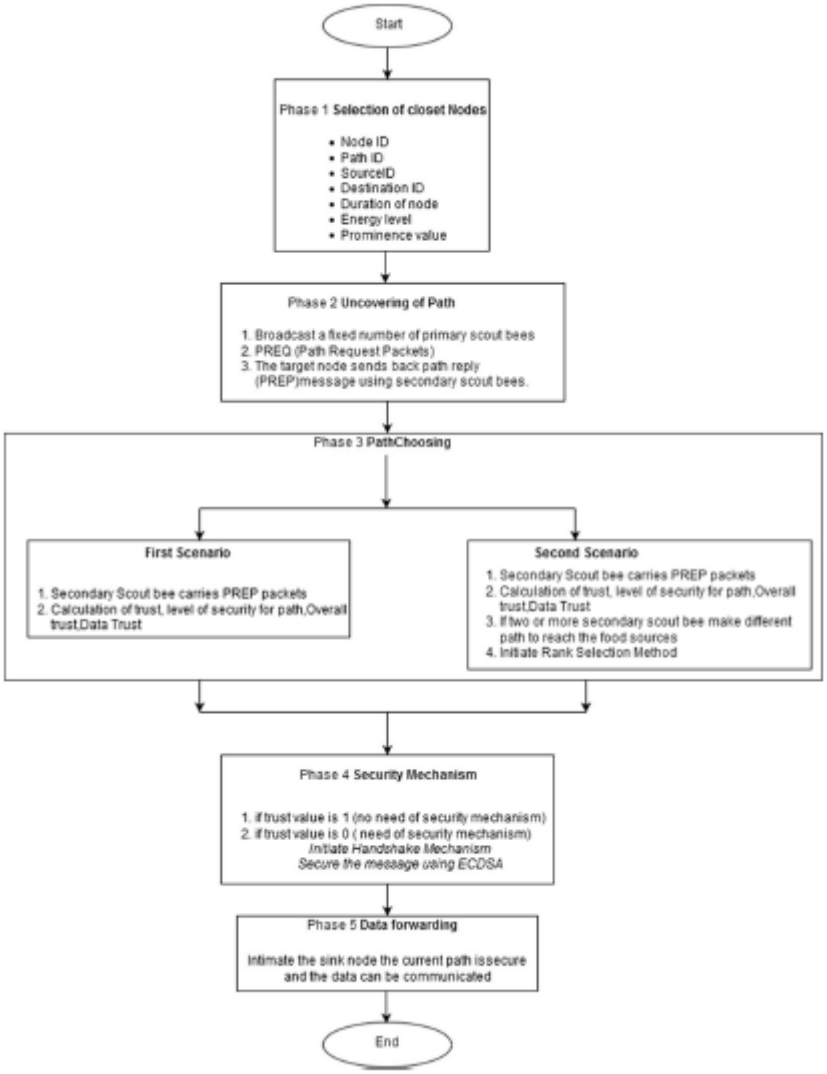

Figure 3.11 – *Workflow of BEEWARE routing scheme (Raghav et al. 2020)*

4. **Chicken Swarm** (Borkar *et al.* 2019) presented an effective Clustering technique based on sensor nodes weight and Adaptive chicken swarm optimization algorithm for Cluster-Head selection to extend lifetime and improve the scalability of the network. For intrusion detection, two stage classification technique known as adaptive SVM classification is proposed. Before classification, a feature reduction is done with aid of RRF algorithm (Rotated Random Forest). The first stage of classification is based on acknowledgement based method to detect whether the corresponding sensor node is malicious or not. Whereas in the second stage, classification is done to detect different types of attacks and corresponding action is performed based on attack identified. The authors concluded that the main reason behind the good effectiveness of the proposed system is that it has used set of classifiers collectively known as RRF compared to one classifier in conventional machine learning algorithm.

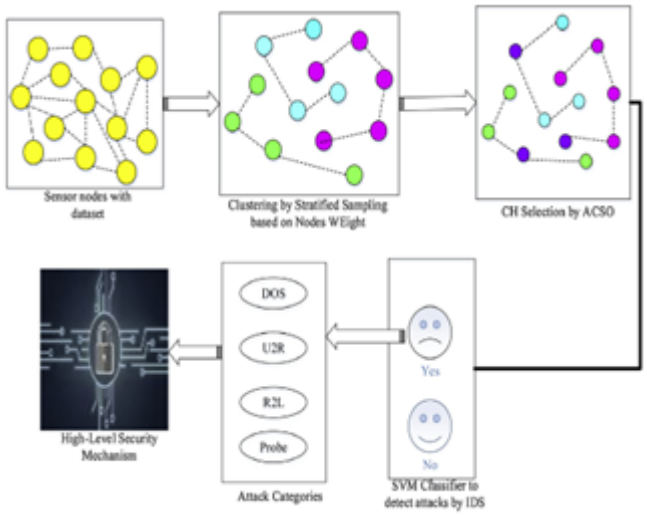

Figure 3.12 – *(Borkar et al. 2019)'s approach*

Other bio-inspired approaches can be found in (Hamad & Abid 2017) (Naseer *et al.* 2020) bio-inspired algorithms based on the Ant Colony system and (Faheem *et al.* 2018) bio-inspired algorithm based on butterfly mating.

Trust based IDS

(Khan *et al.* 2019) proposed a novel clustered trust estimation approach (LTS) for large-scale WSN to detect malicious sensor nodes with low memory and energy consumption. To minimize communication overheads, the proposed LTS performs on two levels: intra-cluster level with distributed approach and inter-cluster level with centralized approach to set precise trust decision of sensor nodes. In centralized approach, Cluster head or base station (trusted node) calculates the trust value of sensor nodes. Whereas in distributed approach, all sensor nodes itself calculate neighbors' trust value for decision making based on a defined threshold value. One of the interesting novelty about the presented scheme is use of a robust trust function with flexible punishment coefficient that can be adjusted according to application requirements. In addition, a simple averaging scheme to aggregate the trust values for cluster heads is introduced. Four kinds of attacks: Garnished attack, Bad mouthing attack, Blackhole attack, Greyhole attack and Ballot-stuffing attack have been simulated on Matlab to assess the effectiveness of the proposed trust model (LTS) considering the fallowing factors: successful interactions, communication overhead, and malicious node detection. The authors concluded that the proposed model is feasible for security enhancement by detecting and mitigating malicious nodes and planed to design a robust, risk-aware trust model for heterogeneous WSN and IoT using machine learning.

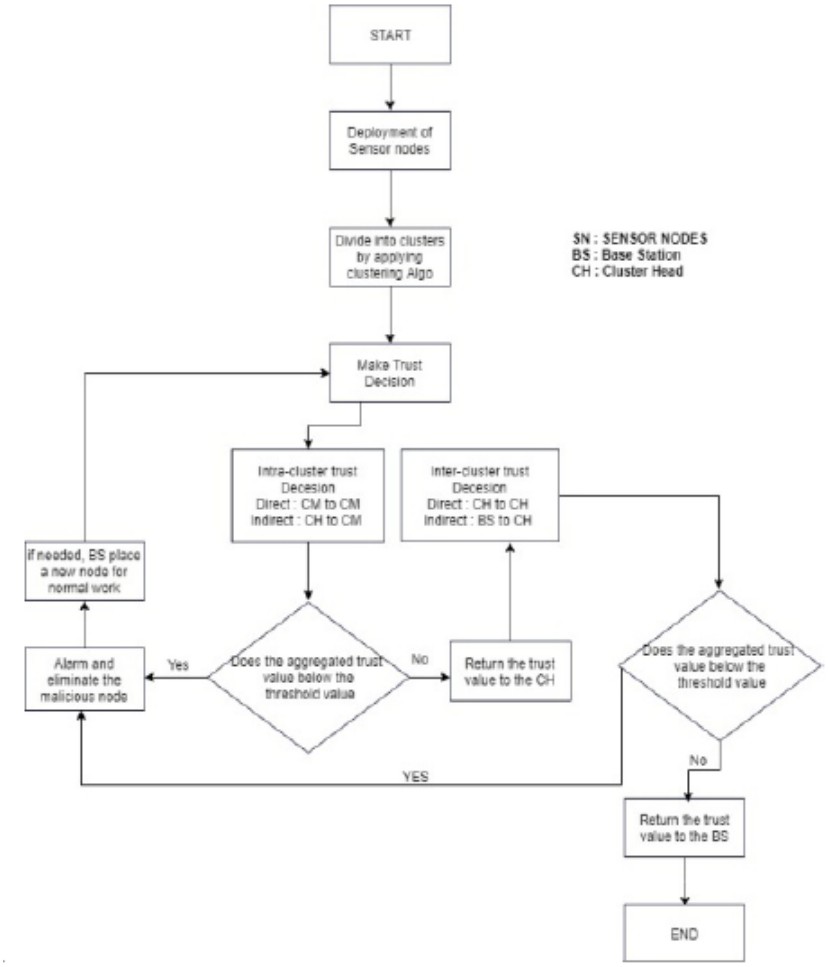

Figure 3.13 – *Flow Chart of (Khan et al. 2019)'s model*

An efficient weighted trust-based malicious node detection (WT-MND) scheme in clustered WSN is presented in (Zawaideh & Salamah 2019). Adopting LEACH protocol, the WT-MND scheme is based on the two main phases of this protocol. The setup phase and the steady-state phase which implicitly implements the WT-MND scheme. The WT-MND scheme is composed of four main components: IT (Indirect Trust) calculation, malicious node isolation, trust-update factor computation, and DT (Direct Trust) updating. In IT calculation, the CH in each cluster calculates the average trust, the weight, and the IT of each Cluster Member i (CMi) based on the transmitted DT values of all other CMs. Next, CH classifies a CM as malicious and isolates if its trust falls below the MAT (minimum acceptable trust). The trust value can be implicitly and adaptively recovered by recalculating the trust-update factor values of the CMs at each round which reflects the realistic behavior of the node. Finally in DT updating, each node updates its TV (Trust Vector) by multiplying its old DT values by the corresponding trust-update factor values. The performance of the developed scheme is assessed over MATLAB simulations considering the DR (Detection Ratio) and MDR for different probabilities P_m of detecting malicious nodes. The WT-MND scheme outperformed the other schemes by achieving a higher DR and a much lower MDR over the range

of Pms and compared to LEACH protocol, the results confirmed that the proposed scheme adds no significant power consumption penalty.

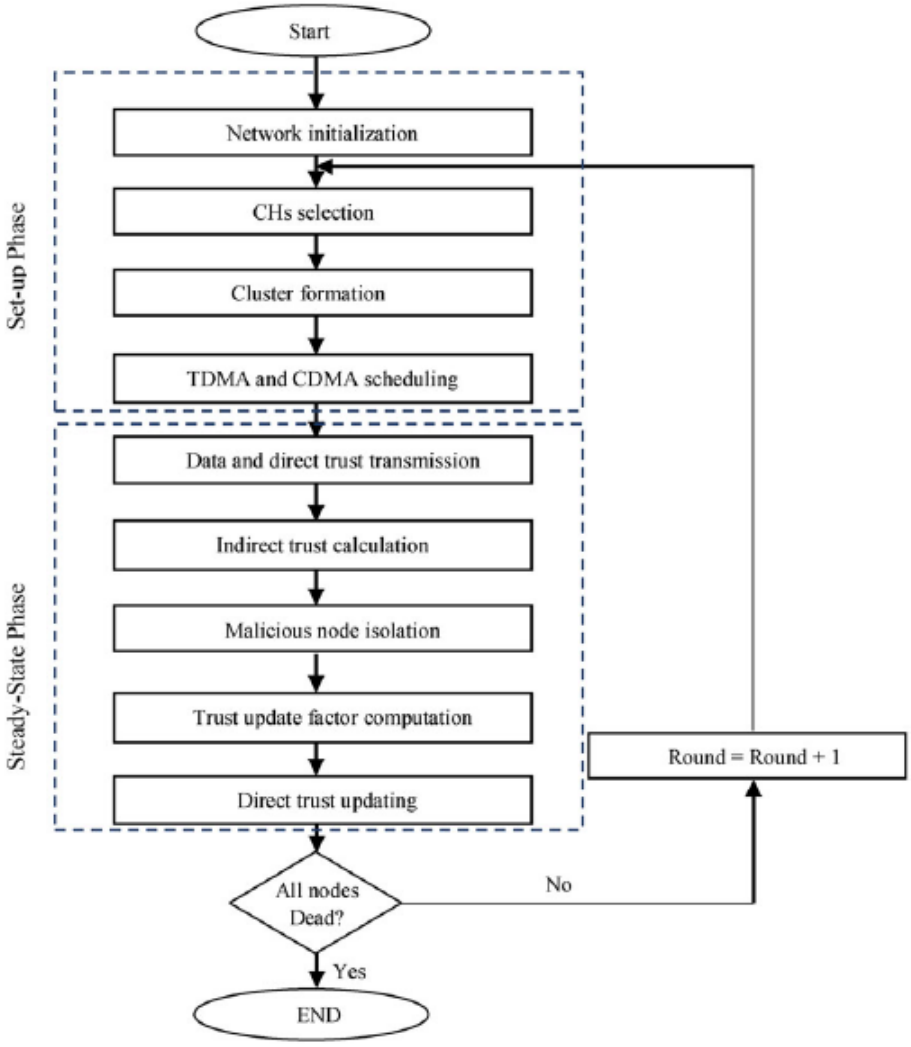

Figure 3.14 – *Functional block diagram of the WT-MND scheme (Zawaideh & Salamah 2019)*

In this research work (Anand & Vasuki 2021) a trust-based DoS attack detection model is proposed to detect selective forwarding and flooding attacks in wireless sensor networks. The proposed detection model consists of three steps: Extraction of network parameters, Monitoring of node behavior and Estimation of reputation and availability factors. In the first step, The following network parameter are extracted: throughput, data rate, packet forwarding rate, energy utilization, and hop count and used to analyze the node status. Direct monitoring and neighborhood monitoring is performed in the second step to estimate the trust factors which helps to detect DOS attacks in the network. The last step considers reputation and availability factors as evaluation parameters to define the node status. Computation of reputation factor includes three steps, namely estimation of trust and instinctive reputation, estimation of trust parameter and malicious grading factor, integration of trust parameter and grading factor. The trust and reputation factors are assessed using a threshold pa-

rameter. The performance of proposed trust-based DoS attack detection in WSN is verified through NS-2.33 simulator in terms of throughput, energy consumption, packet delay, and accuracy. The authors concluded that the proposed model perform better than conventional detection techniques in all aspects.

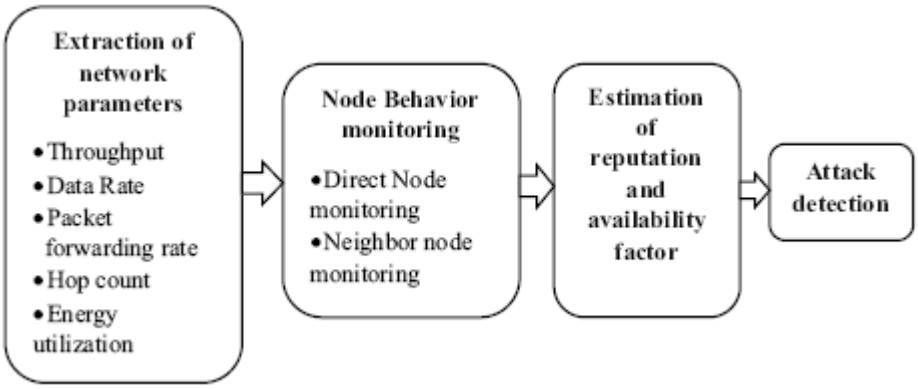

Figure 3.15 – *(Anand & Vasuki 2021)'s Trust based DoS attack detection model*

Game Theory

The authors in (Han *et al.* 2019) proposed an intelligent intrusion detection model based on game theory and an autoregressive model to minimize energy consumption. This model has been developed and improved to a non-cooperative, complete-information, static game model. The main role of the proposed game theory model is to simulate the attack-defense process, to identify the equilibrium solution between the energy consumption and detection efficiency (attacker and IDS) to reach energy saving in the network, and to predict the next targeted cluster and the attack time. The simulation results showed the efficiency of game model in predicting the attack time and the next targeted cluster with energy consumption reduction.

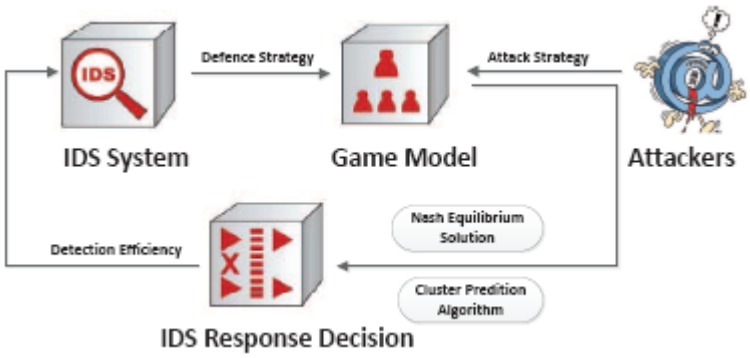

Figure 3.16 – *(Han et al. 2019)'s intrusion detection model based on game theory.*

Statistical model

(Gavel *et al.* 2021) presented a statistical based approach utilizing density estimation for detection the long term anomaly based intrusion in hierarchical WSNs. The proposed approach analyses the intrusion by calculating the PDFs (Probability Density Function) for every two successive pe-

riods of time. The difference values generate time series values which are to be further analyzed using the approximation of Pearson's divergence (PE) i.e. Log Dum Inequality (LSI-D) and Naive Method (NM-D). In addition, the authors proposed a centralized computing approach using an entropy-based method Renyi's Entropy (R-D). To evaluate the proposed scheme, both the distributed as well as centralized computing methods are derived and compared to judge the performance using the real-world dataset from different laboratories i.e. RSS dataset from the University of Michigan [2], AWID wireless networks dataset [3], NSL-KDD dataset [4], and Anomaly based Dataset [5]. The experiment results showed that the performance of LSI-D is much promising than that of the NM-D and R-D, and existing algorithms with low FPR values.

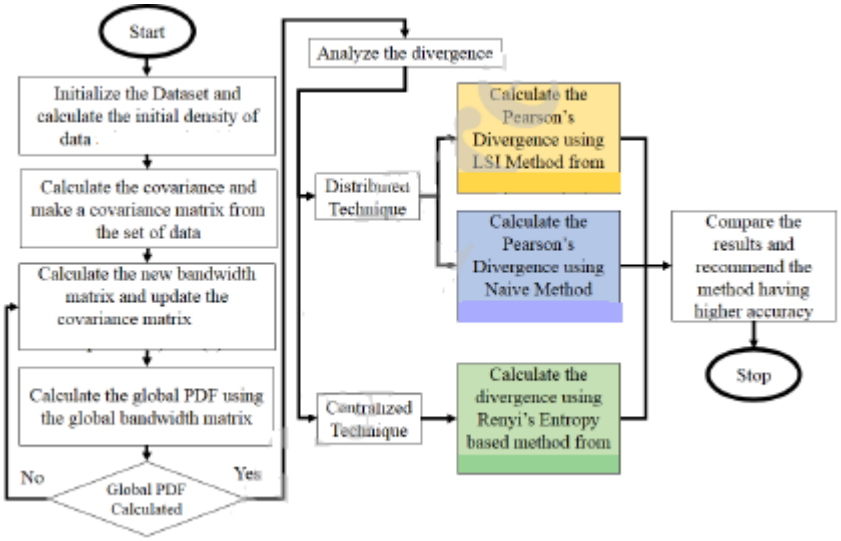

Figure 3.17 – *Workflow of density estimation based IDS (Gavel et al. 2021)*

A Statistical based IDS against Jamming Attacks in Wireless Sensor Networks is proposed in (Osanaiye *et al.* 2018). To detect the different forms of jamming attacks, the proposed approach used packet IAT (Packet inter-arrival time) as the sole metric to distinguish between normal traffic pattern and jamming attack which is well suited to resource constrained sensor nodes and it can be easily measured without introducing complexity and additional overhead to the system. The presented jamming detection technique consists of two phases: training phase and test phase. The first phase involves the capture of normal IAT from legitimate member nodes to the cluster head and also from the cluster heads to the base station to initialize parameters and create the normal profile. The second phase detects a pattern change during a jamming attack using the EWMA algorithm (Exponentially Weighted Moving Average). An alarm is triggered if an attack is detected and the malicious node is removed from the network. EWMA is a statistical monitoring process technique that averages data and continually increases the weight of more recent values of

[2]https://crawdad.org/umich/ rss/20110810/sensor
[3]https://icsdweb.aegean.gr/awid/download-dataset
[4]https://github.com/jmnwong/NSL-KDD-Dataset
[5]https://home.uncg.edu/cmp/downloads/lwsndr.html

the average variable. To assess the proposed work, Trace-driven simulator and CRAWDAD [6] dataset are used. Results obtained showed that the proposed solution can efficiently and accurately detect jamming attacks in WSNs with little or no overhead.

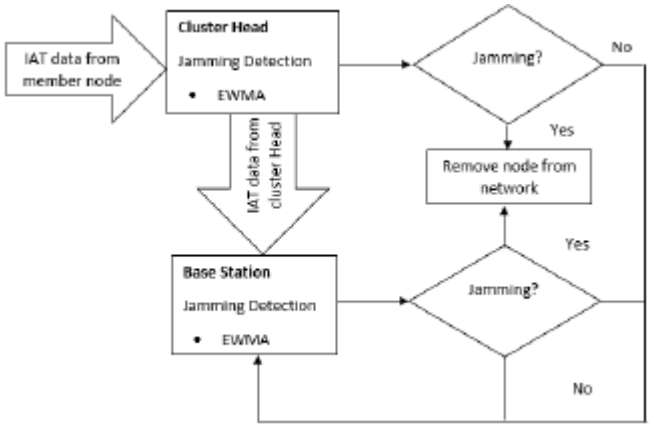

Figure 3.18 – *EWMA DoS jamming detection framework in WSN (Osanaiye et al. 2018).*

(Ioannou & Vassiliou 2018) presented mIDS, an anomaly detection system based on Binary Logistic Regression (BLR) to detect Selective Forward and Blackhole routing attacks in constrained WSNs. BLR is a statistical analysis tool that defines the nature of sensor activity using both malicious and benign activity. mIDS is constituted in two phases: the training and the evaluation phase. The training phase generates a regression model based on the most significant independent variables identifying the malicious activity extracted from the routing network layer of each constrained node. The evaluation phase implements and installs the generated model at each constrained node to be tested in real-time. The proposed mIDS is evaluated using the COOJA simulator, that runs real sensor code, achieving accuracy levels within the range 96% - 100%.

3.4.2 Misuse based IDS

(Mohapatra *et al.* 2020) proposed a Man In The Middle-Intrusion Detection System (MITM-IDS) to detect and isolate attack, and reconfigure the attacked nodes. In the proposed MITM-IDS, the attacker is getting monitored based on signature-ID templates. The Deep Learning (DL) approach is used to generate a refined signatures-based classification rules to detect the abnormal activities. The DL based MITM-IDS analyzes the network by applying intelligent refined signature rules. The MITM-IDS model use a Centralized Database Vetwork (CDN) which contains the entire IDS for constrained WSN setup. The proposed model is validated by considering two factors: throughput and packet loss.The simulation results showed the performance of MITM-IDS in comparison to the non-security environment.

[6] http://crawdad.org/uportorwthaachen/vanetjamming2012

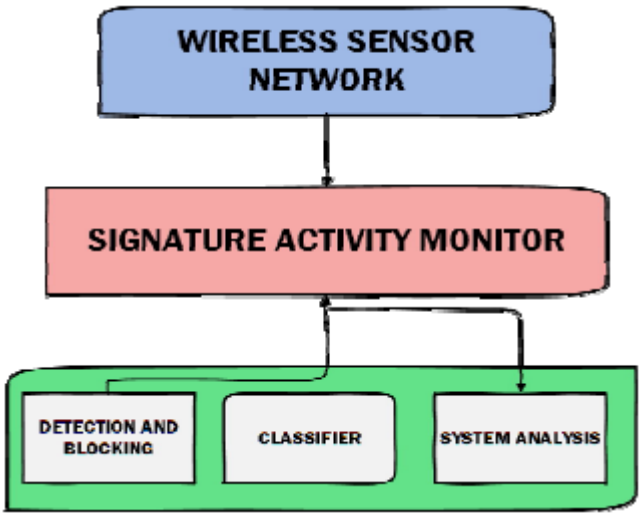

Figure 3.19 – *Architecture of MITM-IDS (Mohapatra et al. 2020)*

A fuzzy rule-based system to avert intrusion is proposed in (Singh *et al.* 2020b). The proposed system works in three phases: feature selection, membership value computation and fuzzified rule applicator to avert malicious nodes. The objective of feature selection is to pick the most significant features for classification procedure from the actual larger set. Membership function represents the value of truth indicated by value 0-1 (degree of membership) and the proposed FzMAI (Fuzzifed Methodology to Avert Intrusion) uses six membership functions as input. Fuzzy rule applicator apply fuzzy rules on the model to get the categorization of nodes as Red: malicious nodes (do not allow malicious nodes to enter the network), Orange: suspicious nodes (marks the node) and Green: normal nodes (it is safe to enter the network). The proposed system is analyzed on the WSNDS dataset (Almomani *et al.* 2016). The authors concluded that FzMAI outperforms all the other considered fuzzy rule-based systems and the system solve the problem of intrusion prevention with low cost intrusion detection.

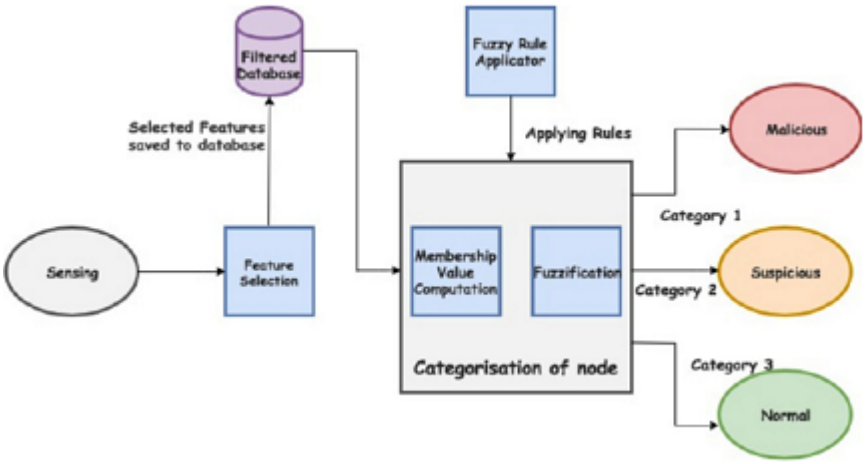

Figure 3.20 – *(Singh et al. 2020b)'s The FzMAI model*

(Lu *et al.* 2018) proposed an intrusion detection system based on evolving class association rules as a security solution for smart human care services. To improve the quality and the diversity of the rules, a new class

association rule selection method is proposed based on Jaccard distance during Genetic Network Programming (GNP) evolution. The benchmark data set NSL-KDD was used to verify the validity of the proposed method.

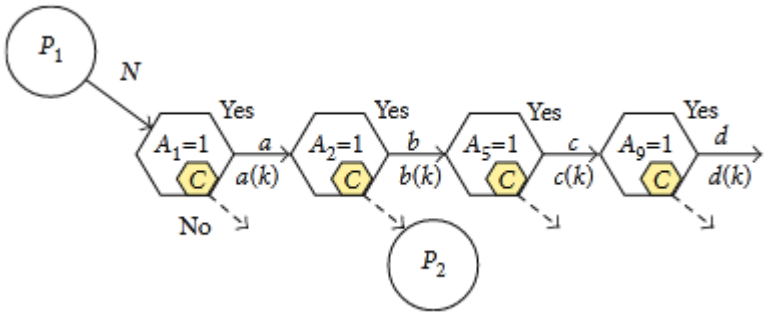

Figure 3.21 – *Class association rule mining based on GNP in (Lu et al. 2018)*

(Kalnoor & Agarkhed 2018) presented the KMP pattern matching based IDS for intruder detection. The KMP pattern matching algorithm is used for string matching and the KMP matcher has with string 'S', pattern 'p' and prefix $\prod$ considered as inputs. In pattern matching process, pattern algorithm is used to match from low level appearance probability to high level appearance probability of letters in the string pattern. The intruder is detected when KMP pattern matching algorithm doesn't match the correct characters. Otherwise it gives an alert message to the administrator. The proposed system considers three attacks: SYN flood attack, smurf Attack and land attack. The parameters considered are Packet Delivery Ratio (PDR) and throughput.

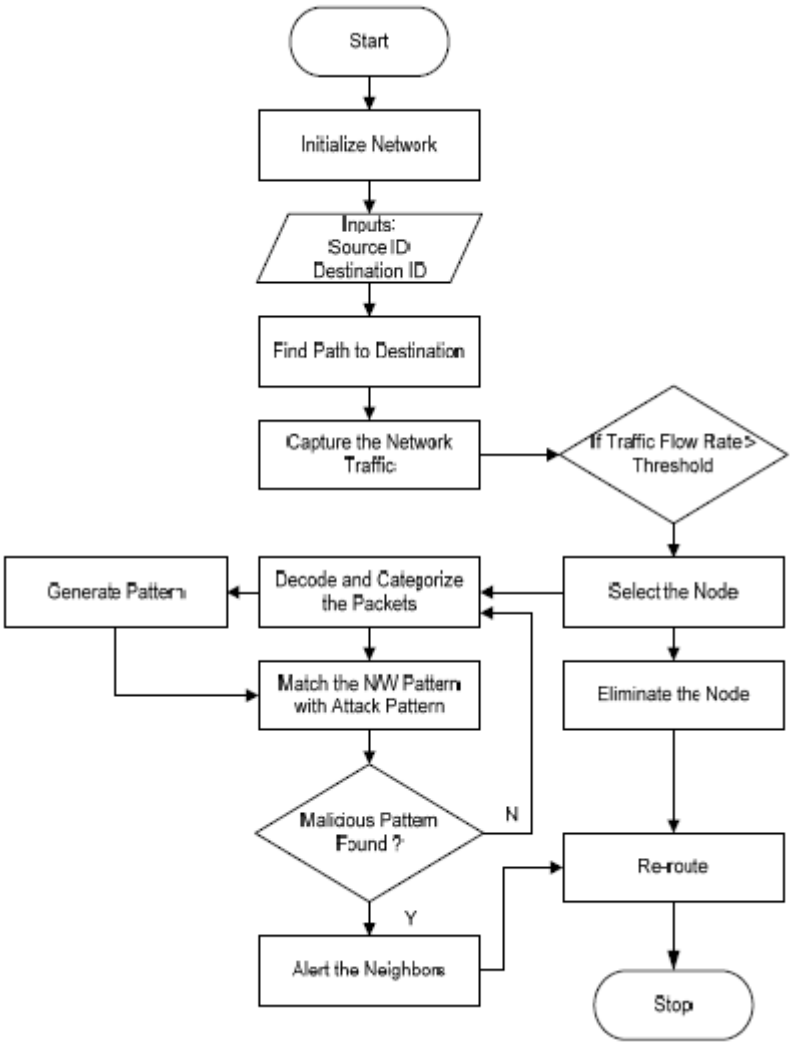

Figure 3.22 – *Flow Chart for (Kalnoor & Agarkhed 2018)'s Intrusion Detection System*

3.4.3 Specification based IDS

A secured AODV protocol against Black-Hole attacks on WSNs is presented in (Fute *et al.* 2020) called Observed AODV (OAODV). OAODV is an intrusion detection system consisting of observer nodes whose role is to monitor, analyze data traffic and generate reports on the errors encountered and it is able to anticipate intruder detection during the route discovery phase. The architecture of the proposed IDS comprises two components: Observer agents and Cluster head. The firsts are responsible for monitoring data flows in their neighborhoods and analysis in order to identify inconsistencies and to detect suspicious behavior of their neighbors. the seconds, coordinate between the observer agents. An observer agent consists of three modules: The first is a probe which captures the packets passing in the neighborhood. The second module is the packet analyzer, it extracts and checks whether packet stamps collected by the probe module comply with the protocol specifications contained in its table of rules or while they are routed correctly. The third module is the report generator responsible for announcing the presence of an intruder in the network and to order its insulation. To evaluate the effectiveness of

the proposed IDS, NS2.35 simulator was used and the following metrics was considered: The packet delivery ratio (PDR), Throughput and End-to-end delay.

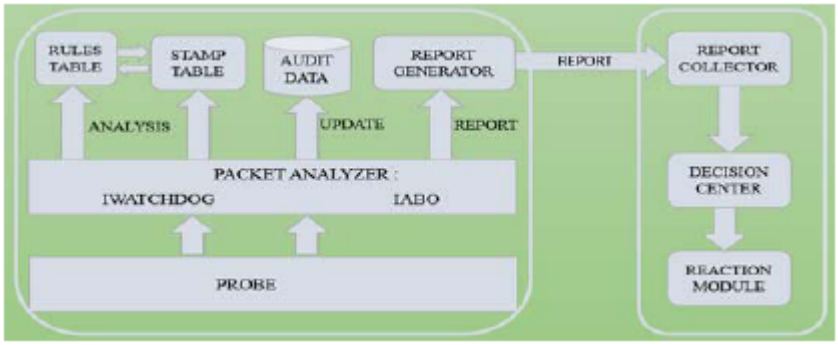

Figure 3.23 – *Intrusion detection based OAODV (Fute et al. 2020)*

(Sadeghizadeh & Marouzi 2018) proposed a specification based lightweight Intrusion Detection System to protect WSNs against the most important of routing protocol attacks. The specifications of the attacks are extracted based on the analysis of the behavior of each type of attack and their operation. The main specification rules are based on the two metrics: Interval between Received Packets (IRP) and Received Signal Strength Indicator (RSSI). The proposed method is organized at two levels of the common nodes (first level) and cluster-head nodes (second level). At the first level, the different specification rules are tested by every node for detecting routing attacks and in case of abnormal activity, the cluster-head is informed for more analysis. At the second level, if the received alarms exceed the defined threshold, the cluster-heads identifies them as attacks, updates thus the list of malicious nodes and sends this list to all member nodes. The threshold Alarm is determined at the beginning of the network based on the degree of neighborhood. In simulations, both static and dynamic clustering is used and the authors concludes that the proposed system is an effective and lightweight IDS in which the performance of the network can be kept in the optimum level.

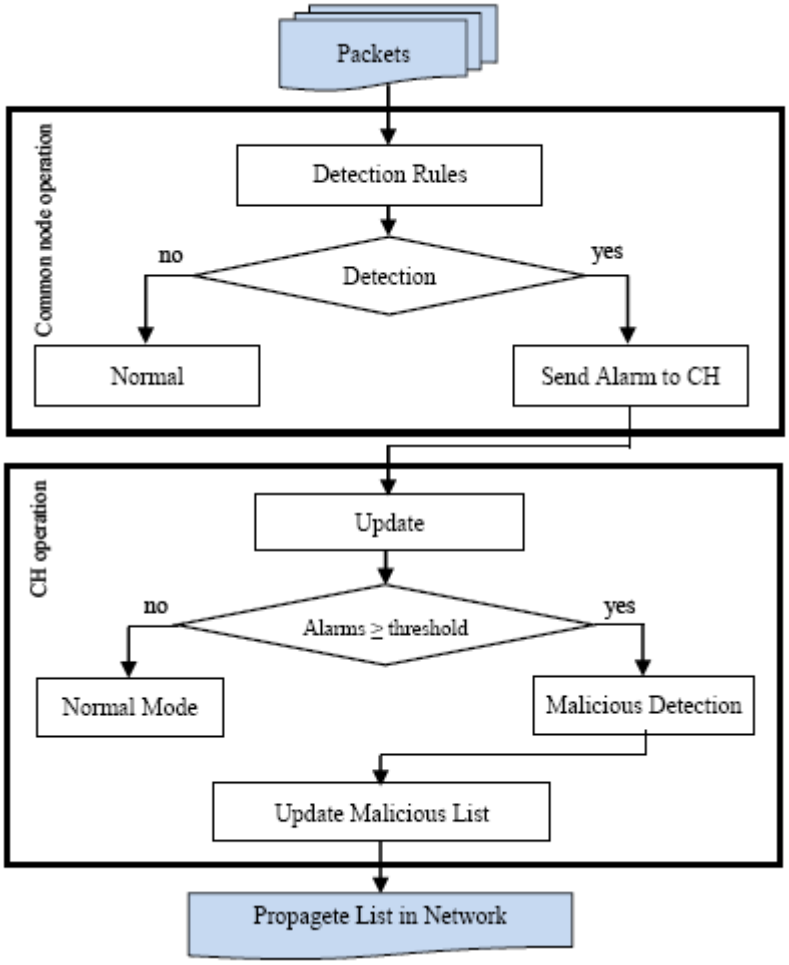

Figure 3.24 – *(Sadeghizadeh & Marouzi 2018)'s Specification based lightweight IDS*

(Bayou *et al.* 2017) presented wIDS a multilayer specification-based Intrusion Detection System for securing Wireless Industrial Sensor Networks (WISN). wIDS has a two-level detection architecture composed of central-IDS agent and several IDS-agents. The central IDS-agent is implemented in the sink of the WISN. It is responsible for monitoring communications, routing tables and transmission scheduling consistency, and global coordination between IDS-agents. Whereas, IDS-agents are implemented in selected sensor nodes to control local communications and all exchanged packets in their neighborhood to check the compliance of each action performed by a sensor node towards the formal model of the expected normal behavior. A wirelessOrBAC extension of OrBAC (Kalam *et al.* 2003) is developed and used to efficiently model WSN-specifications. This extension defines rules of the normal behavior of the expected node to express authorized actions at each protocol layer. In addition, for alerts that are raised by actions deviating from the normal model, the authors defined additional intrusion rules that aim to detect basic attacker actions, such as injecting, deleting, modifying and delaying packets. To evaluate wIDS performances, WirelessHART NetSIM is used and simulation results reported 100% correct identification of attacks.

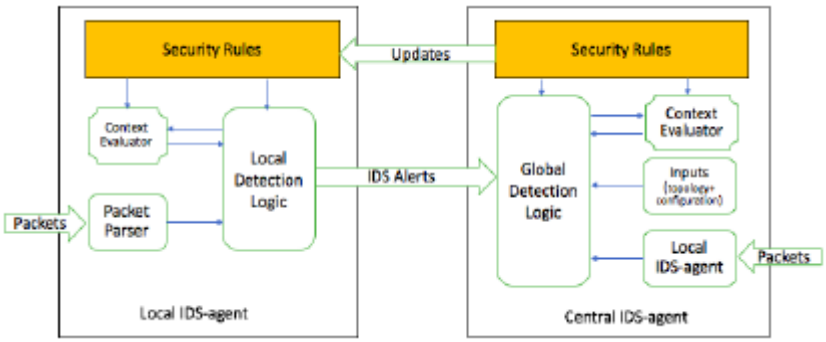

Figure 3.25 – *wIDS a multilayer specification-based IDS (Bayou et al. 2017)*

3.4.4 Hybrid based IDS

A tissue growing procedures based on human immune Biology is presented in (Umarani & Kannan 2021) for hybrid anomaly/misuse detection in WSNs. In the anomaly procedure and for prediction of anomaly presence, a communication network model composed of multiple number of cells and designed with the help of Artificial Immune Systems (AIS) is performed based on effective node aggregation. In the misuse detection, the identification procedure detects the intruder cells (multiple attacks) in the network. The simulation results showed that when both anomaly and misuse detection techniques are combined together, it provides a effective Intrusion detection system.

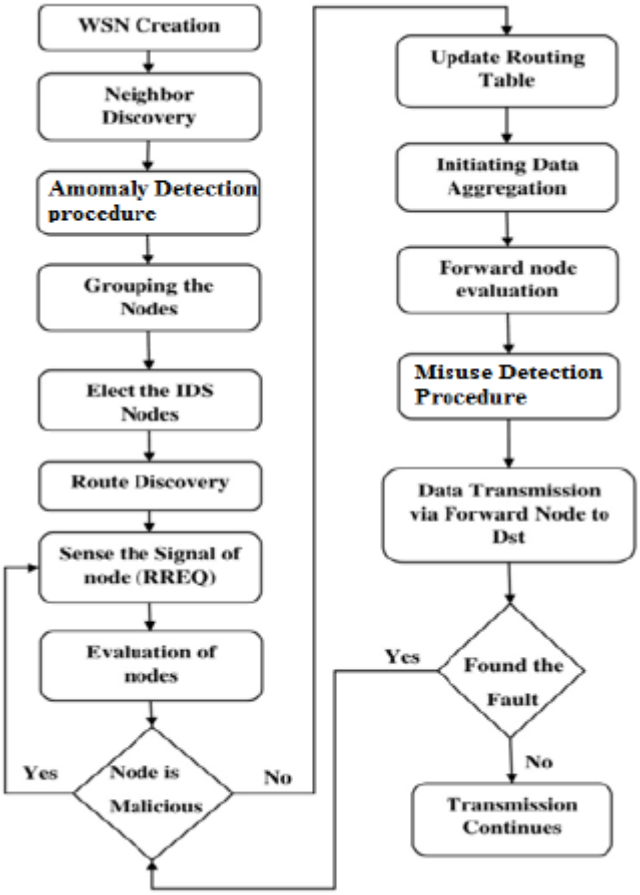

Figure 3.26 – *Synthesis of anomaly and misuse detection procedure in (Umarani & Kannan 2021)*

(Boni *et al.* 2020) introduced a new hybrid-based intrusion detection system (IDS) capable of ensuring a perfect security scheme for WSNs inside a smart environment. The proposed IDS is an electronic device, a sensor with high energy resource and memory storage, assuring the computational tasks of all sensors and filtering all incoming and outgoing communication in the network and this is done based on the watchdog approach. The IDS architecture is centered on three (3) functional modules: an energy module, a detection module, and a communication module. The IDS also introduces the concept of the feedback signal and "trust table" used to launch the detection and isolation procedure in case of attacks. The "trust table" is created during the deployment of the network to maintain a certain trust level in the environment and the feedback signal is an alert that is sent to the sensors with specific instruction. To ensure the entire network security, the authors suggested the deployment of several of the proposed IDSs (scaler distribution) working jointly and adopting cryptographic encryption techniques for communications.

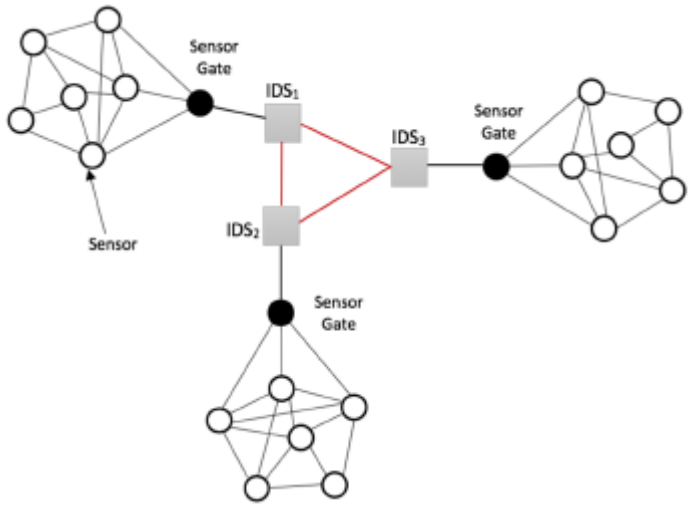

Figure 3.27 – *An overview of the IDS intercommunication hierarchy in a smart environment (Boni et al. 2020)*

An hybrid approach of watchdog and RTT (Round Trip Time) through Energy Efficient Ad hoc on demand Multipath Distance Vector (EE-AOMDV) protocol against Wormhole attack is presented in (Gnanapriya & Ramya 2020). EE-AOMDV protocol permits making multipath between source to destination and for Energy Efficiency, it checks the Energy/Distance proportion of every way accessible in the system, and it selects the optimal path between source and destination. To recognize Wormhole attack, a half and half methodology is used that is a mix of guard dog and RTT. Through this methodology, Wormhole assailants is precisely and productively distinguished and avoided for further transaction. Furthermore, to accomplish the security guaranteeing a lightweight cryptography calculation is used through MD5 to protect data from other forms of attack.

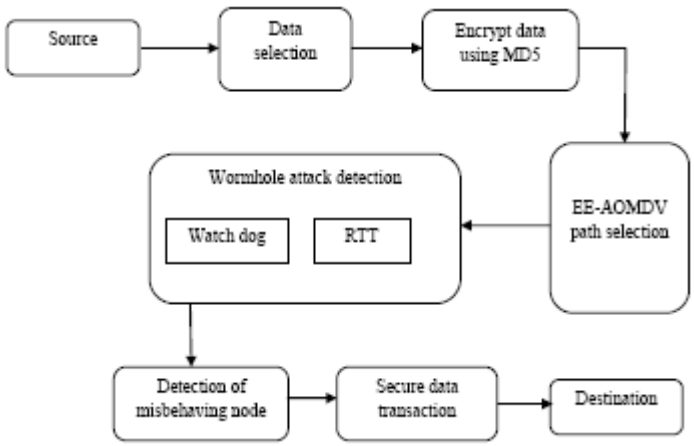

Figure 3.28 – *Working flow of (Gnanapriya & Ramya 2020)'s system*

The following table 3.1 recapitulates the presented Works according to several parameters.

N S: Not Specified

Authors	Detection technique	Methodology	Detection Architecture	Attack	Detection Rate (%)	Energy Saving	Data Set	Simulator
Otoum et al.2019	Anomaly	Machine Learning (Supervised)	Hierarchical	DOS, R2L, U2R et Probe	99.12%	NC	KDD'99	NS-3
Zhang et al.2020	Anomaly	Machine Learning (Supervised)	Hierarchical	DOS, R2L, U2R et Probe	99.12 %(Normal) 98.03% (DOS) 95.74 %(Probe) 76.15% (R2L) 50.00% (U2R)	Yes	NSL-KDD	Matlab
Zhang et al.2021	Anomaly	Machine Learning (Supervised)	Distributed & Cooperative	DOS, R2L, U2R et Probe	98.2%	Yes	KDD'99	Matlab
Li et al.2018	Anomaly	Machine Learning (Semi-Super)	Distributed & Cooperative	DOS, R2L, U2R et Probe	96.5% (Probe) 31.7% (DOS) 90.3% (R2L) 84.8% (U2R)	No	KDD'99	Matlab
Qu et al.2018	Anomaly	Machine Learning (Unsupervised)	Distributed & Cooperative	Black hole Flooding Rushing attack Multiple attacks	Simulation 97.9% ±0.2% Real env 96.5% ±0.38%	No	Simulated attacks + NSLKDD	QualNet + Real WSN
Nivaashini& Thangaraj2018	Anomaly	Machine Learning (Hybrid)	N S	DOS, R2L, U2R et Probe		No	Enriched KDD'99	Weka

Continued

Table 3.1 – *Existing IDS approaches*

Authors	Detection Technique	Methodology	Detection Architecture	Attack	Detection Rate (%)	Energy Saving	Data Set	Simulator
Alaparthy & Morgera2019	Anomaly	Bio-inspired	Distributed & Cooperative	Blackhole, DDOS, Wormhole, Selective forwarding	N S	Yes	Simulated attacks	
Hasan et al.2021	Anomaly	Bio-inspired	Distributed & Cooperative	N S	N S	Yes	Simulated attacks	Matlab
Raghav et al.2020	Anomaly	Bio-inspired	Hierarchical	Flooding, Spoofing and Sybil attacks	N S	Yes	Simulated attacks	Matlab
Borkara et al.2019	Anomaly	Bio-inspired	Hierarchical	DOS, R2L, U2R et Probe	83%	Yes	KDD'99	Python platform
Khan et al.2019	Anomaly	Trust	Distributed & Cooperative	Garnished, Bad mouthing, Blackhole, Greyhole and Ballot stuffing attacks	N S	Yes	Simulated attacks	Matlab
Zawaideh Salamah2019	Anomaly	Trust	Hierarchical	Malicious nodes	99.4% - 98.2%	Yes	Simulated malicious behavior	Matlab
Anand & Vasuki2021	Anomaly	Trust	Distributed & Cooperative	Selective forwarding & Flooding attack	95%	Yes	Simulated attacks	NS-2

Continued

Table 3.1 – *Existing IDS approaches*

Authors	Detection Technique	Methodology	Detection Architecture	Attack	Detection Rate (%)	Energy Saving	Data Set	Simulator
Han et al.2019	Anomaly	Game Theory	Hierarchical	Malicious node	75%	Yes	Simulated malicious behavior	Matlab
Gavel et al.2020	Anomaly	Statistical	Hierarchical	Datasets converted into Normal and Attacks Class	95% (RSS) 97.24 % (AWID) 95.7% (NSLKDD) 99.95% (AD)	No	RSS, AWID, NSL-KDD & Anomaly based Dataset (AD)	NS
Osanaiye et al.2018	Anomaly	Statistical	Hierarchical	Jamming	For *geqslant*20 jammed packets: 100%	Yes	CRAWDAD	Trace-driven
Ioannou & Vassiliou2018	Anomaly	Statistical	StandAlone	Selective Forward & Blackhole attacks	96% - 100%	Yes	Simulated attacks	Cooja
Mohapatra et al.2020	Misuse	Deep Learning	Distributed	Man In The Middle	N S	No	Simulated attacks	RMatlab
Singh et al.2020	Misuse	Fuzzy-rule	N S	Blackhole, Grayhole, Scheduling and TDMA attacks	98.29%	Yes	WSN-DS	Matlab

Continued

Table 3.1 – *Existing IDS approaches*

Authors	Detection Technique	Methodology	Detection Architecture	Attack	Detection Rate (%)	Energy Saving	Data Set	Simulator
Lu et al.2018	Misuse	Genetic Network Programming	N S	Probe, DOS, R2L et U2R	87.58%,	No	NSL-KDD	N S
Kalnoor & Agarkhed2018	Misuse	Pattern matching	StandAlone	SYN flood, Smurf and Land attacks	N S	No	Simulated attacks	N S
Fute et al.2020	Specif	Protocole specif	Mobile agent	Blackhole attacks	N S	No	Simulated attacks	NS-2
Sadeghizadeh & Marouzi2018	Specif	Attack characteristics	Hierarchical	DOS, Hello flood, Sinkhole, Select Forwarding, Sybil attacks	96.2%	Yes	Simulated routing attacks	NS-2
Bayou et al.2017	Specif	Multi-Layer	Mobile agent	DOS, Jamming, Sinkhole, Blackhole, Hello Flood, Selective forwarding, and Forced delay attacks	100%	No	Simulated attacks	Wireless HART NetSIM
Umarani & Kannan2021	Hybrid	Anomaly/ Misuse	Hierarchical	Attacks	N S	Yes	Simulated attacks	NS-2

Continued

Table 3.1 – *Existing IDS approaches*

Authors	**Detection Technique**	**Methodology**	**Detection Architecture**	**Attack**	**Detection Rate (%)**	**Energy Saving**	**Data Set**	**Simulator**
Boni et al.2020	Hybrid	Anomaly/ misuse	Mobile agent	All WSN-attacks	Entire network security	Yes	N S	N S
Gnanapriya & Ramya2020	Hybrid	Anomaly/ specification	Mobile agent	Wormhole attack	N S	Yes	Simulated attack	NS-2

3.5 Dataset for Intrusion Detection Systems

All the works presented in the section above have in common that they require representative network-based datasets. The benchmark datasets are a good basis to train, evaluate and compare the quality of different network intrusion detection systems developed for a given network. The lack of representative publicly available datasets constitutes one of the biggest challenges for anomaly based intrusion detection (Ring *et al.* 2019). The scientist community is working on this problem as several intrusion detection datasets have been published over the last years (Moustafa & Slay 2015) (Ring *et al.* 2017) (Sharafaldin *et al.* 2018) (Sharma *et al.* 2018). However, there is no overall index of existing datasets and it is hard to keep track of the latest developments.

The paper (Ring *et al.* 2019) provides a literature survey of existing network based intrusion detection datasets. The work focuses on attack scenarios within datasets and highlights relations between the datasets. Furthermore, the authors have established a collection of dataset properties as a basis for comparing available datasets and for identifying suitable datasets, given specific evaluation scenarios. A website [7] was created which references to all mentioned datasets and data repositories with update.

Despite all these datasets, there are unfortunately no datasets dedicated to intrusion detection in WSN. According to literature search, the most notable observation was that most of researches implement their own attack scenarios to generate the necessary datasets for machine learning algorithms, and evaluate the performances of the proposed solutions either on simulation tools as NS2, NS3, Omnet++ or on real sensors. So, we conclude that there is no common WSN dataset or benchmark datasets generated from attacks implementations on simulated or real-world WSNs for studying normal and abnormal behaviors, detecting the possible attacks and comparing the performances of different proposed IDSs in literature. However, the first intrusion detection dataset was presented in (Garofalo *et al.* 2013) where a collection of WSN routing data under sinkhole attack was given and made available.

In this first contribution four(04) hours of simulated data through NS3 are collected for 20 nodes and one of these nodes is supposed compromised. The attacked routing protocol is AODV. To validate the collected dataset in detection of sinkhole attack a decision tree (DT) technique based central agent was performed. The generated dataset is given in PCAP format files and is available online on the research group website[8]. A second contribution was presented by (Almomani *et al.* 2016). Four types of DOS attacks in LEACH protocol was implemented in the constructed dataset: blackhole, grayhole, flooding, and scheduling attacks. The dataset was collected from NS2 and then processed to produce 23 features. The collected dataset is

[7] https://www.informatik.uni-wuerzburg.de/datascience/datasets/nids-ds/
[8] http://fitnesslab.altervista.org/index.php/it/?option=comcontent&view=article&id=71

called WSN-DS. Neural network (ANN) was applied to test the constructed dataset and measure its accuracy in detecting and classifying four types of DOS attacks. The well-known KDD intrusion detection dataset (KDDCup'99)[9], developed by MIT Lincolnlab in 1998, is considered in many researches for anomaly, signature and hybrid based IDS in WSN (Zhang *et al.* 2020)(Zhang *et al.* 2021)(Li *et al.* 2018)(Borkar *et al.* 2019).

However,this benchmark dataset is constructed for local area network and not for wireless networks or WSN in particular. Because of the absence of a real sample of the dataset for intrusion detection in WSNs, the KDDCup'99 dataset is used as the sample to evaluate the performance of IDSs in these networks.

The present work focuses on Sinkhole attack detection in AODV protocol. So the (Garofalo *et al.* 2013) dataset is used to evaluate and compare the efficiency of our IDSs to their proposed Decision Tree IDS. The choice of dataset is based on the fact that we work on the same considerations. Effectively, we test intrusion detection capabilities of a IDS against the same cyber attack (Sinkhole Attack), on the same routing protocol and using the same simulation tool NS3.

3.6 Performance Metrics for IDS in WSN

There are evaluation metrics for intrusion detection systems for conventional wired and wireless networks. However, the first attempt that has extended the "conventional" metrics to ones used for evaluation of highly distributed IDSs in WSNs is presented in (Stetsko & Matyas 2009). (Singh 2017) describe a set of 34 metrics that are relevant to IDS for WSN and can be used for its evaluation, unfortunately without defined formula. (Godala & Vaddella 2020) present three (03) performance metrics used to assess the IDS algorithm for WSNs. The main interest of performance metrics is to help designers in designing efficient intrusion detection systems for WSN and to help administrators to choose the best IDS from a set of systems or to optimize a configuration of the IDS according to network topology, sensor nodes capabilities and expected types of attack.

Performance of intrusion detection algorithm can be analyzed by using several measures. (Stetsko & Matyas 2009) divided the measures or metrics into two groups. The first group defines metrics for detection techniques without a response mechanism called metrics of detection. The proposed metrics are Number of False Negatives, Number of False Positives, Memory Usage, Software Complexity, Communication Complexity and Energy Usage. Whereas the second group defines metrics for detection techniques together with a response mechanism called metrics of attack impact. Based on Table 3.2 which summarize the impacts of some attacks in WSN, metrics of attack impact are measured during a period of time of duration and are defined as follows: Number of Lost Packets, Number of Modified Packets, Energy Usage, Average Length of The

[9]http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

Attack / Impact	Packet dropping	Packet delay	Packet modification	Network lifetime
Selective forwarding	X	X		X
Packet alternation	X	X	X	X
Jamming	X	X		X
Sinkhole		X		X

Table 3.2 – *Impact of different attacks (Stetsko & Matyas 2009)*

Shortest Paths, Number of Isolated Nodes and Number of Affected Flows.

In the other hand, (Khraisat *et al.* 2020) represent confusion matrix as evaluation metric and (Godala & Vaddella 2020) add two (02) more measures: Receiver operating curves and Precision-Recall curve. The following section details these metrics.

3.6.1 Confusion matrix

Confusion matrix is a very useful measure to calculate the performance of an IDS. Since intrusion detection in WSN is considered as binary classification problem, the IDS is commonly represented using 2x2 confusion matrix where intrusion is treated as Positive and normal flow is treated as negative as shown in table 3.3.

		Predicted Class	
		Normal	**Intrusion**
Actual Class	**Normal**	True Negative (TN)	False Positive (FP)
	Intrusion	False Negative (FN)	True Positive (TP)

Table 3.3 – *Confusion matrix for IDS evaluation.*

Usually, Effectiveness of the IDS is assessed based on the following Confusion matrix measurement:

1. True Positive Rate (TPR): Represents the ratio between the number of correctly predicted attacks and the overall number attacks. If all intrusions are detected then the TPR is 1 which is extremely rare for an IDS. TPR is also called Detection Rate (DR), Sensitivity or Recall, and can be expressed mathematically as (Equation 3.1):

$$TPR = \frac{TP}{TP + FN} \tag{3.1}$$

2. True Negative Rate (TNR): Also called as specificity and selectivity. TNR defines the percentage of actual normal cases identified correctly and is represented in Equation 3.2.

$$TNR = \frac{TN}{TN + FP} \tag{3.2}$$

3. False Positive Rate (FPR): It represents the percentage of normal flows that are detected as intrusion (false alarm). FPR is defined as (Equation 3.3):

$$FPR = \frac{FP}{FP + TN} \tag{3.3}$$

4. False Negative Rate (FNR): It represents the percentage of actual intrusions predicted as normal flows. FNR shows that the intrusion detection system could not identify the intrusions and is calculated as (Equation 3.4):

$$FNR = \frac{FN}{FN + TP} \tag{3.4}$$

5. Detection accuracy (DA) or Classification Rate (CR): it defines the accuracy of IDS in detecting normal and intrusion flows correctly and is calculated using Equation 3.5

$$DA = \frac{TP + TN}{TP + TN + FP + FN} \tag{3.5}$$

6. Precision (P): It is the percentage of True Positives (TP) instances divided by sum of the positive predictions (TP) and (FP) instances. Equation 3.6 represents the formula for calculating P.

$$P = \frac{TP}{TP + FP} \tag{3.6}$$

7. F1-score or F-measure (FM): It is the harmonic mean of Precision and Recall i.e. represented in Equation 3.7. FM is favored to check effectiveness of IDS when model uses unbalanced input dataset more than to the accuracy or when only one accuracy metric is needed as an evaluation measurement.

$$FM = \frac{2 * Precision * Recall}{Precision * Recall} \tag{3.7}$$

Other metrics can be found based confusion matrix as Geometric mean and Geometric Mean Accuracy Index (GMAI). An efficient IDS is qualified by high Detection accuracy, TPR, TNR, FM and low false alarm rate and FNR.

3.6.2 Receiver Operating Curves (ROC)

To draw a ROC curve, only the true positive rate (TPR) and false positive rate (FPR) are needed as x and y axes, respectively. The ROC graph depicts relative trade-offs between true positive (benefits) and false positive (costs). All points in the ROC space define the detection accuracy of the IDS model.

In figure 3.29, the random guess line or diagonal represents the minimum prediction line. Points above the diagonal represent good detection results (better than random); points below the line represent bad results (worse than random). The (0,1) point is called a perfect classification or 100% accuracy. The Figure 7, shows that the model in the blue line gives high-quality detection results than the green line.

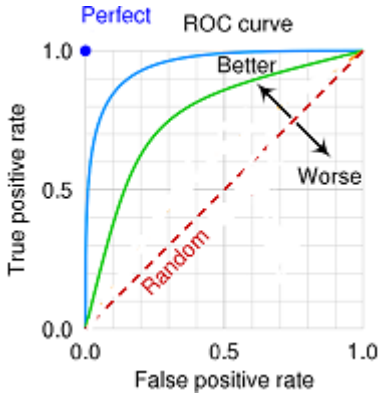

Figure 3.29 – *ROC curve example*

3.6.3 Precision-Recall Curve (PR curve)

Precision-Recall is a useful measure of success of detection when IDS uses very imbalanced dataset. The precision-recall curve shows the trade-off between precision (Y-axis) and recall (X-axis) for different threshold. A high area under the curve shows that the IDS algorithm gives good results, where high precision relates to a low false positive rate, and high recall relates to a low false negative rate. Figure 3.30 shows a simple PR curve where Algorithm 1 gives the best results compared to the Algorithm 2.

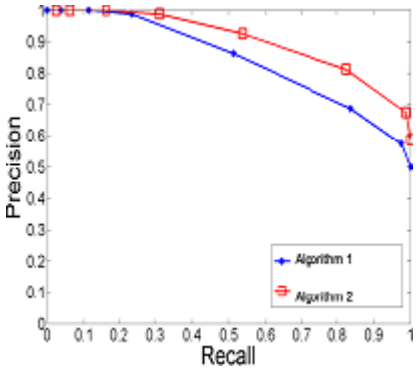

Figure 3.30 – *PR curve example*

3.7 Some open research in IDS

After introducing the basic concepts related to intrusion detection system, we have presented an overview of the various existing IDS in WSN and compared between the different approaches. On the basis of theses outcomes and findings, we identify the following potential research directions for IDS to become more efficient and more appropriate to WSN constraints (Kaur & Rattan 2021) (Godala & Vaddella 2020) (Ghosal & Halder 2017):

1. **Resource Consumption**

   The traditional IDSs solutions are not suitable to WSNs due to their high degree of resource consumption (Storage, Processing and Energy). In fact, Mismanagement of resources in WSN can hinder the proper functioning of the network and considerably decrease its lifetime. An efficient resource consumption IDS can be achieved in different ways.

   Most of proposed IDS solutions for WSN are based on Classification techniques which need time to build a classification model by training and testing data and also require a sufficient memory space to deploy model in sensor nodes. Hence, Developing a compact classification model help to reduce memory space of deployed model.

   The implementation cost of IDS can be saved according to the effects of attacks on energy consumption. Indeed, different attack scenarios in WSN can have different effects on energy consumption. Consequently, the level of intrusion detection to develop will be based on the attack which network is exposed to, which provide an optimal solution .

   Also, Energy efficient IDS can be achieved while deploying the nodes in the network as reconfiguring the nodes later on when the network is running can result in overheads.

2. **Detection Mechanism**

   The choice of the detection mechanism of the attacks influences the final performances of the monitoring system particularly and the security system globally. Most of the IDS for WSN are rule based, their performance is highly dependent on the decision rules designed by the researchers. These rule based systems have the capability to reduce false-positive alarm rate but not adaptive for novel attacks and dynamic changing environment that needs regular updating and time.

   For use of classification approaches, the main drawback is the use of dataset. Those data set were having a number of features to train the systems. This makes network system more complex utilizes excess sensor's resources.

3. **Cross-Layer IDS**

   The maximum number of proposed IDSs are against a specific type of attack, or a set of attacks focused about specific layer of the WSN,

considered as single layer IDSs. So, it is essential to develop Cross-Layer IDS that can detect the different attacks which may occur in different layers of WSN. Using a cross layer IDS, it could not only pass information between layers but also coordinate mechanisms to prevent threats at all layers. Energy saving Cross-Layer IDS is another vital area of future work in WSNs.

4. **Intrusion Dataset**

   From the literature, there is no benchmark dataset specifically for intrusion detection in WSN. So, there is a requirement to develop labeled dataset for WSN to perform training and testing of classification model about the attacks.

Conclusion

Because of the resource constraints of the nodes in such networks, IDS implementations in sensor networks is presently in a premature stage and have not achieved complete automation till date. However, as new technologies emerge, such as mobile sensor nodes, fuzzy logic, neural network, data mining techniques, Machine learning, etc., the use of IDS technology in sensor networks will become more efficient.

Various proposed IDS in WSN are presented according to their detection methodology. Finally, on the basis of all these observations and findings, various challenges in IDS for WSN are summarized.

To overcome these challenges in future, more work is need to be done on those IDS that should be lightweight for resource constraint WSNs and should utilize least amount of energy. Also it should be cross-layer IDS that can detect both known and unknown attacks to provide maximum detection accuracy.

Review of Related Works 4

Contents

Sinkhole attack is an active attack, launched in a Wireless Sensor Network by compromising a legitimate node or by introducing a malicious node in order to gain the traffic routed towards it before reaching the base station, by making a false advertisement in the routing information of its nearest distance to reach the base station. Due to this fake information the data packets under transmission are routed towards the malicious node through which the attacker can gain the access to the information, tamper the information or may even destroy it. Thus, this attack causes a severe threat to the normal functionality of the Wireless Sensor Network. Because of the wider range of applicability of Wireless Sensor Networks in our day-to-day life and in future, the detection and mitigation of Sinkhole attack plays a vital role. Researchers had presented several ways to detect and identify Sinkhole attacks. This chapter reviews and surveys related work on Sinkhole attack detection and also highlights open challenges in dealing with such attacks.

4.1 Approaches for Sinkhole Attack Detection

Several researchers proposed different approaches for the detection of Sinkhole nodes. Some works count the number of hops from the node to the BS, while others use predefined rule sets. Still, other approaches are based on mobile agents, and some works define a trustworthiness threshold and use it to check each node in the network and so on. In this section, we discuss related works designed to defend against Sinkhole attacks. We classify these works with respect to their approaches. Here, we categorized the major approaches and techniques into: Trust based, Mobile agent based, Probability based, Rule based, Hop count based, Geographical based, Cryptographic based, Cross Layer based, Network features based, Machine Learning based and finally bio-Inspired based approaches as illustrates in figure 4.1. The brief presentation of the last work in each approach is given in the following subsections and the Table 4.1 provides a comparison of the presented approaches.

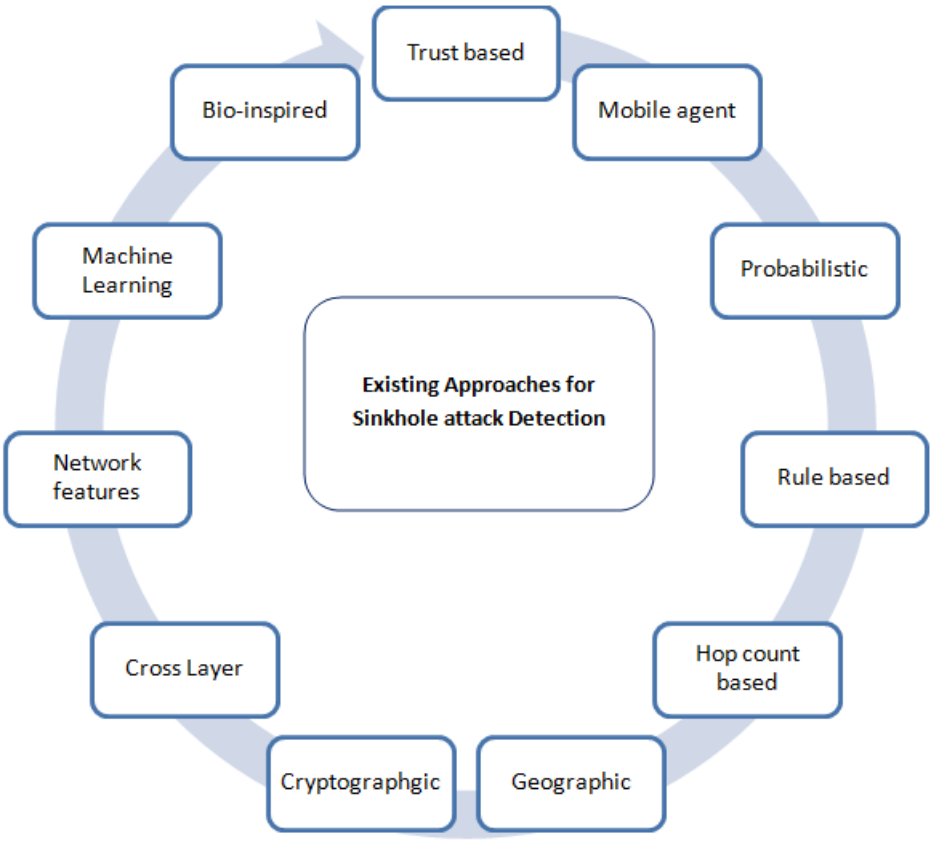

Figure 4.1 – *Existing approaches in Sinkhole attack detection*

4.1.1 Trust based Approach

The authors in (Ghugar & Sahoo 2019) proposed a protocol layer trust-based intrusion detection system (LB-IDS) to detect the attackers at different layers in clustered WSNs. The trust value of a sensor node (SN) is calculated using the deviation of trust metrics at each layer with respect to the attacks. The trust metrics at the physical layer are energy consumption of an SN and the number of messages received from the SN. The trust metrics at the MAC layer are back-off time and the number of successful transmission. The trust metrics at the network layer is the number of hops advertised. For detection, SN calculates its overall trust value by combining the trust values of each layer and sends it to CH (Cluster-Head). Later, the CH compares the received value to a threshold value to decide whether the SN is genuine or malicious. The trust value is recalculated at regular intervals. The authors concluded that the LB-IDS performs better than other scheme in terms of detection accuracy, false-positive rate, and false-negative rate.

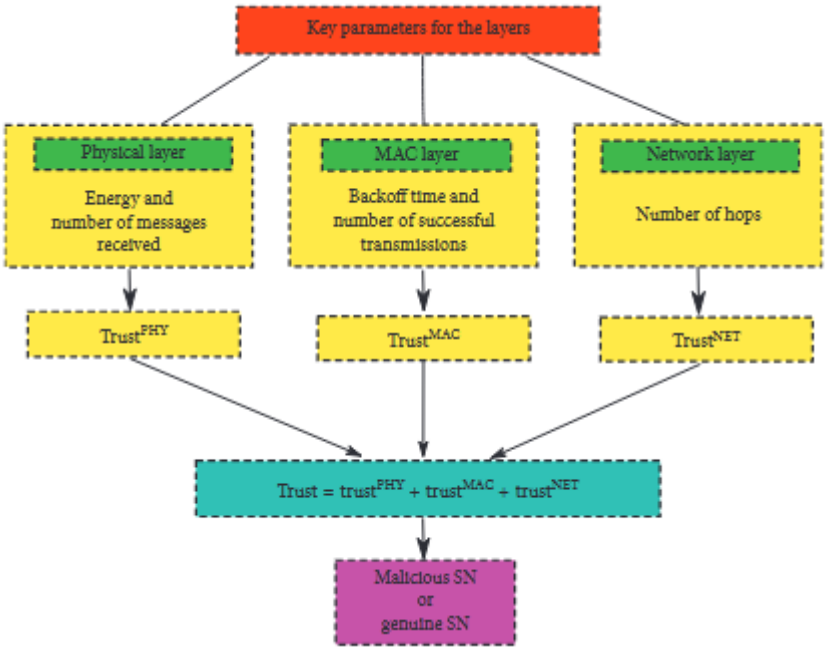

Figure 4.2 – *LB-IDS for clustered WSN (Ghugar & Sahoo 2019)*

(Wazid *et al.* 2016) proposed Sinkhole detection mechanism for the hierarchical wireless sensor networks. The proposed approach can detect three types of Sinkhole attack: Sinkhole message modification nodes, Sinkhole message dropping nodes and Sinkhole message delay. The network model is divided into several disjoint clusters. The cluster head are designed as a powerful high-end nodes and are responsible for monitoring the cluster and for the detection of different Sinkhole attack based on node identification, hop count, coefficient of the suspected node and remaining energy at the nodes. The proposed methodology detects various types of Sinkhole attacks parallel. The simulation results showed that the proposed technique achieves high detection rate and low false positive rate which are significantly better than other related schemes.

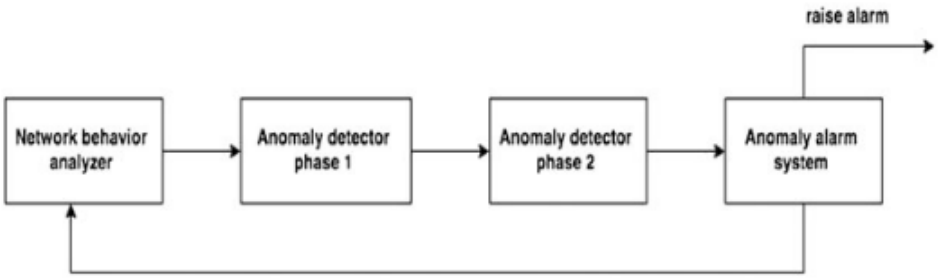

Figure 4.3 – *High-level description of proposed scheme in (Wazid et al.2016)*

4.1.2 Mobile agent based Approach

(Jatti & Kishor-Sonti 2021) presented an effective mobile agent-based algorithm for detection and prevention of Sinkhole attack in WSNs. Use of mobile agents is being done for detecting an attacker node and to inform the neighbour node about the trusted neighbours in their surroundings. The proposed algorithm is divided into two parts: one describes network

configuration and second describes the security of the network. In the first step, The nodes once deployed in the network, the agents start agent cycling with trusting procedure. In second step, as mobile agents are codes in an executing program. It is decoded, such as an attack will not be able to steal or change its data. With the use of unique hash function algorithm, the agents and nodes verify and describe the valid agents and nodes in the network and then the attacker is detected. Based on simulation results throughput, packet delivery ratio and received data packets are increased in proposed agent-based algorithm.

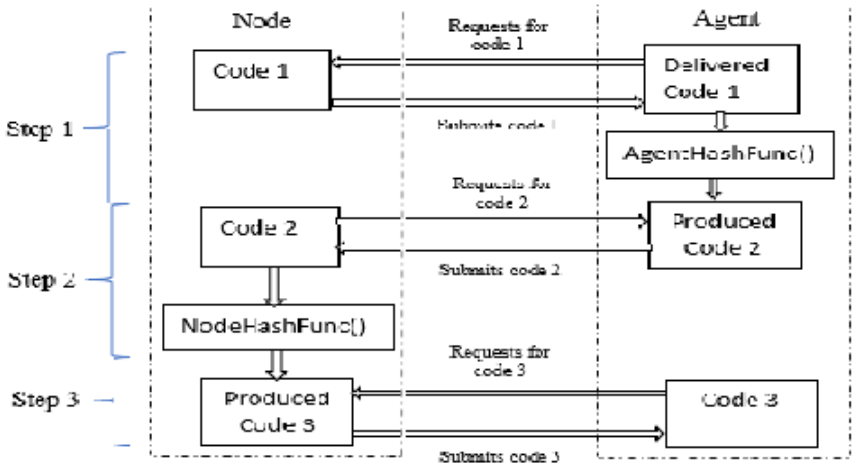

Figure 4.4 – *Detection Algorithm of (Jatti & Kishor-Sonti 2021)*

To detect a Sinkhole attack, a signature-based IDS model is designed in (Kalnoor *et al.* 2017). The proposed model uses a mobile sink throughout a Clustered Wireless Sensor Network (CWSN). In CWSN, an IDS agent is considered to be the node at top level. In each cluster, an agent is elected in IDS such that the attack can be detected with high accuracy. Detection task becomes active only whenever important or abnormal event occurs in the clustered network for energy saving. The proposed technique performs two phases. In the Node Initialization Phase: the detection rate is calculated in two different levels: at sink level and at the agent level. After, the maximum detection rate is calculated by the sink and then coordinates with the new position of the sink advertised to all the IDS agents. In the Detection Phase, the detection of intruder takes place once the advertised message is received to the node outside the area of sink movement. In this case, each agent receives an advertisement from the sink with a particular time period. If an advertisement is received outside this time period, a false advertisement is considered and a detection alarm will be sent to the IDS agent in CWSN. The results showed that the detection rate increased by improving the performance of the network.

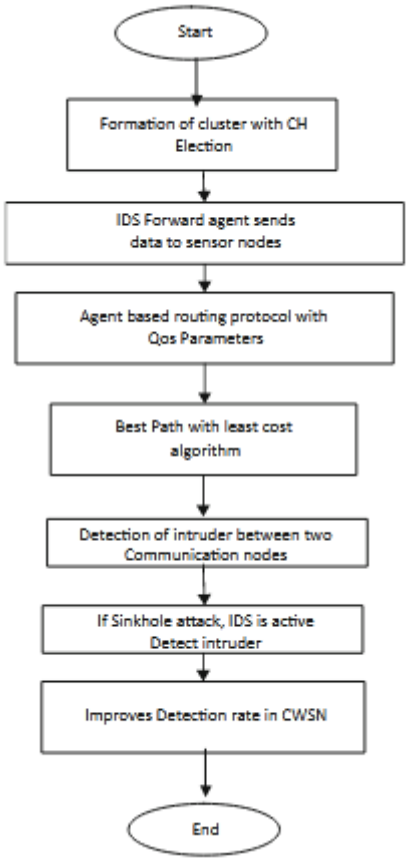

Figure 4.5 – *Flowchart for agent-based routing protocol (Kalnoor et al.2017)*

4.1.3 Probability based Approach

(Jahandoust & Ghassemi 2017) introduced an Adaptive Sinkhole Aware algorithm (ASA) based on the subjective logic and probabilistic extension of timed automata. The aim of the proposed schema is to exploit the probabilistic extension of routing algorithm AODV to route packets over the most reliable nodes (that are not defected by Sinkhole attack). The probabilistic AODV routing tables are updated following the behaviors of nodes through a set of distributed monitor nodes or received data packets in the base station. The ASA algorithm was evaluated on different random topologies with constant and dynamic parameters in case of mobility. The authors concluded that the proposed approach can be used against malicious Byzantine nodes that behave as normal nodes to escape from detection algorithm.

4.1.4 Rule based Approach

A rules-based intrusion detection system for identifying Sinkhole attacks on Mint-Route protocol is introduced in (Raju & Parwekar 2016). The proposed algorithm uses the Received Signal Strength Indication (RSSI) and Hop-Count metrics to detect the malicious nodes and it is based on Hop-count value creation algorithm defined in (Abdullah *et al.* 2015). An alarm is sent by a node to the base station when one of the rules is violated by a route update packet of one of the nodes. The two rules are:"For every incoming route update packet, check the hop-count value with the parent

if its less than the parent, send alert message" and "For every incoming route update packet, check the Nrssi values with parent. If the values are better than the parent node values then generate an alert message". Then, the base station will perform the intersection of all received alert packets within a specified time limit to find Sinkhole id which will be broadcasted in the network.

4.1.5 Hop-Count based Approach

The most popular approach based Hop-Count is defined in (Abdullah *et al.* 2015). This detection approach includes two main steps: Neighbor Database Construction and Sinkhole Node Detection. In the first phase, all nodes keep node ID and hop-Count values in a node neighbor database. In the second phase, a node calculates the average hop-count value without considering the lowest hop-count and compares average and lowest. The malicious node is detected when this lowest value is abnormally small comparing with average hop-count. The simulation results showed that the proposed technique successfully detects the Sinkhole with no intervention from the base station and it can be used to detect wormhole attack.

In (Zhang *et al.* 2019), the authors presented a secure and energy-efficient Sinkhole attack detection scheme. In the proposed IDS the nodes in the network are divided into areas according to their distance from the sink node and their neighbors.A new measure method is introduced which is the frequency of each node by establishing M routes with optimal hops from per node to the Sink node. Using this measure the Sinkhole nodes are then easily detected. Compared with the traditional algorithms, simulation results showed that the proposed scheme can significantly promote the detection rate and also stay a high energy saving results in wireless sensor networks.

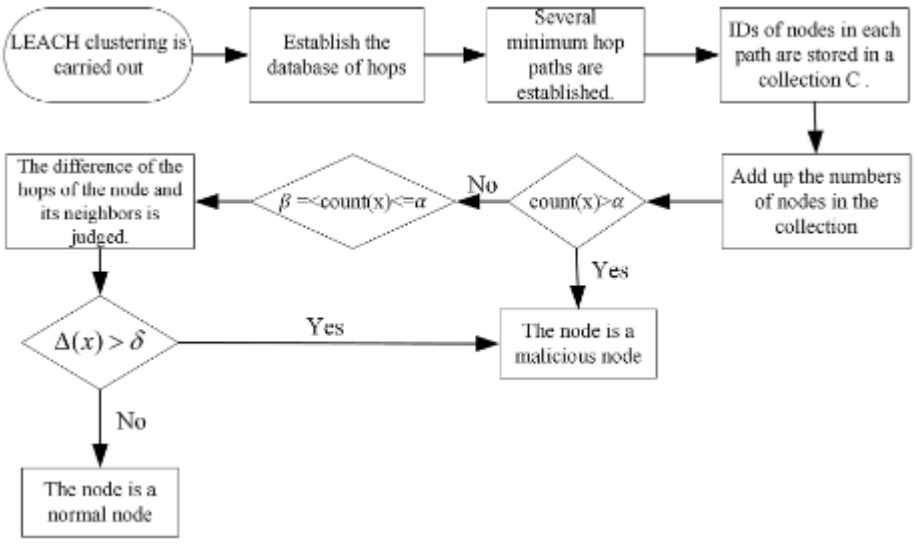

Figure 4.6 – *Flow chart of malicious node detection in (Zhang et al. 2019)*

Hop Count Monitoring Scheme is presented in (Yasin *et al.* 2017) . The proposed schema can detect the Sinkhole attack based upon hop count

observing. Since the hop-count feature is obtained easily from routing tables, the ADS (Anomaly Detection Scheme) is easily implemented. The obtained results showed that the proposed ADS can detect attacks with 96% accuracy and is applicable to all routing protocol that maintains dynamically a hop-count parameter.

4.1.6 Geographical information based Approach

(Han *et al.* 2015) proposed a novel Intrusion Detection Algorithm based on neighbor information against Sinkhole Attack (IDASA). The proposed algorithm performs in three phases: recognizing suspicious nodes, identifying Sinkhole nodes and removing Sinkhole nodes. In the first phase, the shorter and the longer routing path are considered to recognize suspicious nodes. In the second phase, the number of interaction times and ACKs are used to judge whether the suspicious nodes are Sinkhole nodes. The last phase consists to remove Sinkhole nodes. IDASA was evaluated in terms of malicious node detection accuracy, packet loss rate, energy consumption and network throughput in MATLAB. Simulation results showed that the performance of IDASA is better than the novel Agent-Based Approach to Detect Sinkhole attacks (ABAD).

(Nadeem & Alghamdi 2019) introduced a Sinkhole attack detection algorithm that utilizes the distance and energy related information from the data aggregation technique to identify the Sinkhole attack in a Wireless Body Area Sensors Networks (BAN). The simulation results showed that Sinkhole attack could severely degrade the performance of the network (up to 40%) in terms of low throughput, higher delay and packet breakdown. The proposed detection algorithm gave good performance in terms of high success (85% on average) and low (6% on average) false alarm rates.

4.1.7 Cryptogaphic based Approach

(Vidhya & Sasilatha 2017) designed an energy power consumption model in AODV routing protocol based on pure MD5 algorithm to detect Sinkhole attacks. In their network model, the sensor nodes have as role to monitor their region and collect the sensed data that will be routed to the sink. The mobile agents collect information from nodes when a different behaviour is observed, mobile agents are used for reducing the communication. The trust manager receives periodically the updated data from mobile agents in order to verify nodes identity and alert all the nodes in the network of serious threat. The proposed algorithm use MD5 algorithm to generate the public and the private keys for each node in five steps using a cryptographic 128-bit hash function. Each node is assigned with a signature and if any attacker node uses the same signature, it will be detected as Sinkhole. The simulation results showed the achievement of throughput for proposed approach.

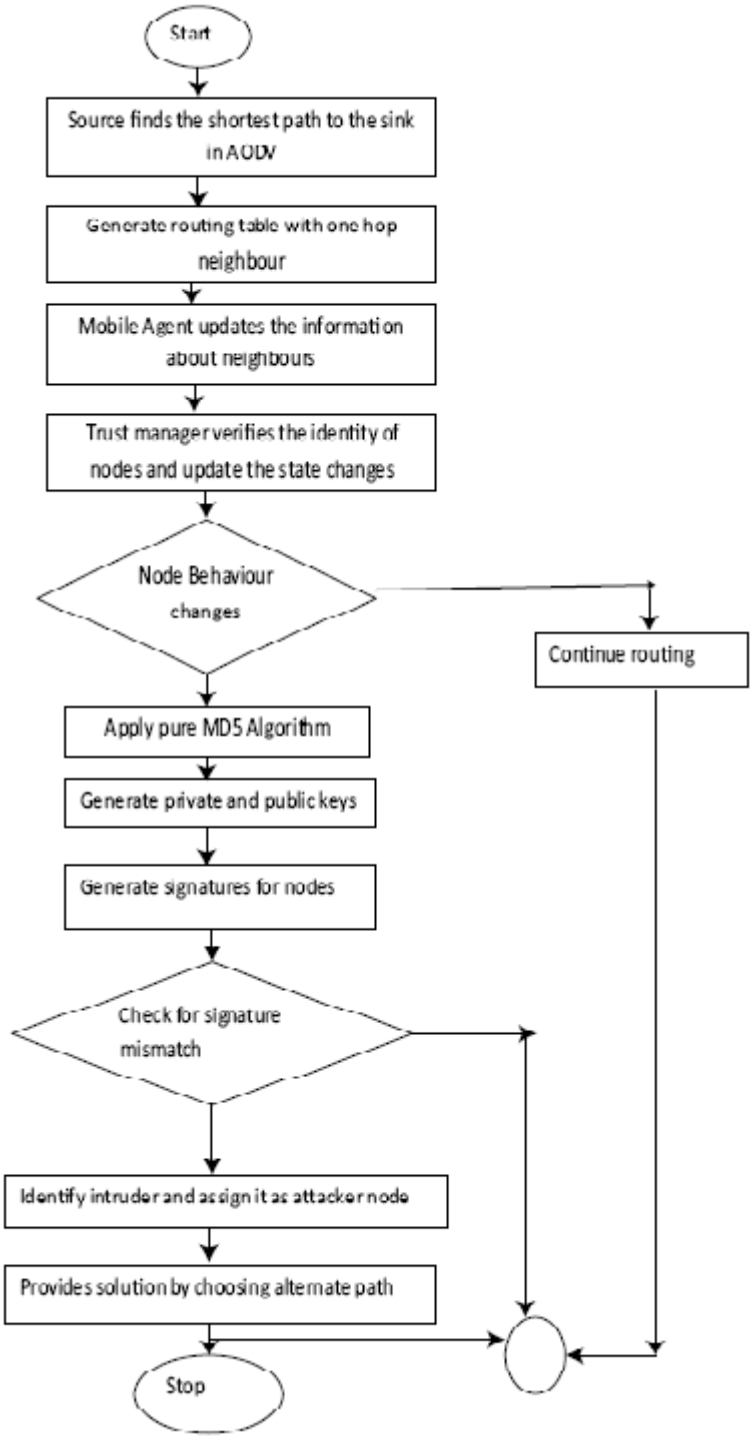

Figure 4.7 – *Intrusion detection mechanism for Sinkhole attack using MD5 algorithm (Vidhya & Sasilatha 2017)*

In (Terence & Purushothaman 2019), the authors developed an IDS based warning message counter method (WMC) to detect blackhole attack, grayhole attack and Sinkhole attack in wireless sensor networks. The authors modeled the network with sensor node and monitor node. Sensor nodes sense the data and forward to the destination node. Monitor node monitors the sensor nodes in their area and identifies the compromised node by maintaining the monitor table. The monitor table updates the

warning count field when no acknowledgement is received from destination node after sending the data packet through the path selected by the source node. The monitor node periodically compares the threshold value with the warning count to detect malicious nodes. After malicious node detection, a light weighted symmetric key cryptography is used to find data modification by the Sinkhole node. In this cryptographic mechanism, each node verifies the received data packet integrity through message authentication code. If verification fails, the data packet will be dropped. Simulation results showed that, WMC detects Sinkhole attack, blackhole attack and grayhole attack with less false positive 8% and less false negative 6%.

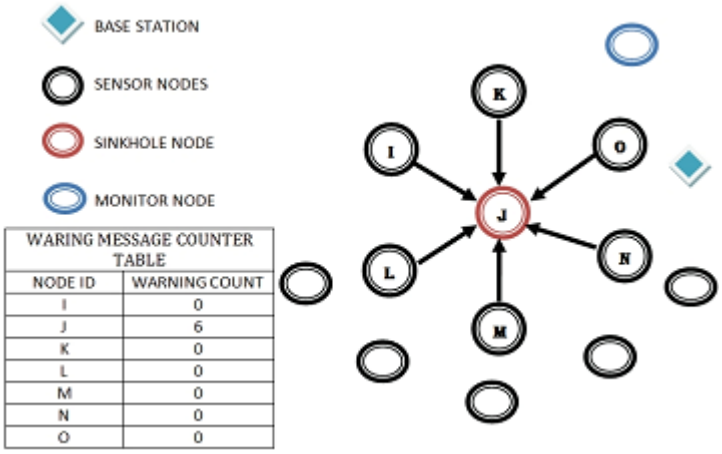

Figure 4.8 – *warning message counter method in (Terence & Purushothaman2019)*

The paper (Babaeer & Al-Ahmadi 2020) presented a lightweight, secure Sinkhole detection and transmission model that uses homomorphic encryption and watermarking techniques. The proposed approach uses two main schemes that rely on communication forms present in the TEEN protocol. These forms are generated and distributed by the BS, and they change every time the cluster formation changes. To ensure data authentication, watermarks are applied to each data packet. These watermarks are produced by the message authentication function and a pseudo-random number generator. Whereas, The homomorphic encryption is used to provide fast and efficient and consumes less energy while identifying sensor nodes for the purpose of Sinkhole detection and prevention. The proposed approach has been 100% successful in securing the network, and showed better results compared with previous works in the following metrics: delay, packet delivery ratio, throughput, and average energy consumption.

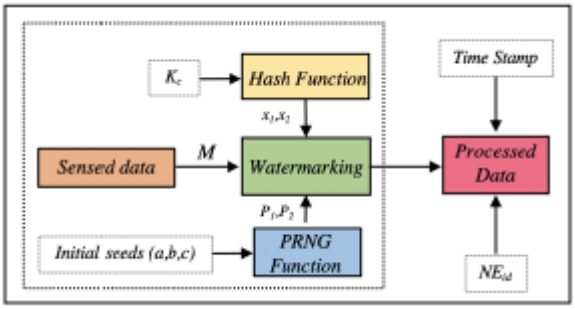

Figure 4.9 – *Watermarking scheme at sensor node (Babaeer & Al-Ahmadi2020)*

4.1.8 Cross Layer based Approach

(Gandhimathi & Murugaboopathi 2016) presented an efficient cross layer technique based mobile agent which detects and prevents multiple attacks, like Sinkhole, wormhole and sybil attack in WSN in two phases. In first phase, attacks are detected by correlating the cross layer features, such as MAC and Network layers. During the second phase, the mobile agent based technique is applied to prevent the attack. The mobile agent is used to aware its neighbours through three-step successful negotiation in order to ignore the traffic generated by the malicious node. Hence it reduces the false positive rate and improving the energy efficiency than the existing approach. In this work, the flat network is used.

In the other hand, (Arya & Binu 2017) used the same technique defined in (Gandhimathi & Murugaboopathi 2016) in hierarchical network to detect and prevent Sinkhole attack only. The proposed approach is a two based procedures. Procedure 1 is the Re Clustering method where pdr (Packet delivery ratio) of the network is analyzed. The Sinkhole attack is detected if a rapid drop in pdr is observed, then link quality will be checked. If any path is accessed more times, then the route is discarded from the routing table. By using geographical routing protocol, the attacked cluster can be analyzed. After identification of the attacker, base station alerts the nodes in the attacked cluster about the presence of the attacker instead of the entire network and the attacker node is discarded. Procedure 2 is the prevention using a mobile agent. Mobile agent is a movable sensor node that collects the information from the attacked cluster and transmits it to the base station directly if any attack is confirmed in a cluster. By using a mobile agent the energy consumption of network, communication overhead and false positive ratio are reduced.

The proposed work in (Ambika 2021) is an improvement of the cross-layer design suggested in (Arya & Binu 2017). The doings of the network and MAC layer were brought in together to enhance security in the network. The proposed study uses signal strength and node identification to track the malicious node in the network. The work suffixed a hash code to enhance security in the WSN and aided in bringing forward secrecy. The energy is reduced by 18.18%, and the security is increased by 22% with the comparison to the previous work.

(Ansar *et al.* 2021) proposed a new Secured-RPL routing protocol to detect and avoid Sinkhole attacks in the WSN, which is called Cross Layers Secured RPL (CLS-RPL). This routing protocol is enhanced of the existing RPL routing protocol. CLS-RPL is a cross-layer routing protocol that uses information from the data link layer in its security mechanism. CLS-RPL uses a new technique and concept in detecting a Sinkhole attack that is based on eave-listening (overhearing) that allows a child node to eave-listening its parent transmission. If the child node does not hear any transmission from its parent node after sending several packets, this means its parent node is a Sinkhole attacker. Otherwise, if the node hears transmission from its parent node, this means that its parent node is legitimate and continues to send more packets. CLS-RPL implements a simple security mechanism that provides a high packet delivery ratio with 52% improvement when compared to RPL protocol.

4.1.9 Netwok features based Appoach

(Karthigadevi *et al.* 2019) Proposed a novel decentralized Sinkhole detection mechanism using Neighbor Density Estimation Technique (NDET) to detect and prevent the Sinkhole attack. The neighbor density is estimated using the neighbor history or neighbor details obtained from different neighbor of the node. The Sinkhole node is detected based on the Traffic Introduction Factor (TIF) which represents the degree of node participation in the transmission. TIF is compared to Transmission Range (TR) threshold to identify the malicious node. Identified malicious node information is distributed to the neighbor nodes, so that the malicious node will be ignored at next transmissions. The simulation results showed that the proposed method reduces the overhead of collecting routes, and increases the network throughput.

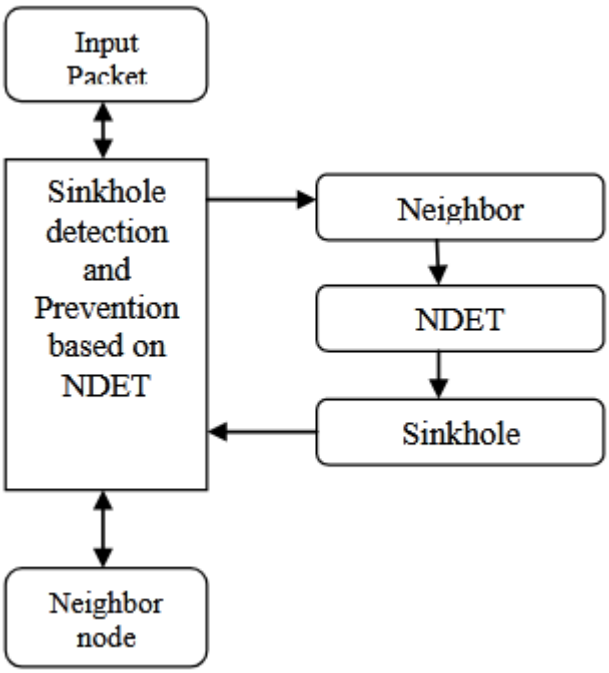

Figure 4.10 – *Sinkhole attack detection in (Karthigadevi et al. 2019)*

A novel Flow Based mitigation model to detect and mitigate Sinkhole attacks with the support of time variant snapshots (FBSD) is presented in (Devibala *et al.* 2017). The proposed FBSD method pass by four phases. Traffic Log Generation which produces logs into the data set. Traffic transition pattern which compute the traversal path of the packet. Time-Variant Snapshot which generates the topology snapshot of the network. Finally Sinkhole Detection which detect the sink node using snapshot of the network taken at different time frames. When a malicious node is identified a control message is sent to all the nodes to avoid sink hole from packet transmission. The proposed method highly reduces the overhead generated by flooding control messages in the network and increases the performance of the network.

4.1.10 Machine leaning based Appoach

The most related work to our research is presented in (Garofalo *et al.* 2013). A decentralized IDS architecture based Decision Tree technique is designed to ensure a trade-off between different requirements: high detection rate and energy saving in AODV protocol. The IDS is composed by a Central Agent (CA) and several Local Agents (LAs): each LA is deployed on a WSN node and the CA is deployed on a server that acts as a base station for the WSN. The chosen anomaly detection technique makes use of threshold metrics on LA: specific events are counted over a given time window. If the number of events exceeds a given threshold, an alarm is raised and sent to the CA. The CA improves the detection capabilities of the proposed architecture through the validation of security alerts raised by LAs when an attack is detected. Detection activities on the CA are based on Decision Trees. To evaluate the effectiveness of the proposed solution a dataset including Sinkhole attack has been created and employed, and it has been made available to facilitate future comparisons of alternative solutions. The results showed a high detection rate obtained through decision tree classification and an energy saving obtained through light detection techniques on the motes using NS-3 simulator.

4.1.11 Bio-inspired based approach

A swarm-based algorithm named artificial bee colony (ABC) is proposed in (Nithiyanandam & Latha 2019). For detecting the Sinkhole attack in WSN network the bees are authorized to pick-up one node that has high probability to be a Sinkhole node. Once the node is chosen, the selected node are compared with the nodeID which sends the route update packet, and a binary search is continued until the Sinkhole node is identified. In comparison procedure, the bee compare the received request with the ruleset it possess and if there is a match between the obtained request (NodeID and link quality) the route will be updated, in case of any mismatch it results in Sinkhole attack detection. The simulation results showed that the proposed algorithm outperforms the existing methodologies in terms of packet loss, packet delivery ratio and energy consumption.

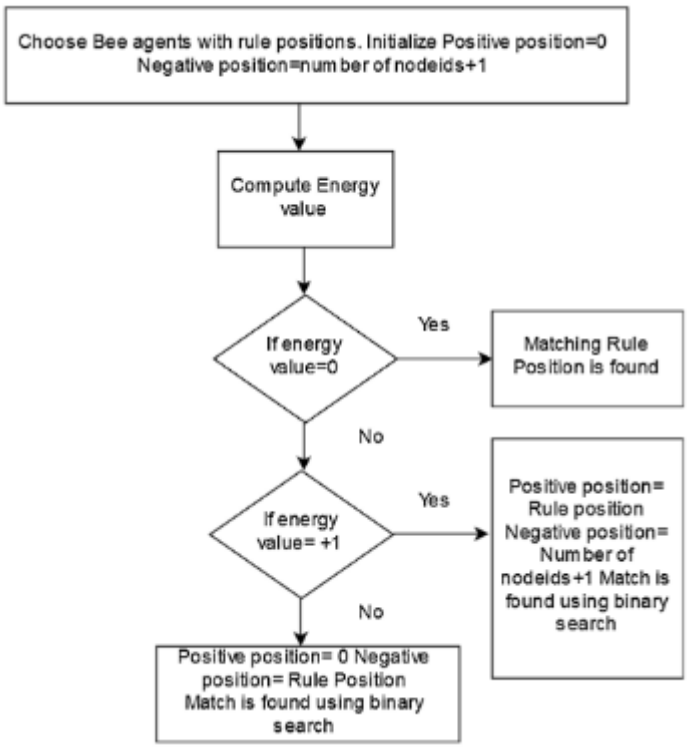

Figure 4.11 – *Flowchart of ABC attack detection proposed in (Nithiyanandam & Latha 2019)*

NP: Not Provided

Approach	Detection Metrics	Protocol	Energy saving	Dataset	Simulator	Accuracy	Drawbacks
Trust based detection (Ghugar & Sahoo 2019)	number of hops	AODV	Yes	Simulation	Matlab	96.83%	Network lifetime reduced due to the computational power in the cross-layer approach
Anomaly based detection (Wazid *et al.* 2016)	Node ID, Hop count, Coefficient the suspected node and Remaining energy	AODV (static clustering)	Yes	Simulation	NS-2	95%	Messages overhead and High energy consumption
Mobile Agent (Jatti & Kishor-Sonti 2021)	Trust based Hash-Function Code	ABADS	No	Simulation	NS 2.35	NP (Not Provided)	conception with no energy issue in mind
Mobile Agent (Kalnoor *et al.* 2017)	delay, bandwidth, loss of packet and energy consumed	Agent-Based QoS Routing Protocol	Yes	Simulation	NP	96.09%	key generation technique in cluster formation needs computational power and energy

Continued

Table 4.1 – *Existing approaches on Sinkhole attack detection*

Approach	**Detection Metrics**	**Protocol**	**Energy saving**	**Dataset**	**Simulator**	**Accuracy**	**Drawbacks**
Probabilistic timed automata (Jahandoust & Ghassemi 2017)	Residual energy and number of forwarded packets	AODV	No	Simulation	Java language and UPPAAL tool	NP	Combination of the formal models leads to intense computation, consequently reducing the network lifetime.
rules-based IDS (Raju & Parwekar 2016)	hop-count and Nrssi	Mint-Route	No	Simulation	Matlab	100%	Energy consumption not considered
Hop Count based approach (Abdullah *et al.* 2015)	Hop Count	Flat protocol	No	Simulation	NP	100%	Detection only with hop distance >=3
Minimum hop route detection (Zhang *et al.* 2019)	Hops	LEACH	Yes	Simulation	Matlab	>95%	Detect one attack at a time. The detection rate depends on the distance between the SN and BS
Anomaly Detection (Yasin *et al.* 2017)	Hop Count	NP	Yes	Simulation	NS-2	96%	No routing protocol is studied

Continued

Table 4.1 – *Existing approaches on Sinkhole attack detection*

Approach	**Detection Metrics**	**Protocol**	**Energy saving**	**Dataset**	**Simulator**	**Accuracy**	**Drawbacks**
Detection based Neighbor Information (Han *et al.* 2015)	The number of interaction times and ACKs	AODV	Yes	Simulation	Matlab	93.33%	Energy depletion in routing path exploration
Local information (Nadeem & Alghamdi 2019)	Residual energy and distance	Aggregation protocol	Yes	Simulation	Castalia based on OMNET ++	high detection >85%	privacy and security issues in BAN
MD5 algorithm based detection (Vidhya & Sasilatha 2017)	Hash function signature	EPC-AODV	Yes	Simulation	NS-2	NP	use of external energy resource
Cryptographic based approach (Terence & Purushothaman 2019)	warning message counter	AODV	No	Simulation	MannaSim Framework patch with NS2	NP	excessive use of the ACK messages which leads to consuming sensor nodes energy. Unable to detect collaborative attacks

Continued

Table 4.1 – *Existing approaches on Sinkhole attack detection*

Approach	**Detection Metrics**	**Protocol**	**Energy saving**	**Dataset**	**Simulator**	**Accuracy**	**Drawbacks**
watermarking technique based detection (Babaeer & Al-Ahmadi 2020)	network key	TEEN	Yes	Simulation	OMNET++	100%	The authentication mechanism implemented in each CH and encryption in each MN lead to consuming their energy and reducing network lifetime
Cross layer detection (Gandhimathi et al.2016)	Number of routed packets, Number of dropped packets and MAC duration	AODV	No	Simulation	NS-2	NP	Energy consumption not considered
Cross layer detection (Arya & Binu 2017)	Number of retransmissions and PDR	LEACH	Yes	Simulation	NS-2	NP	Cryptography increases network energy consumption

Continued

Table 4.1 – *Existing approaches on Sinkhole attack detection*

Approach	**Detection Metrics**	**Protocol**	**Energy saving**	**Dataset**	**Simulator**	**Accuracy**	**Drawbacks**
Cross layer detection (Ansar *et al.* 2021)	number of overhearing	RPL	No	Simulation	Cooja	NP	Energy consumption not considered in number of overhearing computation
Density based detedtion (Karthigadevi *et al.* 2019)	Traffic Introduction Factor (TIF)	NDET	No	Simulation	NS-2	99.1%	Excessive calculation reduces network lifetime
Traffic flow based detection (Devibala *et al.* 2017)	Network snapshot	FBSD	No	Simulation	NS-2	99.1%	Memory overhead by Traffic Pattern and snapshot Generation
Decision tree based detection (Garofalo *et al.* 2013)	10 metrics	AODV	Yes	Cyber security datasets for WSNs	NS-3	97.8% 99.4% 99.5%	Processing overhead over ten (10) detection metrics
Swarm based detection (Nithiyanandam & Latha 2019)	Node ID and Link quality	Flat protocol	Yes	Simulation	NP	NP	unable to detect the Sinkhole attack that tampered on the data

4.2 Challenges in Detecting Sinkhole Attacks in WSN

Based on our review of the scientific literature on Sinkhole attacks detection in WSNs, the following are the main challenges pointed out by the researchers in detecting Sinkhole attack in wireless sensor networks(Rehman *et al.* 2019) (Ali *et al.* 2020a) (Waoo & Tiwari 2021):

1. **Communication modes in WSNs**:

   Communication patterns in WSNs consist in sending all packets to the sink node namely the base station. This communication mode is known by "many to one" pattern. To launch a Sinkhole attack, the attacker need only to comprise nodes near to BS to reroute to itself the entire flow of the network. Since that the communication style itself provides and create occasion to be easily attacked , it become a serious and dangerous challenge in Sinkhole attack detection.

2. **Routing protocols dependency**: Sinkhole attack relies on the features of the used routing protocol in WSNs. The attacker or the intruder exploits the routing metrics based packets transmission to launch Sinkhole attacks. As example, the two routing protocols AODV and MintRoute; for the first protocol the attacker uses minimum hop count number to the BS to attract nodes packets while in the second protocol link quality is used. Consequently, the techniques used by a compromised node in a network differ from a routing protocol to an other, creating hence an impulsive nature to the Sinkhole attack.

3. **Compromise of nodes**: Sinkhole attacks may be outsider as insider attacks. In the first category, the attacker injects a malicious node to the network while in the second the attacker gets the control on a legitimate node by altering with it or by exploiting the vulnerabilities of the target node system. The legitimate compromised node has adequate access network privileges and all the important information on the network which makes the compromised node as a legal part in WSN. This creates hence a new challenge in Sinkhole attack detection where even cryptography could not secure the network. In addition, Once launched successfully, Sinkhole node can be used to launch further attacks, such as selective forwarding attack, wormhole attack, flooding attack, sybil attack and blackhole attack. So, the insider attacks have more serious and dangerous consequences on the WSN compared to outsider attacks.

4. **Resource constraints**: The WSN are characterized by a limited resources i.e limited energy, low communication range, low memory capacity and low computational power which limits the use of powerful techniques designed for other networks in Sinkhole attack detection in WSN. Therefore, the design of new security mechanism in WSN appeals a compatible weak methods considering the constrained resources of WSNs.

5. **Physical attack**: In most of the time, the nodes of a WSN are deployed in a hostile and abundant area with no surveillance. This

make attacker task easy to attack physically the sensor nodes and get illegal access to critical information concerning the network as the authentication keys stored inside the sensor node.

6. **Dynamic topology of WSN**: WSNs are a particular type of Adhoc networks where routing protocol consider the BS as a root. In the WSN, sensor nodes and/or BS may have the ability to move and organize themselves in the network which will affect the power of wireless signals and communication range in the network. In Sinkhole attack detection, dynamic changing in network topology must be considered.

4.3 Performance Analysing Parameters

A lot of parameters are there for calculating the performance and detection rate of Sinkhole attack. In general, the performance of the network is observed based on the QoS parameters for the proposed IDS models. Based on the applications of WSN, the requirements of QoS are (Kalnoor *et al.* 2017; Rehman *et al.* 2019):

4.3.1 Load of the Network (L)

Load of the Network (L): It is the total number of events generated by the nodes over the network per unit of time. This impacts on consumption of energy and bandwidth. At time t, the load on network L is determined using equation (4.1).

$$L(t) = N_{event} + N_{attack} \tag{4.1}$$

Where
N_{event} : The number of new events generated in the network,
N_{attack} : The number of Sinkhole attacks generated.

4.3.2 Energy Consumption (E)

Because of congestion in the network and overhead of communication, the energy consumption becomes an important QoS parameter. E is defined as the total sum of energy consumed to transmit data E_t, energy consumed to receive data E_r, energy for carrier sensing E_c and energy in sleep mode E_s. The energy consumption of the network is carried out using equation (4.2).

$$E = E_t + E_r + E_c + E_s \tag{4.2}$$

4.3.3 Sinkhole Detection Rate

It represents the rate of detection when Sinkhole attack is generated. Sinkhole detection rate SD_R is calculated using equation (4.3).

$$SD_R = \frac{N_D}{N_G} \times 100 \tag{4.3}$$

Where
N_D: Number of Sinkhole attacks detected.
N_G: Number of Sinkhole attacks generated and injected in the sensor network.

4.3.4 Efficiency (EF)

It determines the time needed by the IDS to detect the first occurrence of Sinkhole attack. It is calculated by Equation (4.4).

$$EF = DT - OT \tag{4.4}$$

Where
DT is the time taken to detect first Sinkhole attack.
OT is the time for performing the Sinkhole attack.

For Clustered Wireless Sensor Network (CWSN), (Kalnoor *et al.* 2017) added as metric density of the network defined below.

4.3.5 Density of the network

It is the analysis of behavior of the IDS model when large set of sensor nodes are added and the networks grow to a large extent. The density D is calculated using Equation (4.5).

$$EF = \frac{(N\pi R^2)}{A} \tag{4.5}$$

Where
N is the number of nodes in CWSN.
R is the range of transmission.
A is the region in which N sensor nodes are scattered.

Conclusion

In this chapter, we have studied and reviewed the recent development for detecting the Sinkhole attacks in WSNs. Different researchers and analyzers had presented and shown several ways of intrusion detection proposals based on different methods with various approaches to expose and identify the vicious Sinkhole nodes. We have categorized the presented works into eleven approaches and recapitulated them in a table according several parameters. In the validation of the presented works, some of the researchers have tried the use of real wireless sensor networks and most of them have appealed a simulation tools. Also, we have exposed the open and unattended challenges in dealing with Sinkhole attacks and presented the formulae to calculate some important performance analysis

parameters for Sinkhole attack.

The most challenging problem in Wireless sensor networks is to propose an energy efficient security mechanisms due low resources. In the following and the last chapter, we'll present in detail our energy saving Sinkhole attack detection system in WSNs (Aissaoui & Boukli-Hacene 2021).

Contribution 5

Contents

As discussed in the previous chapter, several approaches have been proposed to detect efficiently the destructive Sinkhole attack in WSNs based on different techniques and calculated parameters. Although most of these works successfully detected the Sinkhole attack but many of them suffer from high energy consumption due to the need for more computational capability which are not available in WSNs.

The objective of this thesis is to design and implement an efficient detection scheme based on SVM technique for intrusion detection system in WSN with energy saving (Aissaoui & Boukli-Hacene 2021). The proposed IDS aims to detect a specific DOS routing attack namely the Sinkhole attack by using only two extracted routing information: hop count (HCNT) and destination sequence number (DSN) on Ad hoc On-demand Distance Vector (AODV) protocol (Perkins *et al.* 2000). We have experimented binary class support vector machines (SVM) to perform SVM classifier. The dataset [1] used in different experimentation is provided by Garofalo et al in (Garofalo *et al.* 2013) for a comparison. The contributions of the proposed approach include:

- Lightweight, secure and efficient protection against Sinkhole attack with no calculated parameters.
- Energy saving in the sensor nodes, increasing the network life-time.
- Standalone (HIDS) and Centralized (NIDS) based detection

The chapter is organized as follows. First, we introduce SVM classification for intrusion detection in WSNs. Next, System architecture and network model are presented. Then, we present the simulation environment and experiment setup. Finally, the obtained results are discussed before concluding the chapter.

5.1 Support Vector Machines for malicious node detection

In the field of machine learning, SVMs are similarly recognized as Support Vector Networks and are defined as supervised machine learning algorithm that analyze data used for classification, regression and distribution estimation (one class SVM) while originally formulated for binary classification (Cortes & Vapnik 1995). In this project, we have used binary SVMs to detect Sinkhole attacks in a sensor network. The choice of the two-class approach is based on the fact that they know the form of the attack a-priory.

A supervised classification task usually involves separating data into training and testing sets. Each instance in the training set contains one "target value" (i.e. the class labels) and several "attributes" (i.e. the features or observed variables). The goal of SVM is to produce a model (based on the training data) which predicts the target values of the test

[1] http://fitnesslab.altervista.org/index.php/it/option=comcontent&view=article&id=71

data given only the test data attributes.

The SVM problem is formulated as follows : given a training set of instance-label pairs $\langle x_i, y_i \rangle$, $i = 1, ..., l$ where $x_i \in R^n$ and $y \in \{1, -1\}^l$, the support vector machines (SVM) require the solution of the following optimization problem (Chang & Lin 2011):

$$\begin{cases} \min\limits_{w,b,\xi} & \frac{1}{2} w^T w + C \sum\limits_{i=1}^{l} \xi_i \\ subject\_to & y_i \left\langle w^T \phi\left(x_i\right) + b \right\rangle \geq 1 - \xi_i, \\ & \xi_i \geq 0, i = 1..l \end{cases}$$

The training vectors x_i are mapped into a higher dimensional space by the function ϕ. SVM finds a linear separating hyperplane with the maximal margin in this higher dimensional space. $C > 0$ is the penalty parameter of the error term. Furthermore, $K\left\langle x_i, y_i \right\rangle = \phi\left\langle x_i \right\rangle^T \phi\left\langle x_j \right\rangle$ is called the kernel function. In this work, the following four basic kernels are used:

- Linear: $K\left\langle x_i, y_i \right\rangle = x_i^T x_j$
- Polynomial: $K\left\langle x_i, y_i \right\rangle = \left\langle \gamma x_i^T x_j + r \right\rangle^d, \gamma > 0$
- Radial Basis Function (RBF): $K\left\langle x_i, y_i \right\rangle = \exp\left\langle \gamma \left\| x_i - x_j \right\|^2 \right\rangle, \gamma > 0$
- Sigmoid: $K\left\langle x_i, y_i \right\rangle = \tanh\left\langle x_i^T x_j + r \right\rangle$

Here, γ, r, and d are kernel parameters.

The proposed approach uses SVM classification technique based on (Garofalo *et al.* 2013)'s dataset.

SVM is adopted in this research because of two main reasons, namely: (1) speed, which allows it to be used in real-time application efficiently, and (2) high scalability, while its complexity is not affected by dimensionality of the feature space (Safaldin *et al.* 2021).

Security is one of the potential applications of SVM in WSNs. The SVMs was used massively in hybrid and combined based IDS for hierarchical WSN (Sedjelmaci & Feham 2011) (Anitha & Anjusree 2014) (Moulad *et al.* 2017) (Borkar *et al.* 2019) (Safaldin *et al.* 2021) and less for flat topology. According to the literature, some of the existing IDS based SVM for flat WSN are (Kaplantzis *et al.* 2007) (Chen *et al.* 2010a) (Chen *et al.* 2010b) (Garofalo *et al.* 2013) (Jianjian *et al.* 2018).

In (Kaplantzis *et al.* 2007), the authors presented the first study to use SVMs for centralized IDS in WSNs without further implications on node power. The proposed system can detect black hole attacks and selective forwarding attacks with high accuracy. The dataset was time collected series information of hop count and bandwidth at the base station from five simulation runs. The resulting data was split into training, testing and validation sets. The one-class SVM was then trained offline using the

training set, parameter selection was carried out based on the testing sets and the validation set was used to generate the final results.

A light-weight anomaly IDS based ontology concept was introduced in (Chen *et al.* 2010a). The proposed system detects sybil attack by comparing the relationship between sensor node data and the constructed ontology. Rough set theory (RST) is used to preprocessing package information and reducing useless information for support vector machine (SVM) training operation and to reduce WSN energy consumption.

Another approach using SVM in conjunction with artificial immunity algorithm for intrusion detection is proposed by (Chen *et al.* 2010b). The proposed immunity algorithm works in the same way the biological immunity principle does. In this solution, immune algorithm (IA) was used to preprocess the network data, to determine a good group of features, and support vector machine (SVM) was adopted to classify and recognize the intruders. Experimental results showed the feasibility and efficiency of the proposed method.

(Jianjian *et al.* 2018) proposed an IDS against Denial Of Service (DoS) attacks based on the improved AdaBoost-RBFSVM method. The proposed technique is based on adjusting the parameter sigma of RBF-SVM, changing the updating rule of AdaBoost weight and setting the alarm threshold. The node DoS attack is detected and removed from the network when the alarm threshold reaches its maximum. The network simulator NS2 was used to simulate the DoS attack in WSN based on the AODV routing protocol and to assesses the performances of the proposed method. The experimental results showed that the proposed IABRBFSVM-IDS can significantly improve the network performance by detecting and removing malicious nodes in the network in term of detection rate, packet delivery rate, transmission delay and energy consumption.

In the present work, the SVM classifier is trained with a series of labeled data already classified into two categories (normal data, Sinkhole attack data), named supervised training, to build a model that predicts whether a new example falls into one category or the other. The working of SVM classifier model generation is given in the figure 5.2. In WSN, our SVM classifiers are used to investigate AODV protocol data for detecting suspect behavior of a node in network.

5.2 System architecture and detection scheme

The proposed system uses the SVM technique to construct an intrusion detection model for Sinkhole attack. The architecture of this system is illustrated in the figure 5.1 . It has two phases: the Off-line phase and the On-line phase. In the first, the system generates its intrusion model while in the second it detects the intrusions.

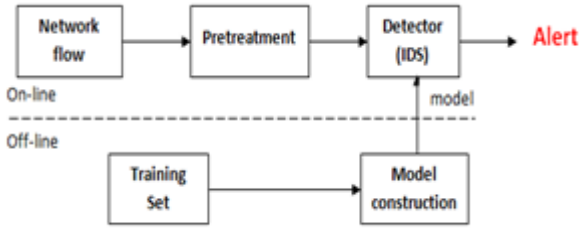

Figure 5.1 – *System architecture*

- Off-line Phase: This phase requires gathering enough historical data that includes both normal and abnormal connections. In this work, we use the collection of AODV routing data under Sinkhole attack given by (Garofalo *et al.* 2013), we called Sinkhole dataset.
- On-line Phase: It consists in setting up the developed IDS. In this phase, the role of the system is to analyze the traffic network and to detect in real time, using the generated SVM classifier, the Sinkhole attack targeting the WSN.

The figures illustrate the different steps for constructing the SVM intrusion detection models.

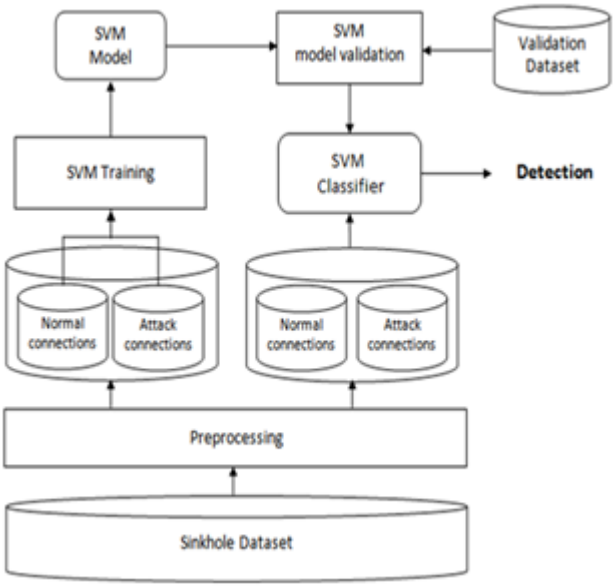

Figure 5.2 – *SVM model based IDS (Aissaoui & Boukli-Hacene 2021)*

The construction of the proposed IDS involves several steps. We present below the different modules and the participation of the different datasets in the construction of intrusion detection model outlined above.

5.2.1 Data preprocessing

Data preprocessing is a data mining technique that involves transforming raw data into an understandable format for further processing. In our case, it is to prepare the data to be directly exploited by the different processing modules (training, validation and classification). The used

dataset is given in pcap format; the classification techniques are not able to handle such a data format.

The pretreatment passes through several steps which are executed successively (or alternatively if necessary):

- Transform pcap files into XML files.
- Extraction of the different information (attributes) necessary in Sinkhole attack detection and transformation of records in a suitable processing format.
- Elimination of redundant records: the dataset contains a large number of duplicate records.

After transformation of pcap files to XML using Wireshark, we extracted time series information of hop count (Hcnt) and destination Sequence Number (DSN) from request and reply AODV packets from each XML file and gathered later in one file to have a two dimensions (2D) attribute vector file. Finally, the obtained data are saved in a suitable format for LIBSVM.

LIBSVM is a popular open source machine learning libraries, developed at the National Taiwan University by Chang and Lin (Chang & Lin 2011). LIBSVM is a simple, easy to use, and efficient software for SVM classification and regression. In our different experiments, we used the library LIBSVM for training, validating and testing the different generated models.

The Sinkhole dataset contains a large number of redundant records. After eliminating the duplicate records, the total number of records in the original dataset and in the final set is given in the table 5.1:

Sets	Normal Records	Attack Records	Total
Original Set	856537	26	856863
Final Set	2156	10	2166
Rate (%)	99.53%	0.47%	100%
Training Set	1941	8	1949
Rate (%)	99.59%	0.41%	100%
Test Set	215	2	217
Rate (%)	99.08%	0.92%	100%

Table 5.1 – *Dataset statistics*

Finally, the resulting smoothed data was split into training (90%) and testing (10%) sets; each containing both types of data: normal data and Sinkhole attack data and for validation set we chose to use the whole training set.

5.2.2 SVM training

The different SVMs were trained offline using the training sets with parameter selection based on validation results (detection rate). SVM was

trained using the labeled training set (90% of the final set) containing both normal and abnormal vectors (1, 1) and the remaining 10% was used for testing step.

5.2.3 SVM model validation

It consists in evaluating the generated SVM classification model on a sample or the entire training set to ensure that the system responds as desired and to obtain the best kernel parameter. We selected SVM model with accuracy higher than 98%.

5.2.4 SVM classification (test)

When the results of the validation step were conclusive, the test set (10%) was used to generate the final results. We used the generated SVM model to process new cases (the test set) whose classification is unknown in order to evaluate the performance of the classifier in terms of classification accuracy (detection rate).

5.3 Experiments and Results

5.3.1 Off-line Phase

All SVM training and testing were carried out using LIBSVM. We chose to experiment linear, polynomial, RBF (Radial Basis Function) and sigmoid kernel function. The training parameters of each kernel were fixed after several experiments. All results are summarized in following tables where only the most accurate SVMs are presented.

Kernel	C	δ	R	d	Detection Rate
Linear	/	/	/	/	99.07%
RBF	128	0.00781	/	/	100%
Sigmoid	1	0.5	0	/	99.07%
Polynomial	1	0.5	0	2	100%

Table 5.2 – *Performances of different SVM kernels*

SVM is complex machinery, where the choice of parameters can greatly influence the results. For example, the RBF kernel, the C and δ parameters have a significant impact on the performance of the SVM classifier. The same problem with the Sigmoid kernel. So, an empirical adjustment has been made to fix the different values, presented in table 5.2, of the different parameters for each kernel.

Table 5.2 shows that the best results are obtained by the RBF and the polynomial kernel function with a detection rate of 100%. To further test the performance of the SVM classifier based polynomial and RBF kernel; we looked for the minimum and necessary attack record number for learning and detecting the Sinkhole attack by decreasing the number of attack vectors in the training set and increasing their number in the test one. The different obtained results are presented in the table 5.3.

The first obtained results were on training and test set of 8 and 2 attack records respectively (see Table 5.1 and 5.2). According to the table 5.3, with 5, 4 and only 3 attack records in training set, we have always arrived to a detection rate of 100%. A detection rate of 99.10% and 99.55% for polynomial and RBF kernel respectively with only 2 attack records. These results explain the performance of the SVM classification method.

Experiments					
Sets	Normal	Attack	Total	Polynomial Accuracy	RBF Accuracy
Training	1941	5	1946	100%	100%
Test	215	5	220		
Training	1941	4	1945	100%	100%
Test	215	6	221		
Training	1941	3	1944	100%	100%
Test	215	7	222		
Training	1941	2	1943	99.10%	99.55%
Test	215	8	223		

Table 5.3 – *Performances of Polynomial and RBF SVMs*

As a conclusion to our different off-line experiments, SVM based RBF kernel will be implemented in our IDS for the real test (the on-line phase). However, the different results presented in the different tables of the off-line phase simulate and show the results of intrusion detections with a centralized IDS where the IDS is installed on the Base Station (BS). The BS controls all traffic through the network and is the only one with the ability to detect the Sinkhole attack and to take the necessary countermeasures.

5.3.2 On-line Phase

The on-line phase of our system consists in implementing the designed IDS in the WSN so that it analyzes in real time the flow exchanged between the different nodes and the base station. Hence, our SVM classifier-based IDS can be implemented in two different ways: either in a centralized architecture or distributed and collaborative architecture called decentralized. In the centralized architecture, our IDS will be placed in the base station (NIDS) which provides all intrusion detection capabilities without any participation of the sensor nodes. In the decentralized one, the IDS is installed on each sensor node (HIDS) and for the detection task, the node can collaborates with its neighbor nodes to make decision and it informs the base station by sending an alert message (see figure 5.3).

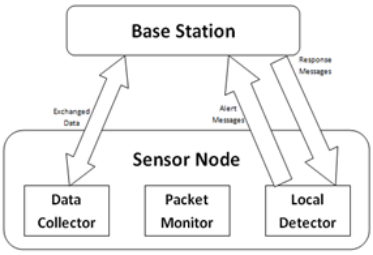

Figure 5.3 – *Decentralized IDS based SVM architecture*

A WSN was simulated to test the two proposed architectures. The simulations are made through NS-3[2] under Sinkhole attack and under the proposed detection scheme as follow: Implementing Sinkhole attack in NS3, Integrating LIBSVM library, Setting up the IDS and Launching the different simulations. Our simulation is conducted over a 100m $\times$ 100m field with distributed 20 sensor nodes. The deployed nodes have fixed positions during the entire simulation time. The initial energy of each sensor node is 2500 joule. The simulation is launched for 1200s and the Sinkhole attack start at second 600 by compromising Node 1. Other simulation parameters are listed in Table 5.4.

Parameter	Value
Simulator	NS-3.26
Protocol	AODV
Number of nodes	19
Number of malicious node	1
Simulation total time	1200 s
Attack Windows	[600s,900s]
Number of packets	1 packet / s

Table 5.4 – *Simulation parameters*

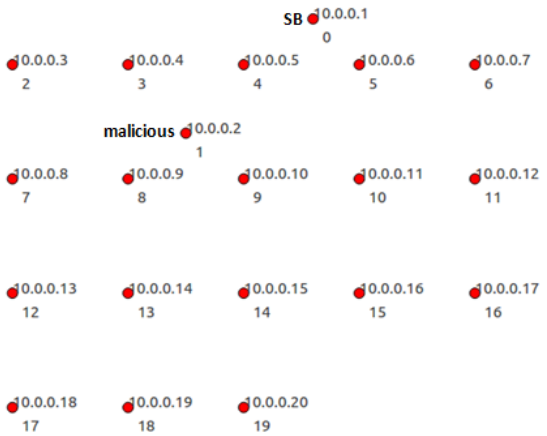

Figure 5.4 – *WSN deployment*

A. **Simulated scenario**

Network scenario under Sinkhole attack In this scenario, a WSN using the AODV protocol is simulated in which one node (node ID 1,

[2]https://www. nsnam. org

see figure 5.4) becomes a Sinkhole attacker and propagates messages to neighbor nodes to attract the packet routed to the BS.

Network scenario with the proposed detection scheme This scenario depicts a WSN in which the proposed model has been implemented to detect and prevent Sinkhole attacks. In our different experiments, we have implemented two types of intrusion detection systems: a HIDS where each node analyzes exclusively the flow concerning its sensor and a NIDS installed on the Base Station (SB) where it analyzes all the traffic circulating in the network.

B. **Evaluation metrics**

To evaluate our proposed IDSs, we have chosen two metrics Detection Rate (DR) and Average Energy Consumption.

The energy consumption of the microcontroller is not considered in NS3 simulator. So to calculate the Computational Energy (Piro 2009) consumed by the detection service, we have exploited the algorithm complexity of LIBSVM library computed in (Abdiansah & Wardoyo 2015) where we were particularly interested in the functions used for prediction (*load_svm_model* and *svm_predict*) and we have opted for microcontroller MICA V3.0 model, where the energy consumed by an instruction is 1.760 nJ. Thus, the energy consumed by our different IDS will be calculated as follows:

Energy_consumed = Total_instruction_number * energy consumed_by_an_instruction

C. **Results and Discussion**

Figure 5.5 gives results of attack implementation (network scenario under Sinkhole attack). Experiments were conducted to look for energy consumption in normal and under attack running. Figure 5.6 gives results of energy consumption for HIDS and NIDS running (network scenario with the proposed detection scheme). Figure5.7 details the remaining energy in each node in normal, HIDS and NIDS running. Finally, the figure 5.8 shows the remaining energy in our different experiments.

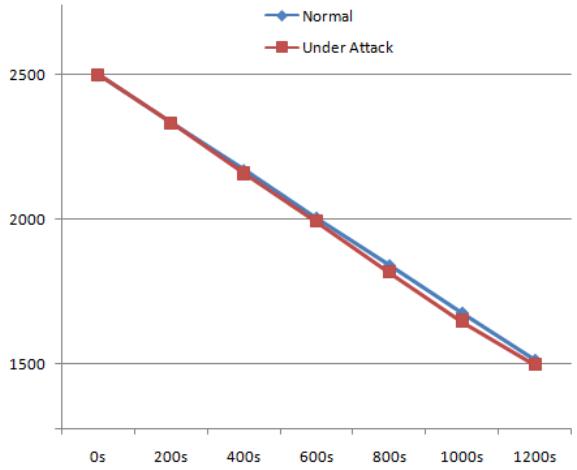

Figure 5.5 – *Energy consumption in normal and under attack running*

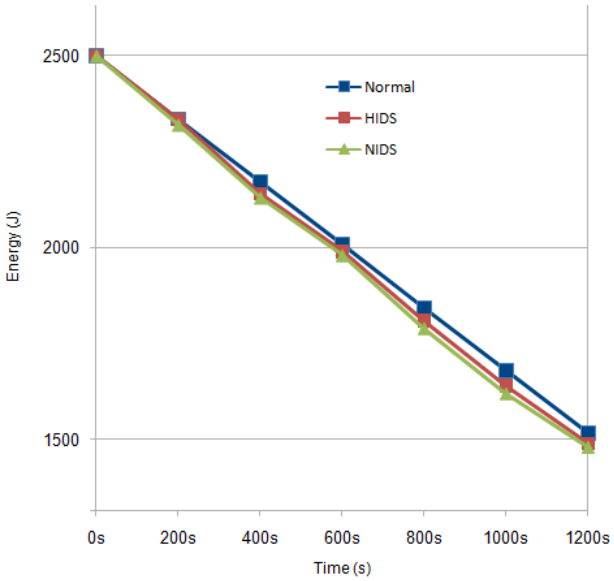

Figure 5.6 – *Energy consumption in Normal, HIDS and NIDS running*

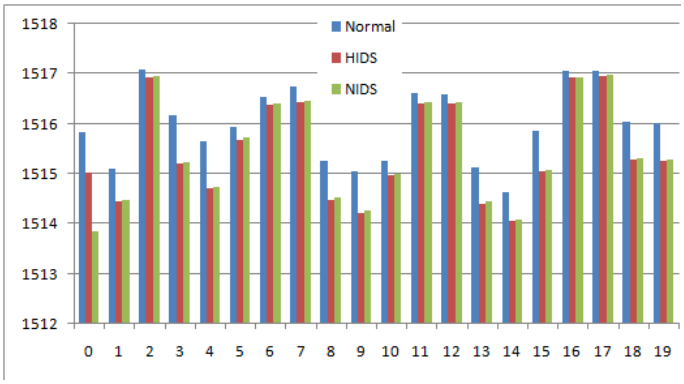

Figure 5.7 – *Remaining Energy in Normal, HIDS and NIDS running*

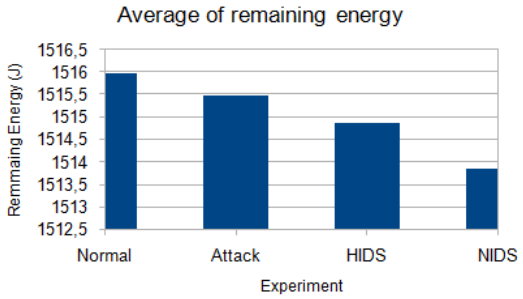

Figure 5.8 – *Comparing Remaining Energy*

The following table shows the average of remaining and consumed energy in simulated networks

Average	Normal	Under Attack	HIDS	NIDS
Average of WSN remaining energy (J)	1515.98	1515.49	1514.87	1513.84
Average of IDS consumed energy (J)	/	/	0,57	0,611
Detection Rate	/	/	100%	100%

Table 5.5 – *Remaining Energy in detection approaches*

Figure 5.5 illustrates the remaining energy of WSN in a normal and under Sinkhole attack. The results show that the Sinkhole attack does not affect the global network energy consumption because the Sinkhole attack aims to attract the flow to the malicious node without launching another attack.

In figure 5.6, we present the energy consumption in WSN under detection tasks. The results show the efficiency of our SVM-IDS where we note a slight increase in energy consumption in the detection task compared to normal running and figure 5.8 confirms the results: the energy consumed in the HIDS is 0.57 J and for the NIDS is 0.611 J (see Table 5.5) in a period of 1200s. On the other hand, the figure 5.7 details remaining energy on each node. The nodes that consumed more energy are the neighboring nodes (node 8, 9, 13 and 14) of the attacking node (node 1). These legitimate nodes are involved in updating their routing table and to notify their neighboring nodes.

Comparing the two IDS, we note that the HIDSs behave in the same way as NIDS with a slight superiority to the detection by HIDS with a detection rate in both of 100%. As a conclusion to our different results, we can say that our detection approach is energy saving with high rate detection. The favored system could be NIDS since the base station can have higher capacity compared to the deployed nodes, in contrary case the distributed architecture HIDS would be chosen.

In Table 5.6, experimental results presented in (Garofalo *et al.* 2013) are compared with our results (Aissaoui & Boukli-Hacene 2021). We can

Approaches	Accuracy
IDS based SVM (Aissaoui & Boukli-Hacene 2021)	100%
IDS based CART (Garofalo *et al.* 2013)	97.8%
IDS based CHAID (Garofalo *et al.* 2013)	99.4%
IDS based C5.0 (Garofalo *et al.* 2013)	99.5%

Table 5.6 – *IDS based SVM comparison*

see that our IDS has higher performances in term of detection rate than the solution proposed in (Garofalo *et al.* 2013).

In this work, we have proposed a centralized and standalone IDSs that use only 2 features to detect Sinkhole attacks with 100% accuracy with no additional computation or send of any information to base station. There is not any extra communication in proposed technique. However in (Garofalo *et al.* 2013), the authors used a distributed agent architecture based decision tree, which needs more then 10 computational parameters in training and detection task with a detection rate less then 100%. Further more, the exchanged messages between local agents and the central agent to make decision generate more traffic in the network with more energy consumption. In (Abdullah *et al.* 2015), the proposed approach can not detect successfully Sinkhole attack when the malicious node is near (1 or 2 hops) the base station. In (Sejaphala & Velempini 2020), the researchers have enhanced the results of (Abdullah *et al.* 2015) by using a statistical model in the detection schema. The model uses a change in position of each node calculated by the base station. This periodic calculation in position changing causes a processor overhead and energy consumption especially with important number of sensor nodes.

5.4 Conclusion

The DOS routing attacks are the most destructive attacks in WSN. They exploit the protocol routing vulnerabilities to launch attacks. In this thesis, we have presented a IDS based on SVM approach to detect Sinkhole attacks in wireless sensor network. Our proposed technique uses only two extracted features (HopCount and Destination Sequence Number) from AODV packets for detecting Sinkhole nodes, with no computational parameters or additional messages. The results show that our system is able to detect attack with 100% accuracy. Our technique is applicable to detect blackhole, wormhole and selective forwarding attacks as they are almost similar to Sinkhole attack and also it can easily be adapted to clustered WSNs.

We have implemented and tested by simulation in NS3 two IDS architectures, centralized (NIDS) and standalone (HIDS), in order to measure the trade-off between detection accuracy and energy depletion in the network. Our results confirm the efficiency of our IDS based on SVM approach in terms of detection rate and energy saving.

Conclusion and Futur work

In order to protect Wireless Sensor Networks (WSNs) from Sinkhole attack, this thesis presented an efficient and secure mechanism based on SVM to detect such attack in WSNs with energy issues in mind. The theoretical part presented the security issues and the proposed security mechanisms in WSN (see Chapter 2). The last proposed works in intrusion detection were reviewed in chapter 3. The chapter 4 gave a detailed overview on the proposed solution against Sinkhole attack in WSNs. We have concluded that the main challenge in detection of any attack in WSNs is achieving high detection rate with low energy depletion.

The proposed IDS is designed only on two extracted data from AODV packets circulating in the network, i.e. Hop Count and Destination Sequence Number (DSN) with no more calculated or combined parameters.

The designed system passed by two main phases: offline phase and online phase. In the first phase, construction of detection model based on SVM was performed. (Garofalo *et al.* 2013)'s dataset was used to train and test the generated SVM model on four kernel functions. Whereas, in the second phase, a real test was performed based on simulation in NS3 tool. Two IDS architectures were simulated in order to pick-up the most suitable for constraint-WSNs in terms of detection rate and energy consumption.

According to the simulation results, our proposed SVM-IDS outperformed existing algorithm in the literature, in terms of detection rate with an energy saving design (Aissaoui & Boukli-Hacene 2021) .

Futur Work

As future work, we propose to

- Study the other attacks present in network layer of wireless sensor network and which are significantly more difficult to detect.
- Test other classification algorithms, such as deep-learning techniques.
- Propose a cross layer approach in order to cope with multi-layer attack and to prolong the network lifetime.
- Adapt the proposed SVM-IDS to a clustered WSN.

Intrusion detection in WSN remains a very active research topic which requires more studies.

Scientific contributions

- Aissaoui, Sihem and Sofiane Boukli Hacene. "Sinkhole Attack Detection-Based SVM In Wireless Sensor Networks." IJWNBT vol.10, no.2 2021: pp.16-31. http://doi.org/10.4018/IJWNBT.2021070102

Bibliography

[Abdiansah & Wardoyo 2015] A. Abdiansah et R. Wardoyo. *Time complexity analysis of support vector machines (SVM) in LibSVM*. International Journal of Computers and Applications, vol. 128, page 28–34, 2015.

[Abdullah *et al.* 2015] Md. I. Abdullah, M. M. Rahman et M. C. Roy. *Detecting sinkhole attacks in wireless sensor network using hop count*. IJ Computer Network and Information Security, vol. 3, page 50–56, 2015.

[Abood *et al.* 2021] M.S. Abood, H. Wang, H.F. Mahdi, M.M Hamdi et A.S. Abdullah. *Review on secure data aggregation in Wireless Sensor Networks*. IOP Conf Series: Materials Science and Engineering, vol. 1076, 2021.

[Acla & Gerardo 2019] H. B. Acla et B. D. Gerardo. *Security Analysis of Lightweight Encryption based on Advanced Encryption Standard for Wireless Sensor Networks*. IEEE 6th International Conference on Engineering Technologies and Applied Sciences (ICETAS), pages 1–6, 2019.

[Ahmad *et al.* 2019] B. Ahmad, W. Jian, R.N. Enam et A. Abbas. *Classification of DoS Attacks in Smart Underwater Wireless Sensor Network*. Wireless Personal Communications, 2019.

[Ahutu & El-Ocla 2020] O. R. Ahutu et H. El-Ocla. *Centralized routing protocol for detecting wormhole attacks in wireless sensor networks*. IEEE Access, vol. 8, pages 63270–63282, 2020.

[Aissaoui & Boukli-Hacene 2021] S. Aissaoui et S. Boukli-Hacene. *Sinkhole Attack Detection-Based SVM In Wireless Sensor Networks*. International Journal of Wireless Networks and Broadband Technologies (IJWNBT), IGI Global, vol. 10, pages 16–31, 2021.

[Ajaykumar *et al.* 2020] N. Ajaykumar, M. Sarvagya et P. Parandkar. *A novel security algorithm ECC-L for wireless sensor network*. Internet Technology Letters, vol. 3, 2020.

[Akyildiz & and 2006] I.F Akyildiz et E.P. Stuntebeck and. *Wireless underground sensor networks: research challenges*. Ad-Hoc Networks, vol. 4, pages 669–686, 2006.

[Akyildiz *et al.* 2002] I.F Akyildiz, W. Su et E. Cayirci Y. Sankarasubramaniam. *Wireless sensor networks: a survey*. Computer Networks, vol. 38, pages 393–422, 2002.

[Akyildiz *et al.* 2004] I.F Akyildiz, D. Pompili et T. Melodia. *Challenges for efficient communication in underwater acoustic sensor networks*. ACM Sigbed Review 1, vol. 2, pages 3–8, 2004.

[Alaparthy & Morgera 2019] V. Alaparthy et S.D. Morgera. *Modeling an Intrusion Detection System Based on Adaptive Immunology*. International Journal of Interdisciplinary Telecommunications and Networking, IGI Global, vol. 11, page 42–55, 2019.

[Albakri *et al.* 2019] A. Albakri, L. Harn et S. Song. *Hierarchical Key Management Scheme with Probabilistic Security in a Wireless Sensor Network (WSN)*. Security and Communication Networks, vol. 2019, 2019.

[Ali *et al.* 2020a] M. Ali, M. Nadeem, A. Siddique, S. Ahmad et A. Ijaz. *Addressing Sinkhole Attacks In Wireless Sensor Networks - A Review*. International Journal of Scientific & Technology Research, vol. 9, pages 406–411, August 2020.

[Ali *et al.* 2020b] S. Ali, A Humaria, M.S. Ramzan, I. Khan, S.M. Saqlain, A. Ghani, J. Zakia et B.A. Alzahrani. *An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks*. International Journal of Distributed Sensor Networks, vol. 16, 2020.

[Aliady & Al-Ahmadi 2019] W. A. Aliady et S. A. Al-Ahmadi. *Energy preserving secure measure against wormhole attack in wireless sensor networks*. IEEE Access, vol. 7, pages 84132–84141, 2019.

[Almomani *et al.* 2016] I. Almomani, B. Al-Kasasbeh et M. Al-Akhras. *WSN-DS: A dataset for intrusion detection systems in wireless sensor networks*. Journal of Sensors, pages 1–16, 2016.

[Ambika 2021] N. Ambika. *Improved Cross-Layer Detection and Prevention of Sinkhole Attack in WSN*. Encyclopedia of Information Science and Technology, Fifth Edition, IGI-Global, pages 514–527, 2021.

[Anand & Vasuki 2021] C. Anand et N. Vasuki. *Trust Based DoS Attack Detection in Wireless Sensor Networks for Reliable Data Transmission*. Wireless Personal Communications, 2021.

[Anantvalee & Wu 2007] T. Anantvalee et J. Wu. *A survey on intrusion detection in mobile ad hoc networks*. Wireless Network Security, page 159–180, 2007.

[Anderson 1980] J.P Anderson. *Computer Security Threat Monitoring and Surveillance*. Technical report, James P.Anderson Co., Fort Washington, Pennsylvania, 1980.

[Anitha & Anjusree 2014] A. S. Subaira P. Anitha et S. Anjusree. *An approach for ids by combining svm and ant colony algorithm*. International Journal of Research in Engineering and Technology, vol. 3, page 459–465, 2014.

[Ansar *et al.* 2021] J. Ansar, A.Q Mohammed et A.E Muhammed. *Sinkhole Attack Detection and Avoidance Mechanism for RPL in Wireless*

Sensor Networks. Annals of Emerging Technologies in Computing (AETiC), vol. 5, pages 94–101, March 2021.

[Aranda† *et al.* 2020] J. Aranda†, D. Mendez et H. Carrillo. *Multimodal Wireless Sensor Networks for Monitoring Applications: A Review*. Journal of Circuits, Systems, and Computers, vol. 29, 2020.

[Arya & Binu 2017] I.S. Arya et G.S. Binu. *Cross Layer Approach For Detection and Prevention Of Sinkhole Attack Using A Mobile Agent*. Proceedings of the 2nd International Conference on Communication and Electronics Systems (ICCES 2017), IEEE Xplore Compliant, pages 359–365, 2017.

[Aslan *et al.* 2020] B. Aslan, F.Y. Aslan et M. Tolga Sakallı. *Energy Consumption Analysis of Lightweight Cryptographic Algorithms That Can Be Used in the Security of Internet of Things Applications*. Security and Communication Networks, vol. 2020, 2020.

[Babaeer & Al-Ahmadi 2020] H.A. Babaeer et S.A. Al-Ahmadi. *Efficient and Secure Data Transmission and Sinkhole Detection in a Multi-Clustering Wireless Sensor Network Based on Homomorphic Encryption and Watermarking*. IEEE Access, pages 92098–92109, 2020.

[Baldovino *et al.* 2018] R. G. Baldovino, I. C. Valenzuela et E. P. Dadios. *Implementation of a low-power wireless sensor network for smart farm applications*. In 2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM). IEEE, pages 1–5, November 2018.

[Banga *et al.* 2021] S. Banga, H. Arora, S. Sankhla, G. Sharma et B. Jain. *Performance Analysis of Hello Flood Attack in WSN*. Proceedings of International Conference on Communication and Computational Technologies, Springer, pages 335–342, 2021.

[Bayou *et al.* 2017] L. Bayou, D. Espes, N. Cuppens-Boulahia et F. Cuppens. *wIDS: a multilayer IDS forWireless-based SCADA Systems*. ICISS 2017: 13th International Conference on Information Systems Security, Mumbai, India, pages 387–404, December 2017.

[Bensaid *et al.* 2016] C. Bensaid, S. Boukli-Hacene et MK.Faraoun. *Detection and ignoring of blackhole attack in vanets networks*. International Journal of Cloud Applications and Computing (IJCAC), vol. 6, no. 2, pages 1–10, 2016.

[Biryukov & Perrin 2017] A. Biryukov et L. Perrin. *State of the Art in Lightweight Symmetric Cryptography*. IACR Cryptol. ePrint Arch, vol. 2017, page 511, 2017.

[Boni *et al.* 2020] K.R.C. Boni, L. Xu, Z. Chen et T.D. Baddoo. *A Security Concept Based on Scaler Distribution of a Novel Intrusion Detection Device for Wireless Sensor Networks in a Smart Environment*. Sensors, vol. 20, 2020.

[Borkar *et al.* 2019] G.M. Borkar, L.H. Patilb, D. Dalgadec et A. Hutked. *A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept*. Sustainable Computing: Informatics and Systems, vol. 23, page 120–135, 2019.

[Boukli-Hacene *et al.* 2006] S. Boukli-Hacene, A. Lehireche et A. Meddahi. *Predictive preemptive ad hoc on-demand distance vector routing*. Malaysian Journal of Computer Science, vol. 19, no. 2, pages 189–195, 2006.

[Bruth & Ko 2003] P. Bruth et C. Ko. *Challenges in Intrusion detection for wireless ad hoc networks*. in Proceedings of Symposium on Application and the Internet Workshop, pages 368–373, 2003.

[Butun 2013] I. Butun. *Prevention and Detection of Intrusions in Wireless Sensor Networks*. Graduate Theses and Dissertations, June 2013.

[Chang & Lin 2011] C. C. Chang et C. J. Lin. *LIBSVM: A library for support vector machines*. ACM Transactions on Intelligent Systems and Technology (TIST), vol. 2, pages 1–27, 2011.

[Chen *et al.* 2010a] R. C. Chen, Y. F. Y. F. Haung et C. F. Hsieh. *Ranger intrusion detection system for wireless sensor networks with Sybil attack based on ontology*. New aspects of applied informatics, Biomedical Electronics and Informatics and Communications, pages 176–180, 2010.

[Chen *et al.* 2010b] Y. S. Chen, Y. S. Qin, Xiang Y. G., J. X. Zhong et X. L. Jiao. *Intrusion detection system based on immune algorithm and support vector machine in wireless sensor network*. International Symposium on Information and Automation, pages 372–376, 2010.

[Chen *et al.* 2017] X. Chen, Y. Xu et A. Liu. *Cross layer design for optimizing transmission reliability, energy efficiency, and lifetime in body sensor networks*. Sensors, vol. 17, page 900, 2017.

[Chen *et al.* 2021] J. Chen, T. Yang, B. He et L. He. *An analysis and research on wireless network security dataset*. 2021 International Conference on Big Data Analysis and Computer Science (BDACS), pages 80–83, 2021.

[Cortes & Vapnik 1995] C. Cortes et V. Vapnik. *Support-vector networks*. Machine Learning, Kluwer Academic Publishers, Boston, vol. 20, page 273–297, 1995.

[daSilva *et al.* 2005] A. daSilva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz et H.Wong. *Decentralized intrusion detection in wireless sensor networks*. in Proceedings of the 1st ACM international workshop on Quality of service and security in wireless and mobile networks. ACM, page 16–23, 2005.

[Devibala *et al.* 2017] K. Devibala, S. Balamurali, A. Ayyasamy et M. Archana. *Flow Based Mitigation Model for Sinkhole Attack in Wireless Sensor Networks using Time-Variant Snapshot*. International Jour-

nal of Advances in Computer and Electronics Engineering (ijacee), vol. 2, pages 14–21, May 2017.

[Dhanda *et al.* 2020] S.S. Dhanda, B. Singh et P. Jindal. *Lightweight Cryptography: A Solution to Secure IoT*. Wireless Personal Communications, vol. 112, page 1947–1980, 2020.

[Dong *et al.* 2020] S. Dong, X. G. Zhang et W. G. Zhou. *A security localization algorithm based on DV-hop against sybil attack in wireless sensor networks*. Journal of Electrical Engineering & Technology, Springer, vol. 15, pages 919–926, 2020.

[Elqusy *et al.* 2017] A.S. Elqusy, S.E. Essa et A. El-Sayed. *A Key Management Techniques in Wireless Sensor Networks*. Communications on Applied Electronics (CAE), vol. 7, pages 8–18, May 2017.

[Faheem *et al.* 2018] M. Faheem, R.A. Butt, B. Raza, M.W. Ashraf, Seema Begum, Md.A. Ngadi et V.C. Gungor. *Bio-inspired routing protocol for WSN-based smart grid applications in the context of Industry 4.0*. Transactions on Emerging Telecommunications Technologies, August 2018.

[Fute *et al.* 2020] E.T. Fute, A.T. Nangue et E. Tonye. *An Efficient and Secured AODV Protocol against Black Hole Attacks on Wireless Sensor Networks*. International Journal of Computer Science and Information Security (IJCSIS), vol. 18, pages 112–119, June 2020.

[Gandhimathi & Murugaboopathi 2016] L. Gandhimathi et G. Murugaboopathi. *Cross layer intrusion detection and prevention of multiple attacks in Wireless Sensor Network using Mobile agent*. Information Communication and Embedded Systems (ICICES), 2016 International Conference on. IEEE, 2016.

[Garofalo *et al.* 2013] A. Garofalo, C. Di Sarno et V. Formicola. *Enhancing intrusion detection in wireless sensor networks through decision trees*. In European Workshop on Dependable Computing. Springer, pages 1–15, June 2013.

[Gavel *et al.* 2021] S. Gavel, A.S. Raghuvanshi et S. Tiwari. *A novel density estimation based intrusion detection technique with Pearson's divergence for Wireless Sensor Networks*. ISA Transactions, vol. 111, pages 180–191, May 2021.

[Gavrić & Simić 2018] Ž. Gavrić et D. Simić. *Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks*. Ingeniería E Investigación, vol. 38, pages 130–138, 2018.

[Ghosal & Halder 2017] A. Ghosal et S. Halder. *A survey on energy efficient intrusion detection in wireless sensor networks*. Journal of Ambient Intelligence and Smart Environments, vol. 9, page 239–261, 2017.

[Ghugar & Sahoo 2019] U. Ghugar et J. Pradhan S.K. Bhoi R.R. Sahoo. *LB-IDS: Securing Wireless Sensor Network Using Protocol Layer Trust-Based Intrusion Detection System*. Journal of Computer Networks and Communications, pages 1–13, 2019.

[Gill & Sachdeva 2018] R. K. Gill et M. Sachdeva. *Detection of hello flood attack on LEACH in wireless sensor networks*. Next-generation networks, Springer, pages 377–387, 2018.

[Giri *et al.* 2021] A. Giri, S. Dutta et S. Neogy. *Information-theoretic approach for secure localization against sybil attack in wireless sensor network*. Journal of Ambient Intelligence and Humanized Computing, Springer, vol. 12, pages 9491–9497, 2021.

[Gnanapriya & Ramya 2020] P Gnanapriya et P. Ramya. *Secure And Energy Efficient Detection of Wormhole Attack in WSN Using Hybrid Approach*. Journal of Xi'an University of Architecture & Technology, vol. 12, pages 267–276, 2020.

[Godala & Vaddella 2020] S. Godala et R.P Vaddella. *Study on Intrusion Detection System in Wireless Sensor Networks*. International Journal of Communication Networks and Information Security (IJCNIS), vol. 12, pages 127–141, April 2020.

[Gulen & Baktir 2020] U. Gulen et S. Baktir. *Elliptic Curve Cryptography for Wireless Sensor Networks Using the Number Theoretic Transform*. Sensors, vol. 20, 2020.

[Gunathilake *et al.* 2020] N. A. Gunathilake, A. Al-Dubai et W. Buchanan. *Recent Advances and Trends in Lightweight Cryptography for IoT Security*. 2020 16th International Conference on Network and Service Management (CNSM), pages 1–5, 2020.

[Hamad & Abid 2017] I. El Haj Hamad et M. Abid. *BTRMC, a bio-inspired trust and reputation model using clustering in WSNs*. 2017 International Conference on Smart, Monitored and Controlled Cities (SM2C), pages 5–11, May 2017.

[Hamsha & Nagaraja 2019] K. Hamsha et G. S. Nagaraja. *Threshold cryptography based light weight key management technique for hierarchical WSNs*. Ubiquitous Communications and Network Computing, vol. 276, page 188–197, 2019.

[Han *et al.* 2015] G. Han, X. Li, J. Jiang, L. Shu et J. Lloret. *Intrusion Detection Algorithm Based on Neighbor Information Against Sinkhole Attack in Wireless Sensor Networks*. The Computer Journal, vol. 58, page 1280–1292, June 2015.

[Han *et al.* 2019] L. Han, M. Zhou, W. Jia, Z. Dalil et X. Xu. *Intrusion Detection Model of Wireless Sensor Networks Based on Game Theory and an Autoregressive Model*. Information Sciences, 2019.

[Hasan *et al.* 2021] B. Hasan, S. Alani et M.A. Saad. *Secured node detection technique based on artificial neural network for wireless sensor network*. International Journal of Electrical and Computer Engineering (IJECE), vol. 11, pages 536–544, February 2021.

[Heidemann *et al.* 2006] J. Heidemann, Y. Li, A. Syed, J. Wills et W. Ye. *Underwater sensor networking: research challenges and potential applications*. In USC/ISI Technical Report ISI-TR-2005-603, 2006.

[Hua *et al.* 2018] P. Hua, X. Liu, J. Yua, N. Danga et X. Zhang. *Energy efficient adaptive slice based secure data aggregation scheme in WSN*. Procedia Computer Science, vol. 129, page 188–193, 2018.

[Ioannou & Vassiliou 2018] C. Ioannou et V. Vassiliou. *An Intrusion Detection System for Constrained WSN and IoT Nodes Based on Binary Logistic Regression*. Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems - MSWIM '18, page 259–263, October 2018.

[Iqbal & Shafi 2019] U. Iqbal et S. Shafi. *A Provable and Secure Key Exchange Protocol Based on the Elliptical Curve Diffe–Hellman for WSN*. Advances in Big Data and Cloud Computing, pages 363–372, 2019.

[Ishmanov & Bin-Zikria 2017] F. Ishmanov et Y. Bin-Zikria. *Trust Mechanisms to Secure Routing in Wireless Sensor Networks: Current State of the Research and Open Research Issues*. Journal of Sensors, vol. 2017, page 16, 2017.

[Jahandoust & Ghassemi 2017] G. Jahandoust et F. Ghassemi. *An adaptive sinkhole aware algorithm in wireless sensor networks*. Ad Hoc Networks, Elsevier, vol. 59, page 24–34, 2017.

[Jamshidi *et al.* 2019] M. Jamshidi, E. Zangeneh, M. Esnaashari, A. M. Darwesh et M. R. Meybodi. *A novel model of sybil attack in cluster-based wireless sensor networks and propose a distributed algorithm to defend it*. Wireless Personal Communications, Springer, vol. 105, pages 145–173, 2019.

[Jatti & Kishor-Sonti 2021] A.V. Jatti et V.J.K. Kishor-Sonti. *Sinkhole Attack Detection and Prevention using Agent Based Algorithm*. Journal of University of Shanghai for Science and Technology, vol. 23, pages 526–544, May 2021.

[Jianjian *et al.* 2018] D. Jianjian, T. Yang et Y. Feiyue. *A novel intrusion detection system based on IABRBFSVM for wireless sensor networks*. Procedia Computer Science, vol. 131, pages 1113–1121, 2018.

[Kakria *et al.* 2015] P. Kakria, N. Tripathi et P. Kitipawang. *A Real-Time Health Monitoring System for Remote Cardiac Patients Using Smartphone and Wearable Sensors*. International Journal of Telemedicine and Applications, vol. 2015, pages 1–11, 2015.

[Kalam *et al.* 2003] A.A.E. Kalam, R.E. Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miege, C. Saurel et G. Trouessin. *Organization based access control*. In: Policies for Distributed Systems and

Networks 2003 Proceedings. POLICY 2003, IEEE 4th International Workshop on, page 120–131, June 2003.

[Kalkha *et al.* 2019] H. Kalkha, H. Satori et K. Satori. *Preventing black hole attack in wireless sensor network using HMM*. Procedia computer science, vol. 148, pages 552–561, 2019.

[Kalnoor & Agarkhed 2018] G. Kalnoor et J. Agarkhed. *Detection of Intruder using KMP Pattern Matching Technique in Wireless Sensor Networks*. Procedia Computer Science, vol. 125, page 187–193, 2018.

[Kalnoor *et al.* 2017] G. Kalnoor, J. Agarkhed et S.R. Patil. *Agent-Based QoS Routing for Intrusion Detection of Sinkhole Attack in Clustered Wireless Sensor Networks*. In: Satapathy S., Prasad V., Rani B., Udgata S., Raju K. (eds) Proceedings of the First International Conference on Computational Intelligence and Informatics. Advances in Intelligent Systems and Computing, vol. 507, pages 571–583, 2017.

[Kandris *et al.* 2020] D. Kandris, C. Nakas, D. Vomvas et G. Koulouras. *Applications of Wireless Sensor Networks: An Up-to-Date Survey*. Applied System Innovation, vol. 3, 2020.

[Kaplantzis *et al.* 2007] S. Kaplantzis, A. Shilton, N. Mani et Y. A. Sekercioglu. *Detecting selective forwarding attacks in wireless sensor networks using support vector machines*. In 2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information. IEEE, pages 335–340, December 2007.

[Kardi & Zagrouba 2019] A. Kardi et R. Zagrouba. *Attacks classification and security mechanisms in Wireless Sensor Networks*. Advances in Science, Technology and Engineering Systems Journal, vol. 4, pages 229–243, 2019.

[Karthigadevi *et al.* 2019] K. Karthigadevi, S. Balamurali et M. Venkatesulu. *Based on Neighbor Density Estimation Technique to Improve the Quality of Service and to Detect and Prevent the Sinkhole Attack in Wireless Sensor Network*. IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), 2019.

[Kashyap 2020] R. Kashyap. *Applications of Wireless Sensor Networks in Healthcare*. In P. Mukherjee, P. Pattnaik, & S. Panda (Eds.), IoT and WSN Applications for Modern Agricultural Advancements: Emerging Research and Opportunities, pages 8–40, 2020.

[Kaur & Rattan 2021] N. Kaur et P. Rattan. *A Critical Review of Intrusion Detection Systems in WSN: Challenges & Future Directions*. Annals of the Romanian Society for Cell Biology, vol. 25, page 3020–3028, April 2021.

[Khan *et al.* 2019] T. Khan, K. Singh, L.H. Son, M. Abdel-Basset, H.V. Long, S.P Singh et M. Manjul. *A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks*. IEEE Access, vol. 7, 2019.

[Khan *et al.* 2020] K. Khan, A. Mehmood, S. Khan, M.A Khan, Z. Iqbal et W.K Mashwani. *A survey on intrusion detection and prevention in wireless ad-hoc networks*. Journal of Systems Architecture, vol. 105, 2020.

[Khraisat *et al.* 2020] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman et A. Alazab. *Hybrid Intrusion Detection System Based on the Stacking Ensemble of C5 Decision Tree Classifier and One Class Support Vector Machine*. Electronics, vol. 9, page 173, 01 2020.

[Kibirige & Sanga 2015] G. Kibirige et C. Sanga. *A Survey on Detection of Sinkhole Attack in Wireless Sensor Network*. International Journal of Computer Science and Information Security, vol. 13, pages 1–9, 05 2015.

[Krontiris 2008] I. Krontiris. *Intrusion Prevention and Detection in Wireless Sensor Networks*. PhD dissertation in University of Mannheim,Germany, 2008.

[Lara-Nino *et al.* 2018] C.A. Lara-Nino, A. Diaz-Perez et M. Morales-Sandoval. *Elliptic Curve Lightweight Cryptography: A Survey*. IEEE Access, vol. 6, pages 72514–72550, 2018.

[Lee *et al.* 2007] H. Lee, Y.H. Kim, D.H Lee et J. Lim. *Classification of key management schemes for wireless sensor networks*. In Advances in Web and Network Technologies, and Information Management, pages 664–673, 2007.

[Li & and 2007] M. Li et Y. Liu and. *Underground structure monitoring with wireless sensor networks*. In IPSN '07 In Proceedings of the 6th international conference on Information processing in sensor networks, page 69–78. Association for Computing Machinery, 2007.

[Li & Wu 2020] Y. Li et Y. Wu. *Combine clustering with game to resist selective forwarding in wireless sensor networks*. IEEE Access, vol. 8, pages 138382–138395, 2020.

[Li *et al.* 2018] Y. Li, M. Du et Y. Li. *Routing Attacks Detection Method of Wireless Sensor Network*. 14th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2018), pages 255–265, 2018.

[Lim *et al.* 2010] H.B. Lim, D. Ma, B. Wang, Z. Kalbarczyk, RK. Iyer et K.L. Watkin. *A soldier health monitoring system for military applications*. In Proceedings of the 2010 International Conference on Body Sensor Networks- Singapore- 7–9 June 2010, page 246–249, 2010.

[Liu & Wu 2021] Y. Liu et Y. Wu. *Employ DBSCAN and Neighbor Voting to Screen Selective Forwarding Attack under Variable Environment in Event-driven Wireless Sensor Networks*. IEEE Access, 2021.

[Lu *et al.* 2018] N. Lu, Y. Sun, H. Liu et S. Li. *Intrusion Detection System Based on Evolving Rules for Wireless Sensor Networks*. Journal of Sensors, pages 1–8, 2018.

[Luhach 2016] A.K. Luhach. *Analysis of lightweight cryptographic solutions for Internet of Things*. Indian Journal of Science and Technology, vol. 9, 2016.

[Manifavas *et al.* 2014] C. Manifavas, G. Hatzivasilis, K. Fysarakis et K. Rantos. *Lightweight cryptography for embedded systems–A comparative analysis*. In Data Privacy Management and Autonomous Spontaneous Security. Springer, pages 333–349, 2014.

[Mehta *et al.* 2018] G. Mehta, P. Singla et R. Mittal. *Security Techniques of WSN: A Review*. International Journal of Computer Science and Mobile Computing, vol. 7, pages 167–172, 2018.

[Mesmoudi *et al.* 2019] S. Mesmoudi, B. Benadda et A. Mesmoudi. *SKWN: Smart and dynamic key management scheme for wireless sensor networks*. International Journal of Communication Systems, vol. 32, 02 2019.

[Messai 2014] M.L. Messai. *Classification of Attacks in Wireless Sensor Networks*. International Congress on Telecommunication and Application'14, April 2014.

[Mitchell & Chen 2014] R. Mitchell et I. R. Chen. *A Survey of Intrusion Detection in Wireless Network Applications*. Computer Communications, vol. 42, page 1–23, 2014.

[Mohammadi *et al.* 2011] S. Mohammadi, R.E. Atani et H. Jadidoleslamy. *Network Topologies in Wireless Sensor Networks: A Review*. Journal of Information Assurance and Security, vol. 6, pages 195–215, 2011.

[Mohapatra *et al.* 2020] H. Mohapatra, S. Rath, S. Panda et R. Kumar. *Handling of Man-In-The-Middle Attack in WSN Through Intrusion Detection System*. International Journal of Emerging Trends in Engineering Research, vol. 8, pages 1503–1510, May 2020.

[Moulad *et al.* 2017] L. Moulad, H. Belhadaoui et M. Rifi. *Implementation of a hierarchical hybrid intrusion detection mechanism in wireless sensors network*. International Journal of Advances in Computer Science Applications, vol. 8, page 270–278, 2017.

[Moustafa & Slay 2015] N. Moustafa et J. Slay. *UNSW-NB15: a comprehensive data set for network intrusion detection systems*. Proceedings of the military communications and information systems conference (MilCIS). IEEE, pages 1–6, 2015.

[Muduli *et al.* 2018] L. Muduli, D. P. Mishra et P. K. Jana. *Application of wireless sensor network for environmental monitoring in underground coal mines: A systematic review*. Journal of Network and Computer Applications, vol. 106, pages 48–67, 2018.

[Nadeem & Alghamdi 2019] A. Nadeem et T. Alghamdi. *Detection Algorithm for Sinkhole Attack in Body Area Sensor Networks Using Local Information*. International Journal of Network Security, vol. 21, pages 670–679, 07 2019.

[Narayanan *et al.* 2021] K. L. Narayanan, R. S. Krishnan, J. E. Golden, Y. H. Robinson et V. Shanmuganathan. *Machine Learning Based Detection and a Novel EC-BRTT Algorithm Based Prevention of DoS Attacks in Wireless Sensor Networks*. Wireless Personal Communications, pages 1–25, 2021.

[Naresh *et al.* 2018] V.S. Naresh, R. Sivaranjani et N.V.E.S. Murthy. *Provable secure lightweight hyper elliptic curve-based communication system for wireless sensor networks*. International Journal of Communication Systems, vol. 31, 2018.

[Naseer *et al.* 2020] A.R. Naseer, V. Neelima et G. Narsimha. *Swarm Intelligence-Based Bio-Inspired Framework for Wireless Sensor Networks*. Wireless Sensor Networks - Design, Deployment and Applications, Siva S. Yellampalli, IntechOpen, September 2020.

[Naz *et al.* 2012] P. Naz, S. Hengy et P. Hamery. *Soldier detection using unattended acoustic and seismic sensors*. In Proceedings of the SPIE 8389, Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR III, 83890T, Baltimore, MD, USA, May 2012.

[Newsome *et al.* 2004] J. Newsome, E. Shi, D. Song et A. Perrig. *The sybil attack in sensor networks: analysis & defenses*. IPSN '04: Proceedings of the third international symposium on Information processing in sensor networks, page 259–268, 2004.

[Nithiyanandam & Latha 2019] N. Nithiyanandam et P. Latha. *Artificial bee colony based sinkhole detection in wireless sensor networks*. Journal of Ambient Intelligence and Humanized Computing, July 2019.

[Nivaashini & Thangaraj 2018] M. Nivaashini et P. Thangaraj. *A Framework of Novel Feature Set Extraction based Intrusion Detection System for Internet of Things using Hybrid Machine Learning Algorithms*. 2018 International Conference on Computing, Power and Communication Technologies (GUCON) Galgotias University, Greater Noida, UP, India, pages 44–49, September 2018.

[Olariu *et al.* 2005] S. Olariu, A. Wadaa, L. Wilson, Q. Xu, M. Eltoweissy et K. Jones. *Providing Holistic Security in Sensor Networks*. In Broadband Satellite Comunication Systems and the Challenges of Mobility, pages 123–134. Springer US, 2005.

[Osanaiye *et al.* 2018] O. Osanaiye, A.S. Alfa et G.P. Hancke. *A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks*. Sensors, vol. 18, 2018.

[Otoum *et al.* 2019] S. Otoum, B. Kantarci et H.T. Mouftah. *On the Feasibility of Deep Learning in Sensor Network Intrusion Detection*. IEEE Networking Letters, 2019.

[Parween & Hussain 2020] S. Parween et S.Z. Hussain. *A Review on Cross-Layer Design Approach in WSN by Different Techniques*. Advances in Science, Technology and Engineering Systems, vol. 5, pages 741–754, 2020.

[Pathan *et al.* 2006] A.K. Pathan, H.W. Lee et C.S. Hong. *Security in wireless sensor networks: issues and challenges*. In 2006 8th International Conference Advanced Communication Technology, IEEE, vol. 2, pages 1043–1048, 2006.

[Perkins *et al.* 2000] C.E. Perkins, S.R. Das et E. Royer. *Ad-Hoc on Demand Distance Vector routing (AODV)*. Mobile Computing Systems and Applications, Prentice-Hall, pages 90–100, 2000.

[Piro 2009] R. M. Piro. *Resource usage accounting in Grid computing*. In Handbook of Research on Grid Technologies and Utility Computing: Concepts for Managing Large-Scale Applications. IGI Global, page 183–193, 2009.

[Qu *et al.* 2018] H. Qu, Z. Qiu, X. Tang, M. Xiang et P. Wang. *Incorporating unsupervised learning into intrusion detection for wireless sensor networks with structural co-evolvability*. Applied Soft Computing, vol. 71, page 939–951, 2018.

[Qurishee *et al.* 2020] M. Qurishee, Weidong B. Atolagbe W. Wu, S. Said, A. Ghasemi et S.M. Tareq. *Wireless Sensor Network and its Application in Civil Infrastructure*. International Research Journal of Engineering and Technology (IRJET), vol. 7, page 155–174, 2020.

[Raghav *et al.* 2020] R.S Raghav, K. Thirugnansambandam et D.KAnguraj. *Beeware Routing Scheme for Detecting Network Layer Attacks in Wireless Sensor Networks*. Wireless Personnal Communications, vol. 112, page 2439–2459, 2020.

[Raju & Parwekar 2016] I. Raju et P. Parwekar. *Detection of Sinkhole Attack in Wireless Sensor Network*. In: Satapathy S., Raju K., Mandal J., Bhateja V. (eds) Proceedings of the Second International Conference on Computer and Communication Technologies. Advances in Intelligent Systems and Computing. Springer, New Delhi, vol. 381, pages 629–636, 2016.

[Rani *et al.* 2020] S. Rani, N. Saravanakumar, S. Rajeyyagari et V. Porkodi S. H. Bouk. *QoS aware cross layer paradigm for urban development applications in IoT*. Wireless Networks, vol. 26, pages 6203–6214, 2020.

[Ranjan & Varma 2016] R. Ranjan et S. Varma. *Challenges and implementation on cross layer design for wireless sensor networks*. Wireless personal communications, vol. 86, pages 1037–1060, 2016.

[Rassam *et al.* 2012] M. Rassam, M. Maarof et A. Zainal. *A Survey of Intrusion Detection Schemes in Wireless Sensor Networks*. American Journal of Applied Sciences, vol. 9, pages 1636–1652, 01 2012.

[Rehman *et al.* 2019] Au. Rehman, S.U. Rehman et H.Raheem. *Sinkhole Attacks in Wireless Sensor Networks: A Survey*. Wireless Personal Communications, vol. 106, page 2291–2313, 2019.

[Riaz *et al.* 2018] M.N. Riaz, A. Buriro et A.Mahboob. *Classification of Attacks on Wireless Sensor Networks: A Survey*. International Journal of Wireless and Microwave Technologies(IJWMT), vol. 4, pages 15–39, 2018.

[Ring *et al.* 2017] M. Ring, S. Wunderlich, D. Grüdl, D. Landes et A. Hotho. *Flow-based benchmark data sets for intrusion detection*. In: Proceedings of the European conference on cyber warfare and security (ECCWS). ACPI, page 361–369, 2017.

[Ring *et al.* 2019] M. Ring, S. Wunderlich, D. Scheuring, D. Landes et A. Hotho. *A survey of network-based intrusion detection data sets*. Computers & Security (Elsevier), vol. 86, pages 147–167, 2019.

[Sadeghizadeh & Marouzi 2018] M. Sadeghizadeh et O.R. Marouzi. *A Lightweight Intrusion Detection System Based on Specifications to Improve Security in Wireless Sensor Networks*. Journal of Communication Engineering, vol. 7, 2018.

[Sadkhan & Salman 2018] S.B. Sadkhan et A.O. Salman. *A survey on lightweight-cryptography status and future challenges*. International Conference on Advance of Sustainable Engineering and its Application (ICASEA), pages 105–108, 2018.

[Saeedi & Al-Qurabat 2021] I. Dakhil Idan Saeedi et A. Kadhum Al-Qurabat. *A Systematic Review of Data Aggregation Techniques in Wireless Sensor Networks*. Journal of Physics: Conference Series 1818, 2021.

[Safaldin *et al.* 2021] M. Safaldin, M. Otair et L. Abualigah. *Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks*. Journal of ambient intelligence and humanized computing, Springer, vol. 12, pages 1559–1576, 2021.

[Sah & Amgoth 2018] D. K. Sah et T. Amgoth. *Parametric survey on cross-layer designs for wireless sensor networks*. Computer Science Review, vol. 27, page 112–134, 2018.

[Saini *et al.* 2021] R. K. Saini, M. Singh et P. Saini. *Improve energy-efficiency of sensors using cross-layer design technique in WSNs*. Journal of Physics: Conference Series, vol. 1714, page 012031, 2021.

[Sajan & Jasper 2021] R. Isaac Sajan et J. Jasper. *A secure routing scheme to mitigate attack in wireless adhoc sensor network*. Computers & Security, Elsevier, vol. 103, 2021.

[Salehi *et al.* 2021] H. Salehi, R. Burgueño, S. Chakrabartty, N. Lajnef et A.H. Alavif. *A comprehensive review of self-powered sensors in civil infrastructure: State-of-the-art and future research trends*. Engineering Structures, Elsevier, vol. 234, May 2021.

[Sandhu *et al.* 2018] J.K. Sandhu, A.K. Verma et P.S. Rana. *A Compendium of Security Issues in Wireless Sensor Networks*. Computer and Cyber Security, 2018.

[Saputra *et al.* 2020] R. Saputra, J. Andika et M. Alaydrus. *Detection of Blackhole Attack in Wireless Sensor Network Using Enhanced Check Agent*. 2020 Fifth International Conference on Informatics and Computing (ICIC), IEEE, pages 1–4, 2020.

[Scarfone & Mell 2007] K. Scarfone et P. Mell. *Guide to intrusion detection and prevention systems (IDPS)*. National Institute of Standards and Technology (NIST) Special Publication, Department of Commerce, U.S, Technical Report, pages 800–94, 2007.

[Sedjelmaci & Feham 2011] H. Sedjelmaci et M. Feham. *Novel hybrid intrusion detection system for clustered wireless sensor network*. International Journal of Network Security & Its Applications (IJNSA), vol. 3, July 2011.

[Sejaphala & Velempini 2020] L. C. Sejaphala et M. Velempini. *The Design of a Defense Mechanism to Mitigate Sinkhole Attack in Software Defined Wireless Sensor Cognitive Radio Networks*. Wireless Personal Communications. Springer, vol. 113, page 977–993, 2020.

[Shah & Engineer 2019] A. Shah et M. Engineer. *A Survey of Lightweight Cryptographic Algorithms for IoT-Based Applications*. In: Tiwari S., Trivedi M., Mishra K., Misra A., Kumar K. (eds) Smart Innovations in Communication and Computational Sciences. Advances in Intelligent Systems and Computing. Springer, vol. 851, pages 283–293, 2019.

[Shankar & Elhoseny 2019] K. Shankar et M. Elhoseny. *An Optimal Lightweight Cryptographic Hash Function for Secure Image Transmission in Wireless Sensor Networks*. In: Secure Image Transmission in Wireless Sensor Network (WSN) Applications. Lecture Notes in Electrical Engineering. Springer, vol. 564, pages pp 49–64, 2019.

[Sharafaldin *et al.* 2018] T. Sharafaldin, A.H. Lashkari et A.A. Ghorbani. *Toward generating a new intrusion detection dataset and intrusion traffic characterization*. In: Proceedings of the international conference on information systems security and privacy (ICISSP), page 108–116, 2018.

[Sharma *et al.* 2013] D. Sharma, S. Verma et K. Sharma. *Network Topologies in Wireless Sensor Networks: A Review*. International Journal of Electronics & Communication Technology, vol. 4, pages 93–97, June 2013.

[Sharma *et al.* 2018] R. Sharma, R. Singla, R. Guleria ASharma, R. Singla et A. Guleria. *A new labeled flow-based DNS dataset for anomaly detection: PUF dataset*. International Conference on Computational Intelligence and Data Science, vol. 132, page 1458–1466, 2018.

[Singh & Verma 2017] R. Singh et A. K. Verma. *Energy efficient cross layer based adaptive threshold routing protocol for WSN*. AEU-International Journal of Electronics and Communications, vol. 72, pages 166–173, 2017.

[Singh *et al.* 2020a] A. P. Singh, A. K. Luhach, X.Z. Gao, S. Kumar et D. S. Roy. *Evolution of wireless sensor network design from technology centric to user centric: An architectural perspective*. International Journal of Distributed Sensor Networks, August 2020.

[Singh *et al.* 2020b] N. Singh, D. Virmani et X.Z. Gao. *A Fuzzy Logic-Based Method to Avert Intrusions in Wireless Sensor Networks Using WSN-DS Dataset*. International Journal of Computational Intelligence and Applications, vol. 19, 2020.

[Singh *et al.* 2021] M. M. Singh, N. Dutta, T. R. Singh et U. Nandi. *A Technique to Detect Wormhole Attack in Wireless Sensor Network Using Artificial Neural Network*. Evolutionary Computing and Mobile Sustainable Networks, Springer, pages 297–307, 2021.

[Singh 2017] H. Singh. *A Metrics Set for Wireless Sensor Networks Intrusion Detection System Evaluation*. International Journal of Advanced Research in Computer Science, vol. 8, pages 273–277, 2017.

[Sobh 2006] T.S. Sobh. *Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art*. Journal of Computer Standards and Interfaces (Elsevier), vol. 28, page 670–694, 2006.

[Solapure *et al.* 2018] S. Solapure, N. Mete, P. Dodake, S. Jadhav et D. Mehetre. *Comparative Survey of Routing Attacks in WSN's*. International Research Journal of Engineering and Technology(IRJET), vol. 5, pages 3210–3217, May 2018.

[Song *et al.* 2020] H. Song, S. Sui, Q. Han, H. Zhang et Z. Yang. *Autoregressive integrated moving average model–based secure data aggregation for wireless sensor networks*. International Journal of Distributed Sensor Networks, vol. 16, March 2020.

[Srinivas & S. S. Manivannan 2020] T. A. S. Srinivas et SS S. S. Manivannan. *Prevention of hello flood attack in IoT using combination of deep learning with improved rider optimization algorithm*. Computer Communications, Elsevier, vol. 163, pages 162–175, 2020.

[Stallings 2000] W. Stallings. *Cryptography and Network Security Principles and Practise*. Cryptography Book, 2000.

[Stetsko & Matyas 2009] A. Stetsko et V. Matyas. *Effectiveness Metrics for Intrusion Detection in Wireless Sensor Networks*. European Conference on Computer Network Defense, pages 21–28, 2009.

[Sun *et al.* 2019] Z. Sun, L. Wei, C. Xu, T. Wang, Y. Nie, X. Xing et J. Lu. *An energy-efficient cross-layer-sensing clustering method based on intelligent fog computing in WSNs*. IEEE Access, vol. 7, pages 144165–144177, 2019.

[Tami *et al.* 2021] A. Tami, S. Boukli-Hacene et M. Ali Cherif. *Detection and prevention of Blackhole attack in the AOMDV routing protocol*. Journal of Communications Software and Systems, vol. 17, no. 1, pages 1–12, 2021.

[Tawalbeh & Tawalbeh 2017] L. Tawalbeh et H. Tawalbeh. Lightweight crypto and security: Foundations, principles and applications, pages 243–261. John Wiley & Sons, 2017.

[Tawalbeh *et al.* 2017] H. Tawalbeh, S. Hashish, L. Tawalbeh et A. Aldairi. *Security in Wireless Sensor Networks Using Lightweight Cryptography*. Journal of Information Assurance and Security, vol. 12, pages 118–123, 2017.

[Terence & Purushothaman 2019] J. S. Terence et G. Purushothaman. *A Novel Technique to Detect Malicious Packet Dropping Attacks in Wireless Sensor Networks*. Journal of Information Processing Systems, vol. 15, pages –203–216, 2019.

[Thahniyath & Jayaprasad 2020] G. Thahniyath et M. Jayaprasad. *Secure and load balanced routing model for wireless sensor networks*. Journal of King Saud University – Computer and Information Sciences, 2020.

[Thangarajana & Bhaaskaran 2018] S. Thangarajana et V.S. Kanchana Bhaaskaran. *High Speed and Low Power Implementation of AES for Wireless Sensor Networks*. Procedia Computer Science, vol. 143, pages 736–743, 2018.

[Tiberti *et al.* 2020] W. Tiberti, F. Caruso, L. Pomante, M. Pugliese, M. Santic et F. Santucci. *Development of an extended topology based lightweight cryptographic scheme for IEEE 802.15.4 wireless sensor networks*. International Journal of Distributed Sensor Networks, vol. 16, 2020.

[Tripathy *et al.* 2021] B. K. Tripathy, S. K. Jena, V. Reddy, S. Das et S. K. Panda. *A novel communication framework between MANET and WSN in IoT based smart environment*. International Journal of Information Technology, vol. 13, pages 921–931, 2021.

[Umarani & Kannan 2021] C. Umarani et S. Kannan. *Construction of Intrusion Detection system for Wireless Sensor Networks by Synthesizing Anomaly and Misuse techniques*. International Journal of Contemporary Applied Researches, vol. 8, August 2021.

[Usha & Muzzammil 2020] J. Usha et H. Muzzammil. *Securing Wireless Sensors in Military Applications through Resilient Authentication Mechanism*. Procedia Computer Science, vol. 171, pages 719–728, 2020.

[Vidhya & Sasilatha 2017] S. Vidhya et T. Sasilatha. *Sinkhole Attack Detection in WSN using Pure MD5 Algorithm*. Indian Journal of Science and Technology, vol. 10, pages 1–6, 2017.

[Waoo & Tiwari 2021] A. A. Waoo et V. Tiwari. *Challenges in Sinkhole Attack Detection in Wireless Sensor Network*. Indian Journal of Data Communication and Networking (IJDCN), vol. 1, August 2021.

[Wazid *et al.* 2016] M. Wazid, A. K. Das, S. Kumari et M. K. Khan. *Design of sinkhole node detection mechanism for hierarchical wireless sensor networks*. Security and Communication Networks, pages 4596–4614, November 2016.

[Wazid 2017] M. Wazid. *Design and Analysis of Intrusion Detection Protocols for Hierarchical Wireless Sensor Networks*. PHD Thesis, 2017.

[Xu *et al.* 2007] Y. Xu, G. Chen, J. Ford et F. Makedon. *Detecting Wormhole Attacks in Wireless Sensor Networks*. IFIP International Federation for Information Processing, vol. 253, pages 267–279, 2007.

[Yasin *et al.* 2017] N. Mohammaed Yasin, N. Balaji, G. Sambasivam, M. S. Saleem Basha et P. Sujatha. *ADSMS: Anomaly Detection Scheme for Mitigating Sinkhole attack in wireless sensor networks*. 2017 International Conference on Technical Advancements in Computers and Communications. IEEE Computer Society, pages 154–159, 2017.

[Yick *et al.* 2008] J. Yick, B. Mukherjee et D. Ghosal. *Wireless sensor network survey*. Computer Networks, vol. 52, pages 2292–2330, 2008.

[Yousefpoor & Barati 2018] M.S. Yousefpoor et H. Barati. *Dynamic key management algorithms in wireless sensor networks: A survey*. Computer Communications, 2018.

[Zala *et al.* 2021] D. Zala, D. Thummar et B. R. Chandavarkar. *Mitigating Blackhole attack of Underwater Sensor Networks*. 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, pages 1–8, 2021.

[Zawaideh & Salamah 2019] F. Zawaideh et M. Salamah. *An efficient weighted trust-based malicious node detection scheme for wireless sensor networks*. International Journal of Communication Systems, vol. 32, 2019.

[Zeng *et al.* 2019] M. Zeng, X. Huang, B. Zheng et X. Fa. *A Heterogeneous Energy Wireless Sensor Network Clustering Protocol*. Wireless Communications and Mobile Computing, page 1–11, 2019.

[Zeng *et al.* 2021] Z. Zeng, F. Zeng, X. Han, H. Elkhouchlaa, Q. Yu et E. Lü. *Real-Time Monitoring of Environmental Parameters in a Commercial Gestating Sow House Using a ZigBee-Based Wireless Sensor Network*. Applied Sciences, vol. 11, 2021.

[Zhang & Zhang 2019] Q. Zhang et W. Zhang. *Accurate detection of selective forwarding attack in wireless sensor networks*. International Journal of Distributed Sensor Networks, vol. 15, page 1550147718824008, 2019.

[Zhang *et al.* 2019] Z. Zhang, S. Liu et Y. Zheng Y. Bai. *M optimal routes hops strategy: Detecting sinkhole attacks in wireless sensor networks*. Cluster Computing, vol. 22, page 7677–7685, 2019.

[Zhang *et al.* 2020] W. Zhang, D. Han, K.C. Li et F.I. Massetto. *Wireless sensor network intrusion detection system based on MK-ELM*. Soft Computing, Springer, vol. 24, page 12361–12374, 2020.

[Zhang *et al.* 2021] T. Zhang, D. Han, M.D. Marino, L. Wang et K.C. Li. *An Evolutionary-Based Approach for Low-Complexity Intrusion Detection in Wireless Sensor Networks*. Wireless Personal Communications, 2021.

[Zhao *et al.* 2019] J. Zhao, J. Huang et N. Xiong. *An Effective Exponential-Based Trust and Reputation Evaluation System in Wireless Sensor Networks*. IEEE Access 7, page 33859–33869, 2019.

[Zou *et al.* 2016] Y. Zou, J. Zhu, X. Wang et L. Hanzo. *A Survey on Wireless Security:Technical Challenges, Recent Advances, and Future Trends*. Proceedings of the IEEE, vol. 104, pages 1727–1765, September 2016.

Titre La sécurité dans les réseaux sans fil

Résumé Les réseaux de capteurs sans fil sont un type spécial des réseaux Adhoc caractérisés par une forte densité, faible mobilité et l'utilisation d'un support sans fil partagé. Cette dernière caractéristique rend le réseau vulnérable à de types variés d'attaques, tels que l'attaque Sinkhole et l'attaque sybil. Dans cette thèse, nous nous intéressons à l'attaque Sinkhole, qui est l'une des plus destructives attaques dans les RCSF. Nous proposons un système de détection pour l'attaque Sinkhole en utilisant les séparateurs à vaste marge (SVM) sur le protocol de routage AODV. Dans les différentes expérimenttaions, un ensemble de données spécial Sinkhole a été utilisé, une comparaison avec d'autres techniques a été menée à base de taux de détection. Les résultats montrent l'efficacité de l'approche proposée.

Mots-clés AODV, SDI, Attaque Sinkhole, SVM, RCSF

Title Security in Wireless Networks

Abstract Wireless sensor network is a special kind of Adhoc network characterized by high density, low mobility, and the use of a shared wireless medium. This last feature makes the network vulnerable to various types of attacks, such as Sinkhole attack, sybil attack. In this thesis, we focus on sinkhole attack, which is one of the most destructive attacks in WSNs. We propose an intrusion detection system for sinkhole attack using support vector machines (SVM) on AODV routing protocol. In the different experiments, a special sinkhole dataset is used, and a comparison with previous techniques is done on the basis of detection accuracy. The results show the efficiency of the proposed approach.

Keywords AODV, IDS, Sinkhole Attack, SVM, WSN

العنوان الأمن في الشبكات اللاسلكية

شبكة الاستشعار اللاسلكية هي نوع خاص من شبكات المخصصة تتميز بكثافة عالية وقابلية تنقل منخفضة واستخدام وسيط لاسلكي مشترك. هذه الميزة الأخيرة تجعل الشبكة عرضة لأنواع مختلفة من الهجمات مثل هجوم البئر وهجوم سيبيل. في هذا العمل، نركز على هجوم البئر ، وهو أحد أكثر الهجمات تدميراً في الشبكات الاستشعار اللاسلكية. نقترح نظام كشف التسلل لهجوم البئر باستخدام آلات أس في أم على بروتوكول توجيه أوديفي . في التجارب المختلفة ، يتم استخدام مجموعة بيانات خاصة بالبئر ، ويتم إجراء مقارنة مع التقنيات السابقة على أساس دقة الكشف. تظهر النتائج كفاءة النهج المقترح.

الكلمات الرئيسية أوديفي ، نظام كشف التسلل ، هجوم البئر ، أس في أم ، شبكة المستشعرات اللاسلكية