Cape Peninsula
University of Technology

ATTACK RESILIENT TRUST AND SIGNATURE-BASED INTRUSION DETECTION SYSTEMS (IDS)

by

SABER A. ARADEH

Thesis submitted in fulfilment of the requirements for the degree

Master of Technology: Information Technology

in the Faculty of Information Technology

at the Cape Peninsula University of Technology

Supervisor **:** Dr. Boniface Kabaso

Cape Town
February 2020

DECLARATION

I, Saber Aradeh, declare that the contents of this dissertation/thesis represent my own unaided work, and that the dissertation/thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

28/02/2020

Signed **Date**

ABSTRACT

The Wireless Sensor Network (WSN) is one of the fastest growing networking sectors in real time monitoring applications mainly in industrial and military fields. The confidentiality of data and a secure communication channel for transmitting data to the destination is a needed requirement in WSN. The necessity of providing efficient security is also a significant concern in WSN based applications due to the physical factors such as the use of the wireless medium for data transmission and requirement of minimum utilization of sensor node resources. The routing and data aggregation protocols are developed to enhance the resource utilization in sensor nodes and achieving an efficient data delivery. Due to data transmission through untrustworthy nodes, the security parameters of WSN are affected by different types of active and passive attacks. The use of security mechanisms such as cryptographic keys, Intrusion Detection System (IDS) and trust management mechanisms can mitigate the problem of security attacks. The strength of the security mechanism in the network can be increased by combing the properties of different security schemes. The trust evaluation using single metrics often does not provide accurate trust value, which in turn leads to a severe impact on network performance. In the proposed IDS based Hierarchical Trust measurement (IDSHT) scheme, the evaluation and validation of sensor nodes during cluster head selection for achieving secure data aggregation is done using multidimensional factors to improve the accuracy of the trust value and prevent attacks such as impersonation attacks. The multidimensional factors used in the hierarchical based environment are Interactive Trust (IT), Content Trust (CT), and Honesty Trust (HT). The IT and HT is the network related trust while the CT is a data related trust. The two-tier hierarchical mechanism consists of two levels of trust evaluation, and they are sensor node level trust evaluation, and cluster head level trust evaluation. The multidimensional trust value for both sensor node level and cluster head level is obtained using direct evaluation between sensor node-cluster head and cluster head-base station respectively. The RSA based signature generation and verification are included in the hierarchical trust mechanism and is called as IDSHT with signature (IDSHT-S), to strengthen the security of the IDSHT scheme. The simulation scenario of the proposed IDSHT is constructed with data dropping, and modification attack scenarios and the performance analysis of IDSHT and IDSHT-S schemes are compared to prove the efficiency of detecting attacks without compromising the performance of the network.

Keywords: WSN, Routing attacks, Public-key Cryptography, RSA, signature-IDS, packet dropping, Trust-based schemes

ACKNOWLEDGEMENTS

I wish to thank:

- My supervisor, Dr. Boniface Kabaso, who provided thorough guidance during the duration of the research study. It would not have been possible without him. In addition, I'd like to acknowledge the other CPUT I.T staff members and students who provided assistance in the research work.
- Dr. Ademola Abidoye from Information Technology (CPUT).
- My family members, my friends, for the emotional support they provided.
- My wife, son and daughters.

DEDICATION

I dedicate my thesis work to my family and many friends. A special feeling of gratitude to my loving parents, my father Abid before passed away, my mother Erfat, and my stepmother Maziunah, also my wife whose words of encouragement. My brothers and sisters, Sabreen, Asma, Osama, Ayman, Mohammed, Ibrahim, Abdullah, Ahmad, Fatemah, Iman and Hanan who have never left my side and are very special. I also dedicate this thesis to my many friends who have supported me throughout the process. I will always appreciate all they have done, especially My brother Osama Aradeh for supporting me.

TABLE OF CONTENTS

CHAPTER THREE: ATTACK RESILIENT TRUST AND SIGNATURE-BASED IDS

CHAPTER FOUR: IMPLEMENTATION SCENARIO OF PROPOSED IDSHT-S SCHEME

CHAPTER FIVE: CONCLUSIONS AND FUTUREWORKS

LIST OF FIGURES

LIST OF TABLES

LIST OF EQUATIONS

GLOSSARY

Abbreviations	Definition/Explanation
ACQUIRE	**Active Query forwarding in sensor networks:** The ACQUIRE is a data-centric routing algorithm that provides superior optimization and involves active query passing in the network. It is a mechanism for extracting data from necessary sensors to respond to the complex, one-shot, and non-aggregated queries for replicated data.
AODV	**Ad-hoc On-demand Distance Vector:** The AODV is a routing protocol used in both wireless and mobile ad-hoc networks. The AODV protocol builds routes between nodes when the source nodes send a request message. In AODV, the multicast members are connected in the form of trees. The use of sequence numbers ensures the route freshness. The routes in AODV protocol remain active as long as data is data is transmitted along the paths from source to destination. AODV protocol considers both unicast and multicast routing protocols.
ATSR	**Ambient Trust Sensor Routing protocol:** The ASTR protocol is a location-based trust-aware routing protocol, which involves a distributed trust management system for secure routing of packets between the sensor nodes. The routing decisions are made based on two parameters such as geographical information and total trust information.
BROSK	**Broadcast Session Key negotiation protocol:** The BROSK is a broadcast negotiation protocol, which is used for securing the communication in sensor networks. The BROSK protocol does not contain any trusted third party or server, and it has less energy consumption. It uses a single master key in each sensor node and a message authentication code for authentication purpose.
BS	**Base Station:** The BS is the important node in the network, which posses high computational power and large memory storage. The main function of BS is to gather the sensed data for final processing. Generally, a BS is also called a sink, and it is considered as the central hub for wireless networks.
CBR	**Constant Bit Rate:** The CBR is related to the quality of service and widely used in telecommunication purposes. CBR is used for streaming multimedia content on a limited capacity channel. The characteristics of CBR include support for timing sensitive traffic, QoS guarantee, and full utilization of channel for providing high-quality service. The CBR provides low latency traffic with predictable delivery. The CBR is used as an application agent in NS2 tool.
CH	**Cluster Head:** The CH is a unique node in the cluster-based networks, which act as an intermediate node between the sensor nodes and sink. The main function of CH is to aggregate the data packets collected from all the nodes in the cluster and forward it to the base station. The work of common nodes is shared by the CH, which in turn reduces the overall energy consumption.
CSMA	**Carrier Sense Multiple Access:** The CSMA is a media access control protocol in which the node verifies the absence of traffic before transmitting through a shared medium. It is a network access method used for avoiding the chances of a collision in the network. The CSMA method requires each node to confirm the status of the route before sending the data packets. It is mainly used in shared network typologies such as ethernet to control access to the network.
CT	**Content Trust:** The CT is one of the trust evaluation methods, which is based on the capacity of each node. The CT is a type of data-related trust. It depends on the observing data and energy consumption of the node.
DoS	**Denial of Service:** DoS is a type of active attack that shutdowns the

services of the network making it unusable for intended users. The DoS stops the service in the network by two types of methods. It is either by flooding the network with unwanted packets or sends a data the triggers the network to crash. In DoS attacks, the adversaries usually send excessive messages to the network or server in the form of authenticating requests. Since the informing traffic is from different sources, it is impossible to stop the attack using ingress filtering. It is also difficult to distinguish the legitimate traffic from abnormal ones immediately. It mainly leads to energy exhaustion in the network that drastically reduces the network lifetime.

EGF **Enhanced Greedy Forwarding:** It is simply efficient and scalable routing protocols, where the selection of only forward nodes in the routing path takes place which reduces the energy consumption of the overall network. It is robust under topological changes and does not require up-to-date, states of the nodes.

FCM **Fuzzy Clustering-Mean algorithm:** The FCM is a method for clustering which allows a particular part of the data to be available for two or more clusters. In FCM, the dataset is grouped into a finite number of clusters with every part of the data belong to every cluster in a certain degree. This method is mainly used in pattern recognition. The probability distribution over the clusters estimates the degree of membership of each data.

GEAR **Geographical and Energy Aware Routing protocol:** The GEAR is a geographic routing protocol that considers the energy levels of the nodes to improve network lifetime. In GEAR, the entire network is divided into partitions, and within each partition, the flooding technique is adopted.

GPS **Global Positioning System:** The GPS is a satellite-based radio navigation system that provides geographical location and time information to the GPS receiver. It is initially developed for accurately determining the geographical locations for military applications. It is a network that incorporates a range of satellites and uses microwave signals for sending the information to the receiver. The GPS is used for tracking locations, objects, and also individuals.

HEED **Hybrid Energy-Efficient Distributed clustering:** The HEED is a clustering based routing protocol, which periodically selects the cluster head, according to the hybrid of the residual energy of the nodes and secondary parameters through constant time iterations. The HEED protocol achieves uniform distribution across the network and a multi-hop inter-cluster network with specified density model.

HT **Honesty Trust:** The HT is one of the trust evaluation methods, which depends on the successful and unsuccessful interactions of a node in the network. The honesty trust component is measured by considering the evidence of dishonesty such as an abnormal trust recommendation, trust fluctuation, and false self-reporting.

IDS **Intrusion Detection System:** The IDS is a device or software that monitors the network for malicious intrusions or activities. Then, the IDS alerts the administrator, when there is an unwanted intrusion or security policy violation which it tries to compromise or steal the information systems. An IDS works by monitoring the network traffic or system activity through examining vulnerabilities in the system, analyzing the patterns and behavior stored in their databases. It monitors both inbound and outbound network activity. Some IDS can take action to the detected intrusions by revoking the malicious nodes.

IoT **Internet of Things:** The IoT is defined as the network consisting of a group of physical objects connected to the internet and can gather information and communicate with each other. The IoT involves the integration of various manufacturing devices that supports sensing, identification, processing, communication, actuation, and networking capabilities. The main goal of the IoT is to generate and analyze real-time data to achieve desired business

	outcomes. The embedded technology in the objects helps in interacting with the external environment. It enables devices to observe, identify, and understand a situation or the surrounding in which deployed without any human intervention.
IT	**Interactive Trust:** The IT is one of the trust evaluation methods in the WSN where it depends on the interaction of nodes in the network. The IT is one of the network related trust, where the threshold value detects the malicious node.
LEACH	**Low-Energy Adaptive Clustering Hierarchy:** The LEACH protocol is a time division multiplexing based clustering and routing protocol, which aims at reducing the energy consumption for creating and maintaining clusters for increasing the network lifetime of the WSN. The LEACH protocol operation involves two phases such as setup phase and steady phase.
LEAR	**Location-based Energy Aware Reliable routing protocol:** The LEAR routing protocol is based on sensor position and clustering, and it aims at exploiting the enhanced greedy forwarding and cluster structure to enhance the network flexibility, end to end delay, and load balancing during cluster head selection.
NAM	**Network Animator**: The NAM is a tool command language-based animation tool for viewing simulation traces and real-time packet delivery. The NAM program reads the input file and draws the network events graphically. It is used to display the progression of packets through the network virtually.
NBC	**Nuclear, Biological and Chemical attack:** The NBC attack is defined as a highly specialized and regulated weapon that disperse nuclear, biological, and chemical agents for causing mass destruction. It causes casualties, destruction of equipment, the inability to use the terrains, and disruption of operations.
NS2	**Network simulator:** NS2 is an open-source simulating software that predicts the behavior of the networks. It provides simulation of TCP, routing, and multicast protocols over both wired and wireless networks. NS2 tool can be deployed in most of the Unix and Windows systems. The NS2 consist of two programming languages C++ and object-oriented tool command language.
OTCL	**Object-oriented Tool Command Language:** The OTCL is an extension of the tool command language. It is also defined as a high-level dynamic programming language. It is one of the powerful scripting languages with programming features. It is supported in Unix, Mac OS, and Windows platforms. TCL provides extension packages for additional functionality, including terminal based applications and database access. Apart from OTCL, the TCL also supports other multiple programming paradigms such as imperative, functional programming, and procedural styles.
PDA	**Personal Digital Assistant:** The PDA is a small handheld device that provides computing and information storage. It is a portable device that acts as a personal information manager. The PDA consist of the touch screen for navigation, a memory card slot for data storage, and internet connection. The functions of PDA are that it can perform as a cellular phone, sending a fax, for web browsing, and an organizer. Wireless PDA connects to the remote computers and databases within the range. The information can be entered using a pen-like a stylus or touch screens instead of keyboards.
PEGASIS	**Power Efficient Gathering in Sensor Information System:** The PEGASIS is an efficient routing protocol where it adopts a chain formation among the sensor nodes so that each node will receive from and transmit to a close neighbor. The PEGASIS protocol achieves equal energy distribution among the sensor nodes in the network.
PK	**Public Key:** PK is a larger numerical value used in cryptography for encrypting data packets. PK is used to convert a message into an unreadable format. In asymmetric key cryptography, PK is used for encrypting the data, and the private key is used for decrypting the data.

QoS	**Quality of Service:** The QoS is the measurement of overall performance of the service, particularly analyzed or determined by the user in the network. The QoS depends on the performance factors such as packet loss, bit rate, throughput, transmission delay, availability, and delay. It can provide different priority to data flows and users based on the application requirement. The QoS in a network is mainly affected by scalability, reliability, network congestion, and maintainability.
RSA	**Rivest-Shamir-Adleman algorithm:** The RSA algorithm is one of the popular public key cryptographic systems used for securing data during communication in the network. The RSA, the public key is used for encryption and the private key is used for the decryption process. It is based on the fact that finding the factors of large composite numbers is difficult, where malicious intruders cannot easily solve the data encrypted. The public key of the RSA algorithm is obtained by multiplying two large prime numbers together and the private key is generated through a different process involving these two prime numbers. The RSA algorithm is a deterministic encryption algorithm that can be used for both public key encryption and digital signatures.
SN	**Sensor Nodes:** The SN often called as motes. The main purpose of SN is to sense the physical data from the environment and transfer it to the destination through the wireless medium. The SN is tiny devices which consist of mainly three components, and they are a sensing subsystem for data acquisition from the monitoring environment, a processing subsystem for local data processing, and a wireless communication subsystem for data transmission. The functionality of the sensor node varies depending on the application requirement. SN is equipped with micro-controller, a radio receiver along with the antenna, an electronic interfacing circuit, and battery as an energy source.
SNEP	**Secure Network Encryption Protocol:** The SNEP is one of the building blocks of security protocols in sensor networks. The SNEP provides data confidentiality, two-party authentication, integrity, and freshness. The SNEP uses counters and achieves semantic security that prevents the eavesdroppers from interfering the message content from the encrypted message.
SPIN	**Sensor Protocols for Information Via Negotiation Protocol:** The SPIN is a data-centric protocol that disseminates information at every node in the network, assuming all the nodes in the network is potential base stations. The SPIN family uses data negotiation and resource adaptive algorithms.
SVM	**Support Vector Machine:** The SVM is a discriminating classifier that is used for classification and regression analysis of data. It performs classification tasks by constructing hyperplanes in the multidimensional spaces, which can be used for purposes such as outlier's detection. SVM handles multiple, continuous, and categorical variables by applying the statistics of support vectors. It is one of the widely used clustering algorithms in industrial applications.
TCP	**Transmission Control Protocol:** The TCP is one of the internet protocol suites. It is a network communication protocol designed for sending data packets over the internet. It is used for creating a connection between two remote computers by transporting and ensuring the data packet delivery.
TDMA	**Time Division Multiplexing Access:** The TDMA is a channel access method for shared medium networks. It allows different nodes or stations to share and use the same transmission channel by dividing the signals into different time slots. Each node transmits or receives data in the allocated time slot.
TESLA	**Time Efficient Streaming Loss-tolerant Authentication:** The TESLA involves broadcast authentication process, which is used for securing

multicast data transmission. The TESLA protocol is based on loose synchronization between the sender and receivers. This authentication protocol provides authentication for data broadcast. The micro version of TESLA is the µ-TESLA protocol.

UDP **User Datagram Protocol:** The UDP is one of the internet protocol suites, which offers only a minimum transport service and non-guaranteed datagram delivery. It is also known as a stateless protocol. The UDP protocol provides checksums for data integrity and port numbers for addressing the functionality of the source and destination datagram. It is one of the transport layer protocols, and the lack of transmission delays makes it reliable for real-time applications such as voice over the Internet.

WSN **Wireless Sensor Network:** The WSN is a wireless network that consists of spatially dispersed sensors that are used for monitoring environmental conditions such as temperature, pressure, humidity and other factors and tracking physical factors such as motion tracking, enemy intrusion detection, etc. The topology of WSN varies from star network to a multi-hop mesh network based on the application requirement. The modern networks are bi-directional and allow control over sensor activity. The WSN can work without any central control point. The WSN has minimum energy, transmission distance, fault tolerance, and storage due to the physical sizes of nodes.

CHAPTER ONE

INTRODUCTION

1.1 Introduction

The rapid growth and advancement of wireless technologies, the Wireless Sensor Networks (WSNs) have widespread applications in a variety of areas, including environmental and battlefield monitoring, smart home systems, forest fire detection, and health monitoring (Akyildiz et.al, 2002). Mostly, the sensors are randomly deployed over a region to build the WSN topology. Due to random deployment, multiple sensors may cover a single area and share the common sensing task. Data aggregation is a key technique to reduce the data volume and extend the lifetime of WSN without degrading the data quality (Fasolo et.al, 2007). The key process of WSN routing protocols is to forward the aggregated data to the sink node, rather than sending all raw data directly to sink node.

Security is the main concern in WSNs, due to the openness of the deployed environment and the wireless medium (Yang et.al, 2015) (Chen et.al, 2009). Due to the infrastructure less architecture and inherent requirements, the WSN poses several weak points that attract malicious nodes. Due to their deployment for special applications, such as civilian and military domains, providing a strong defense system is essential in WSN. The wireless and resource-constraint nature of sensor nodes in WSN makes it vulnerable to the intruders. Different types of attacks are injected to disturb the WSNs data aggregation and routing activities. Those are selfish, dropping, and false data injection attacks. Thus, the security issues need to be effectively addressed in order to utilize the potential of WSNs. Most of the clustering techniques select the Cluster Head (CH) nodes based on the remaining energy level. The selfish attacks do not involve in the CH election process to save its network resources (Li et.al., 2013). The dropping attack drops the received data without forwarding it towards the sink node. The false data injection attack injects the false data value that is deviated from actual value and degrades the quality of data aggregation. The main aim of dropping the false data injection attacks is to make the network resource unavailable to its intended nodes and to degrade the efficiency of the network.

In order to handle such security attacks in WSNs, several defence systems have been suggested conventionally. Among them, most of the security mechanisms follow trust and Intrusion Detection Systems (IDSs) in sensor network (Butun et.al, 2014). The trust is a belief level of a node and it is measured on the basis of routing performance. The IDSs is designed to monitor the network for malicious activities. The conventional IDSs are classified into anomaly, signature, and specification based IDSs. The Anomaly based IDSs learn the normal routing activities and differentiate the malicious activities

during testing. The signature based IDSs exploit the known attacks as reference to differentiate the malicious nodes from legitimate nodes. The specification based IDSs exploits a set of specifications to describe the normal routing activities. Most of them only consider the node routing cooperativeness in the estimation of trust and the detection of intrusions (Yu et.al, 2012) (Khalid et.al, 2013). However, detection of different routing attacks using a single metric is difficult. To detect and isolate various kinds of routing attacks from the WSNs, it is essential to consider the multidimensional factors in the selection of CH nodes for secure data aggregation as well as routers for secure data forwarding. The design of defence systems must provide protection against data confidentiality and authentication features (Chen & Xiangqian ,2009).

One of the main security issue in WSNs is node compromisation, which tends to internal malicious attacks. By injecting the malicious code, it gains control of a legitimate sensor node to launch various malicious attacks. This is defined as node comptonizations. In contrast to the legitimate WSN nodes, the compromised malicious nodes disrupt the normal routing activities and paralyze the network. Normally, malicious nodes compromise the legitimate node in the following methods. Firstly, the malicious node captures the target nodes and reprogram them to perform malicious activities. In another way, the malicious nodes are launched with high computing resources. The malicious nodes breach the security programs installed on the normal nodes and insert the malicious codes. Some of the malicious nodes destroy the legitimate nodes and steal.

1.2 Background to the Research

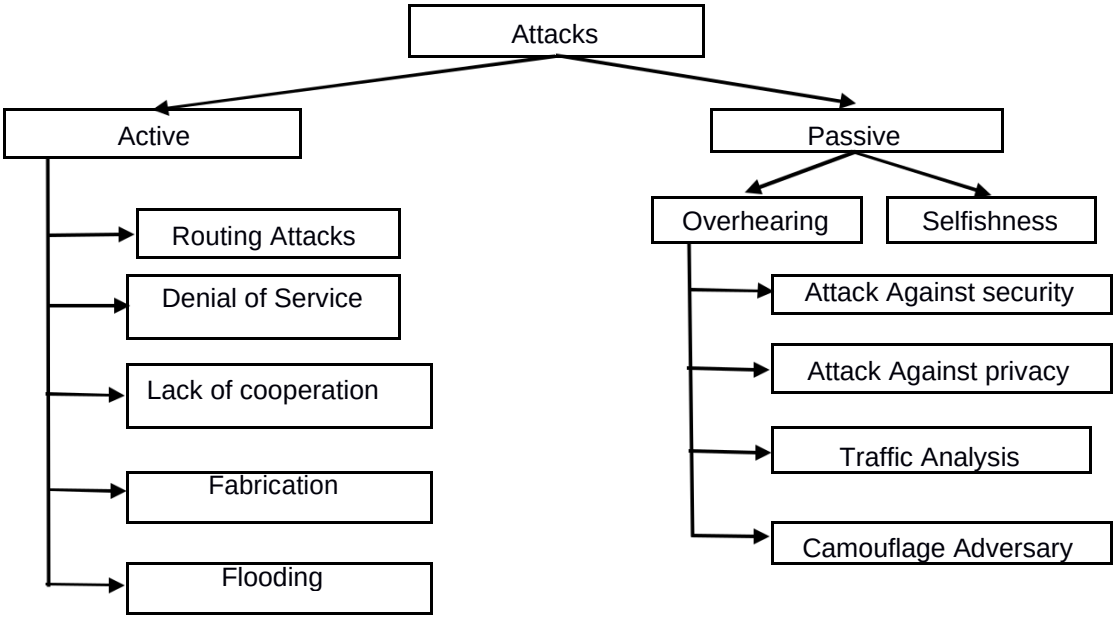

Figure 1. 1: Classification of Attacks in WSN

Adapted from (Pa et al., 2009) (Vi et al., 2017)

The figure 1 illustrates the classification of WSNs attacks and this work focuses on fabrication attacks (Li et al., 2013). The network attacks are classified into active and passive attacks and both of them affect the routing performance in various ways. The active attacks are further classified into internal and external. The internal nodes internally initiate the malicious activities in the network, whereas in external attack, the nodes that do not belong to the network attack the communication. The detection of internal attacks is quite difficult compared to the external attacks.

Fabrication attack is one of the common active attacks, where the injection of false data in the network that affects the trustworthiness between the node the message authentication is mainly affected (Benahmed et.al, 2012) (Elqusy et.al, 2017).
Malicious nodes always consume abnormal energy to launch malicious attacks (Hen et al., 2015).

The WSNs deploy a set of micro sensor nodes in the monitoring area. Each node is constrained with the communication range and battery resources, and it necessitates the requirement of multihop routing protocol, in which a distant node can connect to the base station through multiple routers. The nodes in WSNs act as routers, which involve in packet routing. To deliver the observed data to the intended destination, the nodes have to cooperate and establish the multihop routing paths. The routing protocol includes the procedures for path determination and packet routing. The purpose of WSN routing protocol is to sense, collect, process the sensed information, and forward the results to the sink node cooperatively. Due to the deployment of WSN anytime and anywhere, the WSN is utilized in military defence, industry, agriculture, environmental monitoring, rescue area, and so on. When the WSN is deployed in harsh environment for the survival of human beings, the limited resource devices make the network vulnerable to attack.

The WSNs is a special type of ad hoc network, in which the nodes are equal in battery and capacity status. The sensor nodes are not only involved in the environmental monitoring, but also the nodes act as forwarders to other nodes. The security is the main concern in wireless sensor networks. In particular application of WSN, for instance the military environment, once the attack destroys the deployed sensor devices, this would likely lead to disastrous consequences. Therefore. to prevent the malicious dropping and the selfish attacks, it is essential to build a relatively safe routing environment for sensor networks. Due to the widespread applications of WSN, the security issues and challenges faced during data forwarding are becoming the main research area all over the world (Akyildiz et al., 2002), (Hwang et.al, 2010).

Most important design goals in the design of defence mechanism against network attacks are availability, reliability, resiliency, and self-recovery. The possibility of WSN service access denotes the availability, which ensures the reliable packet delivery even under vulnerable network environment. The characteristics of resilience and self-healing

are interrelated to the service availability. The term resilience defines the tolerate level against vulnerable environment and the ability of the network to provide uninterrupted services to the users. According to the network characteristics like confidentiality, integrity, and reliability, the security services meet the design goals. To meet those security goals in WSN, several security schemes have been proposed in Mobile Adhoc NETwork (MANET). The conventional defence systems are categorized into proactive and reactive. The proactive defence techniques are deployed before the attacks are launched in the network, whereas the reactive defence techniques come into action during an attack.

The example of proactive defence techniques is as follows.

Crypto System: The main aim of the confidentiality and integrity is to initialize and secure transmission of the data packets using cryptosystem. According to the secure cryptosystem, each node has a unique identity and each node verifies the credentials of the sender nodes during communication. To maintained the cryptographic techniques must by using secure key management Maintenance. The security keys are used for encrypting the transmitted data and for ensuring the data confidentiality.

The reactive defence systems are Intrusion Detection System (IDS) and trust. It can identify the malicious nodes that cross through the proactive defence mechanism.

Intrusion Detection System: An IDS in WSN is independent of the network specifications, that means the IDS activities do not interrupt the normal routing activities (Zhang et.al, 2017).

Trust: The trust measurement mechanisms assure the data delivery reliability in the network layer. The concept of trust defines the belief level of a node based on the routing behaviour (Bao et.al, 2007).

If the OT (Overall trust) of SN (Sensor Node) is less, then there is the detection of either data dropping attack or false data injection attack. If the dropping attack is detected, then the alternate sensor is selected as router. If the false data injection attack is detected, then the data of the specific sensor is filtered from aggregation.

If the OT of CH is less then, there is the detection of either data dropping attack or false data injection attack during aggregation. In both cases CH re-election is conducted to select alternate CH.

1.3 Statement of the Research Problem

Presence of malicious nodes in WSNs is one of the major causes of routing attacks. The dropping, modification, and injection attacks target the WSN routing protocols, thus affecting the routing operation as well as the accuracy of data during data aggregation. The injection attacks during data aggregation generate excessive and unnecessary traffic into the network, leading to information overload in WSNs (Zhang et.al, 2017).

The malicious nodes may enter into the network by impersonating as a legitimate node. The inaccurate detection of malicious nodes in WSN is the main hurdle in attaining secure communication in WSN (Yu et.al, 2012) (Khalid et.al, 2013). To minimize the effect of the attacks, research is needed to develop, test and implement a routing attack detection algorithm that may analyse the accuracy of the data aggregation and detection of malicious nodes during the packet routing in WSN.

1.4 Research AIM

The main aim of this research is to secure the WSNs from Active Fabrication Attacks without degrading the performance of the network.

1.5 Objective

1. To detect routing behaviour and for efficient selection of CH nodes, a hierarchical IDS model based on multidimensional factors is constructed.
2. To develop an energy efficient security mechanism to provide a tradeoff between utilization of sensor nodes' resources, and secure data delivery.
3. To evaluate the efficiency of the proposed mechanism for achieving secure routing, data packet dropping, and modification attack.

1.6 Research Question

How can the defence system exactly determine and isolate the selfish, dropping, false data injection, and impersonation attacks from WSN?

1.6.1 Research Sub-Questions

What are the best IDS algorithms that detect malicious node?

1. What are the effects of increasing the number of nodes on the packet delivery ratio?
2. Are there algorithms that can improve the accuracy of data aggregation?
3. What is the packet delivery delay of secure routing Algorithm?

Table 1. 1: Research Questions, Methods and Objectives

Research Problem	Widespread applications of WSN needs to implement a secure and reliable routing protocol	
Research Question	How does the introduction of the IDS in WSN affects the security and performance of the network?	
Research Sub-Questions	**Method(s)**	**Objectives**
1. What are the best IDS algorithms that	DESIGN /Experiment	Develop algorithms by either combining existing solutions or creating a new one

detect malicious node?		
2. What is the effect of increasing the number of nodes on the packet delivery ratio?	Experiment	To understand the effect of increasing the number of nodes on the performance of proposed work
3. How can the algorithm effectively improved the accuracy of data aggregation?	Experiment	To analyse the accuracy of data aggregation process
4. What is the packet delivery delay of secure routing Algorithm?	Experiment	To measure the delay of packet delivery to the sink nodes

1.7 Research Methodology

The figure 2 illustrates the research design and Methodology. It explains the strategies, data generation methods, and data analysis. In such a way, the existing works are analysed to present an effective security scheme for WSNs.

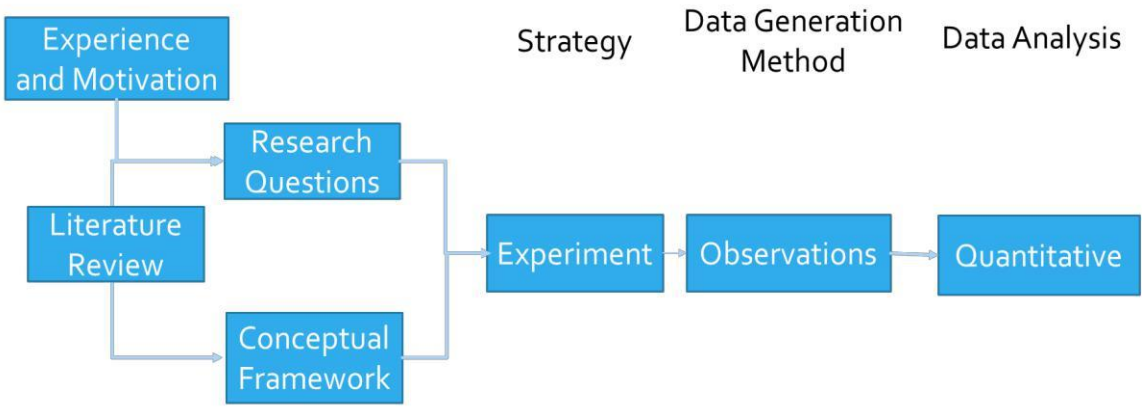

Figure 1. 2: Research Design and Methodology

The research is an experiment type as such it is quantitative in nature. This work will exploit the IEEE 802.15.4. The NS-2 will be used as the simulation tool to analyse the effectiveness of the proposed algorithm. The numbers of nodes will be varied from 20 to 100 in a systematic manner. The performance of the algorithm will be analysed using simulation in the NS2 tool, the simulation graph for performance metrics such as delay, network lifetime, overhead, and packet delivery ratio both the IDSHT-S scheme and IDSHT scheme is presented.

Conventionally, several security schemes model IDS for detecting the malicious nodes in the network. Most of them exploit a single metric to observe the malicious activities in the

network. However, utilizing a single metric in attack detection is not accurate always. The estimation of trust in a multi-dimensional view improves the accuracy of attack detection system.

1.8 Security Framework

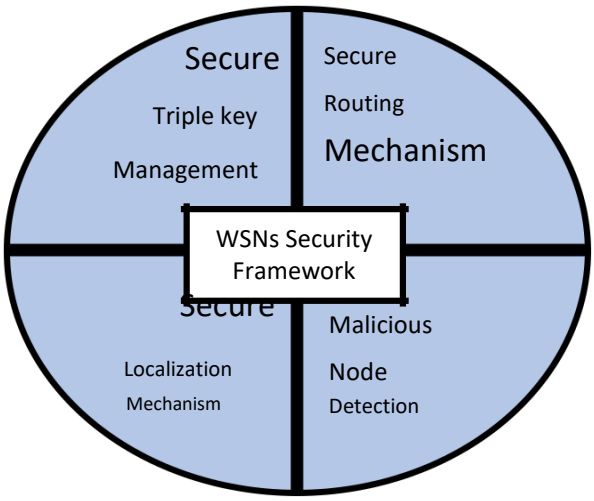

Figure 1. 3: WSNs Security Framework

- **Secure Triple-Key Management Scheme:**

It meets the security goals of confidentiality, integrity and authentication to prevent the Sensor Networks being compromised by an adversary.

- **Secure Routing Mechanism:**

Once the network is deployed, base station builds a table containing IDs of all the nodes in the network.

- **Secure Localization:**

Determining the location of nodes is very important for many sensitive applications. Due to the deployment nature of sensor networks security is a major concern.

- **Securing the Node Location:**

Nodes change their position when they move in a dynamic network or if an adversary has compromised the node.

1.9 Related the work

The routing attacks significantly degrade the performance of the routing protocols. In routing attacks, the primary intention of the attacker is to destroy the overall performance of a network by intentionally dropping packets, drain energy, and report Actual Aggregated Data. (Yu et al., 2011).

The unique characteristics of WSN such as limited resource capability, low bandwidth, and limited data storage, enable restricted operating conditions that need a lightweight security solution. The traditional security mechanisms applicable to networks are not suitable for WSN. Several trust and IDS models have been proposed to provide the secure routing in WSNs.

The countermeasures based on trust-based solutions reveal that it is capable of defending against the majority of attacks related to node misbehaviour where cryptography-based solutions are not effective. The trust defines the belief level of a node according to the routing performance. The nodes are continuously monitoring the routing behaviour of neighbouring nodes for trust management, maintenance, and updating. To improve the routing performance, several security mechanisms have been proposed to measure and select highly trusted nodes.

WSN is emerging as a critical technology due to the advancement of Info algorithm motion and communication technology and the Internet of Things (IoT). Defending against potential attacks significantly degrade the performance and deplete the energy considerably. The trust is an essential concept for lightweight security mechanism. Many reviews discussed the attacks and countermeasures in WSN (Yu et al., 2011). Intrusion detection mechanisms are also available for WSN to eliminate attacks.

The defence models such as IDS, Watchdog, and Pathrater model analysis the routing behaviour during data forwarding (Butan et al., 2014). Watchdog hears the data transmission of nodes with the aim of improving the routing performance even in the presence of attackers in the network. Pathrater determines the route that is free from malicious nodes. The watchdog system maintains a counter to count the data transmission failure. It increases the count when its next hop refuses to route the data packets in a discovered path. However, observing the behaviour of packet forwarding is only capable of detecting the packet dropping attack.

The context-aware trust estimation improves the security solutions in wireless communication (Rostamzadeh et.al., 2015). This research proposes an application-oriented framework that employs a two-layer trust model for information dissemination in vehicular networks. It maintains the trust values of vehicles in the neighbourhoods and segments and ensures that the message is valid and originated and routed through trusted nodes. It is uniquely designed to support unicast, broadcast and multicast messages. The results show the effectiveness and scalability, but it is not suitable for lightweight WSN.

A novel application-independent distributed trust evaluation model enables the nodes to manage the trust values individually for Medical Sensor Networks (MSN) (He et al., 2012). The characteristics of MSNs are susceptible to a variety of attacks that impact the privacy of the patient. By utilizing the lightweight cryptographic techniques with the trust,

it significantly secures the privacy of medical records. It considers the node transmission rate and leaving time for estimating the trust value. By avoiding the less trustworthy nodes, the honest nodes improve the routing efficiency. However, the secure clustering and energy conservation are not considered.

The Link Trust Focuses on link quality and link capacity (LC) as link trust parameters, Data trust the trust assessment of the fault tolerance and consistency of data and Nodes trust the trust value of a sensor and Collecting and managing many recommendations (Hen et al., 2015).

The conventional security solutions mostly exploit the behaviour of packet forwarding in order to detect the dropping attackers. Even though it detects the packet dropping attackers, considering the forwarding behaviour of nodes during path discovery process is also important. The conventional schemes also utilize the multi-dimensional trust measurement in WSN. However, the revoked malicious nodes using the conventional IDS techniques may enter into the network by impersonating as a legitimate node. Also, applying the same trust model on all the sensor nodes is inadequate for cluster based IDSs. Thus, the proposed scheme suggests different multidimensional trust factors for various nodes in WSN and improves the efficiency of the security system.

1.10 Performance Evaluation

Since there is a possibility to launch the impersonation attacks by the malicious nodes those are eliminated from the WSN as per IDSHT. The research will contribute to the development of IDSHT with Signature (IDSHT-S) protocol to identify the impersonation attack. The RSA is used for signature generation and verification process. The proposed IDSHT-S modifies the aodv routing protocol files such as aodv.cc according to the proposed approach. Comparison is made between the IDSHT-S and existing IDSHT. Both are evaluated for the simulation settings as per the simulation model and compared. Metrics such as Packet Delivery Ratio (PDR), Network lifetime, Delay and Overhead are evaluated for the scenarios of varying number of nodes. Numbers of nodes are varied as 40,50,60,70. Graphs are plotted for performance metrics using Xgraph in NS-2.

Packet Delivery Ratio (PDR): The ratio between the total number of delivered packets to the base station and the total number of transmitted packets from the sensor nodes.

Network lifetime: The network lifetime represents the remaining energy of a node, which has minimum energy in the network.

Delay: Every node follows the secure routing protocol to deliver the data packets to the base station. Delay of a packet is defined as the average time taken by a node to deliver the data packets to the base station.

Overhead: The overhead is defined as the total number of control packets used in the network. The routing protocols exploit control packets to detect the routing paths to the

base station. More number of control packets tends the sensors to spend a lot of energy and so maintaining the overhead while providing the network security is essential.

1.11 Research Considerations

The research will comply with ethical principles and requirements of the Informatics and Design Faculty Yeungnam University, Korea. It shall also comply with the general principles of experimental research. It shall not manipulate the processes of performance analysis in quantitative measurement that are used for graph generation. The research will use open-source software as such must comply with terms and conditions thereof. Different simulation experiments are conducted to collect the data points required for graph plot.

Even if the malicious SN or CH nodes are eliminated, there is the possibility for the revoked node to launch impersonation attack and perform other attacks again. To overcome such issue each node is required to attach its signature during data transmission. Security of IDSHT protocol is improved with signature generation and verification mechanism and it is named as IDSHT-S. RSA is used for signature generation and verification. Through the signature mechanism impersonation attack is prevented.

The hierarchical trust-based IDS divides the WSN nodes into sensor nodes and cluster head nodes. It exploits different trust factors to measure the behaviour of nodes with respect to its role, such as IT, HT, and CT. Moreover, the multi-dimensional Trust is maintained in two levels: Multi-dimensional Trust of sensor nodes (SN) is maintained by CH as well as the multi-dimensional Trust of CH is maintained by SN. Trust of SN:

IT for SN (ITSN) - The average number of times the node involved as router in data transmission from CH to BS.

HT - Successful data forwarding Ratio from CH to

BS CT - Data Non deviation Ratio

$$OT = \alpha * IT_{SN} + \beta * HT + \gamma * CT$$ …….. Equation 1.1

Trust of CH:

IT for CH (ITCH) - The average number of times the node is selected as CH

HT - Successful data forwarding Ratio from SN to BS

CT - Aggregation Data non deviation Ratio

$$OT = \alpha * IT_{CH} + \beta * HT + \gamma * CT$$ … Equation 1.2

α, β and γ are weighting factors

If the selfish attack is launched by the node it will announce fake energy value in control information to avoid from selected as CH or router in order to preserve its energy. It reduces the ITSN and ITCH value of the node.

If the dropping attack is launched by the node it will drop the data without forwarding it that reduces HT value.

If the false data injection attack is launched it injects the false data value that is deviated from actual value that reduces CT value.

If the overall trust value OT is less than the threshold, then intrusion is detected at the node.

1.12 Security in Wireless Sensor Network

The WSN is widely used in monitoring and tracking based applications, where large deployment of cheap sensor nodes is advantageous. But the sensor nodes are often prone to malicious attacks, due to several factors such as the use of the wireless medium for data transmission, the necessity of multi-hop communication and deployment in remote areas (Naeem & Loo, 2009). Sometimes data is damaged by traffic congestion and node failures due to energy exhaustion. Malicious intruders also target the routing protocols and data aggregation techniques, which are designed for reducing the large energy consumption in the network. During the data transmission, adversaries interrupt or eavesdrop the data traffic with the aim of creating confusion in the network (Walters et al., 2007). In multi-hop communication, the adversaries often act as intermediate nodes for forwarding data and steal confidential data, and thus the need for trustworthy nodes is a necessary parameter. Thus, securing data during transmission is highly critical in real-time applications, where corrupted data cause unnecessary outcomes. The military and medical field applications mainly need accurate and confidential data at the destination end, but the hindrance due to physical factors and security threats makes it a difficult task. Many security mechanisms have been designed to detect and prevent attacks in the network. The use of cryptographic keys can protect the node from leaking important data. Due to the large storage overhead and complex calculations, the traditional security mechanisms are not suitable for resource constrained WSN. The security mechanisms must consider both the security requirements and the design challenges in the WSN.

1.12.1 Goals of Security Mechanisms

The security mechanisms must aim at protecting the following security requirements are given in Figure 1.4 (Du & Chen, 2008).

Data Confidentiality: The military and medical sectors-based applications involve the transmission of important data to the receiver, which is present in a long-distance range and thus the security in these applications is a major concern. The data confidentiality is one of the important paramounts that need be protected during communication. Most of the attacks aimed at stealing the data rather than physically affecting the service it

performs. Encryption and decryption mechanisms must be used in the communication to protect the data from eavesdroppers.

Data Integrity: During data transmission, the tampering and altering the original data affects the integrity of the network. It occurs mainly due to malicious intruders and due to the physical factors of the deployed environment. Data integrity focuses on the transmission of data without any modification to preserve the originality of data (Durresi et al., 2005). The accuracy of the data is a needed parameter in many applications, where the alteration of data leads to a different turn of events. Introduction of cryptographic algorithms enhances the data integrity of the network.

Privacy of Data: The identity and location of the sensor nodes have to be secured for unintended users. When these two parameters are leaked, it sometimes directly affects the purpose the application, i.e., the location of the base station. The location and identity are exposed mainly due to traffic analysis attacks, and data privacy is affected. The context of privacy protects the location of the node and temporal privacy of events. The privacy techniques have to introduce to protect the privacy of the network (Chow et al., 2014).

Data Freshness: The freshness of the data is important in WSN mainly while monitoring ongoing events. Due to malicious attacks such as replay attacks, the delay of data packets and replaying data is done after a certain interval to disturb the actual event. The encryption keys must be refreshed periodically to assure that the data are updated depending on the current events. The data freshness is ensured by introducing time-based counters while sending data packets.

Authentication: The data authentication is necessary for WSN to assure that the data is from the legitimate user. The conformity of designated users at both the ends is done by use of Message Authentication Code (MAC). The authentication verifies and guarantees every node that is involved in the transmission is uncompromised and verifies the control update packets are from the source. Some authentication protocols affect the performance metrics such as large storage requirement, complex calculations, and increased communication delay. The digital certificates are used for easy and secure authentication to decrease its impact on the resources.

Availability: The data availability is the ability of a node to send the data and also respond to the queries continuously without any delay or issues that may occur due to malicious attacks and physical factors in the environment. In important applications such as in industrial sectors, the availability of data is an essential requirement as it is used to determine the device failures and issues in the network, thus avoiding large impacts in the future (Silva et al., 2012). The availability of the nodes can be confirmed using remote testing and diagnostics.

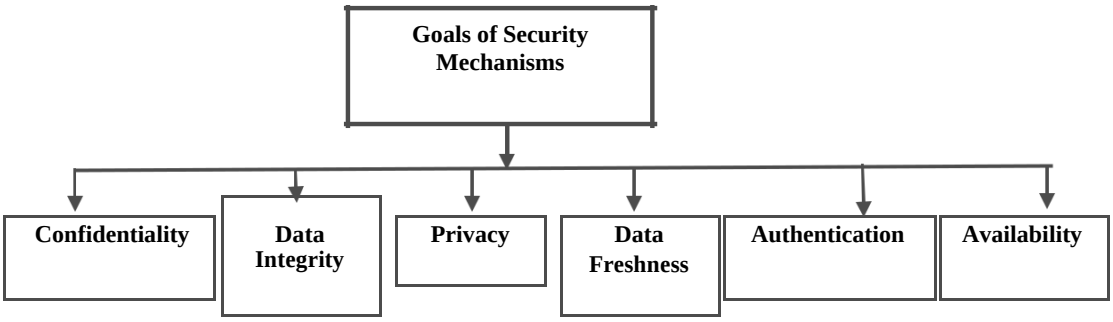

Figure 1.4: Goals of Security Mechanism in WSN

Adapted from (Du & Chen, 2008)

1.12.2 Applications of Secure WSN

The application of WSN is vastly spreading in almost all sectors, where monitoring and tracking of events are done virtually with the necessity of secure transmission (Garcia-Hernandez et al., 2007). The main sectors in which WSN applications used are shown in Figure 1.5.

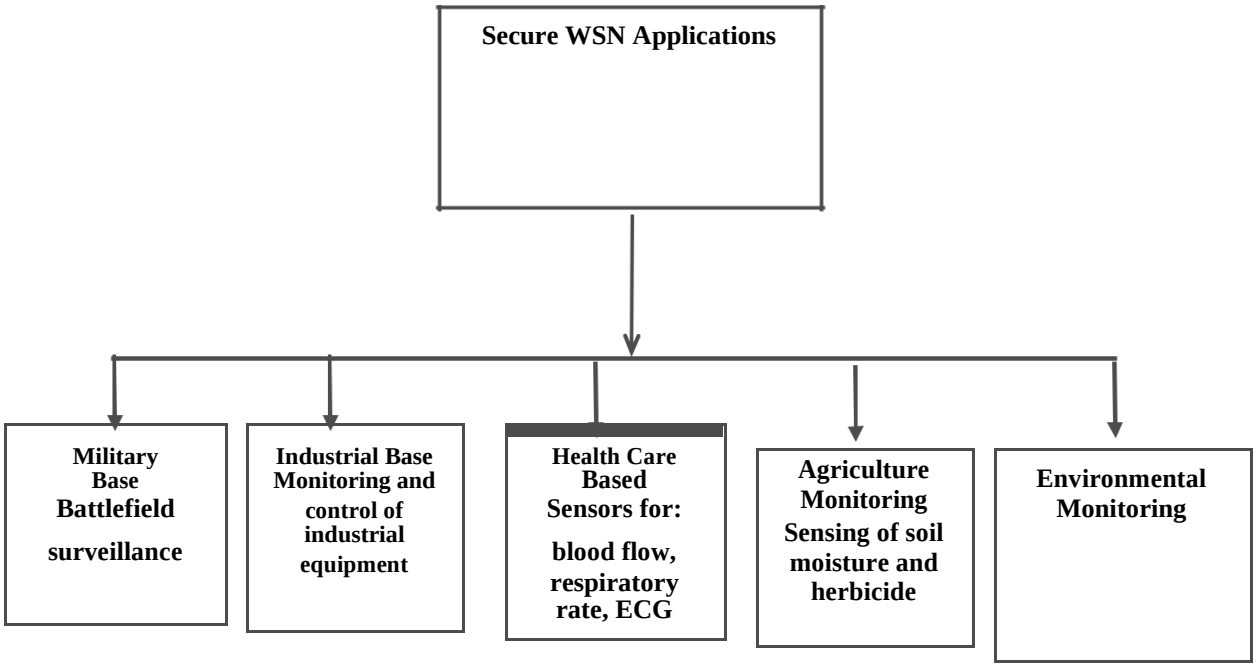

Figure 1.5: Applications of WSN

Adapted from (Garcia-Hernandez et al., 2007)

Military Based Applications: The WSN is required in military applications for transferring critical data rapidly to the designated receiver at the right time in spite of the deployed environment and other physical factors (Winkler et al., 2008). The important requirement in the military based applications is security, as the data which is sensed and transmitted through the wireless medium requires high confidentiality and accuracy. The WSN is used in military based applications, mainly for tracking enemy movements, force

protection, battlefield surveillance, and detection of Nuclear, Biological and Chemical (NBC) attacks (Ahmad et al., 2016). The use of WSN in the military field is to monitor enemy movements and relay emergency alert in case of intrusions in a proactive manner. The collaborative nature of sensor nodes can detect the enemy troops position and location, which helps in taking timely actions. The WSN is also used in tracking friendly forces in the hostile areas and providing them with information regarding the best course of action to be taken on the necessary situation. The NBC attacks can be detected early and accurately using WSN and help in avoiding large causalities. The data monitored in the military applications are mainly required for taking an important decision, and hence modification or interference of data must be avoided. The use of cryptographic keys and authentication mechanism can protect the message from malicious intruders and provide end to end message integrity.

Industrial Based Applications: One of the fast-growing industrial sectors makes use of WSN for improving productivity and efficiency by detecting errors and machine failures. The convenience of installation and use of cheap sensor nodes for detection of equipment faults is an added advantage of WSN in industrial applications. The WSN is used for structural monitoring condition and also machine health, which can detect issues which later can be life-threatening. In industrial applications, robustness is the key factor where many issues such as electromagnetic interference can deteriorate the performance of WSN systems, resulting in faulty detection (Lu & Li, 2014; Mikhaylov et al., 2012). It is also necessary for the sensor nodes to withstand high operating temperature, strong vibrations, and airborne containment. The use of WSN provides many benefits for the industrial applications, but at the same time, the reliability of the data must be managed. The information collected during the monitoring process is vital for process operation and hence secure transmission using security mechanisms is also a needed requirement (Erdelj et al., 2013).

Health care-based Applications: The introduction of Personal Digital Assistant (PDA), which comprises a wearable sensor device has made WSN application an important component in the medical industry. The patient's physiological parameters include vital sign detection, diet and exercise routine monitoring, unconscious detection, and fall detection. These parameters are monitored and measured using these data monitoring systems. Then, the medical emergency alert is sent to the patient or the concerned user who handles the aftermath of the situation. The health care application must support technological feasibility, provide visualization of remote treatment, maintain information sharing and management of patient medical requirements, keep a computerized physician order entry, and the technique must satisfy customer acceptance. The advantage of using sensor devices such PDA in the medical field is to remotely monitor the physiological parameters of patients without affecting their normal routine life and

providing immediate, virtual assistance in case of emergencies (Shnayder et al., 2005; Alemdar & Ersoy, 2010). The problems faced during the use of WSN in the medical field are larger energy consumption, the long-distance data transmission may cause congestion and packet loss due to which proper medical assistance cannot be provided. Several research works are being made to overcome these problems (Aminian, & Naji, 2013).

Agriculture Monitoring: Agriculture is an important economic sector, that needs optimal and profitable use of land and water resources. In WSN based agriculture monitoring systems, the monitoring of environmental factors such as humidity, soil temperature, CO2 concentration, and crop growth is critical to get good productivity (Hwang et al., 2010). Proper irrigation scheduling reduces economic losses that occur due to under irrigation, inadequate nutrient supply, pesticide problems. The sparse deployment of sensor nodes with data collection intervals can increase the lifetime of the network. The design challenges faced in the agriculture-based monitoring system are interference in signal due to the deployment region, limitation of sensor node resources, tuning the application different on the different topology soil structure and other factors.

Environmental Monitoring: The environmental monitoring applications in WSN are used in both indoor and outdoor environments. The outdoor environmental applications are monitoring environmental conditions such as earthquake detection, temperature sensing, weather prediction, cyclone prediction, wildlife tracking, pollution monitoring and so on. The indoor monitoring applications based on WSN are intruders' detection, indoor air quality monitoring, temperature sensing, fire accident detection, and humidity monitoring. The outdoor monitoring systems require proper power management and reduced computations as the transmission coverage of the deployed region is vast. The outdoor environment monitoring systems are also often affected by attenuation of the signal which causes delayed outputs and thus disturbing desired outcomes (Oliveira & Rodrigues, 2011).

Table 1.2: The Uses and Design Challenges of Various WSN Applications

WSN Applications	Uses	Design Requirements
Military-based applications	1. Tracking enemy movements 2. Force protection 3. Detection of battlefield surveillance 4. Battle damage assessment 5. Exploration of enemy forces and terrains 6. Detection of NBC attacks	The necessity of two-way communication leads to security threats The nodes protected with Cryptographic keys must have an anti-tamper mechanism to prevent leakage of data by any third party. The data reliability must be assured without any form of interception or modification.
Industrial based applications	4 Machine Health monitoring 4 In-process part tracking	Radio Frequency (RF) interference due to multipath propagation and noise from other machinery.

	4 Automated problem reporting 4 Structural health monitoring	Sensor nodes are deployed in harsh environmental conditions which includes high operational temperature, atmospheric precipitation, and strong vibrations. WSN must support periodic changes to network topology. Security mechanism in the industrial based applications must handle any form of intrusions.
Health care-based applications	4 vital sign detection, 4 dietary and exercise routine monitoring, 4 unconscious detection 4 fall detection	The longer distance data transmission may cause congestion and packet loss due to which proper medical assistance cannot be provided. large energy consumption.
Agricultural monitoring	1. Monitoring environmental factors such as humidity, soil temperature, CO2 concentration, and luminescence. 2. Monitoring crop growth 3. Controlled use of fertilizers 4. Cattle movement monitoring 5. Groundwater quality monitoring	Proper tuning of the application parameter based on different locations The attenuation of the signal depends on the choice of deployment. The limitation of sensor node resources affects the system performance.
Environmental monitoring	Indoor Monitoring: 1. Temperature sensing 2. Weather prediction 3. Habitat monitoring 4. Traffic monitoring 5. Wildlife monitoring 6. indoor air quality monitoring Outdoor Monitoring: 1. air pollution monitoring 2. forest fire detection 3. greenhouse monitoring 4. animal tracking applications 5. landslide detection	The monitoring sensors must perform a simple operation to prevent unexpected hardware failures. Poor radio connectivity leads to delayed outputs. Power management is essential in hostile and remote monitoring environment.

Adapted from (Ahmad et.al, 2016) (Lu & Li, 2014) (Mikhaylov et.al, 2012) (Hwang et.al, 2010) (Oliveira & Rodrigues, 2011)

1.12.3 Challenges in Designing WSN

The design of small and cheap sensors has its characteristics and challenges when they are used in real time applications, and they are illustrated below.

Scalability: The WSN extends its area by the addition of sensor nodes to the existing network. There is no limitation for adding sensor nodes, and it depends only on the application requirements. When the number of nodes grows, the energy consumption of overall network increases and link breakage can occur (Siji & Eneh, 2015). Thus, extending the network area must also consider the aftereffects that cause an increase in energy consumption and reduction in network lifetime.

Power Consumption: The uninhabited environmental applications need monitoring systems with a longer network lifetime, which is possible by battery-driven sensor nodes.

Most of the energy is consumed by sensor nodes for the sensing, processing, and data transmission purpose, hence the allocation of energy resources for other necessities has to be properly calculated. The energy consumption in data transmission is more compared to energy consumption during data processing (Raghunathan et al., 2002). The overall Power consumption can be reduced by keeping the nodes in, switch off position until they have to perform the work.

Localization: The location of event occurrence is necessary for most of the real-time applications of sensor nodes. For dense network scenarios, the manual configuration of enabling location parameter in sensor nodes is not possible. The collaboration of neighbour nodes plays a significant role in detecting the current location of sensor nodes (Kuriakose et al., 2014). The wrong estimation of node position leads to serious effects on the desired outcome. Hence, the Localization accuracy with minimal energy consumption is one of the challenges of the WSN.

Fault Tolerance: One of the important requirements that need to be focused in WSN is the fault-tolerant capability of sensor nodes. The ability of a network to continue its function in spite of the failure of components is the fault tolerance of the system. The node failure occurs mainly due to battery exhaustion, hardware failure, environmental factors based on node deployment, communication link errors, and due to malicious attacks. The failure of specific nodes can bring the functionality of the entire network. Adopting fault detection such as self-diagnosis, group detection and fault recovery techniques such as multi-path routing can avoid and minimize the impact of node failures (Alrajei et al., 2014).

Quality of services: Due to the limitation of the sensor node's resources, the maintenance of Quality of Services (QoS) is difficult. The requirements of QoS changes based on the network and application scenarios. The necessity of providing efficient QoS in a wireless sensor network is achieved by the following factors (Fonoage et al., 2010).

- Avoidance of path delay, jitters and traffic congestion by congestion control mechanisms.
- Lesser utilization of bandwidth by adopting in-network aggregation.
- Reduction in energy consumption of individual nodes.
- The probability of packet loss must be less.
- Providing efficient data delivery through efficient routing techniques.

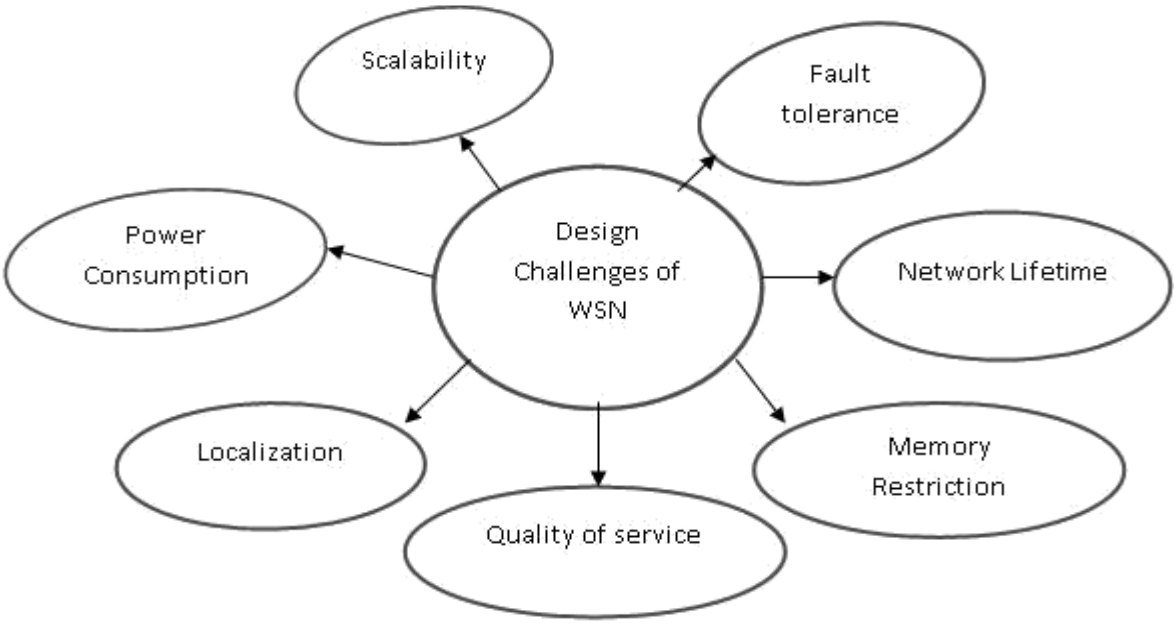

Figure 1. 6: Design Challenges of WSN

Adapted from (Akyildiz et al., 2002)

Memory Restriction: The storage capability of sensor nodes is limited, considering the nodes' physical size and minimum production cost. Some WSN applications require large computations during which the storage scarcity becomes a major issue. Several techniques have been adopted to enhance the storage requirements of sensor nodes (Ez-Zaidi, & Rakrak, 2017). The storage issue can be minimized by reducing the size of stored data, performing efficient query execution, data reallocation where old data are deleted.

Network Lifetime: The network lifetime considers the availability of sensor nodes to sustain in an environment performing their assigned tasks. They directly depend on the energy efficiency and residual energy available. The major factors that affect the network lifetime have increased energy consumption, due to malicious attacks, exhausted storage space and a large number of node failures. Several techniques are adapted to prolong the network lifetime such as time integration, connected coverage, and service disruption tolerance (Dietrich& Dressle, 2009).

1.13 Classification of Security Attacks in WSN

The security in WSN is a major threat due to the factors such as transmission through a wireless medium, restriction of limited sensor node resources, and inability to protect the system physically (Walters et al., 2007) (Biswas & Adhikari, 2015). Even if the necessary security mechanisms have been developed against the malicious attacks, the efficiency is not achieved due to the resource restrictions. The attackers exploit the physical threat in WSN to gain access to the network (Lupu et al., 2009) (Wang et al., 2006). The attacks

can occur either by an internal attacker or external attacker based on the location in which malicious attack occurs. The classification of security attack in WSN is based on attacker location, attacking function, damage level and attacking device is given in figure 2.4

Based on Damaged Level: There are mainly two types of security attacks based on the level of damage an attacker imposes on the network, and they are active attack and passive attack.

Active Attack: The active attack aims at disturbing the network by either removing or modifying the data that is transmitted in the network. These malicious attackers inject false data and drop certain data packet that leads to undesired output. The malicious activities done by active attackers are injecting faulty data, impersonating, packet modification, unauthorized access of data by monitoring and eavesdropping data packets and overloading the network by sending multiple unnecessary packets. The result of these malicious activities causes data alteration, inability to WSN to perform operations, performance degradation, and functionality disruption.

Passive Attacks: The passive attack mainly focuses on stealing information from the network without addressing their presence in the attack. The malicious activities mainly eavesdrop the network traffic to gain relevant knowledge and finding critical nodes. This information is used later to impose a serious attack on the network.

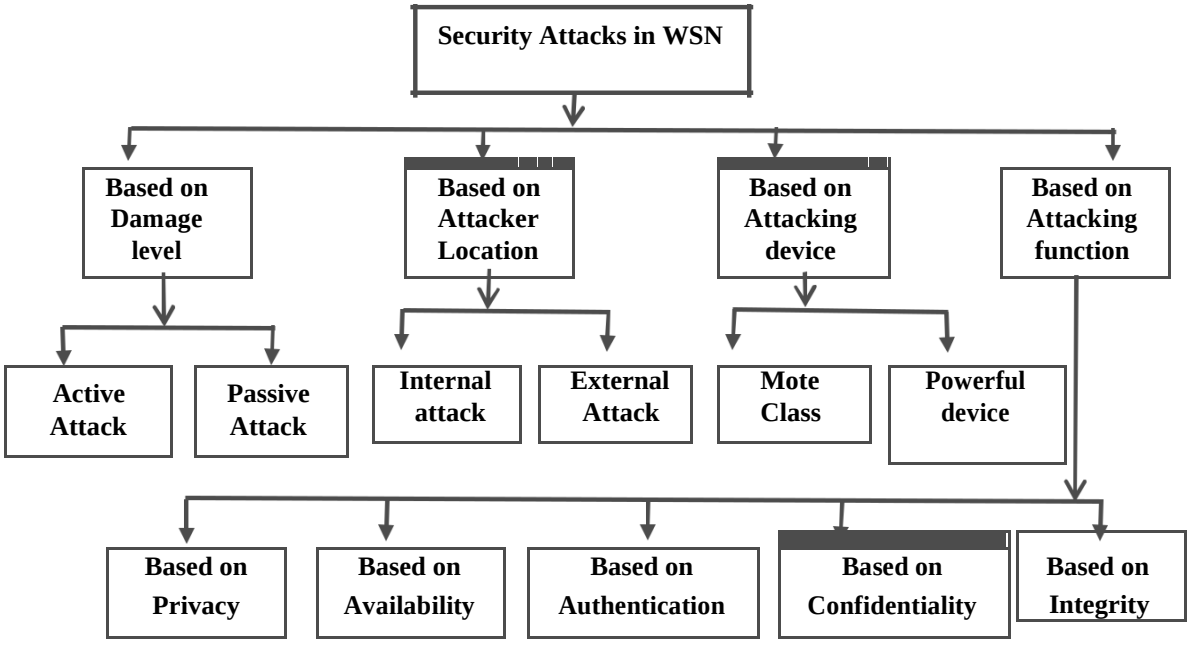

Figure 1.7: Classification of Security Attacks in WSN

Adapted from (Mohammadi et.al, 2011) (Biswas & Adhikari, 2015)

Based on Attacker Location: The security attacks are classified into two types based on the location of the attacker, who imposes unwanted activities in the network. The two types of attacks are internal attacks and external attacks.

Internal Attack: The internal attack causes serious damage to the network by acting as legitimate nodes. These malicious nodes trick the neighbouring nodes to share important information and modify data that pass through them (Ahmed et al., 2018). The internal attackers steal cryptographic keys by imposing different attacks and destroy the functionality of the whole network.

External Attack: The external attack mainly aims to interrupt the service of the network by jamming communication channel, imposing several unwanted activities to increase the resource consumption by nodes and increasing data traffic leading to delay in the network.

Table 1.3: Effects of Security threats in WSN

Security threats	Attacker Type	Security parameters affected	Attack effects
Based on damage level	Active attack	Integrity, availability, authentication	Modification interruption and interception of data
	Passive attack	Privacy, confidentiality	Stealing important information and cryptographic keys by monitoring network traffic
Based on attacker location	External attack	Availability, integrity	Jamming communication channels
	Internal attack	Confidentiality, privacy, authentication	Malicious nodes pose as legitimate nodes to steal information.
Based on the attacking device	Mote class attack	Integrity, availability, authentication	Nodes with limited capabilities to act together for imposing unwanted activities
	Powerful device attack	Privacy, confidentiality, availability	Powerful devices such as malicious network devices pose as an optimal path with high bandwidth and reduced latency

Adapted from (Biswas & Adhikari, 2015)

Based on Attacking Device: The security attack is classified into two types based on the type of device used in inducing security threat to the network, and they are mote class attack and powerful device-based attack.

Mote Class Attack: In mote class attack, the nodes with limited roles are used as the mode for imposing attacks in the network. The mote class attackers mainly spoof routing updates and then create routing loops to disturb the network.

Attack Using Powerful Device: These malicious attackers use the powerful external device to impose an attack on the network. They mainly flood the network with hello packets or exhibit themselves as a routing path for transferring data packets. These

attackers have high bandwidth and low latency communication channels that can easily attract neighbouring nodes in transferring packets through them.

Based on Attacking function: These attacks impose on the network targeting to destroy a particular security parameter in the network, and the parameters are availability, authentication, confidentiality, and integrity.

Attack Based on Availability: The availability is one of the key security goals in WSN, where the network has to be available at the needed time. If the nodes are not available for communication, it can cause huge damage to the functionality of the network. The DoS attack is one of the common attacks that aim at destroying the network availability. The attackers mainly disrupt the network by jamming the communication channel and making it impossible for the nodes to communicate with each other. The attacks also target broadcast messages and inject false messages with the aim of changing the traffic flow.

Attack Based on Authentication: The authentication is important security parameters in the network that confirms an end-to-end message integrity by using encryption and decryption algorithms. But certain malicious attacks focus on targeting authentication mechanisms by stealing cryptographic keys and then posing as legitimate nodes. Due to the limited transmission range, the data and control packets are transmitted through broadcasting. The attacker forges a large number of packets and then gains control of the traffic resulting in transmission of delayed data packets.

Attacks Based on Confidentiality: The malicious attack is imposed mainly with the aim of stealing information and disrupting the confidentiality of the network. These passive attackers eavesdrop the network traffic without actually disturbing any service instantly. After gaining knowledge, these attacks provide a gateway for other serious attacks which affects the network seriously. These attacks can be mitigated by using strong authentication mechanism and use of cryptographic keys.

Attacks based on Integrity: The malicious attacks modify the actual data with the aim of disturbing the actual operation of the network. In most of the active attacks, the attacks aim to disturb the network functionality by modifying data packets or injecting false data and thereby affecting the integrity of the data.

Attacks based on Privacy: The malicious nodes use the loopholes of sensor node limitations for gaining access to the network and thereby affecting the privacy of targeted nodes with sensitive information. The privacy is an important parameter in the military and health care sectors-based applications where leakage of the location of nodes causes undesirable consequences. The attackers affect privacy by monitoring network traffic, gaining access to several nodes, spoofing routing updates. The privacy of data can be protected by using a proper node to node authentication and secure routing protocols.

1.13.1 Types of Active Attacks

In an active attack, the aim of malicious intruders in WSN is to change or disturb the actual data flow and degrade the network performance. The different types of active attacks that cause an interruption in the network are given below

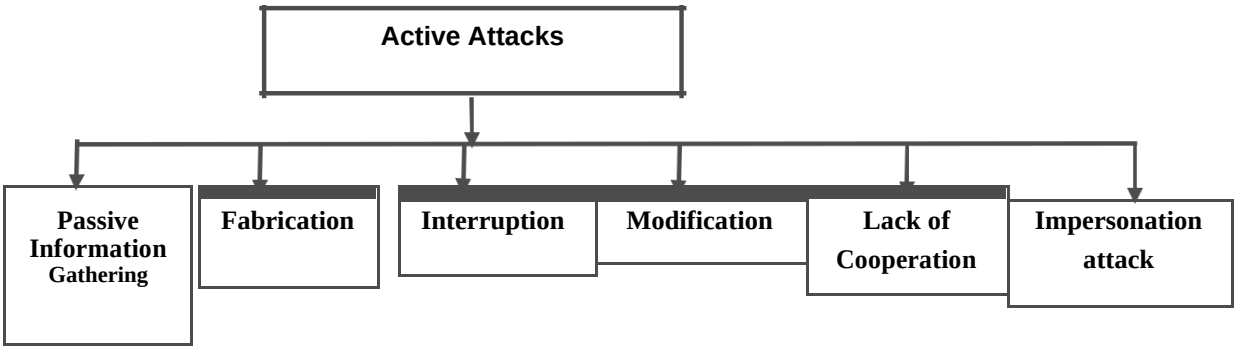

Figure 1.8: Types of Active Attacks in WSN

Adapted from (Benahmed et.al, 2012) (Elqusy et.al, 2017)

Passive information Gathering: In passive information gathering, the malicious attackers with powerful resources to collect information from sensor nodes with weak security features. The intercepted messages are then used to locate the important nodes performing specific activities (Pathan et al., 2006). Apart from gaining information about the location of nodes, other details such as message ID, time stamp are gathered. Strong encryption mechanisms are needed to avoid these types of active attacks.

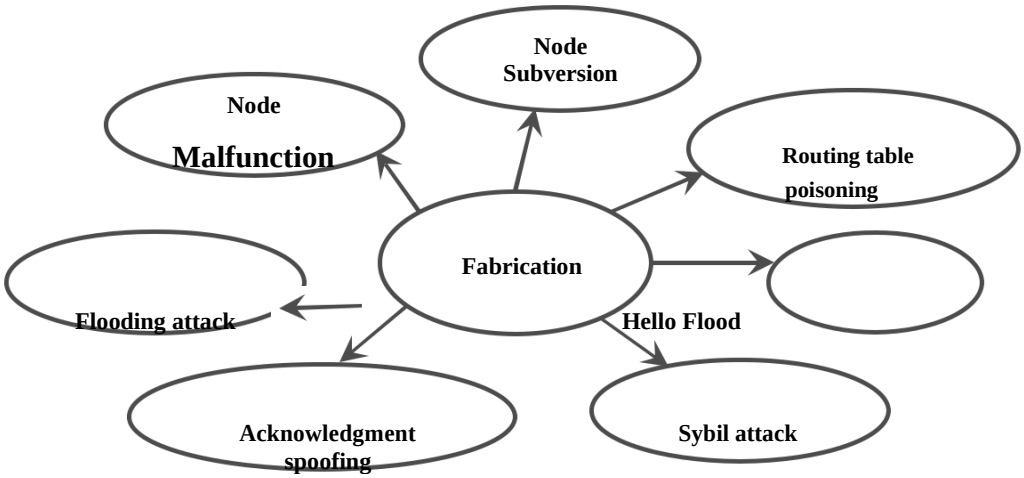

Figure 1.9: Security Attacks Based on Fabrication in WSN

Adapted from (Benahmed et.al, 2012) (Elqusy et.al, 2017)

Fabrication: Fabrication is one of the common active attacks, where the injection of false data in the network that affects the trustworthiness between the nodes. The message authentication is mainly affected by this process, and it also paves the way to other attacks such as DOS attacks by inducing more false data in the network. The fabrication

method is one of the attacks involved in WSN, and they are node subversion, node malfunction, acknowledgment spoofing, sinkhole attack and hello flood attack, sybil attacks

Impersonation: The intermediate nodes play a major role by forwarding data packets from the source to the destined receiver. When the malicious node acts as an intermediate node, the adversary gains the information from the data packets that are forwarded through them. Thereby, it steals the source ID and impersonates as a source to confuse the network. In impersonation attack, the malicious node joins the network and gives false routing information to execute the attack. Sybil attack, false node attack and node replication attack, selective forwarding attack, are the security threats in which common node impersonation attack occurs. The malicious nodes exhibit different energy consumption compared to normal nodes. For example, selective forwarding attack the malicious node has less energy consumption compared to normal nodes, which help to detect the malicious node based on entropy level (Dai et al., 2012). Mutual node authentication needs to be adopted to avoid these attacks from impersonating legitimate nodes.

Lack of Cooperation: In lack of cooperation attack, the nodes do not cooperate and thus denying necessary activities, which in turn causes a disturbance in the network. The node outage attack is a type of lack of cooperation attack, where the functionality of nodes is stopped leading to degradation of system performance.

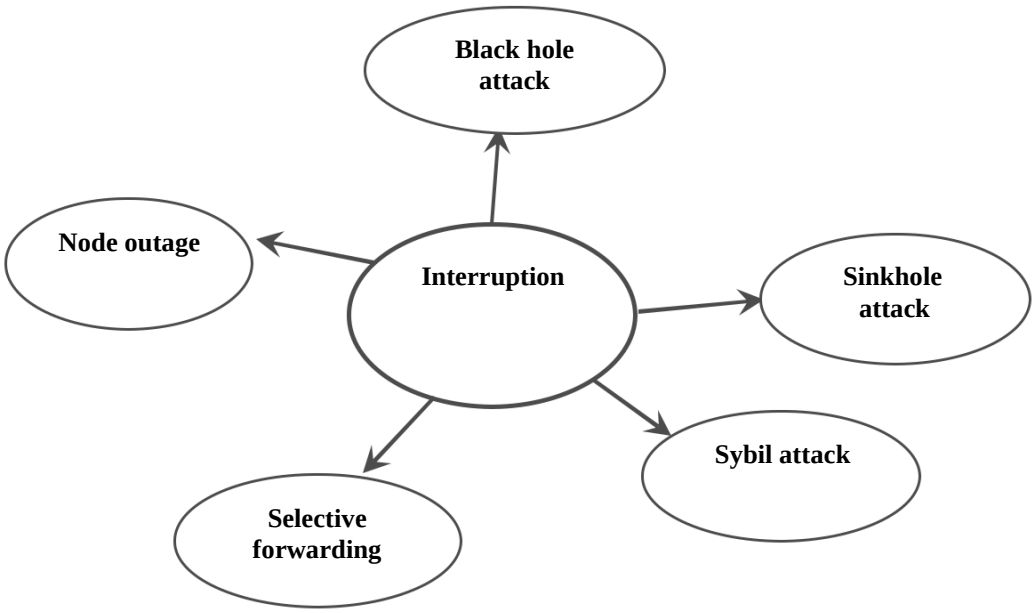

Figure 1.10: Security Attacks Based on Interruption in WSN

Adapted from (Benahmed et.al, 2012) (Elqusy et.al, 2017)

Interruption: The interruption or denial of operation in the network is one of the characteristics of active attacks. In these attacks, the adversary gains access to the network and interrupts the data flow. The common interruption attacks are the black-hole attack, sinkhole attack, selective forwarding attack, node outage attack. The black hole attack is one of the interruption attacks where the nodes are directed with false paths during the pathfinding process and once the legitimate nodes chose the false path, the packet dropping, and interruption of service occurs. Node outage attacks are applied physically or virtually in the network where the functionality of the node services is stopped by the adversaries. The availability and authentication of the network are affected. The use of secure routing protocols and IDS can prevent these attacks.

Modification: In modification attacks, the adversaries impose attacks by deleting, altering and inserting data. These altered data are displayed as the intended data to the legitimate users and hence creating confusion in the network. The common modification attacks are replay attack, collision attack, wormhole attack, desynchronization, and message corruption attack.

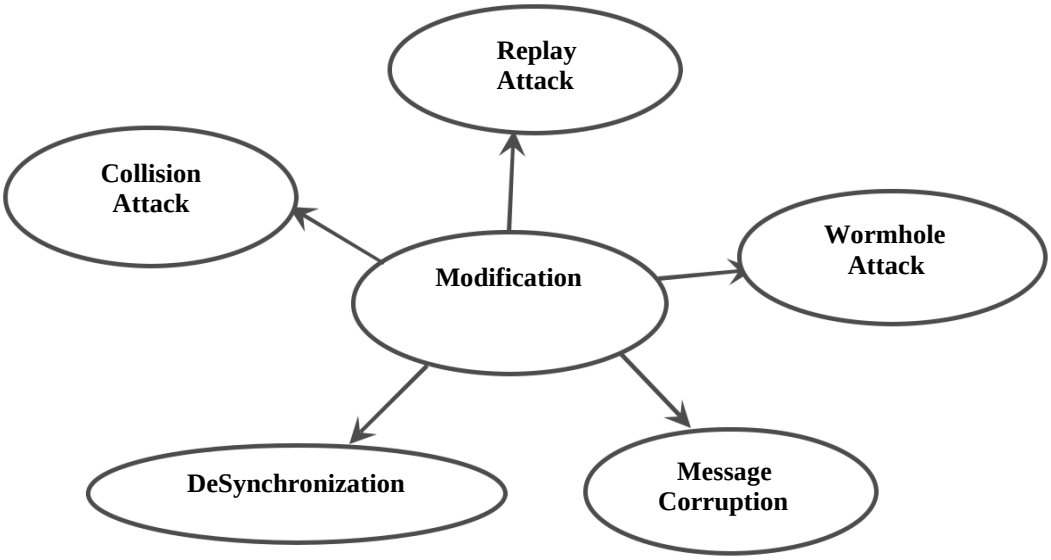

Figure 1.11: Security Attacks Based on Modification in WSN

Adapted from (Benahmed et.al, 2012) (Elqusy et.al, 2017)

1.13.2 Types of Passive Attacks

In passive attacks, the adversary monitors and listen to the network traffic with the aim of stealing information during data transmission. The passive attackers focus only on data retrieval without interrupting the communication channel. The classification of a passive attack is shown in figure 2.9.

Interception: The interception of data is done by a malicious attacker, who acts as a normal node and gather information that passes through it. The data are intercepted and are later used for inducing other serious attacks. The types of passive attacks are eavesdropping attack, traffic analysis, and camouflaged adversaries.

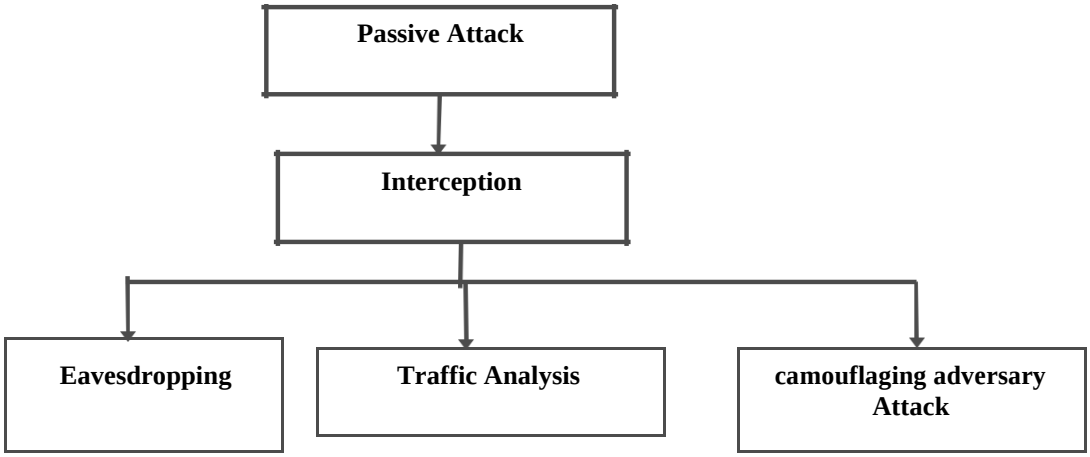

Figure 1.12: Types of Passive Attacks in WSN

Adapted from (Benahmed et.al, 2012) (Elqusy et.al, 2017)

Eavesdropping attack: Eavesdropping attack is one of the serious threats in WSN as they cannot be easily identified and they are prerequisite to other serious attacks. The use of wireless media and other characteristics of WSN makes adversaries steal data easily in the absence of strong security mechanism. The passive attackers steal important information such as route information, identity, and location of important nodes. Many malicious activities initiate their attack pattern after gathering information from eavesdropping activity. The privacy of the data is affected which is a serious threat to the application in military and medical sectors. For example, eavesdropping the communication channel can give out the location of the important node that leads to serious issues. The eavesdropping attack can be mitigated by using authentication mechanisms and cryptographic keys.

Traffic analysis: When the data are encrypted it is not possible to get the information that is transmitted in the network. But using traffic analysis, the flow of data and traffic in the network the location and nature of queries can be obtained. For example, in military applications, the traffic flow is high in the location of a high commander where the information of all decision-making data is sent. By analysing the traffic flow continuously, the location can be obtained which leads to serious undesirable consequences (Deng et al., 2005). Secure routing like multi-path routing techniques can be adapted to provide equal traffic flow which helps to these attacks.

Camouflaging adversary Attack: The camouflaging adversary attack is one of the passive attacks done by an internal attacker, a malicious attacker takes control of the node and then acts as a normal node. Then, these malicious nodes aim to gather information as a priority and impose serious attacks by giving false routing information and causing confusion in the network. These attacks can be mitigated by using mutual node authentication mechanisms and IDS that detect the presence of a similar pattern in the network.

1.14 Types of Secure routing protocols in WSN

The secure routing protocol is an important requirement regarding energy efficiency and securing the data during transmission. Several types of secure routing protocols based on path establishment, network structure and protocol operation are given in the figure 2.10 (Taleb, 2015) (Riad et al., 2013) (Cirstea, 2011).

Path Establishment: Depending on the path establishment, routing protocols are classified into proactive, reactive and hybrid routing protocols (Chen et al., 2010).

Proactive Routing protocol: In the proactive routing protocol, each node maintains, updates of the routes of other nodes in the network. The routing table consistency is maintained by periodically transmitting, routing information to every node in the network. The proactive protocol is also called as table-driven protocol as they store predefined routing information. The routing table contains the destination node field, next node field, hop number field, sequence number field, and time adjustment field. The advantage of the proactive routing protocol is the time delay is minimized, and stability maintained during data transmission. These protocols are not suitable for a large network since the routing information of each node is entered in the routing table leads to increased storage overhead and complexity in maintenance.

Reactive Routing protocol: The reactive routing protocol is called on-demand routing protocols as the routes are updated based on the demand of nodes. In this process, the route is not predefined, but routes are updated when the node wants to transfer the data to the destination. This protocol is more suitable for dynamic network topology where the establishment and maintenance of the routing path are necessary. The three procedures included in the process are route request, route reply and route maintenance, which helps to provide data freshness. When the node wants to communicate with the destination node, it broadcasts a route request to establish a connection. The route reply from the destination node is sent after verifying the destination sequence number with the destination in its routing table. The route maintenance detects link breakage and sends a request error message to source node which in turn request route discovery process.

Hybrid Routing protocol: The hybrid routing protocol integrates the advantage of both proactive and reactive routing protocols. Considering a hierarchical model, the cluster

node adopts the proactive routing protocol for route information while the reactive routing protocol is used when sending data to cluster members or to communicate with other clusters.

Based on Network Structure: Based on the structure of network topology, the routing protocols are classified into flat based, hierarchical based, and location-based routing protocols (Al-Karaki et al., 2004).

Data-Centric and Hierarchical Based Routing Protocols: The data-centric routing protocol is a flat based routing protocol, where the base station sends queries to certain regions and wait for the data from these regions. The data-centric routing protocol adapts multi-hop routing to enhance the energy efficiency of individual nodes and reduce the storage overhead. The hierarchical routing protocol involves a tree-based structure in which the nodes are prioritized with specific roles. A hierarchical routing protocol is an efficient method to reduce energy consumption in the network. The security attack in these protocols does not cause severe damage compared to the data-centric routing protocol, wherein the hierarchical routing protocol the leakage of information from the single node will not expose the data of other nodes.

Location Based Routing Protocol: In the location-based routing protocols, the sensor nodes are categorized based on location in the sensor nodes and routing is done by the geographic location of sensor nodes. The location of the sensor nodes is required to find the distance between neighbouring nodes. The distance between the nodes is estimated based on the incoming signal strength. The energy consumption of the nodes is reduced by placing the nodes in a sleep state when there is no activity in the network. The location-based routing protocols use the area as the target of the packet instead of a node identifier. These protocols consider the mobility of sensor nodes, and it is suitable when the density of the network is increased. The disadvantage of the location-based routing protocol is that the performance of the network is decreased when the network deployment is sparse.

Based on Protocol Operation: The routing protocols are classified based on the protocol functionality, and they are multipath, query-based, negotiation based, QoS based, coherent and non-coherent based routing protocols (Al-Karaki et al., 2004).

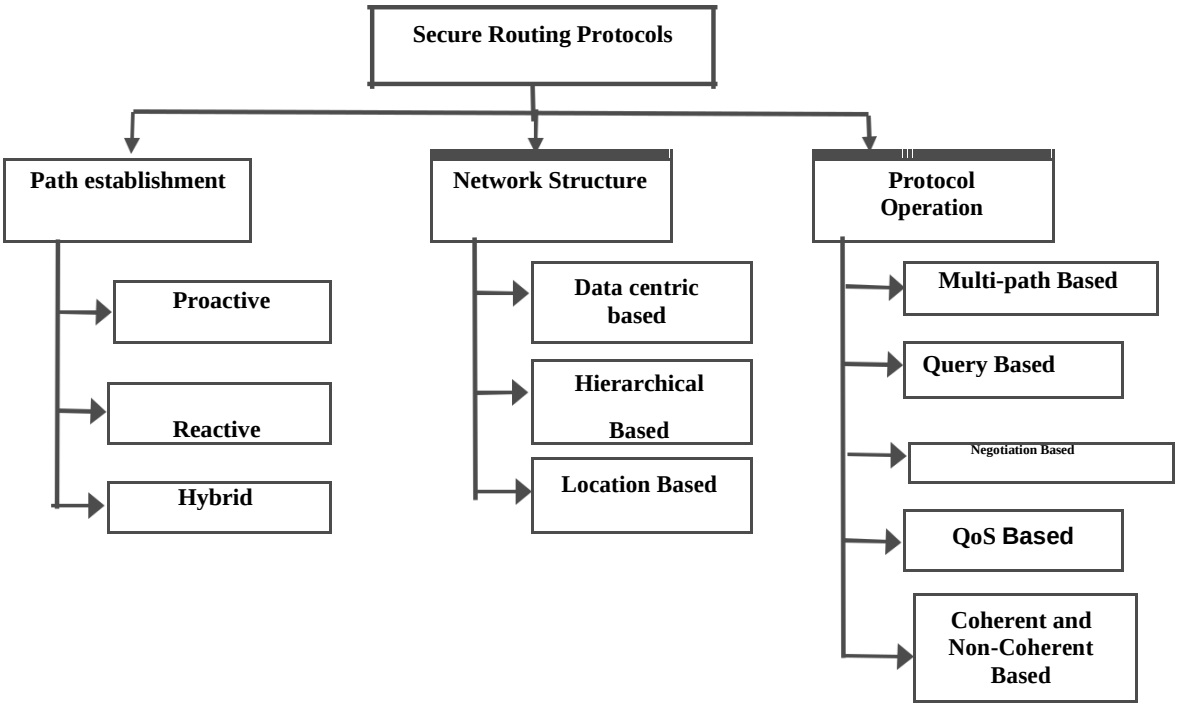

Figure 1.13: Types of Secure Routing Protocols in WSN

Adapted from (Taleb, 2015) (Riad et.al, 2013) (Shabbir et.al, 2017)

Multipath Based Routing Protocol: In the multipath routing protocol, the data is sent through multipath instead of a single path to reduce packet loss in the network. The alternate path is chosen by the nodes when the primary route in which the data is transmitted fails. The alternate paths are kept alive by sending messages periodically. The concept of multipath routing increases energy consumption and latency in the network.

Query-based Routing Protocol: In a query-based routing protocol, the destination node broadcasts the query of the data and node which matches the query sends back the data to the initiated node. The query used in the query-based routing protocols is expressed in the form of natural language or high-level query language.

Negotiation Based Routing Protocol: In the negotiation-based routing protocol, the high-level data descriptors are used to suppress the redundant data transmission through negotiation. The main aim of the negotiation routing protocol is to eliminate message duplication. The negotiation routing protocol involves a series of negotiation messages sent before the actual data transmission to prevent redundant data being sent to the neighbouring nodes or the base station.

QoS based Routing Protocol: The QoS based routing protocol focuses on maintaining the balance between energy consumption and data quality. The node before sending

data to the destination node has to satisfy certain QoS metrics such as delay, residual energy, and bandwidth.

Coherent and Non-Coherent Based Routing Protocol: The routing protocols are classified into coherent and non-coherent based routing protocols based on the data processing involved. In non-coherent based routing protocol, the nodes process the data locally before transmitting the data to other nodes. In the coherent based routing protocol, the minimum data processing such as time stamping, and suppression of duplicate messages occur before forwarding the data to the aggregator nodes which does the further processing. The advantage of the coherent based routing protocol is that it is energy efficient as the nodes perform the processing and in turn reduces the energy consumption and total time.

1.15 Types of Trust-Based Schemes in WSN

The trust-based schemes are broadly classified into infrastructure-based trust, and self-organizing trust and the classification of trust is shown in Figure .

Infrastructure-Based Trust: The trust-based schemes are classified into two types based on the infrastructure for storing trust information, and they are centralized trust-based system and distributed trust-based systems (Elqusy et al., 2017) (Zahariadis et al., 2010).

Centralized trust systems: In centralized trust systems, the trust values of the participants are stored and maintained by the central third party, i.e., base station. The central third party handles the trust values which in turn reduce the storage overhead of individual nodes. The base station takes the responsibility to decide the node's trustworthiness by gathering, trust information on its own or by collecting trust information from specific nodes in the network. The centralized trust-based model has less computational overhead and memory usage. The advantage of centralized trust management that it is not necessary to implement trust evaluation in all the nodes. The disadvantage of centralized trust management is that the communication overhead is large, and it is not suitable for large area network. It also lacks reliability due to the data delay that occurs during the transmission and one to one forwarding of every data with the base station.

Distributed trust systems: In distributed trust management, each node monitors the behaviour of the neighbours and gather measurements for calculating the trustworthiness. The trustworthiness of the nodes is then used during routing decisions. If the trust functionality calculation of individual node increases the communication cost of the overall network also increases. The main advantage of distributed trust management compared to centralized trust management is that there is no single point of failure, i.e., compromising a node does not leak the information of other nodes.

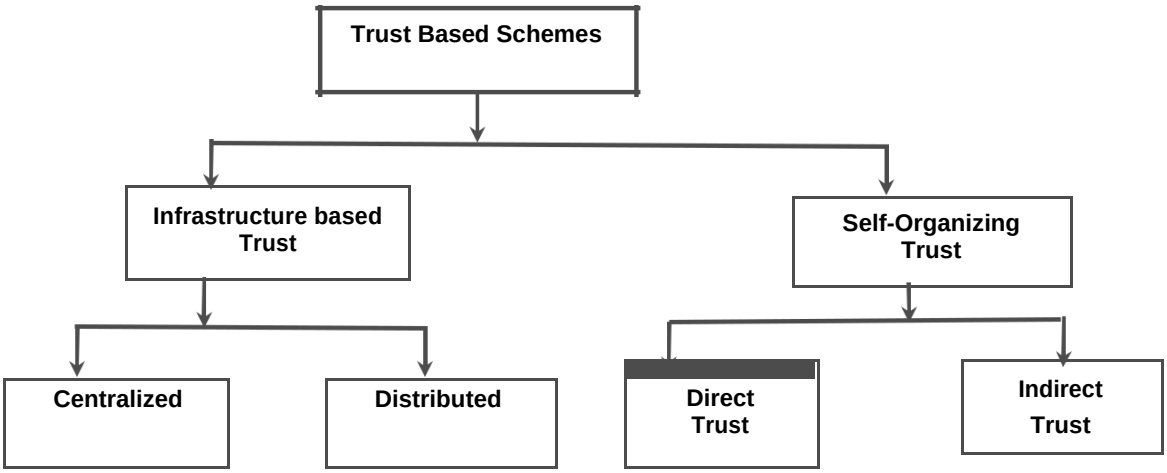

Figure 1.14: Types of Trust -Based Schemes in WSN

Adapted from (Khalid et al., 2013)

Self-Organizing Trust: Based on the self-organizing trust, the trust model is classified into direct trust, indirect trust, and hybrid trust.

Direct Trust: In the direct trust, the trust value of the particular node is determined using different trust metrics for different events in the network. Direct trust can be calculated using the real-time monitoring value and historical data of the sensor node. It considers the trust metrics such as packet sending rate, packet receiving rate, node availability metrics to calculate the trustworthiness of the node. The direct trust is the result of the independent trust evaluation between two intermediate nodes.

Indirect trust: In indirect trust, the evaluation of the node behaviour is estimated using the trust metrics recommended by the trusted third party. When a sender wants to transfer data or communicate with the target node, the cooperation request is sent out by the source node, and the trusted neighbouring node or a base station replies the request with trust metrics after which the unreliable nodes are discarded.

1.16 Types of Intrusion Detection Systems in WSN

The IDS involves real-time monitoring of network activity and detection of unwanted intruders that do not satisfy certain protocols. They are classified into three main divisions such as based on detection methodology, the source of audit data and computing location.

Based on Detection Methodology: The IDS are classified into three types based on the detection methodology, and they are misuse based, behaviour-based, and hybrid-based IDS (Maleh & Ezzati, 2014) (Ning & Jajodia,2003).

Misuse Based IDS: In misuse-based IDS, a sequence of patterns such as attack signature patterns such as previous attack profiles, intrusion patterns are stored in the

database. They are also known as signature-based IDS as the stored signatures are used for detecting unwanted activity. The signature patterns help in effectively and efficiently detecting known attacks due to the predefined knowledge of attack patterns. The drawback of misuse-based IDS is that it cannot be used for detecting unknown attacks, i.e., the unwanted activities that do not attack signature patterns stored in the database.

Behaviour-Based IDS: The behaviour-based IDS is also known as anomaly IDS, where the normal behaviour of network activity, the software running information, operating system and kernel information are stored and compared with the incoming traffic. If any node does not exhibit usual behaviour, the node is said to be malicious. The behaviour-based IDS is advantageous as it detects the unknown attacks compared to signature-based IDS, but the false alarm rate is high in this IDS. Due to malicious activity and delay, the legitimate node is wrongly detected as malicious by behaviour-based IDS.

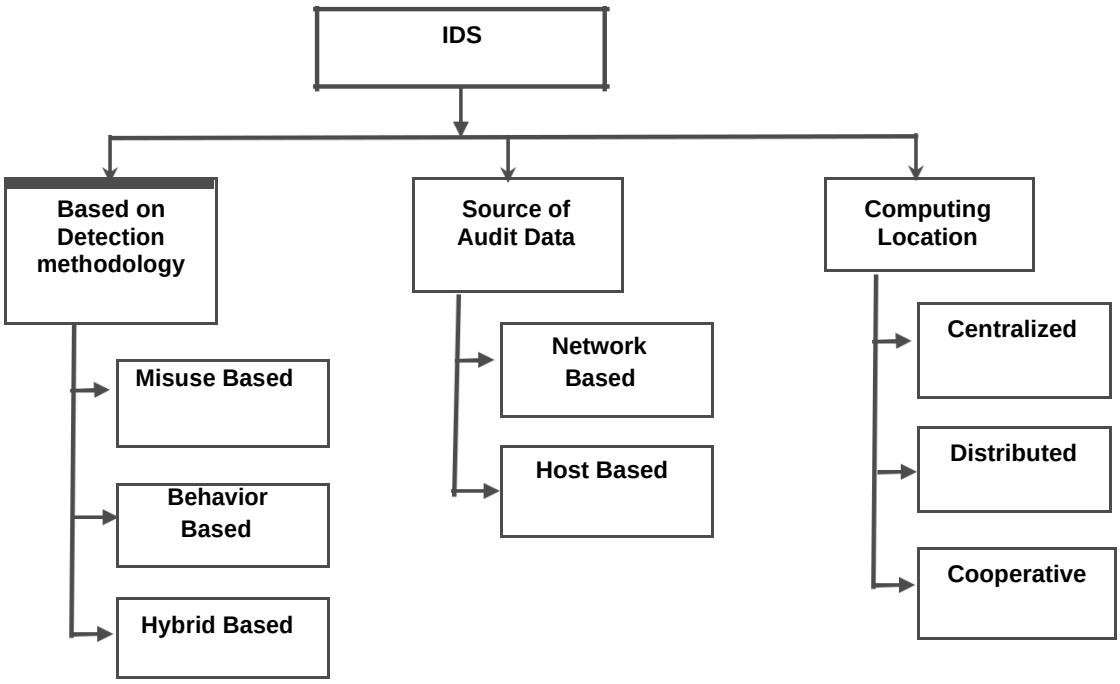

Figure 1. 15: Types of Intrusion Detection System in WSN
Adapted from (Soliman et al., 2012) (Butun et al., 2014)

Hybrid Based IDS: The hybrid-based IDS makes use of the advantage of both signature-based IDS and behaviour based IDS. The hybrid-based IDS is also known as specification-based IDS as manually included specifications are used for detecting unwanted activities in the network. The hybrid-based IDS does not give false alarm rate by avoiding unusual, but legitimate nodes. (Uppuluri, and Sekar, 2001; Balepin et al., 2003). In the specification-based IDS updating changes made in the systems is

necessary to detect unknown attacks. The main advantage of hybrid-based IDS is that the false positive rate is less compared to anomaly detection.

Source of Audit Data: The IDS is classified into two types based on the source of audit data, and they are network-based IDS and host-based IDS.

Network-Based IDS: In network-based IDS, the network traffic is monitored, and attack patterns such as a continuous group of similar packets can be a pattern of DoS attack are detected. The network-based IDS captures and analyses data to detect known attacks by comparing with the patterns and signatures stored in the database and unwanted activities in the network traffic, and they act as packet sniffers. The network-based IDS has scalability problem as the network grows the detection of malicious activities becomes difficult.

Host Based IDS: The host-based IDS is used for monitoring activities in the host systems and analysis events in the system and their network traffic. If any malicious activities are detected in the system, it sends an alert to the administrator for taking action against these attacks. The host-based IDS does system monitoring, log analysis connection analysis and kernel-based intrusion detection. The host-based IDS is suitable for a distributed network, and it can monitor the host's activity, thereby detecting attacks that are not possible by network-based IDS. The main drawback of host-based IDS is that accurate detection is not possible due to lack of content knowledge. The host-based IDS consumes more energy, which in turn affects the host efficiency and delay in an alert generation is also makes it disadvantageous.

Computing Location: The IDS are classified into three types based on location in which computation occurs, and they are centralized IDS, distributed IDS and cooperative IDS (Vasilomanolakis et al., 2015).

Centralized IDS: In centralized IDS, the monitoring, detection, and reporting of malicious activities are controlled from a central location. The centralized IDS monitors the behaviour of respective hosts and their network traffic, which are then shared with the centralized analysis unit. This type of IDS is not suitable for the large-scale network as it leads to larger energy consumption and misleads detection. The inefficiency in network performance and single point of failure occurs due to the use of a centralized analysis unit for controlling malicious activity.

Distributed IDS: The distributed IDS consists of several IDS distributed in the network that communicate with each other and with the centralized server for achieving advanced network monitoring. The distributed IDS uses a peer to peer architecture in data are analysed in the form of distributed manner which shares the tasks on the centralized server with other agents distributed over the network. The advantage of distributed IDS is the ability to detect the attack patterns all over the network and the early detection of

planned and coordinated attacks (Abraham & Thomas, 2006). It also helps in detecting backdoor attackers and unauthorized users before inducing attacks in the network.

Cooperative IDS: In cooperative IDS, fastest threat detection and accurate response are provided based on the collaboration of agents in a distributed manner. The accurate response is achieved by updating threat databases and system event logs from multiple locations. The cooperative IDS analysis the misbehaving metrics and shares the results among the neighbouring nodes to find the source of the attack. The advantage of cooperative IDS is that the false positive rate and false negative rate are drastically reduced.

1.17 Types of cryptographic techniques in WSN

The cryptographic schemes are one of the common security mechanisms, which is used to maintain confidentiality, authenticity, and integrity of the system. There are mainly two main classifications of cryptographic techniques, and they are Symmetric key cryptography and asymmetric Key cryptography, which is shown in figure 1.16.

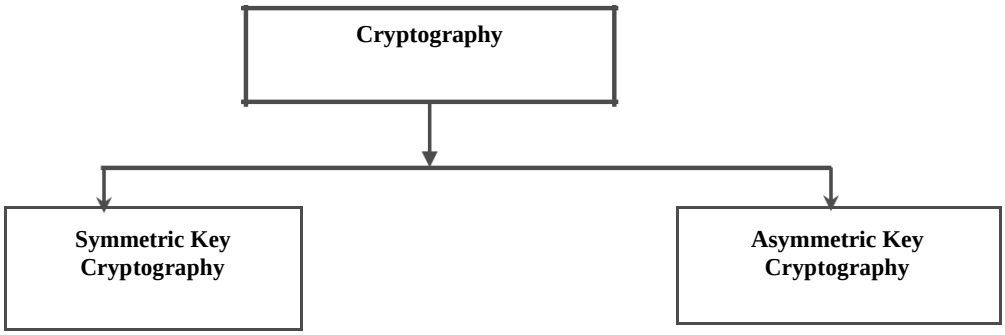

Figure 1. 16: Types of Cryptographic Techniques in WSN

Adapted from (Dogra & Kohli, 2016)

Symmetric Key Cryptography: The symmetric key cryptography is also known as secret key cryptography that uses a single key for encryption and decryption process. There are two forms of symmetric keys such as block ciphers and stream ciphers. The major difference between these two ciphers is the size of the encryption operands. The stream ciphers operate on one bit of plaintext data to produce one cipher bit while the block ciphers operate on a block of plaintext data at a time to produce a block of ciphertext. The advantage of stream ciphers is that it can operate on variable length when the large sequence of plain-text data needs to be encrypted (Zhang et al., 2010). The advantage of secret key cryptography is that the maintenance cost is reduced due to the use of single key and the symmetric keys are computationally intensive. The major problem of symmetric key cryptography is that the leakage of the key from a single node can affect the data secrecy of other nodes, which in turn affect the overall network

performance. Since adversaries target the secret key, they had to be transferred in a secured channel and changed periodically.

Asymmetric Key Cryptography: The asymmetric key cryptography also known as public key cryptography uses public key and private key for encryption and decryption process. The key that is shared by all the nodes in the network is called the public key, and the key that is used secretively is called the private key. In public key cryptography, it is not necessary for the sender to know the secret key and can communicate using the public key. The public key cryptography allows flexible key management and authentication but requires complex computations (Wander et al., 2005). Public key cryptography is advantageous regarding memory usage and security, resilience compared to symmetric key cryptography (Wang et al., 2008). The asymmetric key is slower compared to symmetric key cryptography due to the longer key length and complex computations.

SUMMARY

Explains the background of the thesis. A general discussion about security in WSN is highlighted, and the goals of the security mechanism are explained. The applications with high-security requirements are explained, and the design challenges of WSN are presented. The different security attacks are discussed to understand and analyze how intruders affect the efficiency of the network. The different security attacks are discussed to understand and analyze how intruders affect the efficiency of the network. The different types of secure routing protocols based on path establishment, network structure, and protocol operation are presented. The different trust-based schemes based on infrastructure and self-organization are discussed. The types of IDS based on the detection methodology, the source of audit data, and computing location are explained. The two main types of cryptographic techniques are presented.

CHAPTER TWO

LITERATURE REVIEW

Chapter Two deals with the literature review. This chapter presents the survey of energy efficient routing protocols and in-network aggregation. The review of various threats and their countermeasures are explained in detail. This chapter discusses the different encryption mechanisms and trust-based schemes in WSN. The trust establishment using multidimensional metrics is described. The IDS schemes are explained, and also explains about the signature-based IDS, anomaly-based IDS, and specification-based IDs schemes. This chapter also explains the secure clustering algorithm schemes

2.1 Survey of Energy Efficient Routing Protocols and In-Network Aggregation

The energy efficient routing protocols are surveyed mainly using three categories such as data-centric routing, hierarchical routing, and location-based routing. The Location-based Energy Aware Reliable routing protocol (LEAR) proposed by (Alasem et al., 2011:180-185) is a type of location-based routing protocol, which follows the clustering algorithm. LEAR aims to reduce energy consumption by adopting geographical positioning and clustering technique. In LEAR, the routing table of each node is constructed using a distance of the neighbours which is in turn calculated using location information collected by Global Positioning Systems (GPS). When a node needs to send data, it refers to its routing table and thereby forwarding the data to a neighbouring node, which has the shortest distance. The Enhanced Greedy Forwarding (EGF) is used to select the nearest node based on range. The advantage of LEAR is the reduction in energy utilization by decreasing the number of hops that is required to reach the base station, which also, in turn, improves the communication efficiency and lifetime of the network. The main drawbacks of LEAR are that the use of a GPS device increases the cost of the overall system. In (Yu et al., 2001), the authors proposed the Geographic and Energy Aware Routing protocol (GEAR) which deals with the use of geographic information, while disseminating queries to required locations. The main idea of GEAR is to restrict the number of interests by sending interests to specific regions rather than the whole network. Each node in GEAR keeps an estimated cost and learning cost for reaching the destination through neighbouring nodes. The estimated cost is the combination of residual energy and distance to destination, and the leaning cost is the refinement of estimated cost that includes the routing around holes in the network. When the region of the data source is known, the energy consumption is reduced by minimizing flooding to the geographic area. But this scheme cannot be applied to networks where the destination location is not known in advance.

In (Kulik et al., 2002:9-18), the authors proposed the family of Sensor Protocols for Information Via Negotiation scheme (SPIN), which is a type of data-centric routing

protocol, which uses metadata negotiations to eliminate transmission of redundant data throughout the network. SPIN is well suited for mobile sensor environment as the data forwarding is based on the local neighbourhood information. The advantage of SPIN is that it is enough to update the changes in topology locally at each node only requires the knowledge of the single hop neighbour. The main disadvantage of SPIN is its inability to ensure efficient data delivery, and it has a scalability problem. The Active Query forwarding in sensor networks (ACQUIRE) proposed by (Sadagopan et al., 2003:149-155) is a mechanism for efficient querying in sensor networks. Similar to another data-centric protocol COUGAR (Yao & Gehrke, 2002), the ACQUIRE mechanism considers the network as another distributed database, where complex queries divide into sub-queries. Each node and protocol forward the data-query sent by the base station provides efficient querying by changing the look ahead some hops parameter d. The advantages of ACQUIRE mechanism is that they support low traffic conditions, the query is comprehensive, and it provides superior query optimization. The limitation of the scheme is that it does not support scalability and behaves as flooding when the network size is equal to the node size.

The hierarchical routing protocols are the most energy efficient routing protocols due to the high energy conservation, and many schemes are developed to achieve high efficiency (Dener, 2018:269-286) (Chen et al., 2018:7298-7303) (Khan et al., 2018). The authors in (Razaque et.al, 2016:1-5) discusses the PEGASIS-LEACH (P-LEACH) protocol that combines the properties of both Low Energy Adaptive Clustering Hierarchy (LEACH) (Heinzelman et.al, 2000:10) and the Power-Efficient Gathering in Sensor Information Systems (PEGASIS) (Lindsey & Raghavendra, 2002:3-3) for providing an efficient routing protocol. In P-LEACH, the cluster formation of LEACH has been used in chain-based architecture of PEGASIS. P-LEACH scheme introduces a new dynamic data transfer protocol to transfer data between nodes. The P-LEACH scheme improves network lifetime and energy consumption compared to PEGASIS and LEACH protocol, but lack in efficient cluster head selection.

Table 2. 1: Survey of Energy Efficient Routing Protocols and In-Network Aggregation

Routing Schemes	Type of Routing	Description	Advantages	Limitations
LEAR	Location-aided Routing	LEAR is a location aided routing protocol that takes advantage of clustering topology and information derived from the GPS devices are used for minimizing energy consumption in the network.	Minimized number of hops to reach the base station Communication Efficiency An alternative selection of nodes for transporting packets increases the throughput and efficient load balancing Improves network lifetime	The overall cost of the LEAR scheme is high due to the use of a GPS device.
GEAR		GEAR uses a energy aware and geographically informed neighbour selection heuristics to forward the packet to the destination node.	Overall energy consumption is reduced by limiting the number of interests to certain region.	Delay in the network during data forwarding through alternate path. GEAR is not supported to networks, where the location of destination is not known. Prone to sybil attacks and selective forwarding attacks.
SPIN	Data-Centric Routing	SPIN uses data negotiation and resource adaptive algorithm to disseminate all the information at each and every node assuming all the nodes are potential base stations.	It reduces flooding data cost and avoids collision in the network SPIN is suitable for mobile sensors environment as the topology changes are localized	SPIN does not guarantee efficient data delivery It has limited stability .
ACQUIRE	Data-centric routing	ACQUIRE deals with complex queries for data, where sensor nodes could respond. It integrates query dissemination and response generation	The query is comprehensive It is suitable for low traffic conditions It offers superior query optimization responding to complex and one-shot queries.	If the network size is same as the node size, it behaves as flooding. It does not support scalability
P-LEACH	Hierarchical Routing	P-LEACH is a cluster-based chain protocol that uses an energy efficient routing	It has improved network lifetime, count of dead nodes	It lacks in providing efficient cluster head

		algorithm to transfer data in the network	and energy efficiency compared to PEGASIS and LEACH.	selection.
HEED		HEED is a distributed clustering algorithm that selects cluster head periodically	The cluster head is uniform. HEED increases the network lifetime by distributing energy. It supports long-range communication . HEED works precisely even in the absence of synchronization .	In the scheme, large communicatio n overhead occurs due to the random selection of cluster head. Inappropriate energy consumption for rebuilding clusters in periodic cluster head rotation

Adapted from (Alasem et.al, 2011:180-185) (Yu et.al, 2001) (Kulik et.al, 2002:9-18) (Sadagopan et al., 2003:149-155) (Zaque et.al, 2016:1-5) (Younis & Fahmy, 2004:366-379)

The Hybrid Energy-Efficient Distributed Clustering (HEED) proposed by (Younis & Fahmy, 2004:366-379) is hierarchical clustering-based protocol, which periodically selects cluster heads according to the node's residual energy and inter-cluster communication. HEED protocol extends LEACH by including communication range limits and inter-cluster communication cost information. The advantages of HEED are the distribution of energy increases network lifetime, localized knowledge requirement of the nodes for cluster formation and precise operation even in the absence of synchronization. The limitations of HEED protocol are that higher communication overhead due to a random selection of cluster head and requirement of extra energy for rebuilding clusters during periodic cluster selection.

2.2 Review of Threats and Countermeasures in WSN Routing and Data Aggregation

Several attacks have been imposed in routing and data aggregation methods with the aim of disrupting efficiency and network performance in the system.

In (Newsome et al., 2004:259-268), a systematic analysis of the threat posed by the sybil attack in WSN is presented. The sybil attack is defined as the malicious node legitimately taking on multiple identities of a node in the network. These attacks can affect the redundancy mechanism of the distributed data storage systems in peer to peer network. The authors highlight that the sybil attack is a threat to essential functions such as routing, resource allocation, and misbehaviour detection that can cause severe aftereffects. The taxonomy of sybil attacks is presented to understand and analyse the threat and its countermeasures in the network. The authors also discuss the different

defence mechanisms against sybil suited for WSN. The two methods presented are direct validation and indirect validation. The direct validation is done by radio resource test, where the sensor nodes are assigned to a different communication channel to communicate. Then, the node is said to be legitimate by confirming that there is a data transmission through the communication channel and node is said to a physical identity if there is no transmission through the channel.

In (Wood& Stankovic, 2002: 54-62), the DoS attack is defined as any event that diminishes or eliminates network capacity to perform its expected function. The different DoS attacks are jamming, collision attacks, unfairness attacks, black hole attacks, neglect and greed attack, homing attack, and misdirection attacks. The countermeasures for the jamming attack are by using spread spectrum, priority messages, and lower duty cycle. The countermeasures for misdirection attack is egress filtering and authorization. In (Yu & Xiao, 2006: 8), the authors have discussed the countermeasures taken against selective forwarding attacks. The analysis highlights that the security and on time transmission of packets is the basic need for sensor network and the selective forwarding attacks targets these requirements. The authors also propose a lightweight security scheme for detecting selective forwarding attack. The scheme adopts multi-hop acknowledgment technique which the intermediate nodes send alarm information to the base station and sensor nodes in case of malicious attacks. The authors in (Hu et al., 2006:370-380) proposed a simple method for preventing a wormhole attack where the location information of both the source and destination nodes with loosely synchronized clocks are considered. The authors use either of the two methods such as geographical leashes and temporal leashes to restrict the maximum distance of the packet. The geographic leashes are inefficient compared to temporal leashes, due to the use of broadcast authentication.

Table 2. 2: Threats and Countermeasures in WSN Routing and Data Aggregation

Threat Model	Description	Countermeasures Implemented
The Sybil Attacks in Sensor Networks: Analysis & Defences	In the sybil attack, the malicious attacker poses as multiple identities of a node in the network	Direct validation such as radio resource testing Indirect validation such as approval by a trusted third party Keyspace verification Central node registration
Denial of service in sensor networks.	DoS attack is a type of malicious attack target to affect the network functionality either by flooding the network with unwanted data packets or denying certain service to be executed on the network.	Error correcting codes for a collision attack Rate limitation for exhaustion attacks Redundancy and probing to deal with neglect and greed attack Encryption mechanisms for homing attacks Client puzzles for flooding attacks.
Detecting Selective Forwarding Attacks in Wireless Sensor	Selective forwarding is a type of attack that drops certain packets	Multi-hop acknowledgment

Network	with the aim of disturbing the desired output.	technique such as upstream detection process and downstream detection process Jamming detection technique
Wormhole attacks in wireless networks	In wormhole attack, a pair of colliding attackers record packet overhead at one location and replay them to another location using the private high-speed network	Geographical leashes ensure that receiver must be at the precise distance from the receiver Temporal leashes ensure timestamp is given to each packet.

Adapted from (Newsome et.al, 2004:259-268) (Wood& Stankovic, 2002: 54-62) (Yu & Xiao, 2006: 8) (Hu et.al, 2006:370-380)

2.3 Survey of encryption mechanism in WSN

The encryption schemes in WSN are categorized mainly into two types and they are symmetric key encryption schemes (Perrig et.al, 2002:521-534) (Lai et.al, 2002:7) (Gawdan et.al, 2011:312-316) (Khan et.al, 2017:809-815), and asymmetric key encryption scheme (Chang et.al, 2012:13) (Watro et.al, 2004:59-64).

The authors in (Perrig et al., 2002) introduced two building block security protocols such as SNEP (Secure Network Encryption Protocol) and Timed Efficient Streaming Loss-Tolerant Authentication (µ-TESLA). The SNEP protocol ensures data confidentiality, two-party authentication, and evidence of data freshness. The µ-TESLA protocol is used to ensure authenticated broadcast for the resource constraint sensor network. In SPINS, each node shares a secret key with the base station. During data communication, the two nodes consider an intermediate node such as a base station for setting a new key between them. The advantages of SPINS are resilient to node capture attack, where any node does not leak any information about other sensor nodes, and it is easy to revoke key pairs in case of attacks. The disadvantage of SPINS protocol is that the use of the TESLA protocol leads to storage problems, DoS attacks, and message delay. And lack of end-to-end delay due to in-network processing.

In (Lai et al., 2002:7), the authors have introduced a new protocol called BROadcast Session Key negotiation protocol (BROSK), which uses a symmetric key encryption scheme. In BROSK, the master key is shared by all the nodes in the network. A negotiation message is sent by the source node to establish a session key and thereby the BROSK protocol establish a pairwise session key between every two neighbouring nodes. The advantage of the BROSK protocol is that they require minimal storage overhead due to the commonly shared master key. The limitation of BROSK protocol is that the re-silence is low in the network as the addition and removal of nodes requires a change in keys in the whole network. In (Gawdan et al., 2011:312-316), the Novel Secure Key Management module (NSKM) is based on hierarchical clustering architecture. NSKM provides an efficient key establishment mechanism with acceptable security features.

The seniority in cluster heads is selected based on the location and distance from the base station. There are three keys involved in NSKM scheme, and they are pre-deployed keys, network generated keys, and base station broadcast keys. The advantages of NSKM is that the energy efficient, scalable and does not allow compromise of the entire network in case of active attacks by providing a secure channel for communication between the cluster head and the base station. The main limitations of NSKM are that the scheme is easily affected by active attacks such as hello flood, selective forwarding attack, node capture attack, and sybil attacks. The NSKM scheme is also not suitable for the dynamic clustering environment.

The authors in (Chang et al., 2012:13) have proposed a broadcast authentication scheme based on Rivest, Shamir, and Adleman (RSA) algorithm-based cryptography which adopts multi-modulus RSA for enhancing performance. The rekeying mechanisms are used to overcome the limitation in short module and the use of multi-modulus RSA generation algorithm that assures the authenticity and integrity of broadcast messages. The authentic broadcast scheme consists of three phases such as setup phase, broadcast phase, and update phase. In the setup phase, the necessary public parameters for each sensor is generated by the base station. In the broadcast phase, after deployment, the nodes are updated with on-demand tasks through broadcast messages and an update phase, the base station renews the modulus via the broadcast channel. The Tiny Public Key (PK) proposed by (Watro et al., 2004:59-64) is designed for allowing authentication and key agreement between resource constrained sensor nodes. It uses the RSA certificates for authentication between external parties in the network. TinyPK uses Diffie-Hellman algorithm to be establishing shared keys between external parties and sensor nodes in the network, and it requires two exponential operations. The advantage of TinyPK is that it ensures confidentiality and authentication in WSN thereby providing end to end security. The disadvantage of TinyPK is that the use of the Diffi-Hellman algorithm is sensitive to man middle attack and during the establishment of session key more bandwidth utilization occurs.

Table 2. 3: Survey of different encryption mechanism in WSN

Symmetric Scheme	Description	Advantages	Limitations
SPINS	SPINS is a security protocol, which is made of two building protocols such as SNEP and µ-TESLA, where each node shares a secret key with the base station and base station to act as an intermediate node for communication.	Good re-silent to node capture It is easy to revoke key pairs	The intermediate nodes require direct access to the network It is not scalable The base station is the target of attacks.
BROSK	In BROSK, the master key is shared by all the nodes in the network. BROSK protocol establishes a pairwise session key between every two neighboring nodes by sending negotiation messages.	The requirement of minimal storage space Less computation The absence of key discovery and key exchange phase	Resilience is very low Single node compromises the entire network, by leakage of single master key.
NSKM	NSKM uses symmetric key cryptography for providing an efficient, lightweight, and scalable key establishment mechanism and uses three keys such as pre-deployed key, network generated key and base station broadcast key.	Energy efficient Avoids the compromise of the entire network by providing secure routing between cluster head and base station	The scheme is prone to active attacks such as selective forwarding attack, sybil attack, and node capture attack It's not suitable for the dynamic clustering environment.
Practical RSA signature scheme based on periodical rekeying for wireless sensor networks	It is an authentic broadcast scheme, which is based on RSA signature and it uses multi-modulus and rekeying mechanism to enhance performance	Ensures integrity and authenticity of broadcast messages Key verification is fast Authentic broadcast scheme reduces energy consumption. The rekeying overhead is insignificant.	The scheme is prone to impersonation attack Key generation is slow
TinyPK	TinyPK uses RSA based certificates to authenticate external parties before allowing them to access the network and it is implemented in Mica2 motes in a tiny Operating System (OS) environment	End to end security mechanism achieves energy efficiency Ensures confidentiality and authentication in the network	Prone to attacks such as man-in-middle attack due to the use of the Diffi-Hellman algorithm. More utilization of network bandwidth for setting the session key.

Adapted from (Perrig et.al, 2002:521-534) (Lai et.al, 2002:7) (Gawdan et.al, 2011:312-316) (Chang et.al, 2012:13) (Watro et.al, 2004:59-64)

2.4 Survey of Trust Management in WSN

Several trust-based schemes have been introduced to improve trustworthiness in the network and to achieve efficient routing and improved network performance.

In (Zahariadis et al., 2010:52-68), the author proposed the Ambient Trust Sensor Routing (ATSR) protocol, which uses a trust management system for providing secure routing of data packets in the network. Each node in the network sends the periodic broadcast messages with node Identity (ID) and energy availability. A multicast message such as reputation request message is sent periodically to the neighbouring nodes for obtaining the indirect trust information, and the reply is gathered in from of unicast messages. The trust metrics used by nodes to evaluate the adjacent nodes are forwarding data rate, residual energy, and distance. The advantage of the ASTR scheme is that the data packets are forwarded based on the energy metric of the next hop node thereby achieving energy conservation. The authors in (Liu et al., 2009:291-294) presented a Distributed Event-triggered Trust Model (DETM) in which trust-related information about neighbour nodes is resolved and stored in the form of a set of modules by each node in the network. The sensor nodes store a set of information metrics such as a public key that is shared among neighbouring nodes, reputation, residual energy, and network path. The main advantage of DETM scheme is that the event triggered repute update process reduces the energy utilization of the nodes in the network. The disadvantage of the DETM scheme is that the use of public key cryptography can increase the computational complexity in the network thereby decreasing the throughput.

Collaborative Reputed mechanism (CORE) presented by (Michiard & Molva, 2002:107-121) is a distributed trust model in which reputation is calculated using direct and indirect trust metrics. In CORE, each node in the network maintains a trust table, which consists of positive and negative reputation of other nodes. The route discovery in the network initialization phase is made using a dynamic source routing, and the nodes are assigned to a neutral trust value. Every node monitors its neighbouring nodes concerning trust metrics such as packet forwarding rate, and route discovery, and if the neighbouring node reputation falls below the threshold, the services for the particular node are suspended. The advantage of CORE mechanism is that the use of both first-hand information and second-hand information prevents bad- mouth attacks. The limitation of the scheme is that the CORE mechanism does not take account of the network utilization, where blocking of misbehaving nodes diverts the traffic on the route with legitimate nodes that causes overloading in the particular path. In (Chen, 2009:21-26), the authors proposed the Task-based Trust for Sensor Networks (TTSN), where each node maintains a task-based trust value of neighbouring nodes. Each node supports the reputation based on packet forwarding, sensing, cluster management, time synchronization, and localization. TTSN uses the aging factor γ, to weight each task

reputation score. The TTSN mechanism is prone to packet forwarding, time synchronization, and data manipulation attacks.

Table 2. 4: Survey of Trust Management in WSN

Schemes	Description	Advantages	Limitations
ASTR	ASTR framework uses a trust management system for providing secure routing of data packets in the network.	The packet drop rate due to malicious attacks is reduced Overall throughput is increased.	High utilization of network traffic due to a periodic request for first-hand information and second-hand information
DETM	In DETM, trust-related information about neighbor nodes is resolved and stored in the form of a set of modules by each node in the network	The energy efficiency is achieved in the scheme through the event-triggered repute update.	Use of public key cryptography can increase the computational complexity in the network
CORE	CORE is a distributed trust model where the reputation is calculated using a first hand (direct trust) and second-hand information (indirect).	The network has more defense against such as false praise attacks and bad-mouth attacks.	The system requires frequent contribution by nodes in network traffic.
TTSN	It is a task-based trust management framework in which nodes maintain the reputation of other nodes containing different tasks values for evaluating trustworthiness.	The scheme provides more precision and ambiguity in the network by blocking only the misbehavior of the particular task rather than preventing all communication within the node	The nodes with link problem are also assumed as malicious TTSN is prone to packet forwarding, time synchronization, and data manipulation attacks.

Adapted from ((Zahariadis et.al, 2010:52-68) (Liu et.al, 2009:291-294) (Michiard & Molva, 2002:107-121) (Chen, 2009:21-26)

2.4.1 Trust based Schemes Using Multidimensional factors

Different approaches have been proposed to enhance trustworthiness in WSN and for improving the accuracy of the trust value, multidimensional factors are considered for trust establishment and evaluation (Zhang et al.,2017:12088-12102) (Bao et al., 2012:169-183) (Dhakne & Chatur, 2015:96-101) (Han et al., 2015:2447-2459) (Li et al., 2013:924-932) (Ye et al., 2017).

The authors in (Bao et al., 2012:169-183) proposed a hierarchical trust management scheme in WSN for detecting malicious nodes in the routing process, where the multidimensional metrics are considered. The trust value is calculated by considering social trust and QoS trust, while the validation of the scheme is done using subjective trust and objective trust. The advantage of the scheme is that the false positive rate and false negative rate of the scheme is low, and it achieves a high detection rate compared to traditional anomaly detection schemes. In (Dhakne & Chatur, 2015:96-101), the

authors proposed the Distributed Trust Based Intrusion Detection (DTBID) scheme which considers multidimensional trust factors based on energy, data, and communications, evaluating direct trust, recommendation trust, and detection of malicious nodes based on the deviation of subjective trust and objective trust are used for establishing trust in sensor nodes. The advantages of DTBID is that the use of multidimensional factors provides a high detection rate against attacks such as DoS attacks, selective forwarding attacks, energy exhaustion attacks, tampering attacks. The disadvantage of the scheme is that the data trust is based on one-dimensional data which reduces the detection of attacks based on observation data and the threshold difference between subjective trust and objective trust is not self-adaptive. The authors in (Li et al., 2013:924-932) proposed the Lightweight and Dependable Trust System (LDTS) which uses a clustering algorithm for detecting and preventing malicious and selfish cluster heads. The LDTS adopts self-adaptive weighting mechanism for trust calculation of cluster heads, which is superior to the traditional subjective weight method. It uses direct trust and indirect trust to improve decision making and collaborative processing for detecting malicious behaviour. The advantage of the LDTS scheme is the communication overhead between cluster members is decreased due to the trust calculation mechanism adapted and it is more suitable for large-scale clustered WSN. The limitation of LDTS is that it is necessary for each sensor node in a cluster to store information about the trust of other sensor nodes, which increases the storage overhead at the lower level of the cluster formation. In (Ye et al., 2017), the authors proposed the efficient Dynamic Trust Evaluation Model (DTEM), which combines the properties of direct trust, indirect trust and update mechanism parameters for providing efficient and accurate trust evaluation model. Direct trust is calculated using multidimensional factors such as communication, observing data, and energy with punishment factor and regulatory function. The indirect trust is obtained from the trusted recommendation from the third parties, and the integrated trust is measured by as combining the weighing mechanism for direct trust and indirect trust. The advantages of DTEM are of DTEM is that the computation is less complicated and communication overhead is more. The storage overhead is more for individual nodes, as each node has to store information of another node. The disadvantage is that it has a high detection rate of routing attacks, on-off attack, and black-hole attack. The trust evaluation of DTEM is dynamically adjusted to the requirement of the network.

Table 2. 5: Survey of Trust Management in WSN

Schemes	Description	Advantages	Limitations
Hierarchical trust management for wireless sensor networks	It is a highly scalable cluster-based hierarchical trust management scheme where the trust calculation is done through social, and QoS trust and validation is done using subjective trust and objective trust.	The scheme maintains a sufficiently low positive rate, and it also provides a high detection rate.	Cluster size and trust update interval affect the network performance and network lifetime.
DTBID	It uses multidimensional factors for establishing trust in sensor nodes and addresses the issues of trust detection of malicious behaviour based on the trustworthiness of one node with others.	High detection rate against the DoS attacks, selective forwarding attacks, tampering attacks, and energy exhaustion attacks because of considering a multidimensional trust.	It is not fully resistant against attacks as it considers only 1-dimensional Data for data trust observation. The threshold difference between subjective trust and objective trust is not self-adaptive
LDTS	It is a lightweight and dependable trust scheme based on a clustering algorithm, which aims at reducing the resource consumption and enhancing the reliability of cluster head trust evaluation.	It greatly improves system efficiency The trust mechanism adopted in LDTS reduces communication overhead It is suitable for large-scale clustered WSN	The storage overhead of individual nodes, especially at the lower level is high as each sensor node has to store the trust information of other nodes in the cluster.
DTEM	DTEM implements an efficient dynamic trust evaluation model which dynamically adjusts the weight of direct trust, indirect trust, and parameters for update mechanism.	It effectively defends against routing attacks, information attacks, and trust model attacks. The trust evaluation of DTEM scheme is dynamically adjusted based on the requirement of the network	Since DTEM aims at achieving accuracy by dynamically adapting to the environment, communication overhead is more It requires more storage overhead and energy consumption as each node stores the trust information of another node. There is no central repository for storing information of all the nodes.

Adapted from (Bao et.al, 2012:169-183) (Dhakne & Chatur, 2015:96-101) (Li et.al,2013:924-932) (Ye et.al, 2017)

2.5 Review of IDS Schemes in WSN

Several IDS mechanisms-based schemes have been introduced based on the types of attacks and application requirements to provide efficient detection of attacks before causing severe damage to the systems. (Mitchell et.al, 2017:1-23) (Hindy et al., 2018) (Rassam et.al, 2012:1636) (Can & Sahingoz, 2015:1-6) (Farooq & Khan, 2009:234-241) (Zhang et al., 2017)

In (Mitchell et al., 2017:1-23), the authors presented an IDS survey based on the target WSN, detection technique, collection process, trust model, and analysis technique. The survey concludes that the because of the limited storage, the WSN faces a huge challenge on traffic-based approaches and the dynamic populations makes it difficult to form a trust relationship mainly for multi-trust-based approaches. In (Hindy et al., 2018), the survey deals with the taxonomy of IDS design technique, evaluation metrics, and a survey of IDS implementation. The taxonomy of the threat model, which includes threat sources, active and passive modes, and recent attacks is also discussed in this survey. The authors in (Rassam et al., 2012:1636) introduced the survey based on IDS in WSN, which describes the different types of attacks in WSN and also explains about the requirement of IDS in WSN. The survey also focuses on highlighting the challenges for developing an ideal IDS and state of the art of IDS schemes are presented by categorizing it into four types such as rule-based, data mining, computational intelligence based, game theoretical based and statistical based schemes. The features of each category are presented through the analysis.

In (Can & Sahingoz, 2015:1-6), the authors presented the survey of IDS in WSN and different cyber-attacks in the network is explained. Depending on the different features of WSN, IDS needs different approaches for wired networks and resource constrained WSN, and they are explained in detail. The IDS types such as anomaly based, misuse based and hybrid-based IDS are described, and the necessity of using a key management scheme with IDS scheme is also presented in the survey. In (Farooq & Khan, 2009:234-241), the authors proposed a survey on IDS schemes in WSN, where they have classified the IDS scheme mainly into three categories such as purely distributed, purely centralized, and distributed centralized. The survey concludes that the energy efficient intrusion detection schemes are more suitable for WSN. It describes purely centralized IDS scheme as the most powerful IDS approaches, where the base station takes part in the detection process. It also states the complexity and requirement of specialized routing protocol for gathering data from sensor nodes to the base station. The purely distributed IDS is not suitable for WSN due to their energy efficiency, and the distributed centralized scheme is ideal for WSN because of the energy efficiency and less complexity.

2.5.1 Signature Based IDS and Anomaly Based IDS Schemes

There are different detection schemes proposed in WSN based on signature-based IDS and anomaly detection scheme with each scheme has its features, which is shown in table 3.6.

The authors in (Ioannis et al., 2007:1-10) proposed an IDS based scheme to detect black hole attacks and selective forwarding attack by defining appropriate rules that

characterize malicious behaviour. In this scheme, the nodes monitor their neighbourhood and collaborate sharing valuable information for detecting the attacks. The part of the nodes are activated for monitoring purposes, and decision making is done collaboratively. The advantage of the scheme is that it is energy efficient and requires small communication overhead. However, the scheme is not suitable for applications, where high detection rate and low alarm rate is necessary. In (Roman et al., 2006), the authors presented the general guidelines for applying IDS in a static network. They proposed a novel intrusion detection scheme based on spontaneous watchdogs, where each node elects independently whether they need to monitor the communication of their neighbour. Each node is loaded with an IDS agent which promiscuously monitor the traffic. There are mainly two agents involved in the process, and they are a local agent and global agent. The local agents are active in each node, and it is used for monitoring and analysis local information. The global agents are active only in the subset of the nodes, and they are responsible for analysing packets flowing in their immediate neighbourhood. In this scheme, both the local and global agents reside the same node and observations are stored in the single alert database. Therefore, a collaboration of local and global agents takes place in the same node.

The Sensor based intrusion detection for intradomain distance vector routing proposed by (Mittal& Vigna, 2002) is a signature-based intrusion detection scheme, which is used for detecting routing attacks in the network. In this scheme, the routing information protocol, the network topology, and the position of intrusion detection sensors are used for determining the signature configuration of the sensors and messages that need to exchange for detecting the attacks. The drawback of the scheme is that they lack in identifying the random dropping and modification attacks and the scheme also exhibit high false positive rate due to threshold values and timers. In (Qu et al., 2018), the authors proposed the Lightweight Intrusion Detection technique based on the Fuzzy Clustering Means algorithm (LIDFCM), where the base station senses the abnormal changes in the system. In LIDFCM, the network status is directly mapped into the sensor monitoring data received by the base station that can reduce the energy consumption in the network. The source of the abnormal data is identified using the combination of Fuzzy Clustering-Mean (FCM) algorithm, sliding window procedure, and one class Support Vector Machine (SVM). In this scheme, FCM algorithm is used to cluster the data generated in the initialization stage, and the one-class SVM performs statistical modeling of mapping, normal data in high dimensional space and then establishes a hyperplane that differentiates the standard data from abnormal ones. The sliding window procedure in the scheme uses the temporal correlation between monitoring data to clarify suspicious samples. The advantage of the scheme is that the overall energy consumption is reduced by using the FCM algorithm. The network efficiency and network battery life are

improved, as the IDS is deployed in the base station of the network. The drawback of the scheme apart from the communication attacks, it cannot detect other attacks.

In (Onat & Miri, 2005:253-259), the authors have proposed the novel anomaly-based detection scheme for WSN. Each sensor node in the network builds a statistical model of their neighbour's behaviour which is used for detecting attacks based on impersonation and resource depletion changes. The parameters through which anomalies are detected are averages of receiving power and the packet arrival rate. The drawbacks of the scheme are that the confidentiality of data is not protected as the nodes share the observation with their neighbour nodes and the scheme cannot detect wormhole attack and selective forwarding attacks.

Table 2. 6: Survey of Signature-Based IDS and Anomaly Based IDS in WSN

Schemes	Description	Advantages	Limitations
(Ioannis et.al, 2007:1-10)	Signature-based intrusion detection	The IDS based scheme is used to detect black-hole attacks and selective forwarding attack by defining rules that characterize malicious behaviour	It is energy efficient It requires minimum communication overhead. The IDS based scheme is unsuitable for applications where high detection accuracy and low alarm rate is necessary.
(roman et.al, 2006)		It is a novel based technique for optimal monitoring of neighbours, where the idea of a watchdog mechanism is adapted to monitor the data packets passing through the routing path.	It is considered the selection of global agents This approach does not deal with the collision of packets in highly dense WSN It used for locating and identifying packet droppers and modifiers.
(Mittal& Vigna, 2002)		It is a novel based detection technique that detects attacks against routing infrastructure, which uses the information about network topology and the positioning of sensor nodes to determine the malicious activities in the WSN.	Selective forwarding attacks and modification attacks cannot be determined The path overhead is significantly high The scheme has a high probability of false positive and false negative rates.
(Qu et al., 2018)	Anomaly-based intrusion detection	It is a lightweight intrusion detection mechanism where the source of the abnormal data is identified using the combination of the FCM algorithm, sliding window procedure, and one class SVM.	It has reduced energy consumption. The deployment of IDS in base station improves efficiency and prolong the battery life of sensor nodes.
(Onat & Miri, 2005:253-259)		The scheme is based on sliding window statics, which exploits the stability of neighbour nodes to detect changes.	The scheme requires sharing the observation with neighbour nodes, i.e., Confidentiality is affected

			The scheme cannot detect wormhole and selective forwarding attack.

Adapted from (Alrajeh et al., 2013:167575)

2.5.2 Specification Based IDS Schemes

In (Silva, 2005:16-23), the authors proposed the decentralized IDS model, which depends on the interference of network behaviour monitored by the sensor nodes. It is a specification-based IDS where seven types of rules are considered for auditing data, such as interval, retransmission, integrity, delay repetition, radio transmission range, and jamming. The advantage of the scheme is that energy consumption is minimized in the network. The main drawback is that the scheme exhibits a low detection rate and a high false positive rate. In (Stetsko et al., 2010:420-425), the authors proposed an intrusion detection scheme based on collaboration between neighbours. The scheme implements collaborative tree protocol in a tiny OS environment for detecting mainly three types of attacks such as hello flood attack, selective forwarding attack, and anti-jamming attack. The parameters used to detect these attacks are received signal strength, packet dropping rate, packet sending rate, and packet delivery ratio. The drawback of the scheme is that the communication overhead involved during the collaboration of neighbour nodes in detecting attacks.

In (Mamun et al., 2012), the authors proposed a hybrid detection scheme, where the sensor nodes are divided into hexagonal regions similar to cellular networks. In this scheme, each node is monitored by a cluster node, and regional nodes monitor the cluster nodes. The base station monitors the regional nodes, and the entire model is based on the hierarchical tree-like structure. The base station stores the attack signatures, which are propagated towards the leaf node for attack detection. The scheme also includes predefined specifications of normal and abnormal behaviours, where the anomaly detection technique is adopted by detecting a malicious node that deviates from the specification. The drawback of the scheme is that the exact output of the detection rate and false alarm rate is not determined.

2.6 Survey of Secure Clustering Algorithm in WSN

The most significant routing protocols adopt clustering algorithm to minimize the energy consumption, and also for restricting data transmission through all the nodes for protecting the confidentiality of data and several clustering algorithms in WSN are explained in table 3.7.

In (Loscri et al., 2005:1809-1813), the authors proposed a Two-Level Low Energy Adaptive Clustering Hierarchy (TL-LEACH), which is an extension of LEACH algorithm that includes two levels of cluster heads. In TL-LEACH, the cluster heads collect the data

from member nodes similar to LEACH algorithm, but instead of forwarding to the base station directly, TL-LEACH forwards the data packets to another part of cluster head which acts as a relay station between the cluster head and base station. TL-LEACH adopts two techniques such as self-configuring cluster formation and localized control of data transfer for achieving latency and energy efficiency. The algorithm consists of four phases such as advertisement phase, cluster setup phase, schedule creation, and data transmission. In the first phase, the nodes are classified into primary cluster head, secondary cluster head, and member nodes. The elected primary cluster head nodes advertise other nodes and the mechanism used in this phase is called Carrier Sense Multiple Access (CSMA). The secondary cluster head sends the advertisements to the ordinary nodes. In the cluster setup phase, each secondary cluster head selects which primary cluster head it belongs and informs the same through reply messages. In schedule creation phase, the primary cluster head chooses a Time Division Multiplexing Access (TDMA) for slotting time to each node. In the last step, the formation of cluster occurs, and data transmission occurs using a TDMA schedule allocated to each node. The advantage of the TL-LEACH is that the two levels of hierarchy improve the load distribution in the network and the overall energy consumption is reduced. The disadvantage of TL-LEACH is that the scheme does not support long-range networks and does not ensure load balancing in case of nodes with unequal energy consumption.

In (Soro & Heinzelman, 2005:8), the authors proposed the Unequal Clustering Size (UCS) model for network organization which provides more uniform energy dissipation across cluster head nodes and thereby improving network lifetime. In UCS scheme, the cluster heads are arranged symmetrically in concentric circles around the base station. The base station is present at the centre of the network, and thereby it can easily control the actual sizes of different clusters. It is assumed that the cluster in the same layer has the same size and shape while the size and shape of the clusters in different layer are not identical. The advantages of UCS are that the equal energy consumption is achieved by changing the number nodes in the cluster according to the expected communication overhead. The two-layered network and two hop inter-cluster communication method result in shorter transmission distance. The disadvantage of UCS is that the even though the average transmission distance is less, the necessity of two-hop communication between cluster head and base station increases the energy consumption when the transmission range is increased. The Energy Efficient Clustering Scheme (EECS) proposed by (Ye et al., 2005:535-540) is a clustering algorithm which is advantageous for data gathering applications. In EECS, the network is partitioned into several clusters, and single hop communication takes place between the cluster head and the base station. The nodes first broadcast their residual energy to neighbouring nodes, and the node with more residual energy is elected as a cluster head. In this scheme, the node chooses the

cluster head saving both the energy as well as balancing the workload of cluster heads. The advantages of EECS are that the balancing point is achieved between inter-cluster communication and intra-cluster communication based on distance and energy consumption. The main disadvantage of EECS scheme is that it is not suitable for large-scale networks due to the single hop communication between cluster head and base stations require more energy consumption.

In (Yu et al., 2012:54-61), the authors proposed the Energy Aware Distributed Clustering (EADC) scheme which involves non-uniform deployment of sensor nodes to balance the load across the network. EADC constructs unequal clusters which solve the issues such as energy holes in the network. The cluster head is selected based on the comparison of residual energy of neighbouring nodes and energy of the node itself. In (Ding et al., 2005: 322-339), the authors have proposed the Distributed Weight-based Energy-efficient Hierarchical Clustering protocol (DWEHC), which is a distributed clustering algorithm similar to HEED algorithm. In DWEHC, the balancing of cluster size and optimization of intra-cluster topology using location awareness of nodes. It adopts a multi-level cluster communication and limits the number of children of parent nodes. The main advantage of DWEHC is that cluster head election in the fully distributed clustering method is based on residual energy and the proximity of neighbour nodes, which results in balanced cluster head distribution and lower energy consumption in both intra-cluster and inter-cluster communication. The disadvantage of DWEHC is that it is not suitable for large-scale network due to the single-hop communication between cluster head and base station results in high energy consumption when the transmission distance is increased.

Table 2. 7: Survey of Secure Clustering Algorithm in WSN

Schemes	Description	Advantages	Limitations
TL LEACH	It is an extension of the LEACH algorithm that adopts two levels of cluster heads for efficient data transmission.	The use of primary and secondary cluster heads provides better energy load distribution across the network. Localized coordination in TL-LEACH supports scalability and robustness in the network The total energy consumption is reduced.	The two hop-inter cluster routing of TL-LEACH is not applicable for long range networks Cluster head without energy considerations does not ensure load balancing in case of nodes with different initial energies.
UCS	It is the first unequal clustering model for WSN which adopts multi-layer network to balance energy consumption of cluster heads.	Uniform energy consumption among cluster heads. UCS technique can prolong the network lifetime due to equal energy dissipation in the overall network.	It is not applicable to long-range networks as the use of two hops for communication between source and base station consumes more energy. The UCS scheme

		The average transmission of UCS is minimized.	lacks universality As the location of the cluster head must be at the center, the residual energy is not considered
EECS	It is similar to LEACH scheme, where the network is partitioned into several clusters, and single hop communication between the cluster head and the base station is performed.	Based on energy and distance, the inter-cluster communication and intra-cluster communication is balanced. Low message overheads and uniform energy distribution.	It is not suitable for large-scale networks EECS require global knowledge, i.e., transmission distance between the cluster head and the base station Large control overheard during cluster head selection.
EADC	EADC is an energy-aware clustering algorithm which involves load balancing on cluster heads. The scheme uses a competitive range of efficient cluster head election and routing in sparse-dense regions.	Load balancing is achieved The cluster heads are elected based on residual energy which balances the energy consumption in the network The energy is conserved by switching off redundant nodes based on the schedule.	The network lifetime is not stable due to uneven clustering strategy.
DWEHC	The scheme aims to improve the HEED algorithm by balancing the cluster sizes and optimizing the intra-cluster topology using location awareness of nodes.	Cluster head selection is based on residual energy and proximity to neighbours. Lower energy consumption in both intra-cluster and inter-cluster communication. The clustering process in the scheme does not depend on the network topology or size.	The single hop communication between cluster head and base station results in high energy consumption in large scale network. In the scheme control message, overhead is more due to the iterative nature of DWEHC scheme.

Adapted from (Jan et.al, 2017) (Liu, X., 2012:11113-11153)

SUMMARY

Chapter two deals with the literature review. The several energy efficient routing protocols and in-network aggregation-based schemes are explained along with its advantage and disadvantage. The various types of threat and their countermeasures in WSN are discussed for understanding and analysing the necessity of robust security mechanism in WSN. Various encryption-based schemes are discussed to analysis the advantage and disadvantage of different cryptographic devices. The different trust mechanisms adopted for improving trustworthiness among sensor nodes in WSN is presented. The trust-based schemes based on multidimensional metrics to improve the accuracy of the detection are explained in detail. The survey of intrusion detection schemes is discussed, and the different types of IDS such as signature-based IDS, anomaly-based IDS, and specification-based IDS schemes are explained. The survey of secure clustering algorithm schemes to improve the network performance is also discussed.

CHAPTER THREE

Research methodology for ATTACK RESILIENT TRUST AND SIGNATURE-BASED IDS

Chapter three explains the proposed IDSHT scheme. The overview of the hierarchical clustering-based IDS model is explained, and the cluster head selection in the proposed scheme is presented. This chapter describes the hierarchical trust mechanism in the scheme, and trust evaluation at the sensor node level and the cluster head level are explained in detail. The chapter discusses the signature based IDSHT scheme. The signature generation and verification using the RSA algorithm are presented.

3.1 Overview of IDS Based Hierarchical Cluster-Based Model

The proposed IDS based Hierarchical Trust (IDSHT) model adopts a cluster-based network based on the two-tier hierarchical trust mechanism. Clustering aims to reduce the energy consumption to the nodes in the system. The nodes in the cluster-based network structure are formed to find their nodes neighbour by exchange identity to values higher, lower energy network. Nodes are classified into Cluster Head (CH), Sensor Nodes (SN), and Base Station (BS) in each cluster. The CH is selected based on the Most sensor systems are conveyed at unfriendly conditions to detect and assemble explicit data as sensor hubs have battery limitations. This way, the energy-efficient remote sensor systems (WSNs) It has the properties of extending the life of the system. We propose an energy-efficient multi-level and distance-aware grouping (EEMDC) instrument for WSNs. In this instrument, the region of the system is separated into three consistent layers, which relies on the hop-count-based good ways from the base station. The results show that EEMDC is more vitality productive than other existing customary methodologies. And it forwards the data packets from the member nodes to the level of trust requirements of the nodes must depend on the role it performs in the network. The task of cluster head is to carry all the essential information collected from the members to the base station, and hence the next-hop nodes of cluster head through which it transmits the data to the destination must be more. The cluster-based approach is in the form of a hierarchical, in which the nodes are arranged in the form of clusters (Fasolo et al.., 2007) (Siddiqui et al., 2015). Each group of nodes has a special node called a cluster head, and the data aggregation is done by the cluster head. The member nodes forward the data to the respective cluster heads, which then transfers the aggregated data to the base station. This helps in maintaining load balancing and reducing data transmission overhead. The cluster-based approach is suitable for large-scale networks, where energy efficiency is a needed requirement. The cluster-based approach does not require the knowledge of the entire network, and it is sufficient enough for respective cluster heads know the location of

member nodes. The main advantage of the cluster-based approach is that the collision is avoided by the network, the aggregation efficiency mainly depends on the measured data and the control overhead of individual nodes is reduced. It is necessary to protect the cluster head from malicious attacks using cryptographic keys as they play the aggregator role and have direct contact with the base station. Nodes communicate with their respective CH and the data aggregation is done in the form of an aggregation tree consisting of a root node and leaves (Fasolo et al., 2007) (Siddiqui et al., 2015). The tree structure follows a minimum spanning tree, and it is constructed at the base station. The base station acts as the root node, while the sensor nodes act as the leaves. The constructed aggregation tree is suited in tree-based approach as there is only one root node, i.e., base station and also the tree structure can reduce the communication overhead of the entire network. The in-network aggregation is done a level by level starting from the leaves until it reaches the root node. The tree-based approach has mainly two phases such as distribution phase and a collection phase. CH aggregates the data sent by the sensor nodes before sending it to the BS. The CH transmits the aggregated data to the base station directly. In a node replication attack, the adversary makes the compromised node pose in multiple locations with the same identity to steal the information that is transferred in the network. It is different from the Sybil attack, where a single malicious node acts with multiple identities. The node replication attack can be easily be detected by intrusion detection systems compared to Sybil attacks due to their misbehaviour patterns. These attacks can be prevented by authenticating the nodes by a trusted third party. Belong to a single cluster. The cluster head stores the data in the form of queues that are collected from the SN before forwarding it to the BS.

The following points are the features of the proposed network model are

- The WSN is a cluster-based network, and SN communicates with CH directly, and the respective CHs aggregate the data from SN.
- The CH forwards the aggregated data directly to the BS.
- The data transmission through a wireless medium, the deployed environment, and the limited sensor node resources has caused several types of security attackers to exploit these parameters for stealing valuable information from highly sensitive applications (Elqusy et al.., 2017). The security mechanisms are also being improvised to meet the challenging security threats. The need for trusted nodes and a secure channel is one of the major concerns while developing security mechanisms the combination of both proactive and reactive security mechanisms are needed to strengthen the chance of reducing any form of security attack in the network. The trust measurement must be appropriately managed to achieve accurate attack detection.
- The hybrid model of data transmission uses a storage and forwarding mechanism.
- The observing data are delivered to BS periodically, and the transmission breaks the cycle when an event occurs, or it initiates the query
- The SNs is deployed densely and redundantly for reliability.

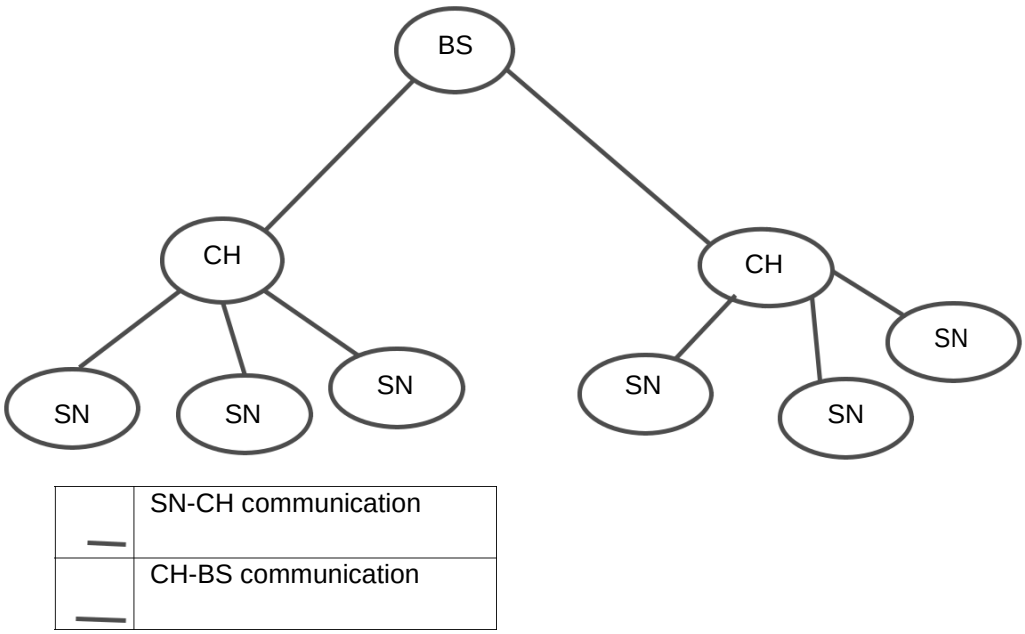

Figure 3. 1: Hierarchical Cluster-Based Topology of Proposed IDSHT Scheme

3.1.1 Cluster Head Selection in the IDSHT Scheme

In the proposed IDSHT model, each node in the network broadcast the control information by attaching its ID and residual energy for identifying their neighbours. In the hello message adversary causes a disturbance in the network by broadcasting hello packets with strong signal strength. Due to this, the legitimate nodes assume that these adversaries are their neighbouring nodes and use these malicious nodes to transfer data packets to the base station. The malicious nodes are present in a longer transmission range that leads to large energy consumption when the legitimate nodes forward the data to the assumed neighbouring nodes. The concept of two-way authentication can detect and prevent these malicious nodes from participating in the routing process. The neighbour nodes take the particular node as a neighbour and update the same in the adjacent table. The nodes are distributed without any particular structure, i.e., irregular arrangement of nodes, and all nodes are equally assigned to roles (Bazzi et al., 2015). The flat routing protocol forwards the data packets in the targeted location by collaborating with the neighbour nodes. As a flat routing structure involves a large number of sensor nodes, it is difficult to assign priorities to the nodes and Equal responsibility of nodes often creates confusion in the network, which in turn affects the integrity of data. After cluster formation, the CH selection is made. In the CH selection, the residual energy and the distance of the node are considered in selecting the unique CH in each cluster. If the residual energy and neighbour. The negotiation directed diffusion energy-aware routing, rumour routing, and active query forwarding in sensor networks Generally, data-centric routing protocols imply the

establishment of two-way communications between neighbouring nodes by sending requests and responds to ensure only the data are sent to the nodes which require it. This method may overcome duplication in data transmission thus conserve overall network energy.

the below equation computes the link cost between two neighbouring nodes **i and j**

$$C_{ij}(k) = \frac{2 * E_{elec} + K + \in_{amp} * K * d_{ij}^2}{e_i} \qquad \text{Equation 3. 1}$$

: Where E_{elec} the Value is 50 nJ/bit

$\in_{amp}$ the Value is 10 pJ/bit/m^2 .

K is the data size

d_{ij}^2 is the distance between node **i** and node **j**.

The node becomes a candidate for the cluster head selection process. The threshold value can be defined as the minimum energy required for receiving data from all nodes, aggregating them, and sending it to the BS. Each node compares the residual energy of their node with the received information of the neighbour nodes, and if the residual energy of their node is higher than that of their neighbour nodes, it announces itself as the CH. Each node receives a CH advertisement from multiple neighbours, and it elects the CH by considering the node which has the highest trust value. After choosing the CH, the other nodes will join the corresponding cluster. Through this method, multiple distributed, one-hop clusters are formed. The CH is elected in multiple rounds to improve energy efficiency and security.

3.2 Hierarchical Trust Mechanism in IDSHT Scheme

One of the major concerns of security mechanisms in WSN is to provide secure transmission of data from the sender to receiver end without much utilization of the sensor node resources. The security in traditional routing protocols placed in a dynamic environment is complicated, and communication is not adequately secured (Flinn et al., 2016). that are used for detecting attacks in the network have used only single metrics for evaluating trust in WSN. The main issue faced during the trust evaluation is the lack of accuracy in detection, which caused malicious nodes being undetected when a strong attack is imposed. In the proposed IDSHT scheme, the two-tier hierarchical mechanisms are introduced, and the trust evaluation for routing behaviour and data aggregation is done using multidimensional metrics such as Interactive Trust (IT), Content Trust (CT), and Honesty Trust (HT). In two tier hierarchical trust mechanism, two levels of trust evaluation are done such as SN trust evaluation and CH trust evaluation. The first level of trust evaluation is simple, as the SN evaluation is done through direct communication between CH and SN in a cluster. The second level consists of the trust evaluation at the cluster head level is explained along with its multidimensional factor evaluation. The

signature generation and verification in the proposed scheme. The two-tier trust evaluation consists of multidimensional trust which includes network related trust and observing data related trust. The IT and HT are the network related trust, while the CT is the data-centric trust. The IT is calculated by the number of interactions of nodes in the network. The interaction of the SN means the number of times the particular SN is involved during data transmission for forwarding and receiving data packets with other SNs. The sensor nodes with the highest number of communications are considered as the trustworthy node.

In IT, the malicious node is identified using the threshold value. When the node exceeds the threshold value considering the number of interactions, then the node is said to be malicious. The HT is calculated depending on the number of successful and unsuccessful interactions in the network. The interaction is meant to be successful when the SN or CH sends data packets to the CH or BS successfully without dropping. The interaction is supposed to be unsuccessful when the data packets are dropped during the communication between the SN-CH or CH-BS. The HT is calculated by considering the ratio of the number of successful interactions by the number of total interactions of the node in the network. The greater the number of successful interactions, the higher the trust degree of the node. The CT is calculated based on the capacity of each node. It is evaluated using the deviation between the observing data and an effective average of the observing data. The trust degree of the CT value of the node is more when the proximity data is high.

3.2.1 Trust Evaluation at Sensor Node Level

The first level of trust is the SN trust evaluation, which is done by CH in a particular cluster using multidimensional metrics such as IT, CT, and HT.

Interactive Trust Evaluation of SNs: The IT is calculated using the number of interactions of the SN in the network. The interactions of the SN include the sending and receiving data packets between the nodes and request sent or forwarded from other nodes. In the SN level trust evaluation, the number of interactions between SN and CH is used for calculating the IT. According to the interaction of members in the networks, the greater the number of interactions, higher the trust value of the node. But, if the number of interactions exceeds the threshold, the node is considered malicious. The attacks imposed by the malicious nodes increase the number of interactions by sending many unwanted data packets in the network. In the proposed IDSHT scheme, unlike trust evaluation in social networks, the IT evaluation method in WSN is inspired by a normal distribution in statistics, and the probability density function is normalized to [0, 1] for calculating the IT when the number of interactions exceeds IT is determined by the number of interactions between nodes in the network. The HT is determined based on the number of successful and unsuccessful interactions in the network while the CT is

determined based on the capacity such as energy and the amount of data transferred by the node in the network. When the maximum data packets exceed the arrived data packet, then the IT is taken as 1, while the maximum data packet is lesser than the arrived data packet, then the value of maximum data packet by the arrived data packet is taken. The IT calculation is given by the equation 4.1.

$$(IT_{SN}) = \begin{bmatrix} 1; \text{ Arrived Data Packet} < \textit{Maximum Data Packet} \\ \text{Otherwise} \\ 1 \Big/ \left(\text{Arrived Data Packet} \Big/ \text{Maximum Data Packet}\right); \end{bmatrix}$$

Equation 3. 2

Interactive Trust of Sensor Node (IT_{SN})

Content Trust Evaluation of SNs: The CT is based on the trust evaluation of the observing data, and it is the data-centric trust evaluation calculated using a CH. The primary purpose of SNs is to sense the different parameters such as temperature, humidity, air pressure, and light intensity and transmit the observing data to the respective CHs. Thus, the deviation between the observing data and the effective average observing data are used for obtaining the CT value. The use of CT is an essential requirement during the trust evaluation as the WSN is a data-centric network and observing data is an important parameter in real-time applications such as environmental monitoring. The tampering attacks in these applications are easily identified using the CT. The CT in SN is calculated using equation 4.2.

$$(CT_{SN}) = 1 - (\text{Deviation}/\text{Average of Sensing Data})$$

Equation 3. 3

Content Trust of the sensor node (CT_{SN})

* Deviation = Sensed Data - Aggregated Data
* Aggregated Data = Average Sensed Data

Honesty Trust evaluation of SNs: The HT is calculated using the number of successful and unsuccessful interactions between the CH and SN in the network. In HT, the CH overhears the SN when the interaction is unsuccessful. The interaction is said to be unsuccessful when the data packets are not forwarded for a particular time interval, forwarded to another node which is not present in the routing table, and if the data packet does not reach the CH. For instance, due to the attacks such as black hole attacks or selective forwarding attacks, all the packets or some of the data packet do not reach the CH and using the HT, these attacks can be detected. The higher the ratio of some successful interactions to the number of total interactions, the higher the trust value. The HT is evaluated using equation 3.5.

$$(HT_{SN}) = \text{Forwarded Data packets to CH/Received Data packets from SN}$$ **Equation 3. 4**

Honesty Trust of Sensor Node (HT_{SN})

Overall Trust Evaluation of SNs: The overall trust value is evaluated by the CH and is calculated by aggregating IT, CT, and honest trust. If the selfish attack is launched by the node, it will announce a fake energy value in the control information to avoid from selected as CH or router to preserve its energy, and thus It reduces the IT value of the SN. If the dropping attack is launched by the node, it will drop the data without forwarding it to the CH, and thus it reduces HT value. If the false data injection attack is launched, it injects the false data value that is deviated from actual value that in turn reduces the CT value. If the overall trust value of SN is less than the threshold, then malicious SN is detected which can be either a data dropping attack or false data injection attack. If the dropping attack is detected, then a different SN is selected as a router. If the false data injection attack is detected, then the data of the specific sensor is filtered from aggregation. If the overall trust value of the SN is less than the threshold, then it is an attacker node. Otherwise, it is not an attacker node. The overall trust evaluation of SN is given in equation 3.6.

$$(OTSN) = \left((W1 \times IT_{SN}) + (W2 \times HT_{SN}) + (W3 \times CT_{SN})\right)$$ **Equation 3. 5**

Overall Trust of Sensor Node (OTSN)

Where w1= 0.2, w2 =0.4 and w3 =0.4 represent the weighting factors

w1 the CT is determined based on the capacity such as energy and the amount of data transferred by the node in the network. Another major problem is providing privacy during data transmission as leakage of data causes severe after-effects.

3.2.2 Trust Evaluation at Cluster Head Level

In the proposed IDSHT, the trust evaluation at the CH level considers only the direct trust calculation using BS-CH evaluation. The trust evaluation in CH is similar to the SN level trust evaluation, and it includes multidimensional factors such as IT, CT, and HT. The IT, the CT, and HT are calculated using the BS-CH evaluation while the CT includes the proximity of aggregated data and effective average observing data.

Interactive Trust Evaluation of CH: The IT at CH level is calculated using some interactions between CH and BS. Interaction refers to all communication behaviour, including sending and receiving of request and data packets. According to the interaction of members in social networks, if the number of interactions between the nodes is high, then the trust value of the CH is also high. The IT evaluation is done by comparing the number of interactions with a threshold value, unlike trust evaluation in social networks. If

the number of interactions in the sensor node exceeds the threshold value, the trust value decreases and then the particular node is considered as a malicious node. Inspired by Normal Distribution in Statistics, the probability density function is normalized to [0, 1] and the calculation of the IT evaluation at CH level is same as the IT calculation at the sensor node level and is shown in equation 3.6.

$$(IT_{CH}) = \begin{bmatrix} 1; & \text{Arrived Data Packet} < \text{Maximum Data Packet} \\ & \text{Otherwise} \\ 1 \Big/ \left(\text{Arrived Data Packet} \Big/ \text{Maximum Data Packet}\right); & \end{bmatrix} \quad \textbf{Equation 3. 6}$$

Interactive Trust of Cluster Head (IT_{CH})

Honesty Trust Evaluation of CH: The HT value is calculated using the number of successful and unsuccessful interactions between the CH and BS. The trust value of the CH is more when the number of successful interactions is more than the number of failed interactions. The interaction is said to be unsuccessful when the CH does not transfer the packet to the BS at a specific time interval, or the data packet is dropped before reaching BS. For example, attacks such as black-hole attack and selective forwarding attack restrict the all or partial data packets from reaching BS. HT is calculated using the ratio of the forwarded data packet to BS by the received data packet of the sensor and is shown in equation 3.6.

$$(HT_{CH}) = \text{Forwarded Data packets to BS/Received Data packets from CH} \quad \textbf{Equation 3. 7}$$

Honesty Trust of Cluster Head (HT_{CH})

Content Trust Evaluation of CH: The CT is defined as the trust value obtained by the deviation between sensing data and an effective average of observed data. The CT of CH is calculated by BS according to the proximity of fusion data and effective average observing data of SN in the cluster. The higher the proximity of data, the higher is the CT of the CH. Since the CHs transmit multidimensional aggregated data to BS, the content trust can detect the variation in observed data.

$$(CT_{CH}) = 1 - (\text{Deviation}/\text{Average of Sensing Data}) \quad \textbf{Equation 3. 8}$$

* Deviation = Reported Data by data - Actual Aggregated Data

* Aggregated Data = Average Sensed Data

Content Trust of Cluster Head (CT_{CH})

Overall Trust Evaluation of CH: The overall trust of CH is calculated using BS by the aggregating the multidimensional factors such as CTCH, HTCH, and ITCH evaluated for

CH and is shown in the equation 4.8. If the node launches the selfish attack, it will forward a false energy value in the control information to avoid from selected as CH to preserve its energy. It reduces the ITCH value of the node. If the node launches the dropping attack, it will drop the data without forwarding it and in turn reduces HTCH value. If the false data injection attack is launched, it injects the false data value which is deviated from actual value and that in turn reduces CTCH value. If the OT of CH is minimized, then presence of data dropping attack or false data injection attack during aggregation is detected. In both cases, the CH re-election is conducted to select alternate CH.

$$(\mathrm{OT_{CH}}) = \left((\mathrm{W1} \times \mathrm{IT_{CH}}) + (\mathrm{W2} \times \mathrm{HT_{CH}}) + (\mathrm{W3} \times \mathrm{CT_{CH}})\right) \quad \textbf{Equation 3. 9}$$

Overall trust of Cluster Head ($\mathrm{OT_{CH}}$)

Where w1=0.2, w2 =0.4 and w3 =0.4 represent the weighting factors.

3.3 Signature Based IDSHT Scheme

The main issue faced in IDS schemes is that even after removing the malicious nodes, further attacks such as impersonation attacks are induced in the network. The impersonation attacks are one of the serious attacks, where the adversary successfully uses one of the identities of legitimate nodes, and it uses these fake identities to provide a gateway for other types of attacks. The main aim of the impersonation attacks is to obtain the confidential information that should be kept secret during the entire data transmission. The impersonation attacks reduce the throughput of the overall network and also the packet delivery ratio is also drastically decreased. These issues in WSN during intrusion detection can be mitigated by attaching a signature to each node in the network. Every node in the network encrypts its data and abstracts the information, which includes the data sending time, node ID and ID of the data. After attaching the signature, data is forwarded to CH, and the CH aggregates the data along with the signature. The aggregated data is then sent to the BS. Through this method, the aggregated data can be verified by BS and confirm that every data forwarded to it is valid. The hierarchical model reduces the energy consumption and the attacks such as impersonation attacks are mitigated. In the proposed scheme, the signature generation and verification are done by the RSA algorithm as one of the popular public-key cryptographic systems used for securing data during communication in the network. The RSA, the public key is used for encryption and the private key is used for the decryption process. It is based on the fact that finding the factors of large composite numbers is difficult, where malicious intruders cannot easily solve the data encrypted. The public key of the RSA algorithm is obtained by multiplying two large prime numbers together and the private key is generated through a different process involving these two prime numbers. The RSA algorithm is a

deterministic encryption algorithm that can be used for both public-key encryption and digital signatures.

3.3.1 Signature Generation and Verification Using RSA Algorithm

The security of the Proposed IDSHT scheme can be improved by using signature generation, and verification mechanism and it is termed as S-IDSHT. In S-IDSHT, each SN generates the public key and private key using the RSA algorithm. The WSN is mainly used for monitoring sensitive information in the deployed environment and transferring them to the target destination through a wireless channel. The role of cryptographic techniques is to prevent any leakage or modification of confidential data (Uluagac et al., 2008). The leakage of data is prevented by encrypting the data using keys and sending the encrypted data to the destination. As most of the encryption and key management schemes require complex computation and increased costs, the need for designing lightweight cryptographic schemes and achieving a trade-off between providing security and limited utilization of resources has become a necessity (Tawalbeh et al., 2017). The two types of cryptographic keys used for authentication and encryption are a public key and private key. The public key is known by designated nodes, while private keys are kept secret by specific nodes. A digital signature is used for authentication and maintaining the message's integrity. The digital signature involves three algorithms such as key generation, signing, and signature verifying algorithm. The advantage of using a digital signature is that it is difficult to forge a user's signature without knowing the private key. Both IDS and trust-based schemes make sure that the attacks are not initiated in the network. The cryptographic schemes alone cannot provide an effective security mechanism, and it must be combined with other security mechanisms to achieve all the security requirements of WSN. The data aggregation during this process reduces the energy consumption of the overall network. The BS collects the data from all the CHs and decrypts the aggregated data using the unique private key and verifies that the received data signature is the same as the original data. If the signature of the original data is not the same as that of the received data, then the node is said to be an adversary, and it is an impersonation attacker. If the signature of the original data is the same as the signature of receiving data, the node is said to be legitimate. In the Proposed S-IDSHT, the data integrity and confidentiality of the data is secured, and efficient data transmission is achieved.

SUMMARY

In Chapter four, the proposed IDSHT scheme is explained in detail. The overview of the hierarchical clustering model adopted in the proposed IDSHT scheme is presented. The cluster head selection based on residual energy and transmission distance is discussed. The two-tier hierarchical trust mechanism is explained. The trust evaluation at sensor node level is presented, and the multidimensional factors such as interactive trust, content trust, and honesty trust are evaluated. The multidimensional factors of the sensor node are used for finding the overall trust of the sensor node. The trust evaluation at cluster head level is explained, and the multidimensional factors from the cluster head are evaluated along with the overall trust. The signature based IDSHT scheme is presented to prevent impersonation attacks. The signature generation and verification process are done using the RSA algorithm, and it is explained in detail.

CHAPTER FOUR

IMPLEMENTATION SCENARIO OF PROPOSED IDSHT-S SCHEME

Chapter Four deals with the implementation of the Proposed IDSHT-S scheme. The evaluation of the proposed IDSHT-S scheme in a WSN is explained. This chapter presents the simulation setup and parameters used for creating the simulation in the NS2 tool. The network scenario of the IDSHT-S scheme is explained. This chapter also presents a data dropping and impersonation attacker model with the detection of these attacks using the proposed scheme. The performance analysis of the proposed scheme by comparing with the existing IDSHT-S scheme is discussed. The simulation graph for performance metrics such as delay, network lifetime, overhead, and packet delivery ratio for both the IDSHT-S scheme and IDSHT scheme is presented.

4.1 Evaluation of Proposed IDSHT-S Scheme in WSN

The proposed IDSHT-S scheme adapts a hierarchical cluster-based structure to ensure secure and efficient data transmission during routing and data aggregation process. The trust evaluation in the proposed scheme is based on the two-tier hierarchical trust mechanism, and the two levels of trust evaluation include the SN level and CH level. The trust value is calculated using multidimensional factors such as IT, CT, and HT. These multidimensional factors are used for finding the overall trust for SN and CH. Thus, the overall trust obtained improves the accuracy of the detection, providing a reduced false alarm rate. The IDS is used for detecting the attacks, and the malicious nodes are revoked from the network. In spite of removing the malicious nodes, the attacks such as impersonation attacks can target the cluster-based network posing as a legitimate node. The issue is solved by introducing IDSHT-S scheme, where the data is verified using signatures. The signature generation and verification in the proposed IDSHT-S scheme are done using the RSA algorithm. SNs encrypt the data before transferring the data to the CH, which act as an intermediate node and aggregator. The CH decrypts the data, aggregates it, and encrypts it using its public key and forwards to BS, which verifies the data is genuine by comparing the signature of the received data with the signature of original data.

4.2 Simulation Setup and Parameters for Proposed IDSHT-S Scheme

The simulation scenario of the IDSHT-S scheme is constructed using the Network Simulator (NS2) tool. The proposed scheme is developed by modifying the Ad-hoc On-Demand Distance Vector (AODV) protocol files in NS2. In the experimental phase, the node formation is the first phase. The in-network aggregation is done a level by level starting from the leaves until it reaches the root node. The tree-based approach has

mainly two phases such as the distribution phase and a collection phase. In the distribution phase, the cooperative or aggregate queries are sent all over the network. In the collection phase, the flow of data aggregation occurs from the source node to the root node., the best path from the source to reach the destination is estimated by the AODV protocol. The AODV protocol is modified according to the application requirement. In the proposed scheme, the AODV routing protocol is modified based on IDSHT and IDSHT-S scheme objective. The number of nodes used is 100 nodes constructed in an 800m* 800m area. One node is set as a receiver, and all other nodes are set as a transmitter, which is competing for the channel. The transport agent used is User Datagram Protocol (UDP). The application agent used in the network scenario is Constant Bit Rate (CBR), and the network is loaded with (N-1) CBR flows, where N is defined as the number of nodes in the network. The C++ is used for detailed protocol implementation, and it defines the internal mechanism, i.e., the backend of the simulation objects. The Object-oriented Tool Command Language (OTCL) is used to set the simulation by assembling and configuring the objects. It is also used for configuring and scheduling discrete events, and it acts as the front-end mechanism for the simulation objects. The communication of the nodes is set at 100, and the initial energy of each node is taken as 10 joules. The overall simulation time is taken at 50 seconds.

Simulation Components for Network Scenario: The components used for constructing the proposed IDSHT- scheme network scenario is listed below

NS2 Tool: The NS2 is an open-source event-driven simulator tool that is used in studying the dynamic nature of communication networks. The NS2 simulation tool is used for performing simulation in both the wired and wireless sensor networks. The NS2 provides default implementations for network nodes, links between two nodes, routing algorithms, traffic generators, and transport level agents. The simulation can be modified by adding functionality to these implementations. The NS2 consist of two key languages C++ and OTCL programming languages.

C++: The C++ is a high-level programming language used for graphical applications, and it is used in the back - end mechanism in NS2 tool. Th C++ programming language is used for running the simulation, and all the C++ files are compiled and linked to create an executable file. C++ programming language is employed in NS2 tool for creation of object because of its efficiency. It also provides detailed and complete control over the packet process.

OTCL: The OTCL is a scripting language used for configuration and setup of the simulation in NS2 tool. In NS2, the C++ objects are made available to the OTCL interpreter and can be controlled by OTCL level. The event scheduler and the basic network component elements in the data path are written using the C++ files. The NS2 is considered as a TCL interpreter regarding user’s perspective which takes the OTCL

script as configuration object and C++ objects to simulate network component and produce a trace file.

NAM Output: The NAM stands for Network Animator and is used to represent the network and packet traces graphically. It supports topology layouts, packet level animation, and data inspection tools. It reads large animation data sets produced by NS and presented in the form of visualized data. Topological information such as node-link and packet traces presented in the form of trace file need to be generated to view the NAM output.

X-Graph: The X-graph program draws the graph on an X - display such that the data read from either data files or standard input if no files are displayed. The X-graph is used for plotting the network parameter characteristics such as a packet delivery ratio, delay, throughput, network lifetime, overhead, etc.

UDP: A UDP agent accepts data in variable size chunks from an application and does data segmentation when required. Unlike Transmission Control Protocol (TCP), the UDP is a connectionless protocol that allows applications to exchange datagram. It uses the port for differentiating the applications used in the network.

CBR: CBR is an application layer component that generates constant traffic during the simulation, i.e., the number of bits transmitted per second along the digital network is kept constant.

AODV Protocol: AODV protocol is the routing protocol designed for wired and wireless ad-hoc networks. It is used in path establishment between source and receiver and supports both multicast and unicast routing. It is also called as on-demand routing as the path establishment is done based on the request of the source. There are four messages used in the AODV protocol, which are modified based on application requirements.

Route Request Message: A route request message is a control packet broadcasted by the source node when there is no route entry to reach the destination node.

Route Reply Message: The broadcast message received by the nodes verifies their routing table and nodes with a valid route to destination sends a unicast route reply message to the target.

Route Error Message: All the nodes monitor the nearby routes. When a route is broken or invalid, a route error message is sent to the nodes that use it as the routing path.

HELLO Message: The HELLO messages are local broadcast messages which are used for identifying the neighbour nodes, and these messages are also used to confirm that the link is active.

Table 4. 1: The Simulation Parameters of the Proposed IDSHT-S Scheme

Parameter	Values
SIMULATOR	Network Simulator 2
NUMBER OF NODES	100
AREA	800m x 800m
COMMUNICATION RANGE	250m
INTERFACE TYPE	Phy/WirelessPhy
MAC TYPE TOOL TO ANALYZE THE EFFECTIVENESS OF THE PROPOSED ALGORITHM	IEEE 802.11
QUEUE TYPE	Droptail/Priority Queue
QUEUE LENGTH	50 Packets
ANTENNA TYPE	Omni Antenna
PROPAGATION TYPE	Two Ray Ground
ROUTING PROTOCOL	IDSHT, IDHST-S
TRANSPORT AGENT	UDP
APPLICATION AGENT	CBR
INITIAL ENERGY OF EACH NODE	10 Joules
THE OVERALL SIMULATION TIME	50seconds

4.2.1 Network Scenario of IDSHT-S Scheme

The network scenario in the proposed IDSHT-S scheme is built in a hierarchical structure, and the cluster-based routing is used to provide an efficient data transmission. Firstly, the cluster-based network structure is formed. The nodes find their neighbour by exchange identity and residual energy values and nodes with higher energy, and lower energy is given with specific roles. The nodes are divided into member nodes, CH and, BS. The CH acts as an intermediate node for forwarding data collected from the member's nodes. The CH aggregates the data packets by compressing the data and sending it in limited data packets. The original data can be retrieved from the base station. The use of CH also improves the security and energy consumption in the network. The sensor data gathered by CH are aggregated before forwarding it to the base station.

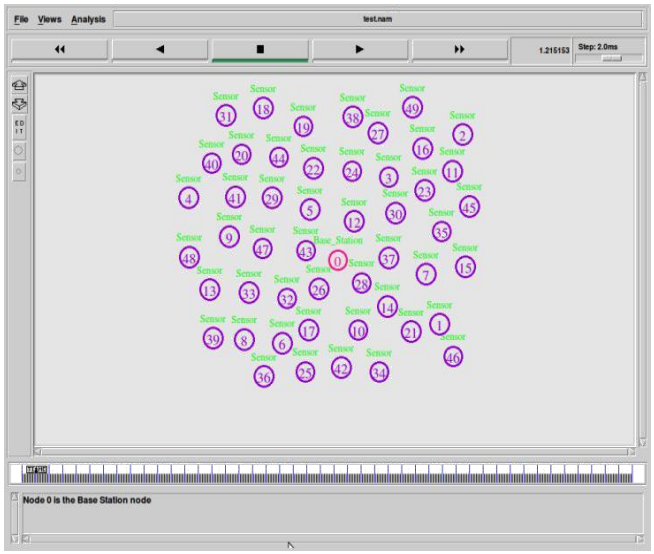

Figure 4. 1: The Network Scenario of the Proposed IDSHT-S Scheme

Neighbour Identification and CH Selection: The clusters are formed by initially identifying the neighbour nodes based on the residual energy and transmission distance between them. The nodes with higher residual energy are taken as a cluster head, and other nodes join the particular cluster. For example, node 6 lists its neighbour ID and its residual energy and compares its residual energy with the residual energy of neighbour nodes. Then, node 6 selects the high residual energy neighbour as its CH, where CH of node 6 is node 39. Similarly, every node selects its CH.

Attacker Model: Consider node 15 as an attacker node showing fake information with the residual energy value is displayed as 80 joules and neighbour count as 100. Let node 1 be the neighbour node. Node 1 lists its neighbour ID, and its residual energy and compares its residual energy with the neighbours. Then, node 1 selects the neighbour node with the highest residual energy as its CH, where CH of node 1 is node 15. Similarly, every node selects its CH through this method. Thus, the attacker node is selected as CH.

Detection of attacker During CH Selection: In the proposed IDSHT scheme, the highest weight attacker node is selected as CH. Hence, the attacker CH drops the packets, forwarding through it. The honesty trust used in trust evaluation is calculated by taking the ratio of received data to forwarding data. Thus, the honesty trust used in the proposed IDSHT-S scheme detects the attacker CH.

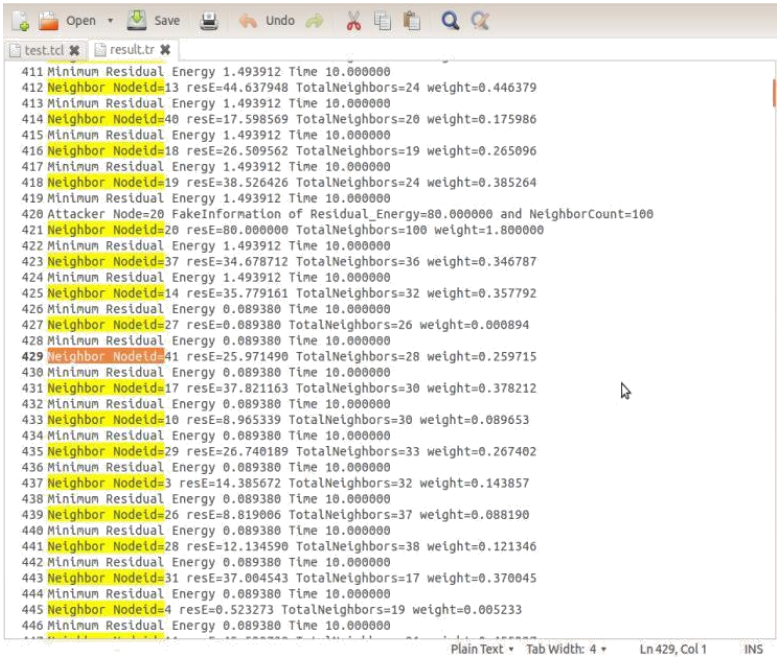

Figure 4. 2: Trace File Output for Neighbor Node Identification and Cluster Head Selection

4.2.2 Data Dropping and Impersonation Attacker Model and Detection

Consider a cluster of 50 SNs which monitors the temperature in an environment and node 0 be the base station. Let each node sense the temperature value and forward the data to the respective CH. The CH aggregates the data collected from the member nodes before forwarding the data packets to the destination. The network scenario for the temperature sensing environment is shown in figure 5.3.

Table 4. 2: Temperature Values of the Sensor Node in a Temperature Sensing Environment

Sensor Node	Temperature Value	Sensor Node	Temperature
1	22	17 (Impersonation node)	21
2	25	18	27
3	26	19	24
4	23	20	28 (Data dropped)
5 (Malicious node)	54 (False data)	36	25
6	54	36 (Impersonation node)	25
7	28	39	27
8	25	40	21
8 (Impersonation node)	25	42	22
9	21	43	29
10 (Malicious node)	54 (False data)	44	20
11	28	45	20
12	22	46	28
15	22 (Data dropped)	47	26
16	24 (Data dropped)	48	20
17	21	49	28

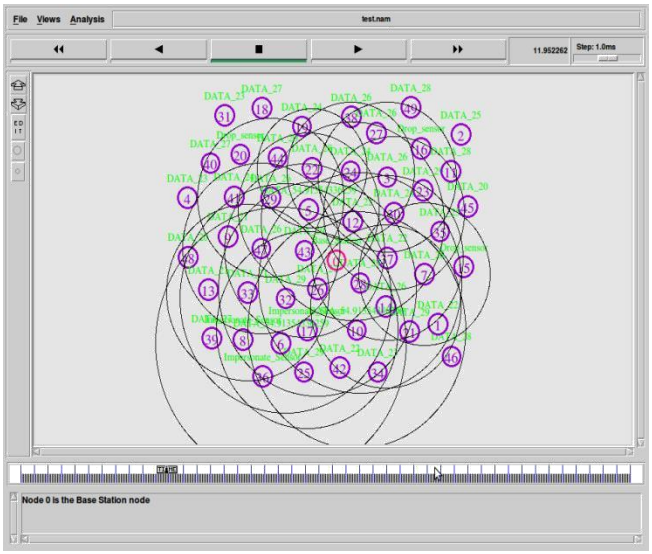

Figure 4. 3: Temperature Sensing Nodes in Hierarchical Network Scenario

Data Dropping Attacker model: In data dropping attack, the malicious node drops the data packets before reaching the destination and aim at affecting the desired outcome. In this example, Let the nodes 15, node 16, and node 20 be affected by data dropping attack and the temperature values such as 22, 24, and 28 respectively is dropped before reaching the base station. The trace file output of the data dropping attack in SNs is shown in figure 4.4.

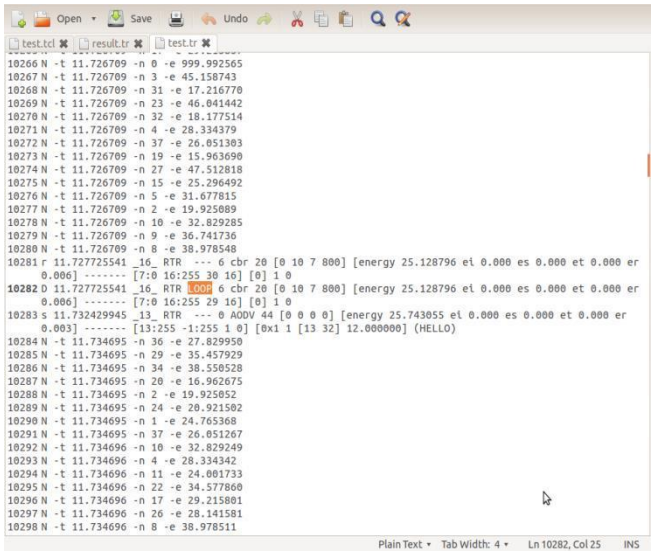

Figure 4. 4: The Trace File Output for Data Dropping Attacker Model

Detection of Data Dropping Attack: In the Proposed IDSHT-S scheme, the multidimensional factors such as IT, CT, and HT are calculated, and the overall trust evaluated is used for finding the data dropping attack. Let CH node 20 is the attacker node, and it drops the data packets before reaching the destination. The ITCH value

calculated for CH be 1.0 and the HTCH calculated for CH be 0. The content trust is calculated by considering the observing data and the value obtained is 0.02. The overall trust is calculated using the multidimensional factors and the value is 20. The attacker detection time of the node 20 is 13.626. Since the trust value evaluated is above the threshold value, the node 20 is detected as the attacker node.

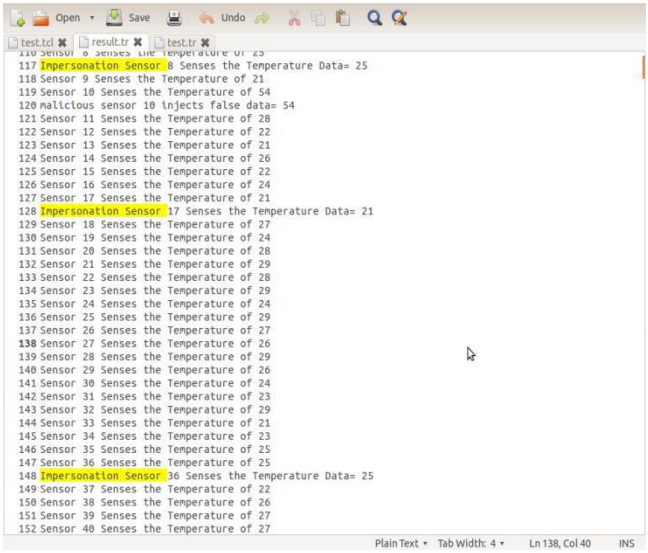

Figure 4. 5: The Trace File Output for Impersonation Attacker Model

Impersonation Attacker Model: The impersonation attack also known as spoofing attack takes the identity of another node in the network and aims at creating confusion in the network. Let the nodes 8, 17, and 36 are the impersonation attacker nodes. These impersonation attacker nodes send multiple data to the BS using the fake IDS or the stolen identities of other nodes.

Detection of Impersonation Attacker: The use of signatures can detect the impersonation attacks in the network. In the proposed IDSHT scheme, the signature generation and verification are done using the RSA algorithm. The RSA algorithm generates the public key and private key for each node in the network. The SNs encrypt the data packets using the public key and forwards it to the CH. The CH decrypts using the private key, and it compares the original data with the received data. If the received data is different, then the node is an impersonation attacker. For example, let the impersonation node be 34, and the temperature value forwarded to the CH is 64. Let the original data value is 34. Then, the CH decrypts the data and compares the original data value with the received data. The values are not equal, and hence the node 34 is detected as an impersonation attacker node. Then, the trace file for the key generation in the proposed scheme is shown in figure 5.6.

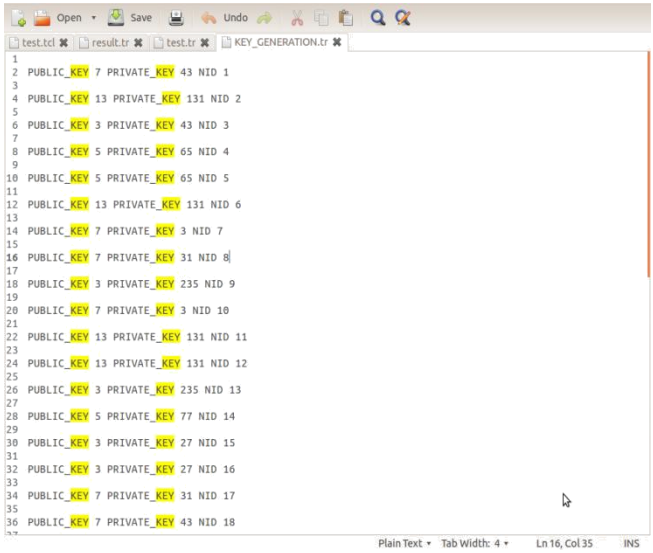

Figure 4. 6: The Trace File Output for Key Generation Using RSA Algorithm

4.3 Performance Analysis of Proposed IDSHT-S Scheme

The performance analysis for the proposed IDSHT-S scheme is done by comparing the performance metrics of the existing IDSHT scheme and proposed IDSHT-S Scheme. The performance of the hierarchical clustering model adopted, and the RSA algorithm used for securing the data packets improves the network security and network performance parameters. The simulation graph for the performance metrics is plotted by increasing the nodes and their corresponding metric values. The performance metrics used for comparison are the packet delivery ratio, network lifetime, delay, and overhead.

Packet Delivery Ratio: The packet delivery ratio is defined as the ratio of some data packets sent by the SN and the number of data packets received by the destination node. It can also be defined as the ratio between the total number of delivered packets to the BS and the total number of transmitted packets from the CH. The packet delivery ratio is calculated using the equation 5.1.

$$\text{Packet Delivery Ratio} = \frac{P_{Recieved} \times 100}{\sum_{i=1}^{n} P_{Generated}} \qquad \textbf{Equation 4. 1}$$

Packet Delivery Ratio

Where $P_{Received}$- total number of packets received by the sink node

$P_{Generated}$- Total number of packets generated by the sensor node

n- Number of nodes

Network Lifetime: The network lifetime is defined as the operational time of the network during which it can perform the designated task. It is also defined as the time until the first

sensor's energy is exhausted. It depends on the battery lifetime of the network. The network lifetime of the network is calculated using equation 5.2.

$$\text{Network Lifetime} = \frac{\text{Average Energy consumed by nodes}}{\text{Simulation time}} \times \text{Initial Energy} \times n \quad \textbf{Equation 4.2}$$

Network Lifetime

Where n - Number of nodes in the network

Delay: Delay of a packet is defined as the average time taken by a node to deliver the data packets to the base station. When the delay increases, the reliability of the data transmission decreases.

Delay= Average time taken by a node to deliver data to target (s) **Equation 4. 3**

Delay of a packet

Overhead: The overhead is defined as the total number of control packets used in the network. Large control overhead results in large energy consumption in the network and in turn affect the network performance.

Overhead= Total number of control packets (packets) **Equation 4. 4**

The overhead

4.3.1 Number of Nodes Vs Packet Delivery Ratio

The packet delivery ratio depends on the number of data packets received at the base station and the number of packets forwarded by the CH after aggregation process. The simulation graph shown in figure 5.7 is drawn by taking the number of nodes in X-axis and packet delivery ratio in Y-axis. The packet delivery ratio values expressed in percentage for both existing IDSHT scheme and proposed IDSHT-S scheme is shown in table 5.3. When the number of nodes is taken is 40 nodes, then the packet delivery ratio for IDSHT scheme is 2.09%, and the packet delivery ratio for the proposed IDSHT-S scheme is 72.4%. When the number of nodes is taken as 70 nodes, then the packet delivery ratio for the IDSHT scheme is 2.81%, and the packet delivery ratio for the proposed IDSHT-S scheme is 81.1%. The difference of the packet delivery ratio between the proposed IDSHT-S scheme and the IDSHT scheme, when the number of nodes is 40 and 70 is 70.3% and 78.2% respectively. The packet delivery ratio for the proposed IDSHT scheme has a drastic increase compared to the packet delivery ratio of the IDSHT

scheme. The packet delivery ratio for the proposed IDSHT-S scheme is higher as the attacks such as data dropping attack, and the impersonation attack is detected in the CH, and the data dropped, or interruption in the routing path is avoided in the proposed scheme. Hence the packet delivery ratio is increased compared to the IDSHT scheme.

Table 4. 3: Values for Number of Nodes vs Packet Delivery Ratio

Number of nodes	Packet Delivery Ratio (%)	
	IDSHT-S Scheme	IDSHT Scheme
40	72.4	2.09
50	76.3	1.43
60	59.7	0.65
70	81.1	2.85

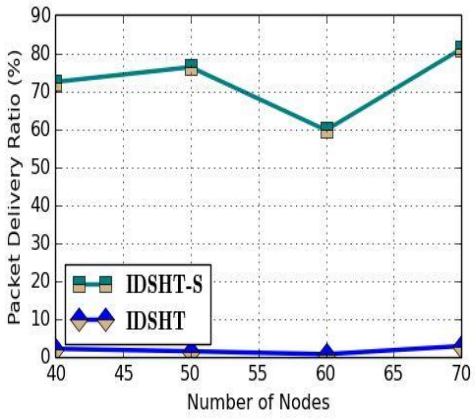

Figure 4. 7: The Simulation Graph for Number of Nodes vs Packet Delivery Ratio

4.3.2 Number of Nodes Vs Network Lifetime

The network lifetime is indirectly proportional to the energy consumption in the network. When energy consumption is large, the network lifetime is drastically reduced. The battery exhaustion attacks mainly occur due to malicious attackers and the proposed scheme aims at revoking these malicious attackers. The simulation graph shown in figure 5.8 is drawn by taking the number of nodes on X-axis and network lifetime values in the Y-axis. The network lifetime values for both proposed IDSHT-S scheme and IDSHT scheme is shown in table 5.4. When the number of nodes is taken as

40 nodes, then the network lifetime of proposed IDSHT-S scheme is 23.7×10-3 and the network lifetime of the IDSHT scheme is 22.1×10-3. When the number of nodes is taken as 70 nodes, then the network lifetime of the proposed IDSHT-S scheme is 32.9×10-3 and the network lifetime of the existing IDSHT scheme is 31.7×10-3. The difference of the network lifetime between the proposed IDSHT-S scheme and the IDSHT scheme for

nodes 40 and 70 are 6.75 ×10-3 and 3.64×10-3. The network lifetime of the proposed IDSHT-S scheme is high compared to the existing scheme as the trust evaluation is done only using direct trust validation and the energy consumption during trust evaluation is decreased compared to the existing scheme. Another reason for the increased lifetime in the proposed scheme is that the impersonation attack and data dropping attacks utilized unnecessary energy consumption, and the revoke of these attacks improved the energy efficiency, which in turn increased the network lifetime in the network.

Table 4. 4: Values for Number of Nodes vs Network Lifetime

Number of nodes	Network Lifetime $\times 10^{-3}$	
	IDSHT-S Scheme	IDSHT Scheme
40	23.7	22.1
50	26.2	25.2
60	33.8	33.6
70	32.9	31.7

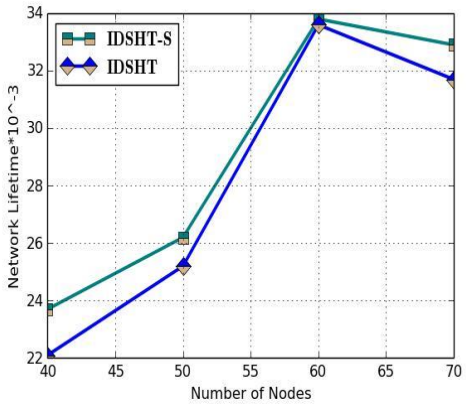

Figure 4. 8: The Simulation Graph for Number of Nodes vs Network Lifetime

4.3.3 Number of Nodes Vs Overhead

The Overhead is defined as the number of control packets exchanged in the overall network. The control packets are sent by the nodes for establishing links, route discovery request, trust evaluation, and for initiating transmission before sending data to the location. The simulation graph of overhead shown in figure 5.9 is drawn by taking some nodes in X-axis and overhead regarding packets in Y-axis. The overhead values expressed regarding packets are given in table 5.5 for both the proposed IDSHT-S scheme and IDSHT scheme. When the number of nodes is taken as 40, then the overhead of the IDSHT-S scheme is 1.32×103 packets, and the overhead of the IDSHT scheme is 1.53×103 packets. When the number of nodes is taken as 70 nodes, then the overhead of the IDSHT-S scheme is 2.30×103 packets, and the overhead of the IDSHT scheme is 3.50×103 packets. The difference of the overhead between the proposed IDSHT-S scheme and IDSHT scheme for 40 is 0.21×103 packets where the control

overhead of IDSHT-S scheme is slightly higher due to the key generation and verification process. The number of nodes is increased to 70 nodes, then the control overhead of the IDSHT-S scheme is decreased by 1.2×103 packets. One of the reasons for the decrease in control overhead in proposed IDSHT-S scheme is that trust evaluation process involves only direct trust between the SN-CH and CH-BS unlike the existing scheme, where the trust evaluation considers both direct trust and feedback trust from neighbors. The other important reason the control overhead of the proposed scheme is reduced is revoking the impersonation attacker in the network using the RSA algorithm. The control packets forwarded by the fake identities are revoked in the network.

Table 4. 5: Values for Number of Nodes vs Overhead

Number of nodes	Overhead (Packets)×10^3	
	IDSHT-S Scheme	IDSHT Scheme
40	1.32	1.53
50	1.36	2.29
60	2.11	2.65
70	2.30	3.50

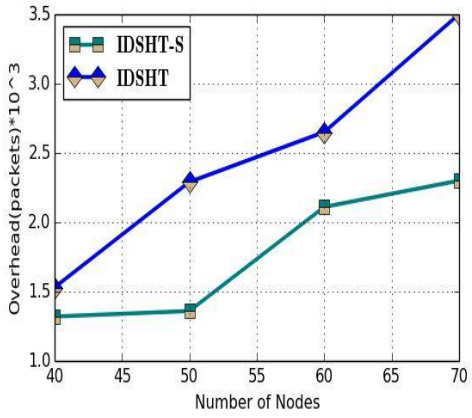

Figure 4. 9: The Simulation Graph for Number of Nodes vs Overhead

4.3.4 Number of Nodes Vs Delay

The delay in WSN is defined as the time taken by the data to reach the destination, i.e., base station. The delay of data packets affects the performance of the network. The delay in the system is mainly caused due to the dropping of the data packet; node collision depends on the time is taken for trust evaluation and other factors. The simulation graph for the delay shown in figure 5.10 is drawn by taking the number of nodes in X-axis and the delay expressed in seconds in Y-axis. The delay values obtained by increasing the number of nodes for both the proposed IDSHT-S scheme and IDSHT scheme is shown in table 5.6. When the number of nodes is taken as 40 nodes, the delay in the IDSHT-S scheme is 2.12s, and the delay in IDSHT scheme is 0.48s. When the

number of nodes is taken as 70 nodes, the delay in the IDSHT-S scheme is 0.5s, and the delay in IDSHT scheme is 0.74s. When the number of nodes is taken as 40, the difference of the delay between the IDSHT-S scheme and IDSHT scheme is 1.64s, i.e. the proposed scheme has 1.64s lesser delay of data packets to the destination compared to the delay in the existing IDSHT scheme. When the number of nodes is like 70, then the delay in the proposed IDSHT-S scheme is 3.21s lesser in delaying the data packets to destination compared to the existing IDSHT scheme. The delay in the proposed scheme is decreased due to reduced control overhead packets and increased residual energy due to the hierarchical cluster-based structure used, and the trust evaluation is done only by direct trust evaluation. The impersonation attacks which are undetected in the existing scheme uses fake identities and forwards data packets randomly to the different routes. Thus, the delay is more in the IDSHT scheme. In the proposed IDSHT-S scheme, the detection and prevention of impersonation attacks help in reducing the delay and improving the network performance.

Table 4. 6: Values for Number of Nodes vs Delay

Number of nodes	Delay(s)	
	IDSHT-S Scheme	IDSHT Scheme
40	2.13	0.49
50	0.04	0.46
60	0.06	2.84
70	0.51	3.72

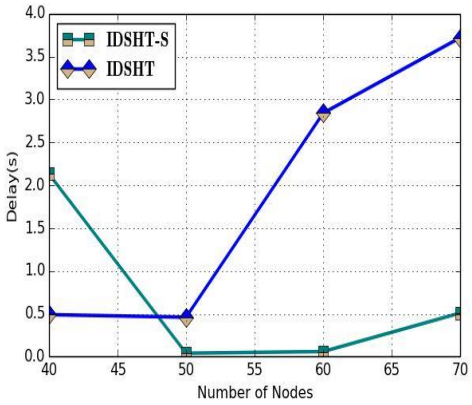

Figure 4. 10: The Simulation Graph for Number of Nodes vs Delay

SUMMARY

In chapter five, the implementation of the proposed IDSHT-S scheme is presented. The evaluation of the IDSHT-S scheme in a hierarchical cluster based WSN is explained. The simulation setup and the parameters used for constructing the network scenario in an NS2 environment is presented. The network scenario for the proposed IDSHT-S scheme is explained in detail. The data dropping and impersonation attacker model are presented

to prove the efficiency of the proposed scheme in detecting these attacks. The performance analysis of the proposed scheme is presented in the form of a simulation graph. The performance metrics such as packet delivery ratio, delay, overhead, and network lifetime are used for comparing the performance between the proposed IDSHT-S scheme and IDSHT scheme. Thus, the conclusion is derived that the proposed scheme has an increased packet delivery ratio and network lifetime compared to the existing IDSHT scheme. The control overhead and delay are less in the proposed scheme.

CHAPTER FIVE

CONCLUSIONS AND FUTUREWORKS

5.1 Conclusions

Several trust-based security mechanisms have been developed to provide a secure routing and data aggregation in WSN. The trade-off between energy efficiency and accurate trust calculation is one of the major concerns while developing intrusion detection schemes in WSN. In the proposed IDSHT-S scheme, a multidimensional two-tier hierarchical trust-based mechanism is adopted, which includes interactive trust, honesty trust, and content trust for cluster head selection during data aggregation. The IDHST scheme supports WSN dynamic environment, transition state of nodes, and variation in trust values. IDHST-S includes both direct evaluations for trust calculation in a fixed hop range. The trust evaluation is maintained at two levels, where the multidimensional trust of sensor node is maintained by the cluster head and the multidimensional trust of cluster head is calculated from the base station and cluster head interaction, feedback evaluation from one-hop neighbours, and interactions with other cluster heads. The honesty trust is calculated using the number of successful and unsuccessful interactions between the two nodes. The content trust is calculated based on the observing data by cluster heads and it is a network relates trust. The interactive trust is evaluated by calculating the number of interactions between the nodes and cluster heads. The overall trust is evaluated using multidimensional metrics and they are used for detecting several attacks such as impersonation attack, dropping attack, and selfish attack in the network. The reduction of false positive and false negative rate is achieved in the network. The security of the network can be improved by using signatures to protect the data in the network. In this IDSHT-S scheme, the RSA algorithm is used for signature generation and verification process. Through signature based IDSHT-S scheme, the attacks that are imposed by impersonating revoked nodes can be detected and eliminated. A simulation environment is constructed using the NS2 simulation protocol, where the proposed scheme is constructed with an example of temperature sensing environment and the performance analysis of the proposed IDSHT-S is compared with the existing IDSHT scheme. The simulation result shows an improved packet delivery ratio, storage overhead and delay compared to the existing IDSHT scheme.

5.2 Future Works

There are some directions to improve the performance of the proposed scheme further, and the directions are given below

1) To improve intrusion detection mechanisms by integrating techniques for detecting unknown attacks in the network
2) To overcome the inefficiencies of slow key generation and decryption process in RSA algorithm
3) In future, the isolation and periodic re-election of cluster head need to be adopted to enhance the overall security of WSN.

REFERENCES

Abraham, A. and Thomas, J., 2006. Distributed intrusion detection systems: a computational intelligence approach. *In Applications of Information Systems to Homeland Security and Defense* :107-137

Ahmad, I., Shah, K. and Ullah, S., 2016. Military Applications using Wireless Sensor Networks: A survey. Int. J. Eng. Sci, 6(6): 7039.

Ahmed, M.R., Huang, X. and Sharma, D., 2012. A taxonomy of internal attacks in wireless sensor network. Memory (Kbytes), 128: 48.

Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E., 2002. Wireless sensor networks: a survey. *Computer networks*, *38*(4): 393-422.

Al Shehri, W. 2017. A survey on security in wireless sensor networks. *International Journal of Network Security & Its Applications*, *9*(1): 25-32.

Alasem, R., Reda, A. and Mansour, M., 2011. Location based energy-efficient reliable routing protocol for wireless sensor networks. *Recent Researches in Communications, Automation, Signal processing, Nanotechnology, Astronomy and Nuclear Physics,* WSEAS Press, Cambridge, UK,:180-185.

Alemdar, H. and Ersoy, C., 2010. Wireless sensor networks for healthcare: A survey. *Computer networks*, 54(15): 2688-2710.

Al-Karaki, J.N. and Kamal, A.E., 2004. Routing techniques in wireless sensor networks: a survey. *IEEE wireless communications*, 11(6):6-28.

Alrajeh, N.A., Khan, S. and Shams, B., 2013. Intrusion detection systems in wireless sensor networks: a review. *International Journal of Distributed Sensor Networks*, 9(5) :167575.

Alrajei, N., Fu, H. and Zhu, Y., 2014. A survey on fault tolerance in wireless sensor networks. In 2014 American Society For Engineering Education North Central Section Conference ASEE NCS Conference, 4, April.

Aminian, M. and Naji, H.R., 2013. A hospital healthcare monitoring system using wireless sensor networks. *J. Health Med. Inform*, *4*(02): 121.

Arfat,Y. and Shaikh, R.A., 2016. A Survey on Secure Routing Protocols in Wireless Sensor Networks. *International Journal of Wireless and Microwave Technologies (IJWMT)*, *6*(3): 9-19

Balepin, I., Maltsev, S., Rowe, J. and Levitt, K., 2003, September. Using specification-based intrusion detection for automated response. *In International Workshop on Recent Advances in Intrusion Detection*, Springer, Berlin, Heidelberg:136-154

Bao, F., Chen, R., Chang, M. and Cho, J.H., 2012. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. *IEEE transactions on network and service management*, 9(2):169-183.

Bazzi, H.S., Haidar, A.M. and Bilal, A., 2015. Classification of routing protocols in wireless sensor network. *International Conference on Computer Vision and Image Analysis Applications (ICCVIA)* : (pp. 1-5), January

Biswas, S. and Adhikari, S., 2015. A survey of security attacks, defenses and security mechanisms in wireless sensor network. *International Journal of Computer Applications*, 131(17): 28-35.

Butun, I., Morgera, S.D. and Sankar, R., 2014. A survey of intrusion detection systems in wireless sensor networks. IEEE communications surveys & tutorials, 16(1):266-282

Can, O. and Sahingoz, O.K., 2015. A survey of intrusion detection systems in wireless sensor networks. *6th IEEE International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO)* :1-6, May

Ch, S.A., Omair, M.M., Khan, I.A. and Malik, T.A., 2011. Ensuring reliability and freshness for data aggregation in wireless sensor networks. International Journal of Machine Learning and Computing, 1(3): 224

Chang, S.Y., Lin, Y.H., Sun, H.M. and Wu, M.E., 2012. Practical RSA signature scheme based on periodical rekeying for wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 8(2):13.

Chen, H., 2009. Task-based trust management for wireless sensor networks. *International Journal of Security and its applications*, 3(2):21-26.

Chen, J.L., Ma, Y.W., Hsu, Y.M. and Huang, Y.M., 2010, February. Adaptive routing protocol for reliable wireless sensor networking. *The 12th International Conference on Advanced Communication Technology (ICACT)*, 1: 358-363

Chen, P., Zhang, Y. and Dai, W., 2018. LEACH protocol based on Clustering and Multi-leader Selecting in Wireless Sensor Network. *In 37th Chinese Control Conference (CCC)*: 7298-7303, July

Chow, C.Y., Xu, W. and He, T., 2014. Privacy enhancing technologies for wireless sensor networks. *In The Art of Wireless Sensor Networks*. Springer, Berlin, Heidelberg :609-641

Cirstea, Cosmin, 2011. "Energy efficient routing protocols for wireless sensor networks: A survey." *IEEE 17th International Symposium for Design and Technology in Electronic Packaging (SIITME)*, pp. 277-282 .

Dener, M., 2018. A New Energy Efficient Hierarchical Routing Protocol for Wireless Sensor Networks. *Wireless Personal Communications*, 101(1):269-286.

Deng, J., Han, R. and Mishra, S., 2005. Countermeasures against traffic analysis attacks in wireless sensor networks. In null:113-126, September

Dhakne, A.R. and Chatur, P.N., 2015. Distributed trust based intrusion detection approach in wireless sensor network. *In Communication, Control and Intelligent Systems (CCIS)*: 96-101, November

Dietrich, I. and Dressler, F., 2009. On the lifetime of wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 5(1): 5.

Ding, P., Holliday, J. and Celik, A., 2005. Distributed energy-efficient hierarchical clustering for wireless sensor networks. *In International conference on distributed computing in sensor systems* . Springer, Berlin, Heidelberg: 322-339, June

Du, X. and Chen, H.H., 2008. Security in wireless sensor networks. IEEE Wireless Communications, 15(4).

Durresi, A., Paruchuri, V., Kannan, R. and Iyengar, S.S., 2005. Data integrity protocol for sensor networks. *International Journal of Distributed Sensor Networks*, 1(2): 205-214.

Elqusy, A.S., Essa, S.E. and Ayman, E.S., 2017. A Survey of Wireless Sensor Network Attacks. Communications, 6: 10-20

Erdelj, M., Mitton, N. and Natalizio, E., 2013. Applications of industrial wireless sensor networks. Industrial Wireless Sensor Networks: Applications, Protocols, and Standards: 1-22.

Ez-Zaidi, A. and Rakrak, S., 2017. An Efficient Approach for Storage Balancing in Wireless Sensor Networks. *International Journal of Online Engineering (iJOE)*, 13(09): 4-18.

Farooqi, A.H. and Khan, F.A., 2009. Intrusion detection systems for wireless sensor networks: A survey. *In Communication and networking* :234-241

Fasolo, E., Rossi, M., Widmer, J. and Zorzi, M., 2007. In-network aggregation techniques for wireless sensor networks: a survey. IEEE Wireless Communications, 14(2)

Fedor, S. and Collier, M., 2007. On the problem of energy efficiency of multi-hop vs one-hop routing in wireless sensor networks. *21st International Conference on Advanced Information Networking and Applications Workshops, AINAW'07,* 2: 380-385, May

Flinn, J., Ortiz, H.S.C. and Yuan, S., 2016. A secure routing scheme for networks with unknown or dynamic topology using A-star algorithm. In *Proceedings of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp): 3, January

Fonoage, M., Cardei, M. and Ambrose, A., 2010. A QoS based routing protocol for wireless sensor networks. IEEE 29th International on Performance Computing and Communications Conference (IPCCC): 122-129, December.

Garcia-Hernandez, C.F., Ibarguengoytia-Gonzalez, P.H., Garcia-Hernandez, J. and Perez-Diaz, J.A., 2007. Wireless sensor networks and applications: a survey. *International Journal of Computer Science and Network Security*, 7(3): 264-273.

Gawdan, I.S., Chow, C.O., Zia, T.A. and Sarhan, Q.I., 2011. A novel secure key management module for hierarchical clustering wireless sensor networks. *Third International Conference* on Computational Intelligence, Modelling and Simulation (CIMSiM): 312-316, September

Guyeux, C., Makhoul, A. and Bahi, J.M., 2014. A security framework for wireless sensor networks: theory and practice. *In IEEE 23rd International WETICE Conference* :269-274, June

Han, G., Jiang, J., Shu, L. and Guizani, M., 2015. An attack-resistant trust model based on multidimensional trust metrics in underwater acoustic sensor network. *IEEE Transactions on Mobile Computing*, 14(12):2447-2459.

Han, G., Jiang, J., Shu, L., Niu, J. and Chao, H.C., 2014. Management and applications of trust in Wireless Sensor Networks: A survey. *Journal of Computer and System Sciences*,80(3): 602-617

Heinzelman, W.R., Chandrakasan, A. and Balakrishnan, H., 2000, January. Energy-

efficient communication protocol for wireless microsensor networks. *Proceedings of the 33rd annual Hawaii international conference on System sciences* :10

Hellaoui, H., Koudil, M. and Bouabdallah, A., 2017. Energy-efficient mechanisms in security of the internet of things: A survey. *Computer Networks,* 127: 173-189

Hindy, H., Brosset, D., Bayne, E., Seeam, A., Tachtatzis, C., Atkinson, R. and Bellekens, X., 2018. A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets.

Hu, Y.C., Perrig, A. and Johnson, D.B., 2006. Wormhole attacks in wireless networks. IEEE journal on selected areas in communications, 24(2): 370-380.

Hwang, J., Shin, C. and Yoe, H., 2010. Study on an agricultural environment monitoring server system using wireless sensor networks. *Sensors*, *10*(12): 11189-11211.

Ioannis, K., Dimitriou, T. and Freiling, F.C., 2007. Towards intrusion detection in wireless sensor networks. *In Proc. of the 13th European Wireless Conference* :1-10, April

Ishmanov, F., Malik, A.S., Kim, S.W. and Begalov, B., 2015. Trust management system in wireless sensor networks: design considerations and research challenges. *Transactions on Emerging Telecommunications Technologies*, 26(2): 107-130

Jan, B., Farman, H., Javed, H., Montrucchio, B., Khan, M. and Ali, S., 2017. Energy Efficient Hierarchical Clustering Approaches in Wireless Sensor Networks: A Survey. *Wireless Communications and Mobile Computing*.

Karlof, C. and Wagner, D., 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications:* 113-127, May

Khalid, O., Khan, S.U., Madani, S.A., Hayat, K., Khan, M.I., Min‐Allah, N., Kolodziej, J., Wang, L., Zeadally, S. and Chen, D., 2013. Comparative study of trust and reputation systems for wireless sensor networks. Security and Communication Networks, 6(6):669-688.

Khan, A., Shah, S.W., Ali, A. and Ullah, R., 2017. Secret key encryption model for Wireless Sensor Networks. *14th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*: 809-815, January

Khan, M.K., Shiraz, M., Zrar Ghafoor, K., Khan, S., Safaa Sadiq, A. and Ahmed, G., 2018. EE-MRP: Energy-efficient multistage routing protocol for wireless sensor networks. *Wireless Communications and Mobile Computing*.

Khelifa Benahmed, Madjid Merabti, andHafid Haffaf, 2012.Distributed monitoring for misbehavior detection in wireless sensor networks. *Security and Communication Networks*, *6,* August.

Kulik, J., Heinzelman, W. and Balakrishnan, H., 2002. Negotiation-based protocols for disseminating information in wireless sensor networks. Wireless networks, 8(2/3):169-185.

Kuriakose, J., Amruth, V., Sandesh, A.G., Abhilash, V., Kumar, G.P. and Nithin, K., 2014. A review on mobile sensor localization. *In International Symposium on Security in Computing and Communication.* Springer, Berlin, Heidelberg: 30-44, September

Lai, B., Kim, S. and Verbauwhede, I., 2002. Scalable session key construction protocol

for wireless sensor networks. *In IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES)* : 7, December

Li, X., Zhou, F. and Du, J., 2013. LDTS: A lightweight and dependable trust system for clustered wireless sensor networks. *IEEE transactions on information forensics and security*, 8(6):924-935.

Liao, H.J., Lin, C.H.R., Lin, Y.C. and Tung, K.Y., 2013. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1):16-24

Lindsey, S. and Raghavendra, C.S., 2002. PEGASIS: Power-efficient gathering in sensor information systems. *In Aerospace conference proceedings*, 3: 3-3.

Liu, S., Pang, L., Pei, Q., Ma, H. and Peng, Q., 2009, August. Distributed event-triggered trust management for wireless sensor networks. *Fifth International Conference on Information Assurance and Security IAS'09*, 2: 291-294, August

Liu, X., 2012. A survey on clustering routing protocols in wireless sensor networks. sensors, 12(8) : 11113-11153.

Loscri, V., Morabito, G. and Marano, S., 2005. A two-levels hierarchy for low-energy adaptive clustering hierarchy (TL-LEACH). *In 62nd IEEE Vehicular Technology Conference (VTC)*, 3 :1809-1813, September.

Lu, X. and Li, W., 2014. A systematic review on industrial wireless sensor networks. *proceeding of Sustainable Design and Manufacturing*.

Lupu, T.G., Rudas, I., Demiralp, M. and Mastorakis, N., 2009. Main types of attacks in wireless sensor networks. In WSEAS international conference. proceedings. recent advances in computer engineering, 9, September.

Maleh, Y. and Ezzati, A., 2014. A review of security attacks and Intrusion Detection Schemes in Wireless Sensor Networks.

Mampentzidou, I., Karapistoli, E. and Economides, A.A., 2012. Basic guidelines for deploying wireless sensor networks in agriculture. *4th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)* : 864-869, October

Mamun, M.S.I. and Kabir, A.F.M., 2012. Hierarchical design based intrusion detection system for wireless ad hoc network.

Manap, Z., Ali, B.M., Ng, C.K., Noordin, N.K. and Sali, A., 2013. A review on hierarchical routing protocols for wireless sensor networks. *Wireless personal communications*, 72(2): 1077-1104

Mathews, M., Song, M., Shetty, S. and McKenzie, R., 2007. Detecting compromised nodes in wireless sensor networks. *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing,* IEEE, 1: 273-278, July

Michiardi, P. and Molva, R., 2002. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. *In Advanced communications and multimedia security*: 107-121.

Mikhaylov, K., Tervonen, J., Heikkila, J. and Kansakoski, J., 2012. Wireless sensor networks in industrial environment: Real-life evaluation results. *2nd Baltic Congress on*

Future Internet Communications (BCFIC): 1-7, April.

Mitchell, R. and Chen, R., 2014. A survey of intrusion detection in wireless network applications. *Computer Communications*, 42 :1-23.

Mittal, V. and Vigna, G., 2002. Sensor-based intrusion detection for intra-domain distance-vector routing. *In Proceedings of the 9th ACM conference on Computer and communications security*: 127-137, November.

Mohammadi, S., Atani, R.E. and Jadidoleslamy, H., 2011. A comparison of routing attacks on wireless sensor networks. organization, 4: 21

Naeem, T. and Loo, K.K., 2009. Common security issues and challenges in wireless sensor networks and IEEE 802.11 wireless mesh networks, 3(1)

Newsome, J., Shi, E., Song, D. and Perrig, A., 2004. The sybil attack in sensor networks: analysis & defenses. *In Proceedings of the 3rd international symposium on Information processing in sensor networks:* 259-268, April.

Ning, P. and Jajodia, S., 2003. Intrusion detection techniques. *The Internet Encyclopedia*, 2:355-367.

Oliveira, L.M. and Rodrigues, J.J., 2011. Wireless Sensor Networks: A Survey on Environmental Monitoring. JCM, 6(2): 143-151.

Onat, I. and Miri, A., 2005, August. An intrusion detection system for wireless sensor networks. *IEEE International Conference on Wireless And Mobile Computing, Networking And Communications(WiMob)*, 3 :253-259

Ouadjaout, A., Bagaa, M., Bachir, A., Challal, Y., Lasla, N. and Khelladi, L., 2010. Information Security in Wireless Sensor Networks. In *Encyclopedia on Ad Hoc and Ubiquitous Computing: Theory and Design of Wireless Ad Hoc, Sensor, and Mesh Networks*: 427-471

Pathan, A.S.K., Lee, H.W. and Hong, C.S., 2006. Security in wireless sensor networks: issues and challenges. *The 8th International Conference on Advanced Communication Technology(ICACT)*, 2: 6, February

Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V. and Culler, D.E., 2002. SPINS: Security protocols for sensor networks. Wireless networks, 8(5), pp.521-534.

Qu, H., Lei, L., Tang, X. and Wang, P., 2018. A Lightweight Intrusion Detection Method Based on Fuzzy Clustering Algorithm for Wireless Sensor Networks. *Advances in Fuzzy Systems.*

Raghunathan, V., Schurgers, C., Park, S. and Srivastava, M.B., 2002. Energy-aware wireless microsensor networks. *IEEE Signal processing*, 19(2): 40-50.

Rassam, M.A., Maarof, M.A. and Zainal, A., 2012. A survey of intrusion detection schemes in wireless sensor networks. *American Journal of Applied Sciences*, 9(10):1636.

Razaque, A., Abdulgader, M., Joshi, C., Amsaad, F. and Chauhan, M., 2016. P-LEACH: energy efficient routing protocol for wireless sensor networks. *In Systems, Applications and Technology Conference (LISAT)*, IEEE Long Island : 1-5, April

Ren, X. and Yu, H., 2006. Security mechanisms for wireless sensor networks. *IJCSNS International Journal of Computer Science and Network Security*, 6(3): 155-156

Riad, A. M., Hamdy K. El-Minir, and Mohamed El-hoseny, 2013. Secure Routing in Wireless Sensor Networks: A State of the Art. *International journal of computer applications*, 67 (7)

Roman, R., Zhou, J. and Lopez, J., 2006. Applying intrusion detection systems to wireless sensor networks. *In IEEE Consumer Communications & Networking Conference (CCNC)*

Sabor, N., Sasaki, S., Abo-Zahhad, M. and Ahmed, S.M., 2017. A comprehensive survey on hierarchical-based routing protocols for mobile wireless sensor networks: review, taxonomy, and future directions. *Wireless Communications and Mobile Computing*, 2017

Sadagopan, N., Krishnamachari, B. and Helmy, A., 2003, May. The ACQUIRE mechanism for efficient querying in sensor networks. *IEEE International Workshop on Sensor Network Protocols and Applications*:149-155

Shabbir, N. and Hassan, S.R., 2017. Routing Protocols for Wireless Sensor Networks (WSNs). In Wireless Sensor Networks-Insights and Innovations. InTech.

Shnayder, V., Chen, B.R., Lorincz, K., Fulford-Jones, T.R. and Welsh, M., 2005. Sensor networks for medical care.

Siddiqui, S., Khan, A.A. and Ghani, S., 2015. A survey on data aggregation mechanisms in wireless sensor networks. International Conference on Information and Communication Technologies (ICICT) : 1-7, December

Siji, F.G. and Eneh, I.I., 2015. Improving the Scalability of Wireless Sensor Networks by Reducing Sink Node Isolation. *International Journal of Applied Information Systems (IJAIS)*, 8(7)

Silva, A.P.R., Martins, M.H., Rocha, B.P., Loureiro, A.A., Ruiz, L.B. and Wong, H.C., 2005. Decentralized intrusion detection in wireless sensor networks. *In Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks* :16-23, October

Silva, I., Guedes, L.A., Portugal, P. and Vasques, F., 2012. Reliability and availability evaluation of wireless sensor networks for industrial applications. *Sensors*, 12(1): 806-838.

Soliman, H.H., Hikal, N.A. and Sakr, N.A., 2012. A comparative performance evaluation of intrusion detection techniques for hierarchical wireless sensor networks. *Egyptian Informatics Journal*, 13(3):225-238.

Soro, S. and Heinzelman, W.B., 2005. Prolonging the lifetime of wireless sensor networks via unequal clustering. *19th IEEE International Proceedings on Parallel and Distributed Processing Symposium* :8, April.

Stetsko, A., Folkman, L. and Matyas, V., 2010, September. Neighbor-based intrusion detection for wireless sensor networks. *6th International Conference on Wireless and Mobile Communications (ICWMC)*, 2010 : 420-425

Taherkordi, A., Taleghan, M.A. and Sharifi, M., 2006. Achieving availability and reliability in wireless sensor networks applications. *The First International Conference on Availability, Reliability and Security,* IEEE: 7, April

Taleb, R.A., 2015. A Study of Secure Routing Protocols for Wireless Sensor Networks.

Journal of Emerging Trends in Computing and Information Sciences, 6(3).

Tawalbeh, H., Hashish, S., Tawalbeh, L. and Aldairi, A., 2017. Security in Wireless Sensor Networks Using Lightweight Cryptography. *Journal of Information Assurance & Security*, *12*(4)

Uluagac, A.S., Lee, C.P., Beyah, R.A. and Copeland, J.A., 2008, . Designing secure protocols for wireless sensor networks. In *International Conference on Wireless Algorithms, Systems, and Applications,* Springer, Berlin, Heidelberg: 503-514, October

Uppuluri, P. and Sekar, R., 2001, October. Experiences with specification-based intrusion detection. *In International Workshop on Recent Advances in Intrusion Detection*, Springer, Berlin, Heidelberg: 172-189.

Vasilomanolakis, E., Karuppayah, S., Mühlhäuser, M. and Fischer, M., 2015. Taxonomy and survey of collaborative intrusion detection. ACM Computing Surveys (CSUR), 47(4):55.

Wagner, D., 2004. Resilient aggregation in sensor networks. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks: 78-87, October

Walters, J.P., Liang, Z., Shi, W. and Chaudhary, V., 2007. Wireless sensor network security: A survey. Security in distributed, grid, mobile, and pervasive computing, 1: 367.

Wang, Y., Attebury, G. and Ramamurthy, B., 2006. A survey of security issues in wireless sensor networks.

Warneke, B.A. and Pister, K.S., 2002. MEMS for distributed wireless sensor networks. *9th International Conference on Electronics, Circuits and Systems,* IEEE, 1:291-294

Watro, R., Kong, D., Cuti, S.F., Gardiner, C., Lynn, C. and Kruus, P., 2004. TinyPK: securing sensor networks with public key technology. *In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*: 59-64, October

Winkler, M., Tuchs, K.D., Hughes, K. and Barclay, G., 2008. Theoretical and practical aspects of military wireless sensor networks. *Journal of Telecommunications and Information Technology* : 37-45.

Yan, S. and Yang, M., 2014. Research on analysis routing protocol for wireless sensor networks. *Journal of Chemical and Pharmaceutical Research*, 6(6): 919-922

Yanhua, H. and Zhang, X., 2016. Aggregation Tree Based Data Aggregation Algorithm in Wireless Sensor Networks. *International Journal of Online Engineering (iJOE)*, 12(06): 10-15.

Yao, Y. and Gehrke, J., 2002. The cougar approach to in-network query processing in sensor networks. *ACM Sigmod record*, 31(3): 9-18.

Ye, M., Li, C., Chen, G. and Wu, J., 2005. EECS: an energy efficient clustering scheme in wireless sensor networks. *24th IEEE International on Performance, Computing, and Communications Conference (IPCCC)* :535-540, April

Ye, Z., Wen, T., Liu, Z., Song, X. and Fu, C., 2017. An Efficient Dynamic Trust Evaluation Model for Wireless Sensor Networks. *Journal of Sensors*, 2017.

Younis, O. and Fahmy, S., 2004. HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. *IEEE Transactions on mobile computing*, 3(4):366-

379.

Yu, B. and Xiao, B., 2006. Detecting selective forwarding attacks in wireless sensor networks. *20th international in Parallel and distributed processing symposium (IPDPS):* 8, April

Yu, J., Qi, Y., Wang, G. and Gu, X., 2012. A cluster-based routing protocol for wireless sensor networks with nonuniform node distribution. *AEU-International Journal of Electronics and Communications*, *66*(1): 54-61.

Yu, Y., Govindan, R. and Estrin, D., 2001. Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks.

Yu, Y., Li, K., Zhou, W. and Li, P., 2012. Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. *Journal of Network and computer Applications*, 35(3): 867-880

Zahariadis, T., Leligou, H., Karkazis, P., Trakadas, P., Papaefstathiou, I., Vangelatos, C. and Besson, L., 2010. Design and implementation of a trust-aware routing protocol for large WSNs. *International Journal of Network Security & Its Applications (IJNSA)*, 2(3):52-68.

Zeb, A., Islam, A.M., Zareei, M., Al Mamoon, I., Mansoor, N., Baharun, S., Katayama, Y. and Komaki, S., 2016. Clustering analysis in wireless sensor networks: the ambit of performance metrics and schemes taxonomy. *International Journal of Distributed Sensor Networks*, *12*(7): 4979142

Zhang, Z., Zhu, H., Luo, S., Xin, Y. and Liu, X., 2017. Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks. *IEEE Access*, 5:12088-12102.

Zhou, W., Jia, Y., Peng, A., Zhang, Y. and Liu, P., 2018. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal*

Feb 2020