Intrusion Detection System in Wireless Sensor Network

A dissertation submitted in partial fulfillment of the requirements for the degree of

Master of Technology

submitted by

Atul Agarwal

Roll No. 14MI550

Under the guidance of

Dr. Narottam Chand Kaushal

Department of Computer Science & Engineering

National Institute of Technology Hamirpur

Hamirpur, India-177005

May, 2019

Department of Computer Science & Engineering
National Institute of Technology Hamirpur
Himachal Pradesh, India-177005

Candidate's Declaration

I hereby declare that the research work presented in the dissertation entitled **"Intrusion Detection System in Wireless Sensor Network"** in partial fulfillment of the requirements for the award of the Degree of **Master of Technology** and submitted in the Department of Computer Science and Engineering of the National Institute of Technology Hamirpur is an authentic record of my own research work carried out during a period from July 2018 to May 2019 under the supervision of **Dr. Narottam Chand Kaushal**, Associate Professor, Department of Computer Science and Engineering, National Institute of Technology Hamirpur.

The matter presented in this dissertation has not been submitted by me for the award of any other degree of this or any other Institute/University.

Atul Agarwal

This is to certify that the above statement made by the candidate is true to the best of our knowledge and belief.

Dr. Narottam Chand Kaushal
Associate Professor

Date:

The M.Tech Viva-voce examination of Atul Agarwal, M.Tech. student has been Successfully held on .....

Signature of Supervisor **Signature of External Examiner**

ACKNOWLEDGMENTS

It is an incredible delight for me to express my regard and profound feeling of appreciation to my M.Tech. supervisor **Dr. Narottam Chand Kaushal**, Associate Professor, Department of Computer Science & Engineering, National Institute of Technology Hamirpur, for his shrewdness, vision, ability, direction, eager association throughout my M.Tech. course at NIT Hamirpur. I am exceptionally obliged to him for showing me both composition and research aptitudes which have demonstrated to be gainful for my momentum research and future vocation. Without his unlimited endeavors, information and guidance this research would not have been conceivable. It has been a significant learning background for me to work under his watch.

My appreciation is additionally stretched out to every one of the teachers and staff individuals from **Computer Science & Engineering Department and Computer Centre** for their convenient assistance and collaboration stretched out over the span of research.

I am obliged to my family and friends for their ethical help, love, consolation and favors to finish this research. Without their devotion and reliability I couldn't have achieved this undertaking.

At last, I am obligated and appreciative to the Almighty for helping me in this endeavor.

(Atul Agarwal)

Abstract

Wireless sensor networks are most widely used in networking because of their large application domain. These networks have appealing features, like multihop wireless communication, deployment in a hostile unprotected environment, low installation cost, auto-configurable, etc. Wireless sensor networks are used in almost every field because wireless sensors are very easy to deploy and maintain where wired surveillance is very difficult. Sensors are small devices deployed in the unprotected region and are vulnerable to attacks. Its large application domain and deployment in unprotected and unattended environment causing network services to be compromised. Security mechanisms, cryptography, etc. can provide security to outside attacker but intrusion detection system is must to detect networks compromised nodes and to continue network services. To collect information from the surroundings sensor node senses information and follows multi-hop communication and the data reaches to sink. In these networks, there is no monitoring of information flow, hence security is a big concern. To provide security in wireless sensor network operations, all kinds of intrusions should be detected and appropriate action must be taken against them in order to ensure that there is no harm done to the sensor network. Out of several detection techniques, this dissertation report focuses on signature-based, anomaly-based and hybrid-based techniques. Various detection models are examined based on certain parameters.

This dissertation report presents an intrusion detection system in wireless sensor networks. This research work uses a data-set of security attacks on wireless sensor network and classifies attacks with training set accuracy of 99.24% with a categorical loss of 0.0271 and testing set accuracy of 99.32% with a categorical loss of 0.0250 using neural network classifier. This work can be categorized as signature based intrusion detection system and it can detect blackhole, grayhole, scheduling and flooding attacks. This report also summarizes various intrusion detection algorithms with their features which are used in wireless sensor networks.

Contents

List of Figures

List of Tables

List of Acronyms/Abbreviations

BS	Base Station
CDMA	Time-division Multiple Access
CH	Cluster Head
CIA	confidentiality Integrity Availability
CPU	Central Processing Unit
CSMA	Carrier Sense Multiple Access
CWSN	Clustered Wireless Sensor Network
DDoS	Distributed Denial of Service
DoS	Denial of Service
HIDS	Host-based Intrusion Detection System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
LEACH	Low Energy Adaptive Clustering Hierarchy
MAC	Media Access Control
MANET	Mobile Ad-hoc Network
NIDS	Network-based Intrusion Detection System
NN	Neural Network
OSI	Open Systems Interconnection
QoS	Quality of Service
RNN	Random Neural Network
SN	Sensor Node
SVM	Support Vector Machine
WSN	Wireless Sensor Network
WSN-DS	Wireless Sensor Network Dataset

Chapter 1

Introduction

Wireless sensor network (WSN) are collection of number of sensor nodes having the property of auto-configuration and self-organization. Network architecture follows decentralization and is distributed in nature. WSN has a number of application in the areas of environmental monitoring like air, water and soil, structural monitoring, human activity, and behavioral monitoring, military surveillance, asset tracking and many more [1]. The advantage of WSN nodes is their small size and these can be placed at some place where surveillance by a wired network or human is not possible. These small nodes are deployed in thousands in number to monitor temperature, pressure etc. These nodes are always prone to physical damage because these are deployed in the open environment which is not protected. Self-organizing and auto-configuration in nature, limited battery, computation power, and bandwidth, distributed and decentralization, multihop communication in wireless medium, are some characteristics which may lead to exposing this network to many security attacks in all OSI model layers. To detect an inside attack intrusion detection system is introduced which can deal with wide range attacks in WSN.

Security attack in WSN is either active or passive. In passive attack attacker generally, hide and collects data by tapping communication link but does not modify it. Traffic analysis, malfunctioning of a node, eavesdropping comes under passive attack. The active attack affects the operation of the network. An active attack can lead to termination or degradation in networking services. Denial-of-service (DoS, DDos), network jamming, wormhole, blackhole, sinkhole attacks are grouped in active attacks [2]. Solutions to these attacks (active or passive) in any network involves prevention, detection, and mitigation [3]. In prevention step, the technique provides defense mechanism against attack i.e. it prevents the attack. Detection step comes into action when an attacker has found a way to pass prevention technique. This

involves to detect or identify the node which has been attacked and compromised (being aware of the presence of attack). Mitigation aims to remove the attack detected in the detection step by taking action against the compromised node.

IDS functionality is defined by the detection method which are mainly of two types - Anomaly-based, misuse-based. Anomaly-based technique tries to finds the deviation from normal behavior. To flag operation as an anomaly, the regular observation of system must be there to accommodate system changes. Misuse-based technique tries to detect previously known attack with high detection rate by comparing the new attack signature with known signatures.

1.1 Wireless Sensor Netowrk

Sensor nodes of WSN have capabilities to self-organize and auto-configure to create a network which can serve the purpose. WSN has several features like self-organization and auto-configuration in nature, distributed and decentralization, multi-hop communication etc. The first wireless network of sensors was used and created by US military to detect submarines of Soviet in 1950. From that time till now WSNs are used in various military to civil applications. Each sensor node consists of 5 main components - Sensing hardware, Transceiver, Micro-controller/CPU, Memory unit, Battery which supplies power to every unit. WSN are application specific so, different types of WSNs are used for different domain of application [4] as shown in Table 1.1.

1.2 Attacks in WSN

WSNs are vulnerable to many attacks because of wireless multihop communication medium, decentralization, deployment in unprotected environment. Any attempt that tries to affect confidentiality, integrity and availability (CIA - Model) is defined as attack. Confidentiality ensures that only intended receiver has received message sent by sender and there is no unauthorized monitoring of message. Integrity ensures that message is not modified or altered. Availability ensures that when data is requested it is made available by source without much delay. It must consume less time in

Table 1.1: Types of WSN.

WSN Type	Deployment	Cost	Challenge
Terrestrial	Structured or unstructured	Cheap	Management of hundreds and thousands of nodes
Underground	Structured	Expensive in node deployment and maintenance	Difficult to recharge battery, high attenuation and signal loss
Underwater	Structured or unstructured	Expensive in node deployment and maintenance	Communication - long propagation delay, sensor failure, Energy conservation
Multimedia	Structured or Unstructured	Low cost sensor nodes	high energy, bandwidth required with significant computation power
Mobile	Can move on their own	Expensive	Localization of nodes

response. There are different threat model of attack in WSN [5]:

- **Mote-class vs Laptop-class Attack** When the attack is on few sensor nodes inside WSN it is a mote-class attack and if the attack is done using a more powerful device, i.e. intense attack then it is a laptop-class attack.
- **Active Attack vs Passive Attack** An active attack is also known as a direct attack because it modifies the data being transferred between two nodes. Passive attack referred as less powerful, silent in nature than active attack. It is only used to collect information without modifying it. These attacks do not harm resources.
- **Internal vs External Attack** These attacks are classified based on the domain of nodes as if the intruder node belongs to the network itself then it is an internal attack otherwise it is an external attack.

There are mainly 2 types of attacks [6]- Active attack and Passive attack. Passive attacks are the attacks which are difficult to detect as compromised node in passive attack do not alter data. Passive attacks are only used for traffic monitoring or traffic analysis and do not harm the system. Passive attacks are big threat to confidentiality. Main emphasis in passive attack is to prevent attack rather than detection. Active attacks tries to modify and change the data transmitted on the network and always

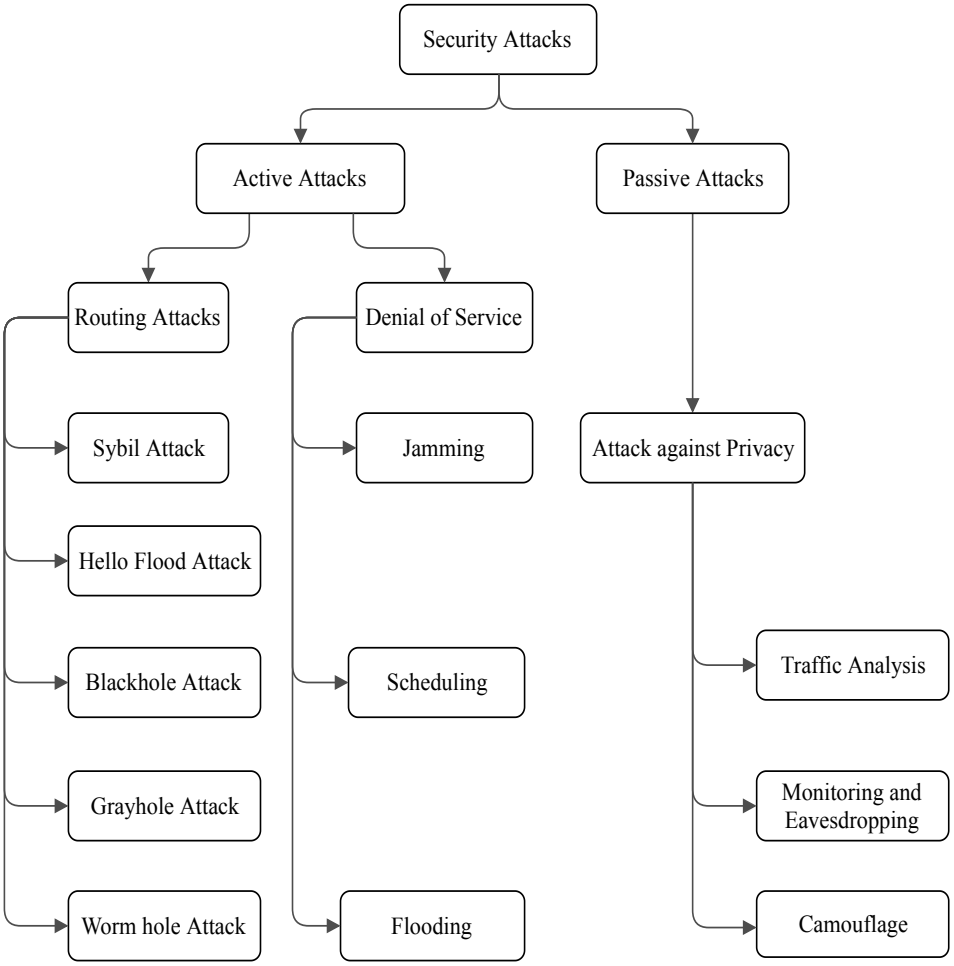

Figure 1.1: Attacks in WSN.

damages the system. Active attacks are threat to integrity and availability. Main emphasis in active attack is to detect attack. These attacks are found in the form of fabrication (e.g. Denial of Service -DoS attack), interruption (e.g. Masquerade attack), modification (e.g. replay attack). Different type of attacks (active and passive attacks) in WSN are classified in Figure 1.1 [7–9] -

i. **Wormhole Attack or Tunneling Attack** [9] Attacker tries to create a low latency link between two or more nodes which have better communication resources. These nodes can establish tunnels to communicate and data packets are tunnelled. This attack can change the network topology, can destruct packet, can change message stream by copying the packet at one place. After that, it rematches the same packet at different positions.

ii. **Sinkhole Attack** [10] In sinkhole attack, the compromised node advertises fake routing to attract network traffic from neighboring nodes. Sinkhole attack is

carried out by advertising fake high energy quality route to base station (BS). It is very likely that neighboring node to this compromised node will forward their data packets to this node which are destined to BS. Also, this attack can be used to trigger other attacks like selective forwarding attack.

iii. **Blackhole Attack** [11] Blackhole attack is carried out by reprogramming of some of network nodes such that these network do not forward data packets, according to routing algorithm, which are received. All data in this black hole region will be lost and it will cause delay and low throughput. This attack is hardly prevented because it shows original route information. This attack can be considered as denial-of-service attack.

iv. **Traffic Analysis** [12] Traffic analysis is the process of examining data packet transfer from one sensor node to another node to extract information from the patterns. Attacker can find the location of BS by traffic analysis. Data in WSN routed from sensing nodes to BS via multihop communication follows same path until topology changes. By analyzing these traffic patterns location of BS can be found easily. Attacker once find the location, can directly attack BS.

v. **Denial-of-Service (DoS or Distributed DoS)** [13] DoS attack is an attack in which the resource become so busy that it is unavailable to intended users. It stops a service from functioning efficiently, for e.g. internet site takes too long to respond in case of DoS attack. DoS attack aims networks bandwidth and connectivity so there is disruption in services of network. It directly affects the performance of the system. There are number of techniques available to prevent DoS attack which are mainly based on artificial intelligence, game theory, soft computing etc.

vi. **Replay Attack** [14] It is a security failure in which firstly unauthorized information is stored and then it is re-transmitted to the receiver which can lead to duplicate transaction, false authentication, and many other unauthorized operations. Replay attack can be used as preliminary attack to many other DoS attack, by continuously observing and replaying the message exchange between two entities. Man-in-the-middle attack is a famous replay attack.

vii. **Jamming Attack** [15] Jamming attack targets the physical layer of the network and it can damage the whole network because the physical layer provides modulation, encryption, and many other important functions. Jamming in WSN carried out by interfering with the radio frequencies that are used by network for communication. It can be viewed as special type of DoS attack.

viii. **Sybil Attack** [16] Sybil attack is threat to integrity of network as compromised node in this attack tries to forge many fake identities to change network protocols. This lead to believe that a genuine node has many neighbor. It is an internal, passive attack. When a system is hijacked and it starts claiming for multiple identities then its a case of sybil attack. This attack is generally found in a distributed peer to peer network.

ix. **Selective forwarding attack** [17] It is a type of blackhole attack, as it is also related to the dropping of the data packet. It is carried out by internal nodes by drop data packets, selectively. If all packets are dropped by a node then it is a blackhole attack. This attack is difficult to detect as there is always some data packet loss in WSN due to unreliability.

x. **Scheduling attack** [18] It is a type of DoS attack Which mainly occurs in setup phase of LEACH protocol. At the time of time-slot allotment to member nodes by cluster head (CH), attacker node acting as CH will allocate same time slot to many member nodes to send the data which will cause data collision.

xi. **Flooding attack** [18] Flooding attack is carried out in LEACH protocol when compromised node sends large number of CH advertisement message with high energy. This will waste a lot of time to decide CH. Also, energy of the sensor nodes will be wasted in receiving these many number of messages.

1.2.1 Attacks on Different Layers of OSI Model

WSN network architecture mainly follows OSI model. This section presents possible attacks on each layer [19]. Physical layer and Data-link layers are mainly compromised by using passive attacks. Physical layer is attacked by jamming, interceptions and eavesdropping attacks where data link layer is attacked by traffic analysis, traffic

monitoring. Black hole, Sink hole and Wormhole attacks are used to attack network layer to affect resources and network performance actively. Flooding and network consumption are also attacks found in network layer. Transport layer finds difficulties in data corruption and repudiation where transport layer is attacked by session hijacking. There are some attacks in WSN which can affect more than one layer of OSI architecture. Dos, Replay are multilayer attacks.

1.3 Limitations and Challenges of WSN

Sensor nodes in WSN collects data using their sensing hardware, compute or process this data using CPU, communicate with other nodes. This data is being further processed at CH and then forwarded to BS. WSN provides efficient and low cost solutions to bridge the gap between real world and electronic world. However, WSN should be able to manage and configure itself as there is no human intervention after node deployment. WSN nodes have limitation in their storage capacity, processing power, battery power due to which these network have certain limitations and faces several issues [20].

i. **Security** WSN nodes can be deployed where surveillance using wired network or human is not possible. Also, these nodes are deployed in hostile unprotected environment where security of data is a big concern. Security is a broad term can be classified to confidentiality, integrity and availability of data. To make sure authenticity of network various cryptographic and secure mechanism have been introduced that can provide security up to some extent for outsider attacks. Data should not be altered or changed as it plays important role to maintain integrity. If there is a compromised node inside the network then it should be detected and all other nodes must have information about this compromised node. To do this, one needs to install IDS.

ii. **Energy** Sensor nodes consumes energy in every operation like sensing, processing data, communication, etc. Power source of a sensor node is a battery which is very tough to be recharged or replaced due to geographic conditions and critical application environment. So, efficient use of power source is essential in order to ensure that sensor node is alive for further operations. Mainly, energy

is consumed in sensing transducer, analog to digital converter, computing unit, transmission and receiver energy. To conserve energy some of the sensing nodes need to be idle/sleep mode. Clustering of sensors can also be applied in order to conserve energy.

iii. **Routing Protocol** Routing protocols in WSN are different from routing protocols of MANET because WSNs are data-centric, unique identification number can not be assigned to sensor nodes as assigned in MANET because sensor nodes are very large in number, requirement of sensor network is application specific. To conserve energy aggregation of data is desired. Design of routing protocol must support ad-hoc node deployment to form connection between two randomly deployed nodes. Protocol must use limited energy and computation power without losing accuracy.

iv. **Data Collection and Transmission** Sensor nodes performs data gathering task which includes periodic data collection by sensing environment, process data and then transmit it to BS or sink node. In data gathering process redundant data must not be processed more than once because it will consume energy. To save energy clustering routing algorithms can be applied so low energy nodes will transmit data to high energy nodes where all processing of data will take place before sending to base station.

v. **Quality of Service (QoS)** QoS is a measure of the level of service provided by network. WSN are used in real-time and critical application so desired quality service is very important. Change in network topology makes it difficult to achieve desired level of QoS. These mechanisms to provide QoS, must be aware of the fact that WSN data is aggregated and processed at various nodes and there is unbalanced traffic in the network. Scalability in WSN must not have any effect on QoS. Sometimes it is possible that network uses more energy to provide desired level of QoS.

vi. **Limited storage and processing power** Sensor nodes have limited amount of memory to store any code or data. Any security, QoS mechanism must have limited code that can be stored in nodes memory. WSN supports in-network

processing with limited CPU power. Reduction in communication cost can be done by avoiding processing of redundant data.

Furthermore, finding locations of each sensor node in the network is a key challenge known as Localization problem. Localization process is mainly divided into two steps-target/source localization node self-localization. WSN architecture needs secure and energy efficient routing algorithms with good QoS. Addition or removal of sensor nodes in network must not affect its performance that is scalability with QoS. MAC layer issues, operating system, network architecture, node deployment, decentralized management, fault tolerance, robustness, heterogeneity, real time operation, data aggregation and data dissemination are some issues that are to be considered while designing or deploying any WSN.

1.4 Applications of WSN

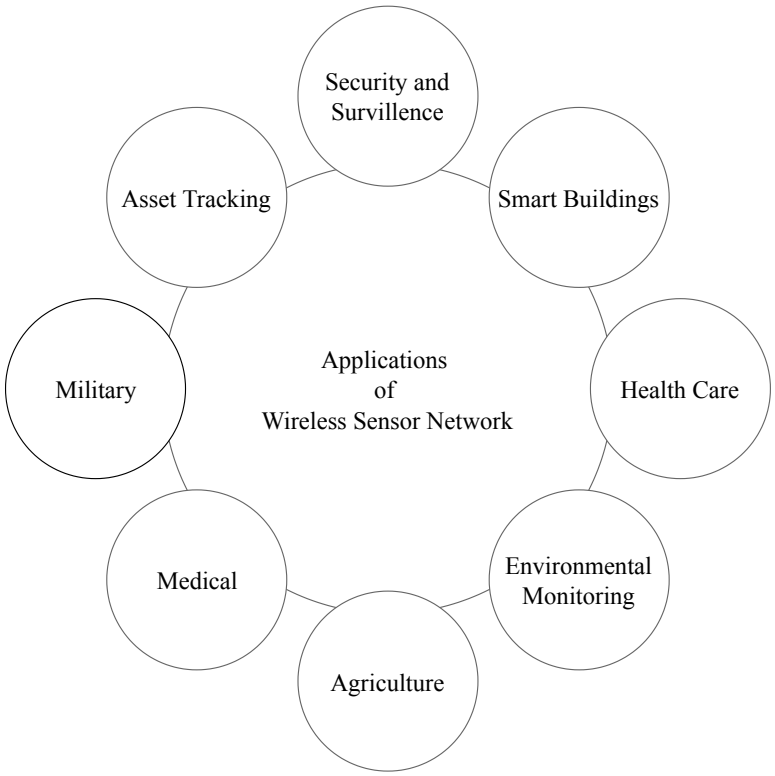

Figure 1.2: Applications of WSN.

WSNs are built using radio transceiver, sensing hardware, micro-controller, memory unit and battery. This sensor nodes senses data from surrounding and then this data is transmitted to main BS after processing. Features of WSNs like, mobility, fault tolerance, heterogeneity, auto-configuration, self-management, scalability etc are the reason of wide application range of WSN. Main application domains [21] of WSN are shown in Figure 1.2.

In agriculture, temperature and pressure with healthy environment is measured using WSN for better crop. Monitoring of environment helps to predict weather, monitoring of old buildings, bridges helps to avoid any accident. Asset tracking helps in finding the location of asset, vehicle tracking helps in smart parking and to avoid congestion. In military, surveillance of enemy helps to plan perfectly.

1.5 Motivation

Application domain of WSN is very wide in the fields of medical to military and data plays very important role in every field. Intrusion is any activity in a network, which is not authorized and affects network's services, resources or data either passively or actively. Such activity if not prevented in the first line of defense in WSN security then IDS comes into play as the second line of defense. The network member nodes detects any suspicious behavior to detect intrusion. After detection, it cannot take action on it but it raises an alarm to the controller. IDS provides information to the controller about intruder information (identification of node or region, location, time and date of intrusion, an activity of intrusion, type of intrusion, etc). This information is used in the third line of defense i.e. in mitigating the attack.

1.6 Problem Statement and Objectives

In order to provide protection to WSNs many solutions such as cryptographic and secure routing, key exchange and authentication are proposed. These methods are used to provide security from outside attack up to some level but these cannot eliminate all security attacks. To detect an inside attack IDS is introduced which can deal with wide range of attacks in WSN. Main motive of this research is to design an IDS which

can deal with intrusion attacks efficiently. Main focus in this research has been on high detection rate and low false positive rate.

1.7 Organization of Dissertation

The dissertation is structured in chapters. Chapters are organization as follows:
Chapter 1 starts with brief introduction about WSN and IDS. Going forward, it gives a detailed overview of WSN followed by attacks in WSN. Various security attacks in wireless sensor network like DoS attack, replay attack, traffic analysis, blackhole, wormhole, sinkhole attacks etc has been discussed. Also, it is shown that which type of attack may occur on which layer of the OSI model. Different classes and types of attack are discussed in great detail. Then limitations and challenges faced by WSN are discussed. After that, brief introduction to applications of WSN is provided. This chapter ends with motivation for this research work, problem statement and objectives of this research.

Chapter 2 provides a detailed description of IDS. This chapter starts with introduction of IDS and it's components. After that, classification of IDS based on detection method, source of data etc. is discussed in great detail. Later in the chapter literature survey of various IDS is discussed. Various approaches of detection are discussed which are based on different fields like Neural network, support vector machine, cluster-based approaches etc. A tabular comparison of some detection techniques is also presented in this chapter which includes limitations and features of particular approach. Chapter ends with summary of limitations faced in current IDS.

Chapter 3 is focused on the proposed system for attack detection. It starts with the system model of proposed approach followed by dataset description used for training purpose. After that, proposed approach of neural network model is discussed. A systematic flow chart of algorithm is also discussed in this chapter. Steps of detection model are described in procedure section. This chapter ends with summary of proposed system.

Chapter 4 presents results of research work. It starts with discussing the simulation environment briefly followed by 3 comparison graphs of WSN energy model. After that, this chapter presents the 2 accuracy graphs of neural network model.

Chapter 5 concludes the dissertation. Conclusion explains the main findings and limitation of this research work with scope of future work.

Chapter 2

Background and Literature Review

The computer systems and the networks of these systems are increasing day by day and security of data share by these networks is being an issue over the years. Security techniques of classical networks cannot be applied here because WSN has certain limitations of resources like energy, memory, CPU, etc. Security mechanism of network must be able to ensure confidentiality, integrity, availability and authenticity.

2.1 Intrusion and Intrusion Detection

An intrusion in any system is an attempt to unauthorized access of system's data or resources. This unauthorized access can be limited to only monitoring and analyzing traffic patterns or it can be an attempt to modify or alter the data packets. Try to make resources busy and unavailable for the intended authorized access is also an intrusion attack. An IDS basically monitors and analyzes the network traffic for any suspicious activity by any of the network node. IDS tries to analyze network behavior and monitors user activity. IDS comes under passive defence category as these system tries to detect intrusion attack rather than preventing attack. These systems can only capable of reporting and alarming to administration to take some action. An IDS which can also take some required action to prevent the attack on its own, is known is Intrusion prevention System (IPS). An IDS is a tool which either installed at network strategic points or at each host to detect any suspicious or malicious behavior. If any such behavior is found which can harm the system nodes or system's activity it notifies to the concerned authority. An IPS can perform all tasks of IDS, in addition to that it can also take desired action on its own to prevent the attack. An ideal IDS tries to minimize false positive rate with high detection rate. Also less energy consumption and faster computation or attack detection is desired feature of IDS. Main components of any IDS are shown in Figure 2.1 [22] are:

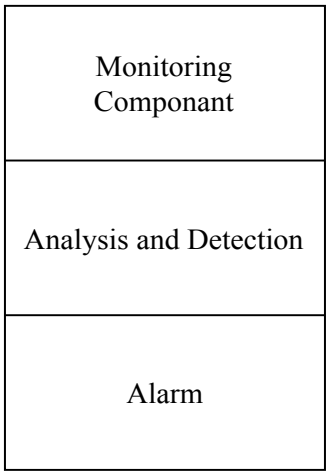

Figure 2.1: Components of IDS.

i. **Monitoring** This component mainly monitors traffic in the network, availability of resources. Events at each node, network congestion, packet delay, neighbor monitoring is also done by monitoring component.

ii. **Analysis and Detection** This module of IDS implements the detection method for intrusion. It is the main component in the IDS where all monitored traffic patterns, events are analyzed to make decision regarding maliciousness of a node.

iii. **Alarm** Alarm component is responsible for generating responses as alarm to administration if a malicious activity is detected.

Mainly there are two types of IDS- Rule-based (signature-based) IDS and Anomaly-Based IDS [23]. Rule-based IDS can detect previously known attacks with high precision because it takes help of built-in signatures. A rule-based technique was developed [24] which compares the incoming information with known information. But the problem was that signature-based IDS cannot detect a new attack because its signature is not present. Anomaly-based IDS detects intrusion by monitoring statistical behavioral, can detect the new attack as well as common attacks having more false positive rates i.e. normal packet declared as abnormal. One particular method of threshold was developed to detect the new attacks [25]. Also, there can be multiple anomaly attacks or some attacks which are consisting of both the attacks, can be detected using Hybrid IDS (HIDS) [26]. In HIDS, anomaly-based IDS is used as a filter and another one is used as the second level of IDS.

In [27], A. Mehmood et al., provided that knowledge-based IDS (KB-IDS) can be applied on cluster-based WSN in order to secure the network. Their method keeps a record of networks internal nodes behavior. They placed knowledge base at the base station and inference engines were used by CHs to access the knowledge base. Because of the continuous monitoring of nodes they were able to sense any potential threat and generate events against them to tackle the attack. This information goes to the BS through the inference engine. The BS concludes and reports back to the CH for the suspicious node.

In [28], HIDS on Cluster-based WSN (CWSN) is discussed. CH collects the data from other sensor nodes in that cluster and aggregates it because CH has the higher capability. In this paper it they used 3 models - anomaly detection, misuse detection with decision-making model. First two models were able to detect intrusion from a large number of packets and then results from these two models were combined by decision-making model i.e. if an intrusion has occurred then this model will classify its type. This model then will inform to the administrator about the attack with details.

In [29], three different individual intrusion detection systems were proposed for the heterogeneous wireless sensor network. An IDS was designed each for the CH, SN and BS. The capability of IDS was depending upon the attack on a particular node. For sink node, IDS has the learning capabilities which helps network to deal with unknown attacks. For CH node, a host-based IDS was proposed without learning capability. This helps the network to detect known attacks and avoid resource wasting, efficiently. To detect and update the class of attack it uses a feedback mechanism. A simple and fast misuse IDS was proposed for SNs.

In [30], an intrusion detection system is discussed which uses Energy trust in WSN. This method specifically focuses on detecting hybrid DoS attack using effective node energy analysis. This method predicts energy consumption and correlates it with the security of nodes. The method assumes that a sensor node can monitor their own energy level and consumption. It also faces a problem when a node is being under attack by flooding then enemy may try to control the node which can show fake energy information.

In [31], KMP Pattern matching technique was used to detect an intruder. In this,

after receiving a pattern, a pattern matching linear time algorithm is used. When features are matched, accordingly a rule is applied to the data packet. Then it calls a plug-in, which is used to find the intrusion. If there is no problem and received packet found to be with the correct pattern then it is forwarded to its neighbors. If a suspicious pattern is detected then it performs three functions namely, alert(): to give warning, logto(): to put information of intrusion in the database table, and trace instruction to trace out the intruder.

In [32], IDS based on improved AdaBoost- Radial basis function in Support vector machine is discussed. This system can detect and resist against DoS attack effectively. This system uses RBF-SVM as AdaBoost classifier by training. The IABRBFSVM algorithm is proposed by using the influence of parameter and model training error e on AdaBoost weights. Significantly improves network performance and lifetime, with short computation time and higher detection rate.

In [33], the intrusion detection method is discussed for cluster WSN, which uses trust values and multi-agent framework functioning. Trust value calculation and accuracy are calculated by Mahalanobis distance. Reduction in false positive rate is done by calculating tolerance factor in trust value calculation. This system was scalable as it uses a multi-agent framework. The proposed system was fault tolerant and can detect multiple attacks at the same time with a high detection rate.

In [34], anomaly-based IDS was proposed to detect new attacks, initially. Then, in order to understand routing in WSN for intrusion detection, they found a set of features. These features can be applied to all protocols. This IDS was able to detect main attacks in WSN but active sinkhole attacks can be detected effectively. Also, this method consumes less power as it does not require communication between nodes.

In [35], an IDS for cluster-based WSN is discussed. This IDS has different detection frameworks for different levels. The first framework runs at IDS agent at a low level, which is a specification based protocol. The second framework runs at the head node of the cluster (CH, medium level), which is a binary classification protocol. Also, to check trust level of cluster members (agents) a reputation protocol is used by CH. At Base station (higher level) a voting mechanism is applied which is used by CH to monitor its CH neighbors. This system was able to detect blackhole, wormhole, flooding, and selective forwarding attacks. The detection rate was almost 100%.

Time, energy consumed to detect was very low.

In [36], an IDS was proposed with an evolving mechanism to extract rules which are used for intrusion detection. Diversity and quantity of rule sets were controlled by measuring the distance between the rules of same class and different class.

2.2 IDS - Features and Limitations

Every IDS has certain features like ability to tune to specific attack, helps to meet security regulations, increases efficiency etc and limitations like no prevention of attack, no processing for encrypted data, false positive rate etc. Table 2.1 presents summary of specific features and limitations of research work done in this field. It includes work done in different areas in the field of IDS like Neural Network, Clustering, SVM, Multi-agent trust based schemes.

Table 2.1: Study of various intrusion detection systems.

S.N.	**Proposed System**	**Method**	**Features**	**Limitations**
1.	A. Mehmood et al. [27]	Cluster-based IDS, uses knowledge base for storing patterns, inference engine.	SN monitors traffic and send observed events to CH which is further forwarded to BS where action against malicious node is taken.	Heavy load on SN inside the cluster, faster battery drainage for CH.
2.	S. S. Wang et al. [29]	3 different IDS for heterogeneous WSN- For sink node, IDS has the learning capabilities, For CH node, a Host based IDS, misuse IDS for SNs.	Can detect known, unknown attacks, avoids resource wasting, uses feedback mechanism.	Consumes high energy as it uses learning and feedback mechanism.

Table 2.1 Continued from previous page

S.N.	Proposed System	Method	Features	Limitations
3.	D. Jianjian et al. [32]	Improved AdaBoost-Radial basis function in Support Vector Machine.	Detects DoS attack efficiently, improves network performance, short computation, high detection rate.	Only Focused on DoS attack, can;t detect multiple attacks.
4.	X. Jin et al. [33]	Uses trust values and multi-agent framework functioning, uses Mahalanobis distance.	Reduction in false positive rate, scalable system, fault tolerant, can detect multiple attacks at the same time.	Trust value calculation and accuracy are calculated by Mahalanobis distance.
5.	H. Sedjelmaci et al. [35]	3 different detection frameworks- specification based, binary classification protocol, vote mechanism.	Detection rate was almost 100%. Time, energy consumed to detect was very low.	System was able to detect only black hole, wormhole, flooding and selective forwarding attacks.
6.	A. Saeed et al. [37]	Uses Random Neural Network, without any dedicated hardware.	Very effective in low-power WSN, detects any performance degradation anomaly attack, can also detect previously unknown attacks.	Computation time, energy consumption was high as compared to others at the cost of accuracy.

Table 2.1 Continued from previous page

S.N.	Proposed System	Method	Features	Limitations
7.	W. Meng et al. [38]	K-nearest neighbor (KNN) algorithm with filtering. Built with three components.	Resolves issues of network packet overload, false alarm rate. Provides efficient signature matching.	Expensive in terms of time for computation.
8.	G. Gowrisona et al. [39]	Uses Neural Network with KDD Cup99 data.	An adaptive method with higher detection accuracy. Detects DoS attacks with enhanced rules by learning. Efficient computational complexity of O(n).	No knowledge management system, implementation has to be in cloud-based environment.

2.3 Classification of IDS

IDS classification has two broad categories - Signature-based and Anomaly-based, which are based on intrusion detection strategy. IDS can also be classified based on the location of data in two categories - Host-based and Network-based. More classification categories are shown in Figure 2.2 [22, 40] are described below.

2.3.1 Detection Method

IDS functionality is defined by the detection method. It describes how a detection system will behave in order to detect any malicious activity in the network. Research field in WSN mainly focuses on these following detection methods.

- **Anomaly-based** Anomaly-based IDS uses heuristic approaches to classify network activities as malicious or normal. This detection method finds the devi-

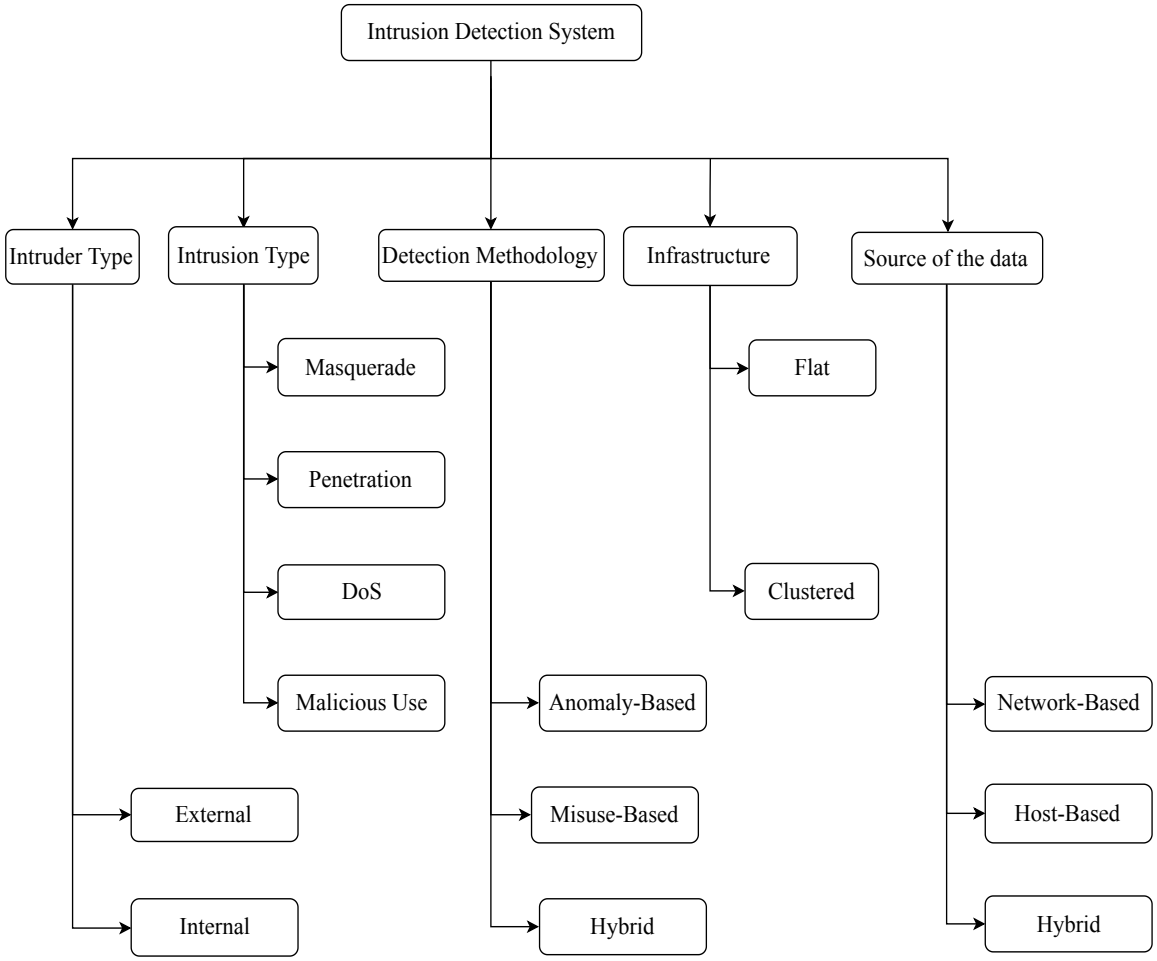

Figure 2.2: Classification of IDS.

ation from normal behavior and uses threshold value to classify attacks. To flag operation as an anomaly, the regular observation of system must be there to accommodate system changes. This may lead to performance overhead. It sometimes fail to detect well-known attack but works well in case of unknown attacks. In [4] an IDS is proposed which is capable of learning and detecting new attacks using unsupervised neural network. Anomaly-based identification can be factual based, information based or AI based.

- **Misuse-based (Signature or Rule-based)** In this detection method predefined rules are already there against attacks to tackle them. Using this method one can detect previously known attack with high detection rate by comparing the new attack signature with known signatures and predefined rules. If there is a new attack, signature-based detection would not be able to compare with any reference signature (profile) hence this attack wont be detected. In [41, 42],

a signature based IDS is presented. Every node has IDS so it is host based IDS. The architecture design for [41] is such that it detects data-packet drop and false routing attack and [42] is designed to detect only sinkhole attack.

- **Hybrid IDS** These systems uses the combination of anomaly-based and misuse-based detection to detect new attacks using learning algorithms and to detect well-known attacks, respectively. Hybrid systems are increasingly productive regarding detection rate with low false positive rate. Also, these system uses high computation and hence results in more energy consumption. A hybrid IDS is proposed in [43] which uses distributive algorithm to train support vector machine (SVM) and create misuse detection model.

2.3.2 Source of Data

IDS can be classified in 3 categories based upon the location of the data. It describes the location of the data where it is monitored. Data can be monitored on individual nodes or on the strategic point of network.

- **Network-Based** NIDS are deployed at strategic points so that it can monitor the packets transmission in network that is coming and going out to all network devices. This monitoring of data is then analyzed and compared with the signatures of known attacks. It is easy to deploy on the network boundary with low cost where it can monitor all traffic.

- **Host-Based** HIDS is implemented on individual host systems in the network and monitors all incoming and outgoing traffic instead of the whole network. HIDS is more helpful if the malicious node is inside the network.

- **Hybrid IDS** It uses mobile agents to efficiently use a combination of NIDS and HIDS. Performance of hybrid IDS of better in terms of detection rate compared to NIDS and HIDS but hybrid system consumes more energy in detection process.

2.3.3 Intruder Type

IDS classification based on an intruder node can be of two types - internal and external. It describe the location of the compromised node. In external intruder, attacker or compromised node is not present in the network whereas in case of internal intruder, it is present in the network. Internal intruder further can be classified as selfish node and malicious node in the way in which they affect the network's operation. Selfish node uses the network to forward own data packets, saves battery life for own operations, no cooperation in data forwarding, no direct damage to other nodes. On the other hand, malicious node damages other nodes, not focused on saving own battery life, tries to damage network services.

2.3.4 Intrusion Type

It describes a way of attack in which system is compromised. In masquerade attack, attacker uses fake identity to gain unauthorized access. Penetration is an attempt to unauthorized access by breaching networks security. In DoS attack, attacker node tries to extra use of network resource so authenticated users cant access resources. Malicious use of resources is an attack on network resource.

2.3.5 Infrastructure Type

IDS can be classified into 2 groups based on network infrastructure - Flat and Clustered. In flat infrastructure, all nodes can participate in all networking activities because it is assumed that all the nodes in the network have equal capabilities. In clustered, nodes are grouped which is known as clusters and each group is assigned a head known as CH.

2.4 Summary

This chapter discusses about big threat to sensor netwaork i.e. intrusion and its detection. Various detection techniques involving neural networks, fuzzy logic, trust values have been discussed. Features and limitations of certain detection mechanism have also been enlisted in tabuler form. Major limitations in detection for current

systems is that there is always a trade-off between accuracy and real-time performance. One detection method cannot detect all the intrusions because of new attacks are being introduced as time is progressing. Also, resource usage limitations makes is more difficult. To design an ideal IDS, which is capable of detecting all attacks with high accuracy and with limites resource use, will always be an challenge in this domain of research.

Chapter 3

Proposed System

3.1 Introduction

Earlier in Section 1.2, different categories of attack in WSN and how these attacks affect the networks's performance, resources of network has already been discussed. Effect on performance of network demands these attacks to be detected efficiently so that some sort of necessary action can be taken to remove malicious node or activity from the network. Hence, for the normal operation and services of network detection of intrusion attack is required. This proposed work uses a dataset of WSN built on top of LEACH. This dataset is used to feed in neural network learning procedure.

3.2 System Model

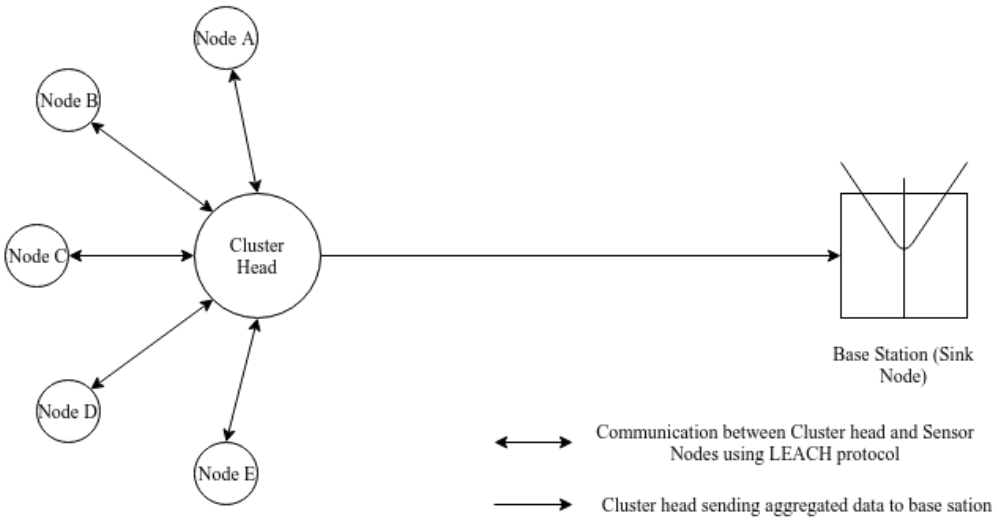

Figure 3.1: System model for dataset.

This section presents the system model which is used in dataset. It is basically a model of LEACH-clustering routing algorithm. Figure 3.1 describes how data from each sensor node is sent to CH. CH processes data and after performing data aggregation it further sends it to BS.

3.3 Dataset

WSN-DS [44] dataset used in this approach helps in classification and detection of attack. This dataset consists of LEACH-clustering protocol normal activities with attacks of like blackhole, grayhole, scheduling, and flooding. These attacks are implemented on top of LEACH protocol.

To build the dataset it was required that each sensor node must monitor it's neighbor. Distribution of load and number of neighbor sensor nodes to monitor was a challenge which was taken care by many experiments. In the beginning of data collection, each node broadcasts *Hello* message. After it, each node starts monitoring some nodes (5 nodes - result from experiments) from which it has received broadcast message. Then each node sends all details to it's CH which is further sent to BS at the end of each round. Dataset built with this procedure has 19 features which can help to know maliciousness of a node. These attributes are shown in Table 3.1.

Table 3.1: WSN-DS description.

S.N.	Attribute	Detail
1.	Node ID	A unique ID for every node. E.g. 002 001 042 presents node number 42 in first round and second stage
2.	Time	Current time
3.	Is_CH	Node is cluster head? (Flag - 0 or 1)
4.	who_CH	Cluster head ID
5.	Dist_to_CH	distance b/w node and cluster head
6.	ADV_S	no. of advertisement message broadcast to nodes by cluster head

7.	ADV_R	no. of advertisement message received by nodes from cluster head
8.	JOIN_S	no. of join request message sent to cluster head by nodes
9.	JOIN_R	no. of join request message received by cluster head from nodes
10.	SCH_S	no. of TDMA schedule message sent to nodes by cluster head
11.	SCH_R	no. of TDMA schedule message received by nodes from cluster head
12.	Rank	node ordering in TDMA schedule message
13.	DATA_S	no. of data packets sent to cluster head from sensor node
14.	DATA_R	no. of data packets received by cluster head from sensor node
15.	Data_Sent_To_BS	no. of data packets sent to BS by CH
16.	dist_CH_To_BS	distance b/w CH and BS
17.	send_code	cluster sending code
18.	Consumed energy	energy consumed
19.	Attack Type	Type of sensor node - blackhole, grayhole, scheduling, flooding or normal

3.4 Proposed Approach

This section describes how proposed system works. Basically, to simulate the attack environment, energy model of leach is implemented with attacks of like blackhole attack on top of leach which is described in section 3.4.1. Also, by using this WSN-DS dataset an Neural Network classifier is also trained to classify attack models which is presented in section 3.4.2. Cumulatively, this approach can be referred as signature-based (rule-based or misuse) IDS.

3.4.1 LEACH

Wireless sensor network has some limitations described in section 1.3, like limited battery power. So, energy needs to be utilized efficiently in multihop wireless communication to minimize dead nodes, while network remains operational. To maintain continuous network services chosen communication protocol has to be energy efficient. The dataset WSN-DS was also created using such protocol Low Energy Adaptive Clustering Hierarchy (LEACH).

LEACH [45] is an adaptive protocol which uses clustering of sensor node and distributes energy load equally in all nodes of cluster. This routing algorithm works in two phases as shown in Figure 3.2. Phase 1 is Setup-phase where election of CH, joining of member node in clusters, and TDMA time slots allotted to each member node by CH. In phase 2 which is steady-state phase, member nodes sends their data to CH in their allotted time slot. LEACH also involves data aggregation at CH, aggregated data is then sent to BS.

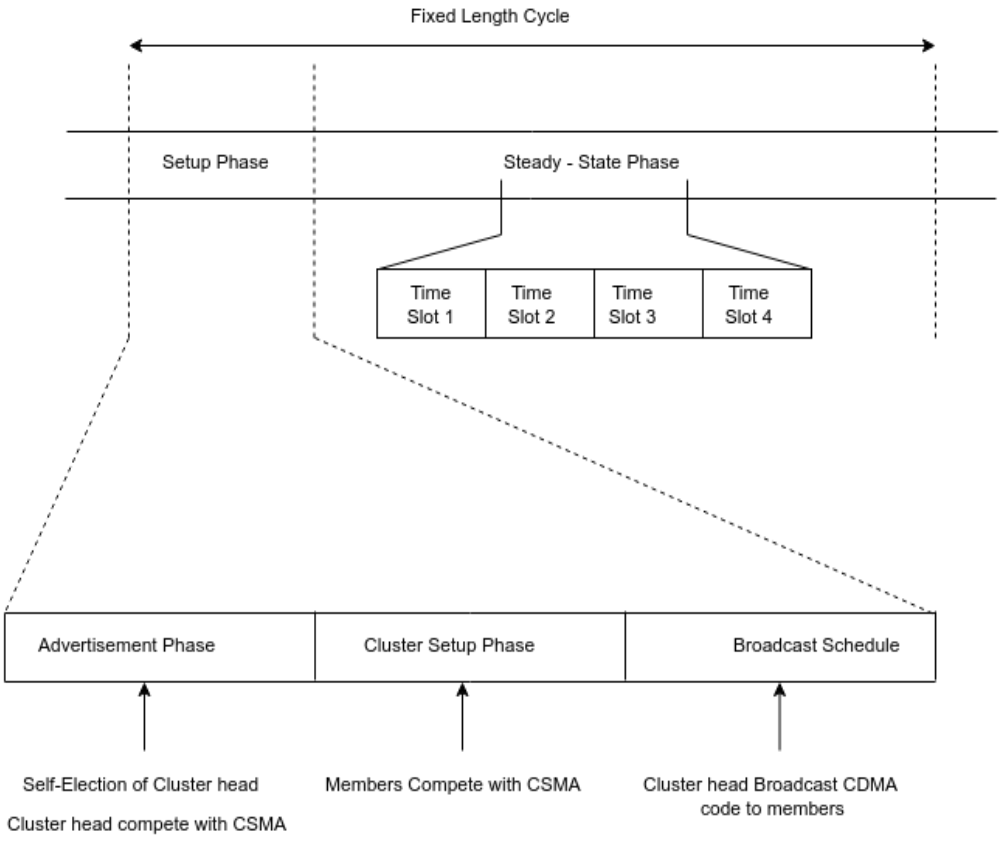

Figure 3.2: LEACH-phases.

3.4.2 Neural Network

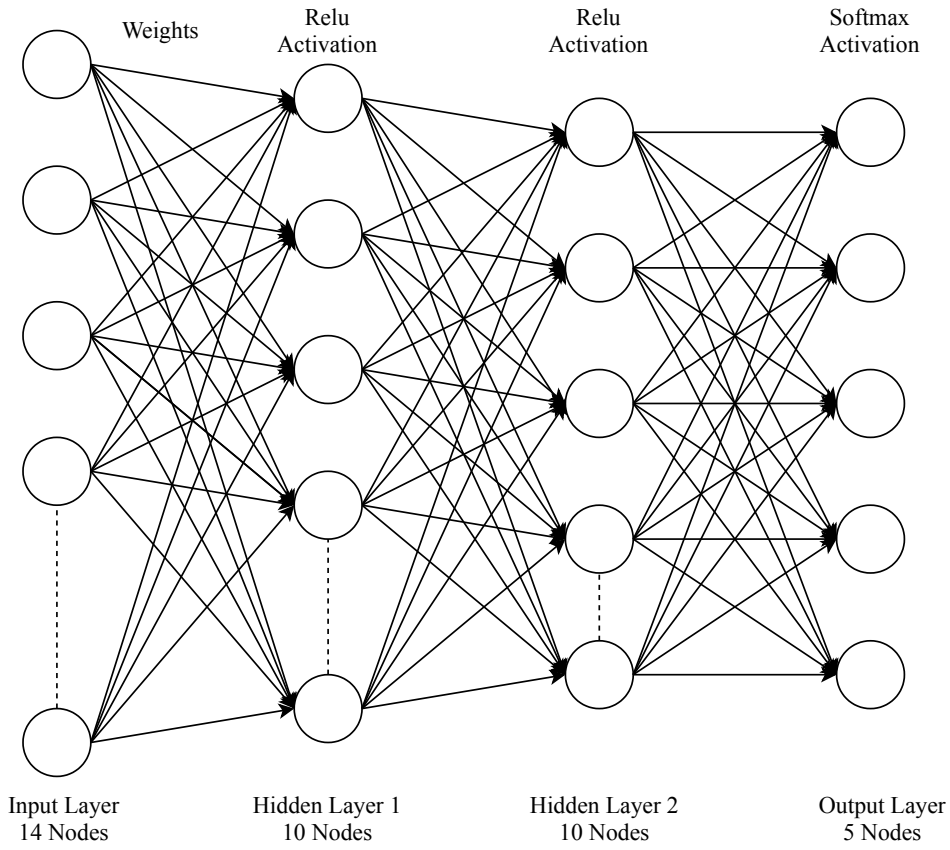

Figure 3.3: Neural network model.

A NN classifier consists of number of neurons units, arranged in layers. Each layer takes some input vector and gives output by applying a non-linear function. This output works as input to next layer in feed-forward manner. In general, there is no feedback to previous layer. Final output layer has implementation of classification of attack. Figure 3.3 shows Neural Network model of this proposed system.

This work uses WSN-DS dataset to train our neural network which contains 374661 observations on different attacks on top of LEACH. The dataset contains data about Grayhole attack, Blackhole attack, Scheduling attack, Flooding attack together with normal behaviour of network in LEACH protocol. The dataset contains 19 features explained earlier in Table 3.1.

3.4.3 Flowchart

The process that is being used in this work to train network is learning process. Figure 3.4 shows self-explanatory flowchart for learning process of neural network model.

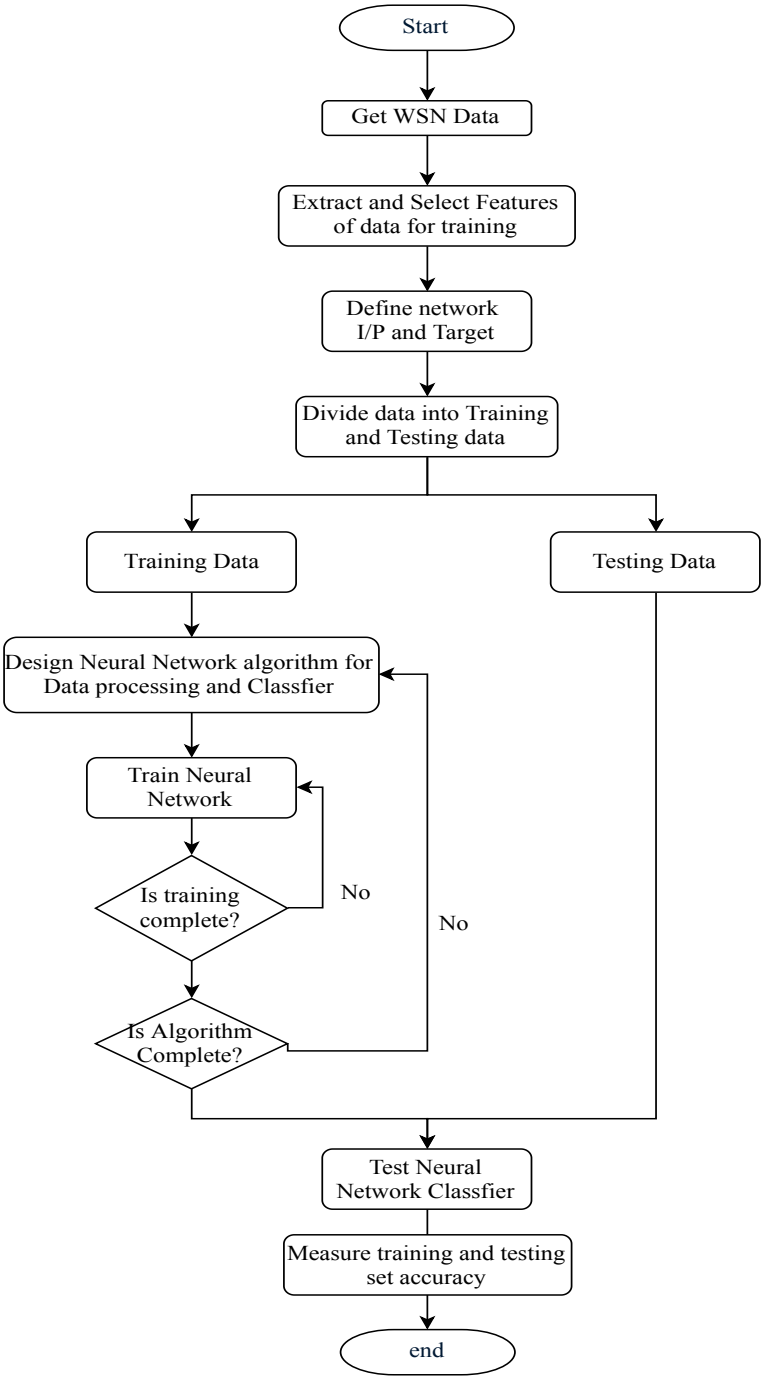

Figure 3.4: Flow chart for neural network model.

3.5 Procedure

To train this neural network one feature *Attack Type* is used as label. Out of other remaining 18 features, 14 features has been used to get the best result out of training. Training starts by building a sequential model using Keras API which is a high-level API to build and train models in Tensorflow (an online machine learning library for research) . This sequential model assemble layers in stack. This model has a flexibility to add number of hidden layers using its built in functions. Detailed working of neural network model is explained in this section. Neural Network working model can be described in following 6 steps:

i. **Analyze the Dataset** Data is very important in every application of Neural Network learning. Analyzing data helps in feature extraction and selection. Analyzing dataset also includes analyzing Dataset, Attribute characteristics, Number of Instances, Attributes etc. Here, data is analyzed with the help of Pandas library of python.

ii. **Prepare the dataset** Raw data is of no use. To make use of any data it must be structured in proper way. Here, representation of analyzed data in a n-dimensional matrix is done using NumPy library of python.

iii. **Create the Model** Neural networks large number of neurons are arranged in sequential layer using *Sequential* model of Keras API. Here, neural network fully connected layered model was created using *Dense* function. Our model has 1 I/P, 2 hidden, 1 O/P classification layers as shown in Figure 3.3. I/P layer was initialized with 14 neurons (14 selected features). Relu (Rectified linear unit) activation function was used for I/P, and hidden layer with uniform weight distribution. Softmax activation function was used for O/P classification layer.

iv. **Compile the Model** To compile this model *loss*, *optimizer*, and *metrics* parameters are needed to make neural network learn during each iteration. This NN model uses *categorical_crossentropy* which is loss function to minimize the error term between expected and actual output. *Adam* optimizer is used to

search for different weights for neuron connections. Also, to measure the classification accuracy this system uses *accuracy* as it's metric.

v. **Fit the Model** Compiled model is ready to be trained using dataset. To fit data into model keras gives *fit* function which accepts training I/P data, training O/P data, validation data, iterations.

vi. **Evaluate the Model** After fitting data into model its evaluation is required. *Evaluation* function of model takes input data and actual output data. It predicts output using input data based on what it has learned, which is then compared with actual output.

3.6 Summary

In this chapter, a supervised neural network learning approach has been discussed which helps to build signature-based IDS using dataset. The proposed algorithm can be divided into two parts. In first part data collection, data analysis, and data preparation is done. Dataset is divided into 75-25% as training and testing data. Training data is then fed into neural network model for training purpose. After completion of training model evaluation is performed using testing dataset. Evaluation results have been shown in section 4.4. After that in second part, to simulate the WSN environment (mainly LEACH protocol and attacks), energy model of WSN is implemented in Octave. Evaluation of this part is done by analyzing energy left in the network, dead and alive nodes, data packets delivered to CH and BS etc. Evaluation results of this part is shown in chapter 4.

Chapter 4

Simulation and Results

This chapter presents the simulation and results of the research work. Simulation of this work is done in two parts. Part 1 uses Octave to simulate the energy model of WSN to examine some of the features of WSN-DS. This phase yields graph comparison between normal activity and attack. Part 2 is simulated using python and it's libraries. This work trains neural network model to classify attack category and then provides result graph in terms of accuracy. The simulation parameters used for part 2 simulation are shown in Table 4.1.

4.1 Residual Energy Comparison

Residual energy comparison presents the results of reading of energy model of WSN in case of two attacks - sinkhole and blackhole. These attacks are implemented in LEACH routing protocol and resultant graph 4.1 reading shows comparison with normal behavior of system without attack. It is observed from the graph that energy left in the network is highest in case of no attack while network energy goes zero in case of sinkhole attack at the earliest because compromised nodes advertise their fake high energy [10]. In case of blackhole attack the nodes which are compromised, do

Table 4.1: Network parameters.

Parameter	**Value**
Network area	200 x 200
Sink Node location	100, 100
Number of Nodes	100
Initial Energy	50 J
Energy for transmitting and receiving single bit	50 nJ
Number of rounds	1500
Routing Protocol	LEACH
MAC protocol	CSMA/TDMA

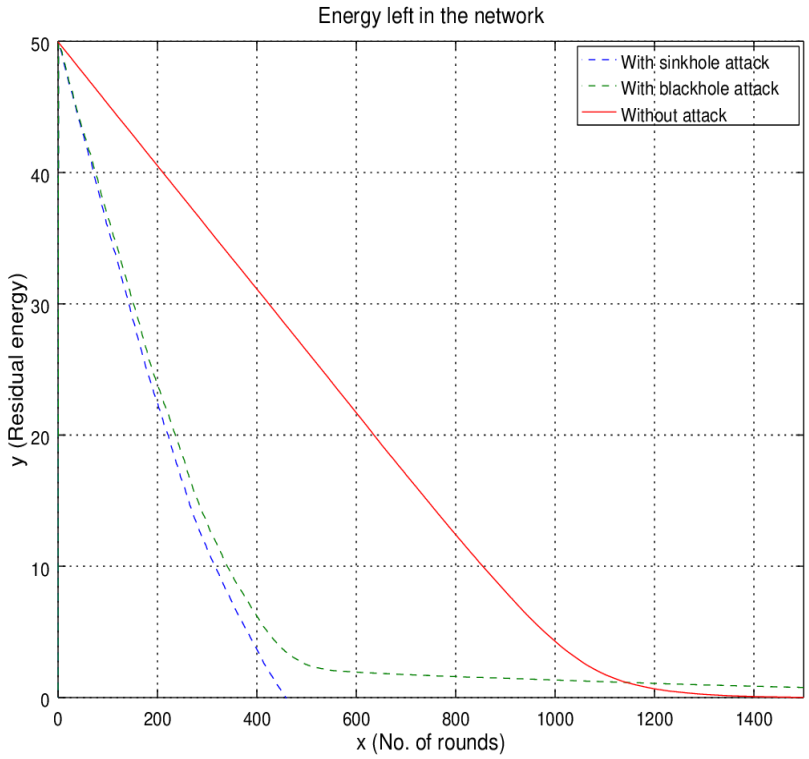

Figure 4.1: Energy model of WSN.

not forward data packets hence their residual energy remains in the network [11].

4.2 Alive Node Comparison

This section presents the results of reading of sensor nodes that are alive in WSN. Graph 4.2 shows comparison between blackhole, sinkhole and no attack situation in LEACH protocol. Graph shows that alive nodes in the network are more in case of no attack while all nodes in network are dead in case of sinkhole attack earliest. This graph has been plot based on remaining energy of each node. A node is considered dead if it's energy is zero.

4.3 Packets Sent to Base Station Comparison

Data packets sent to base station from cluster heads are shown in Figure 4.3. The graph shows comparison between blackhole, sinkhole and no attack situation in LEACH protocol. This graph shows that Packets Sent to BS in the network are more in case

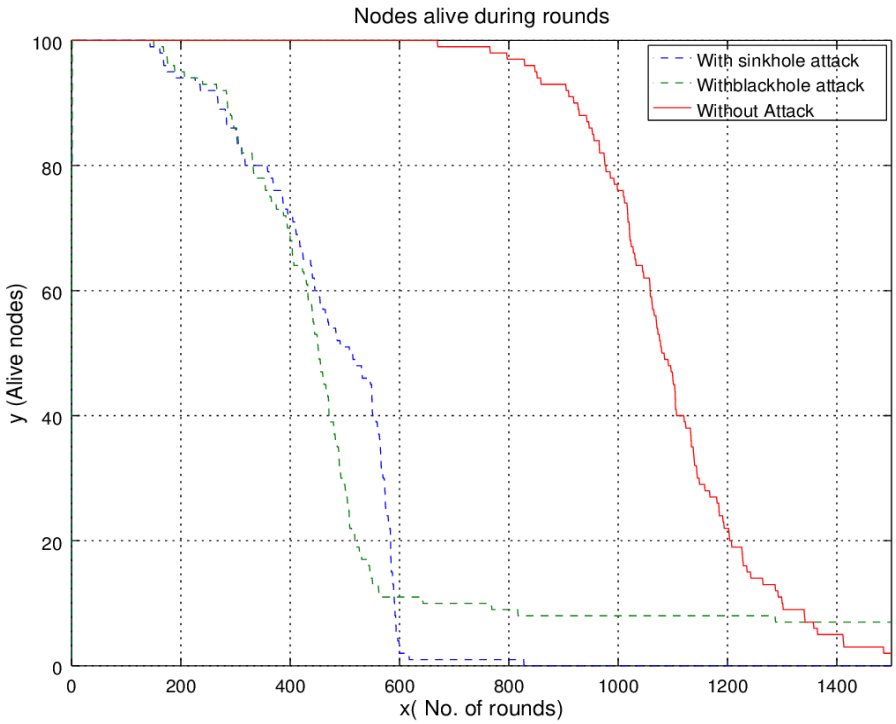

Figure 4.2: Alive nodes.

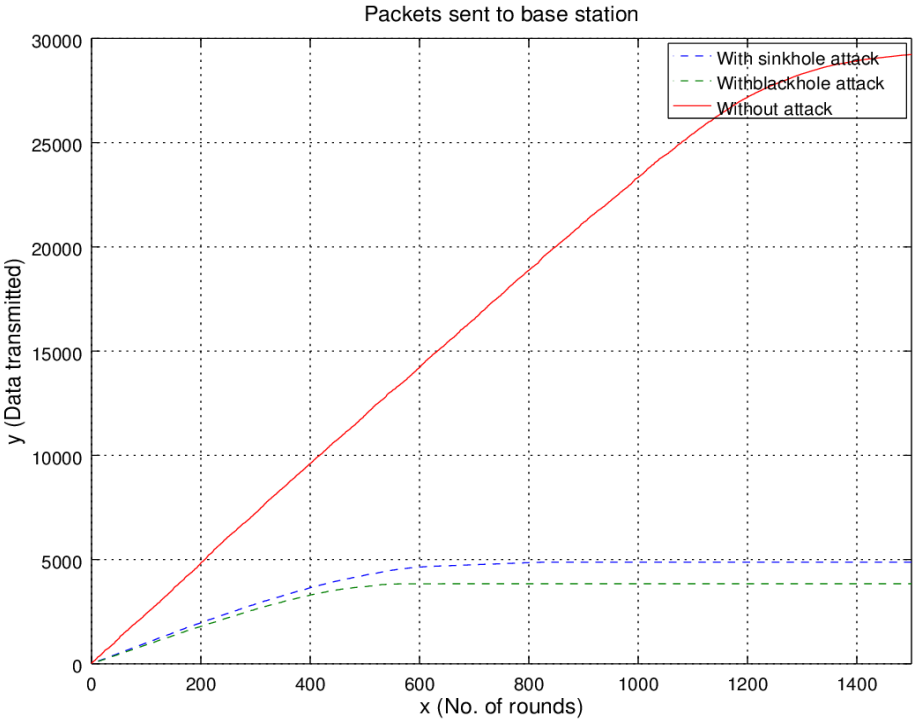

Figure 4.3: Data packets sent to base station.

of no attack and minimum in case of black hole attack as compromised node drops all the data packets.

4.4 Neural Network Model Results

Neural network model is being used to detect if any activity is malicious or not. WSN-DS dataset used to train neural network model. This section shows the results of training and testing this model. Two graphs, Figure 4.4 and Figure 4.5 shows accuracy of this model with 2 hidden layers and 3 hidden layers, respectively.

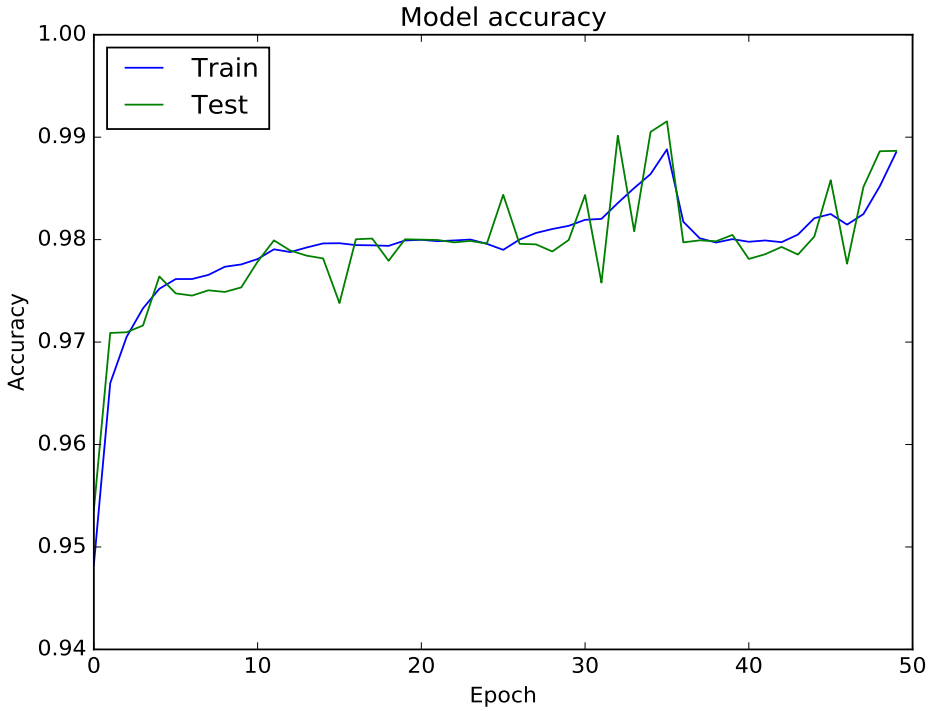

Figure 4.4: Neural network model accuracy result with 2 hidden layers.

X-axis on grpah shows iterations (epochs), Y-axis shows the accuracy metric. The model has been trained for 50 iterations. The accuracy achieved with 2 hidden layers for training set is 98.85% and for testing set is 98.84%. The accuracy achieved with

Table 4.2: Neural network model results.

NN Model Result in	Training data		Validation data		Testing data	
Hidden layers	Accuracy (%)	Loss	Accuracy (%)	Loss	Accuracy (%)	Loss
2	98.85	0.0390	98.87	0.0363	98.84	0.0346
3	99.24	0.0271	99.31	0.0250	99.32	0.0244

3 hidden layers for training set is 99.24% and for testing set is almost 99.32%. These results observed here for testing set are varying in the small range only. Table 4.2 shows simulation results with losses.

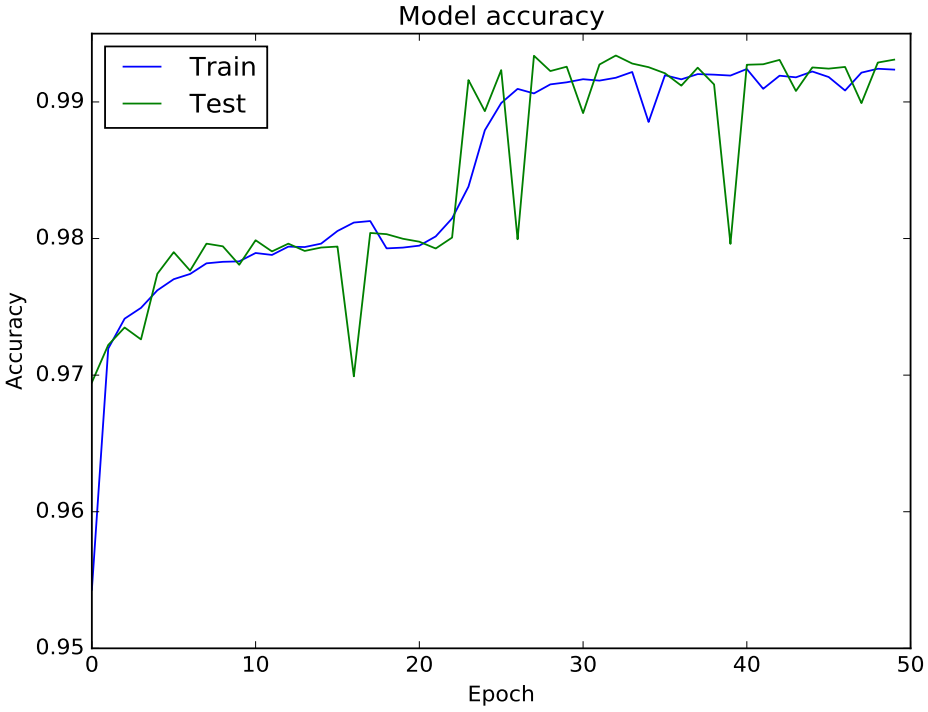

Figure 4.5: Neural network model accuracy graph with 3 hidden layers

4.5 Comparison with other Neural Network Algorithms

A. saeed et al. [37], presented an intrusion detection mechanism which is very effective in low-power WSN. This IDS mechanism uses a Random Neural Network (RNN). The IDS detects any performance degradation anomaly attack. It does not require any dedicated hardware and its attack detection accuracy was found to be 97.23%. This model detects any anomaly by identifying any deviation of an event from previously learned normal network operations. This mechanism can also detect previously unknown attacks.

In [46] O.C. Turkish, to avoid big security deficiencies an IDS for WSN using neural network is proposed. The proposed system was trained and tested by KDD99 dataset.

This work was able to detect four group attack types from the dataset Dos, Remote to Local Attack, Probing Attack, User to Root Attack. Performance of network using 41 features and 67500 observations came true as 0.8488. Fewer the training samples lesser the success rate for different attack types. They also showed that the success rate can be changed by number of hidden layers, number of neurons in each layer, feature selection etc.

4.6 Summary

To analyze certain features of dataset like, residual energy in the network, alive nodes, data packets sent to BS etc energy model of dataset is simulated in the Octave tool. Resultant graphs of these simulations helps to differentiate between attack and no attack situation. All the simulation in this part is performed for 1500 rounds of LEACH protocol which is shown on X-axis of each graph and Y-axis has specific feature. Also, This chapter presents a neural network learning approach to detect an intrusion activity using a dataset which is built using LEACH protocol. The accuracy measure of detection are 98.85% if 2 hidden layers used for learning, and accuracy reaches to 99.24% if 3 hidden layers used.

Chapter 5

Conclusions and Future Scope of Work

Applications of wireless sensor networks are so wide that WSN is reaching in all areas from military to medical. In all applications, data plays an important role and hence it must be kept secure. Various possible attacks try to modify data or analyze it. An outsider attack can be detected or prevented using cryptographic and other security mechanisms. When the attacker resides inside the network, in this situation the node which is compromised and under attack can lead to various security problems. Using this node any data/information passing through this node can be manipulated. So, it is important to detect these inside attacks and prevent any data loss. IDS are designed for this purpose.

Some of the IDS system are able to detect known attack while some were able to detect unknown attacks too. Hybrid systems have also been designed in order to detect all kinds of security attacks in the wireless sensor network. Accuracy and high detection rate of some of these detection mechanisms were about 100% and hence low false positive rate. Some IDS can detect all the attacks, while on the other hand some of those were designed to detect specific attacks efficiently. Features and limitations of different detection methodologies have been compared. Conclusively, this survey paper concludes various types of IDS. In the process of analyzing different detection techniques, it is observed that anomaly-based detection methods normally use statistical algorithms whereas signature-based detection methods generally uses knowledge-based algorithms. Also, it can be inferred that hybrid systems are more efficient in terms of detection rate with low false positive rate as compared to the anomaly and signature-based techniques. The work presented in this research can be summarized as follows:

5.1 Conclusions

The research work embodied in this dissertation has addressed the problem of intrusion detection in WSN with accuracy of about 99% by using a neural network model and dataset to make neural network learn. Various aspects of the research problem are investigated and flaws in WSN security, IDS and its components, a detailed review of different IDS to tackle various attacks has been presented in earlier sections. The main findings are summarized below.

- In the process of analyzing different detection techniques, it is observed that anomaly-based detection methods normally use statistical algorithms whereas signature-based detection methods generally uses knowledge-based algorithms.
- It can be concluded that hybrid systems are more efficient in terms of detection rate with low false positive rate as compared to the anomaly and signature-based techniques.

5.2 Future Scope of Work

The proposed method works fine for Grayhole attack, Blackhole attack, Scheduling attack, Flooding attack. But, there are few limitations, as listed below, in this work which can be addressed in future.

- Currently, proposed system is only able to cope with 4 types of attack. This research work can be extended by generating and collecting more data of different attack categories.
- Dataset creation can have more features by observing/monitoring the Sensor nodes behavior closely.
- Number of observation vector of attacks can be more to detect any attack more accurately by training the neural network and adding more hidden layers.
- The proposed approaches uses only feed forward network for classification, back-propagation algorithm can be implemented to achieve more accuracy.

List of Publications

Paper accepted in international conference:

[1] A. Agarwal and N.C. Kaushal, "A Study of Intrusion Detection System in Wireless Sensor Network," *4th International Conference on Internet of Things and Connected Technologies (ICIoTCT)*, 2019.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, no. 4, pp. 393–422, 2002.

[2] D. G. Padmavathi, M. Shanmugapriya *et al.*, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *arXiv preprint arXiv:0909.0576*, 2009.

[3] A. Fuchsberger, "Intrusion detection systems and intrusion prevention systems," *Information Security Technical Report*, vol. 10, no. 3, pp. 134–139, 2005.

[4] K. Mehta and R. Pal, "Energy efficient routing protocols for wireless sensor networks: A survey," *International Journal of Computer Applications*, vol. 165, pp. 41–46, 05 2017.

[5] T. Roosta, S. Shieh, and S. Sastry, "Taxonomy of security attacks in sensor networks and countermeasures," in *The first IEEE international conference on system integration and reliability improvements*, vol. 25, 2006, p. 94.

[6] A. Wahid and P. Kumar, "A survey on attacks, challenges and security mechanisms in wireless sensor network," *International Journal for Innovative Research in Science and Technology*, vol. 1, no. 8, pp. 189–196, 2015.

[7] P. Nayak, V. Bhavani, and B. Lavanya, "Impact of black hole and sink hole attacks on routing protocols for wsn," *International Journal of Computer Applications*, vol. 116, no. 4, 2015.

[8] K. Abirami and B. Santhi, "Sybil attack in wireless sensor network," *International Journal of Engineering and Technology (IJET)*, vol. 5, no. 2, pp. 620–623, 2013.

[9] M. Singh, K. Babbar, and K. L. Jain, "A survey on intrusion detection system in wireless sensor networks," *International Journal of Wireless Communications and Networking Technologies*, vol. 3, no. 3, 2014.

[10] S. A. Salehi, M. Razzaque, P. Naraei, and A. Farrokhtala, "Detection of sinkhole attack in wireless sensor networks," in *2013 IEEE International Conference on Space Science and Communication (IconSpace)*, 2013, pp. 361–365.

[11] M. Wazid, A. Katal, R. S. Sachan, R. Goudar, and D. Singh, "Detection and prevention mechanism for blackhole attack in wireless sensor network," in *2013 International Conference on Communication and Signal Processing*, 2013, pp. 576–581.

[12] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks." in *SecureComm*, vol. 5, 2005, pp. 113–124.

[13] S. Patil and S. Chaudhari, "Dos attack prevention technique in wireless sensor networks," *Procedia Computer Science*, vol. 79, pp. 715–721, 2016.

[14] V. Sharma and M. Hussain, "Mitigating replay attack in wireless sensor network through assortment of packets," in *Proceedings of the First International Conference on Computational Intelligence and Informatics*, 2017, pp. 221–230.

[15] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in wsns," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[16] K.-F. Ssu, W.-T. Wang, and W.-C. Chang, "Detecting sybil attacks in wireless sensor networks using neighboring information," *Computer Networks*, vol. 53, no. 18, pp. 3042–3056, 2009.

[17] L. K. Bysani and A. K. Turuk, "A survey on selective forwarding attack in wireless sensor networks," in *2011 International Conference on Devices and Communications (ICDeCom)*, 2011, pp. 1–5.

[18] I. Almomani and B. Al-Kasasbeh, "Performance analysis of leach protocol under denial of service attacks," in *2015 6th International Conference on Information and Communication Systems (ICICS)*, 2015, pp. 292–297.

[19] T.-G. Lupu, I. Rudas, M. Demiralp, and N. Mastorakis, "Main types of attacks in wireless sensor networks," in *WSEAS international conference. proceedings. recent advances in computer engineering*, no. 9, 2009.

[20] S. Sharma, R. K. Bansal, and S. Bansal, "Issues and challenges in wireless sensor networks," in *2013 International Conference on Machine Intelligence and Research Advancement*, 2013, pp. 58–62.

[21] S. J. Ramson and D. J. Moni, "Applications of wireless sensor networksa survey," in *2017 International Conference on Innovations in Electrical, Electronics, Instrumentation and Media Technology (ICEEIMT)*, 2017, pp. 325–329.

[22] N. A. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: a review," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, p. 167575, 2013.

[23] S. Khan, J. Loo, and Z. Ud Din, "Framework for intrusion detection in ieee 802.11 wireless mesh networks," *International Arab Journal of Information Technology*, vol. 7, no. 4, pp. 435–440, 2010.

[24] S. Jha and M. Hassan, "Building agents for rule-based intrusion detection system," *Computer Communications*, vol. 25, no. 15, pp. 1366–1373, 2002.

[25] M. Xie, S. Han, B. Tian, and S. Parvin, "Anomaly detection in wireless sensor networks: A survey," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1302–1325, 2011.

[26] H. Sedjelmaci and M. Feham, "Novel hybrid intrusion detection system for clustered wireless sensor network," *arXiv preprint arXiv:1108.2656*, 2011.

[27] A. Mehmood, A. Khanan, M. M. Umar, S. Abdullah, K. A. Z. Ariffin, and H. Song, "Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks," *IEEE Access*, vol. 6, pp. 5688–5694, 2018.

[28] K. Yan, S. Wang, and C. Liu, "A hybrid intrusion detection system of cluster-based wireless sensor networks," in *Proceedings of the International MultiConference of Engineers and Computer Scientists*, vol. 1, 2009, pp. 18–20.

[29] S.-S. Wang, K.-Q. Yan, S.-C. Wang, and C.-W. Liu, "An integrated intrusion detection system for cluster-based wireless sensor networks," *Expert Systems with Applications*, vol. 38, no. 12, pp. 15 234–15 243, 2011.

[30] X. Jinhui, T. Yang, Y. Feiyue, P. Leina, X. Juan, and H. Yao, "Intrusion detection system for hybrid dos attacks using energy trust in wireless sensor networks," *Procedia computer science*, vol. 131, pp. 1188–1195, 2018.

[31] G. Kalnoor and J. Agarkhed, "Detection of intruder using kmp pattern matching technique in wireless sensor networks," *Procedia Computer Science*, vol. 125, pp. 187–193, 2018.

[32] D. Jianjian, T. Yang, and Y. Feiyue, "A novel intrusion detection system based on iabrbfsvm for wireless sensor networks," *Procedia computer science*, vol. 131, pp. 1113–1121, 2018.

[33] X. Jin, J. Liang, W. Tong, L. Lu, and Z. Li, "Multi-agent trust-based intrusion detection scheme for wireless sensor networks," *Computers & Electrical Engineering*, vol. 59, pp. 262–273, 2017.

[34] C. Eik Loo, M. Yong Ng, C. Leckie, and M. Palaniswami, "Intrusion detection for routing attacks in sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2, no. 4, pp. 313–332, 2006.

[35] H. Sedjelmaci, S. M. Senouci, and M. Feham, "An efficient intrusion detection framework in cluster-based wireless sensor networks," *Security and Communication Networks*, vol. 6, no. 10, pp. 1211–1224, 2013.

[36] N. Lu, Y. Sun, H. Liu, and S. Li, "Intrusion detection system based on evolving rules for wireless sensor networks," *Journal of Sensors*, vol. 2018, 2018.

[37] A. Saeed, A. Ahmadinia, A. Javed, and H. Larijani, "Random neural network based intelligent intrusion detection for wireless sensor networks," *Procedia Computer Science*, vol. 80, pp. 2372–2376, 2016.

[38] W. Meng, W. Li, and L.-F. Kwok, "Efm: enhancing the performance of signature-based network intrusion detection systems using enhanced filter mechanism," *computers & security*, vol. 43, pp. 189–204, 2014.

[39] G. Gowrison, K. Ramar, K. Muneeswaran, and T. Revathi, "Minimal complexity attack classification intrusion detection system," *Applied Soft Computing*, vol. 13, no. 2, pp. 921–927, 2013.

[40] A. H. Farooqi and F. A. Khan, "Intrusion detection systems for wireless sensor networks: A survey," in *International Conference on Future Generation Communication and Networking*, 2009, pp. 234–241.

[41] K. Ioannis, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in *Proc. of the 13th European wireless conference*, 2007, pp. 1–10.

[42] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "Intrusion detection of sinkhole attacks in wireless sensor networks," in *International symposium on algorithms and experiments for sensor systems, wireless networks and distributed robotics*, 2007, pp. 150–161.

[43] Y. Li and L. E. Parker, "Intruder detection using a wireless sensor network with an intelligent mobile robot response," in *IEEE SoutheastCon 2008*, 2008, pp. 37–42.

[44] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, "Wsn-ds: a dataset for intrusion detection systems in wireless sensor networks," *Journal of Sensors*, vol. 2016, 2016.

[45] N. Palan, B. Barbadekar, and S. Patil, "Low energy adaptive clustering hierarchy (leach) protocol: A retrospective analysis," in *2017 International Conference on Inventive Systems and Control (ICISC)*, 2017, pp. 1–12.

[46] O. C. Turkish, "A neural network based intrusion detection system for wireless sensor networks," 2015.