Security Analysis of AODV Protocol in Wireless Sensor Networks

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

In

Computer Science and Engineering

Submitted By

Niharika Girnar

(801532035)

Under the supervision of:

Dr. Sanmeet Kaur

Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

June 2017

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "Security Analysis of AODV Protocol in Wireless Sensor Networks", in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Computer Science and Engineering* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Sanmeet Kaur and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Niharika

(Niharika Girnar)

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

Sanmeet Kaur

(Dr. Sanmeet Kaur)

Assistant Professor

Computer Science and Engineering Department

ACKNOWLEDGEMENT

The successful completion of any task would be incomplete without acknowledging the people who made it possible and whose constant guidance and encouragement secured the success.

First of all I wish to acknowledge the benevolence of an omnipotent God who gave me strength and courage to overcome all obstacles and showed me the silver lining in the dark clouds. With the profound sense of gratitude and heartiest regard, I express my sincere feelings of indebtedness to my guide **Dr. Sanmeet Kaur**, Associate Professor, Computer Science and Engineering Department, Thapar University for her positive attitude, constant encouragement, keen interest, invaluable cooperation, generous attitude and above all her blessings. She has been a source of inspiration for me, I am grateful to **Dr. Maninder Singh**, Head of Department and **Dr. Ashutosh Mishra**, P.G. Coordinator, Computer Science and Engineering Department, Thapar University for the motivation and inspiration for the completion of this thesis. I will be failing in my duty if I do not express my gratitude to **Dr. S. S. Bhatia**, Senior Professor and Dean of Academics Affairs at the University for making provisions of infrastructure such as library facilities, computer labs equipped with Internet facility, immensely useful for the learners equip themselves with the latest in the field.

Later but not the least I would like to express my heartfelt thanks to my parents, my sister and my friends who with their thought provoking views, veracity and whole hearted co-operation helped me in doing this thesis.

Niharika Girnar

(801532035)

Abstract

WSN leads to the vision of a connected world of physical and virtual processes, services and objects which are capable of providing multiple services within a network. WSN is a major part of future that mainly integrates and enables numerous communication solutions and technologies.

WSN networks are always under threat of malicious attacks because of opening deployments in various domains. It's heterogeneous and distributed characteristics make conventional intrusion detection methodologies hard to deploy. WSN is a combination of a variety of nodes within the same network, which work on unique addressing schemes. They are able to communicate with each other and cooperate with their surrounding nodes to reach common goals. One of the most challenging topics in WSN networks is security. Hence, Intrusion detection proves itself as a necessary and useful technique to keep the security and availability of WSN networks. This technique can monitor the security condition within the network. Further, they make an alert when an intrusion behavior is detected.

IDS are categorized into signature-based and anomaly-based detection on the basis of technique in detecting an intrusion. Signature-based IDS depends on a set of pre-defined malicious activity patterns and attack signatures to detect intrusions while anomaly-based IDS relies on deviations from normal behaviors to detect intrusions. Signature-based IDS is better than an anomaly-based IDS in detecting previously known attacks, but the former is ineffective against unknown or polymorphic attacks. On the other hand, anomaly-based IDS is capable of detecting unknown attacks in the absence of a predefined pattern.

In this thesis we present analysis of AODV networks under black hole and flooding attack. The networks have been evaluated under evaluation metrics like packet status, jitter and throughput. Also, each network has been analyzed using machine learning algorithms.

Table of Contents

CERTIFICATE ii
ACKNOWLEDGEMENT iii
Abstract iv
Table of Contents v
List of Figures vii
LIST OF TABLES ix
Chapter-1 Introduction 1
1.1 Introduction to Wireless Sensor Networks 1
1.2 Need of Intrusion Detection System in WSN networks 3
1.3 Intrusion Detection System 3
1.3.1 Classification of IDS 4
1.3.2 Architecture of IDS 9
Chapter – 2 Protocols & Attacks in WSN Network 11
2.1 Protocols in WSN networks 11
2.2 AODV 12
2.2.1 Message format in AODV 13
2.3 Attacks in WSN 14
Chapter -3 Literature Survey 17
3.1 Overview of WSN and IDS 17
3.2 Overview of Techniques of IDS 17
3.3 Related work of Black hole attack and Flooding Attack in WSN 18
3.4 Related work in Security of WSN 20
Chapter 4 Problem Statement 22
4.1 Problem Statement 22
Chapter – 5 Proposed Methodology and Implementation Details 24
5.1 Proposed Methodology and Work Flow 24
5.2 The Network Simulator (NS2) 25
5.2.1 NS2 Overview 25
5.2.2 Tool Command Language (Tcl) 26

5.2.3 The Network Animation (NAM) 26
5.2.4 The Tracegraph 28
5.3 Overview of used classification techniques 28
5.4 Simulation in NS2 29
5.4.1 General workflow of the simulation in NS2 29
5.4.2 Simulation of AODV networks 30
Chapter – 6 Results, Evaluation and Analysis 33
6.1 Evaluation Metrics 33
6.2 Analysis of Black hole attacks in an AODV network 33
6.3 Analysis of Flooding Attack in an AODV network 39
Chapter 7 Conclusion and Future work 44
7.1 Conclusion 44
7.2 Future Scope 44
References 46
Video presentation 51
Research Publication 52

List of Figures

Figure No.	Description	Page No.
1.1	Physical architecture of WSN [2]	1
1.2	Signature based detection	5
1.3	Anomaly based detection	6
1.4	Classification of IDS [50]	7
1.5	Network IDS [50]	7
1.6	Host IDS	8
1.7	Architecture of IDS	10
2.1	Control message in AODV	13
2.2	RREQ Format	13
2.3	RREP Format	14
2.4	RERR Format	14
2.5	Representation of replay attack	15
2.6	Worm hole attack [14]	16
2.7	Black hole attack in AODV [33]	16
5.1	Work Flow of the thesis	25
5.2	Running program in NS2	27
5.3	Trace File Format	28
5.4	Black hole attack simulation in an AODV network using NS2	32
5.5	Simulation of AODV protocol under flooding attack	33
6.1	Dropped packets in AODV network under black hole attack	36

Figure No.	Description	Page No.
6.2	Jitter of the dropped packets in black hole attack……	37
6.3	Throughput of dropping packet in AODV network……	38
6.4	Packet status of sent packets in Flooding attack…….	41
6.5	Jitter of sent packets in flooding attack…….	42
6.6	Throughput sent packets in flooding attack……	43

LIST OF TABLES

Table No.	Description	Page No.
3.1	Summary of Black hole attack and Flooding Attack in WSN	19
5.1	Description of the fields of the tracegraph format	28
5.2	Table 5.2: Simulation information of AODV protocol under black hole attack	31
5.3	Simulation information about flooding attack under flooding attack	32
6.1	Simulation information of the malicious node in Black Hole Attack	35
6.2	Machine Learning classification analysis results for Black Hole	39
6.3	Simulation information of malicious node in flooding attack	40
6.4	Machine learning classification analysis results for Flooding Attack	44

Chapter-1

Introduction

This chapter an introduction to WSN networks is presented. The of intrusion detection system in WSN networks is discussed. Later, in the chapter Intrusion Detection System, its types and architecture is discussed.

1.1 Introduction to Wireless Sensor Networks

Wired networks were used popularly to connect a computer network to the Internet, but recently, the wireless network has become more abundant in the broad scenario. A wireless network allows inter-connectivity of heterogeneous systems by enabling systems to communicate and exchange information [1]. Figure 1.1 shows the basic configuration of WSN network.

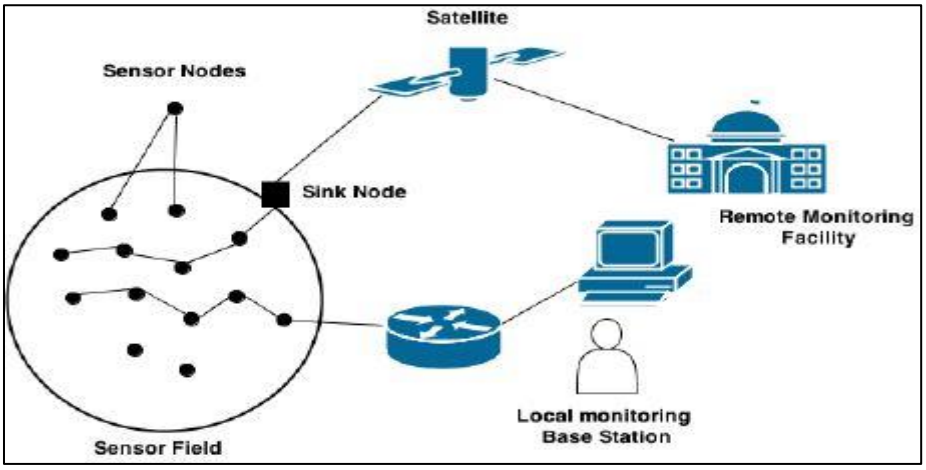

Figure1. 1: Physical architecture of WSN [2]

A WSN network is a set of nodes that collectively sense and control the environment. WSNs include actuator nodes, sensor nodes, clients and gateways. Sensor nodes have the duty to collect data for transmission to other nodes by hopping. In the process of transmitting the data, the information can be passed through multiple nodes in order to get its destination. Also, multi hop routing can be done to get to gateways and then the information may finally reach the management node through the Internet or satellite. The

user manages and configures the management node and also, takes care of the collection of the monitored data and the monitoring missions. The cost of WSN has dropped dramatically as the related technology has matured.

Some standards of WSN have been developed such as ISA 100.11a, WirelessHart, Zigbee®1 *etc*. The market of WSN has increased to a great extend in the last decade. Its application includes home applications, industrial automation *etc*. There are distributed independent devices which make the use of sensors to keep an eye on physical conditions. The application also extends up to automation, industrial infrastructure, health, consumer areas *etc*. Research in the area of WSN was started in the early 1980s, when the DAPRA (United States Defense Advanced Research Projects Agency) started with distributed sensor networks (DSNs) program for US military [4]. ARPANET (Advanced Research Projects Agency Network) has also made a major contribution in research work in the domain of WSN.

On WSN networks, regardless the geographic location we can access information and services in a wireless network. The wireless network can be with infrastructure or without infrastructure.

- **Infrastructure Networks**

These networks are made up of fixed and wired gateways. Within a communication radius the communication of mobile hosts is done with a bridge on the network. Movement within the network is possible. In case, the mobile unit is not in the range of present bus station, it communicates with another base station within its range. The process is called hand-off and in this approach the position of the base stations is fixed.

- **Infrastructure less (Adhoc Networks)**

In an adhoc environment all the nodes are moving. These nodes can be connected dynamically in any random pattern. Each node in this network can act as a router and takes part in maintenance and discovery for the nodes in the network. Adhoc networks hold a great importance in emergency situations like search and rescue operations.

Most rapidly growing infrastructure less technology is MANET. It is based on self-organizes network. MANETS are deployed in real world applications where the topology of the network changes very quickly.

Though MANET has the weakness of limited bandwidth, battery power, computational power; an extensive research work is going on to overcome these weaknesses. MANETS are different from wired networks and therefore, the security solutions that apply to wired networks cannot be applied to MANETS and this makes these wireless networks more vulnerable to any security attacks. Due to commencement of powerful wireless devices MANETS have become a popular option.

1.2 Need of Intrusion Detection System in WSN networks

A WSN network is always vulnerable to security threats. The malicious activities within the network can degrade network performance. There are a variety of attacks possible within a WSN network such as Sybil attacks, Denial of service attacks *etc*. Hence, it is observed that secure routing protocols are not enough to provide security to a WSN network. Therefore, Intrusion Detection System is one of the possible solutions to this problem. The aim of IDS is to analyze the network by data collection and detect the malicious activity in the network. A lot of research has been done and numerous IDS have proposed with the aim of proving security to the WSN network.

1.3 Intrusion Detection System

The process of identifying attacks in a system or a network is intrusion detection. The major categories of intrusion detection are misuse detection and anomaly detection. There are several methods to secure a network. Some of them are antivirus, honeypots, firewalls, an intrusion detection system *etc*. A firewall is understood as a collection of software and hardware that aims to secure a network from an outside network. A firewall authenticates each packet and only allows the valid packets to pass through. The validation of a packet is based upon a set of rules. Honeypots are used by users to detect the unauthorized party in the network. Here, the attacker is not aware that he is being observed from the start. When the attacker attacks the network, the information is sent to the authenticated user. Information such as IP address is collected and this information

can be used for tracking back the attacker. An antivirus is one of the popular ways by which users secure their systems for any type of attacks. On the other hand intrusion detection system collects and observes information from a network to avoid any kind of security breaches in the network. Intrusion detection was initially built to detect the vulnerability of the network. IDS can be software or an appliance that is physical which aims to monitor the network and detect the malicious activities within the reach of the network. It can detect attacks by checking the header of the packet travelling on the network.

An intrusion detection system (IDS) monitors traffic in the network, which flows within the network to find any malicious activity going on in the network. An intrusion detection system can determine the differences between normal and malicious activities. Some of them are:

- Denial of Service –Tasks that prevents the system from reaching its set target.
- Disclosure – unauthorized access of private information.
- Manipulation –unauthorized modification of data within the network.
- Masqueraders –A malicious entity behaves like an authorized system in order to gain important information from the system.
- Replay – It is the retransmission of important messages to produce harmful effects to the system.
- Repudiation – It is the denial of actions.
- Device Malfunctions –Failure of the system.

1.3.1 Classification of IDS

The categorization of intrusion detection can be done according to data source, structure, timing analysis, behavior after an attack *etc*. which are shown in figure 1.5 .

a) **Approach**: On the basis of approach, IDS can be divided into signature and anomaly detection.

- Signature Based Detection: Here, known patterns are matched with the present events and alerts are generated if the patters are matched. This technique is efficient

when the signatures have already been stored in the database of attacks and this technique is ineffective when unknown attacks are to be identified [6]. There is a difficulty in updating the information regarding new attacks in this new type. While in the misuse intrusion detection system the database regarding the packets is already prepared. With the help of this approach intruders can be easily be detected. This technique uses pre-known attack scenarios and also, compares with the traffic that is approaching the network. The detection approaches such as pattern recognition, colored petri-nets, expert system are grouped on the misuse. The figure below shows the basic mechanism. The major advantage of using this approach is that it achieves less false positive rates.

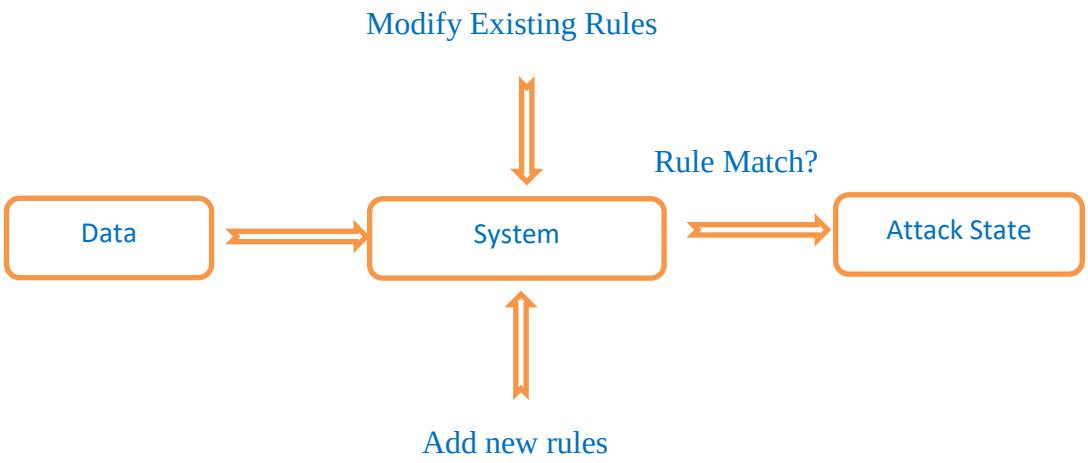

Figure1. 2: Signature based detection

- Anomaly Detection: In this technique profile of the normal user is created. Further, the current behavior is observed and it is observed if there is any mismatch within the profiles created and intrusion is detected using the results. In order to match the user profiles it is required to develop initial profiles that will be used to train the system according to user behavior. There is always a requirement to update the normal behavior of the system [7]. Behavior is detected on computer network. Profiles are stored in the databases where some threshold value is set. If in case, there is a deviation from the normal profile and there is a difference from the set threshold value then an alert is generated. The major advantage of using anomaly over misuse is that the intrusions which have not happened yet can be detected easily. The anomaly-based IDS

aims to point out activities that are not similar to the normal expected behavior of the system [8]. A difference in behavior between current behavior and the specifications will be marked as malicious [9]. The figure below demonstrates the mechanism.

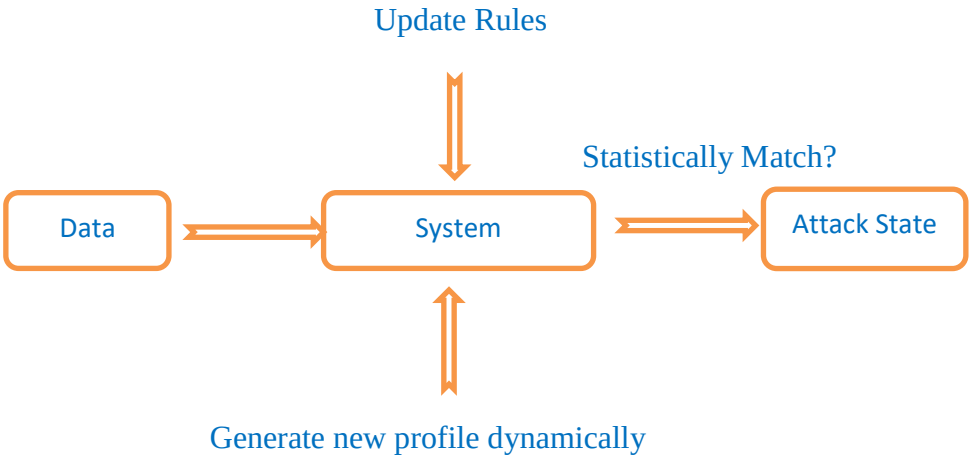

Figure1. 3: Anomaly based detection

b) **Behavior after an Attack**: Here, the behavior is the set of actions the systems take whenever an intrusion is detected. The behavior can be of two types, that is active or passive.

- Active IDS: Active IDS detects as well as responding by logging out the malicious attacker and can even block ports. It generates alerts also patches the software holes.

- Passive IDS: Passive IDS does not respond to any type of attacks. An alert is generated when malicious traffic is observed and further, it logs the network traffic in log files. The aim of such systems is to analyze and monitor the network traffic.

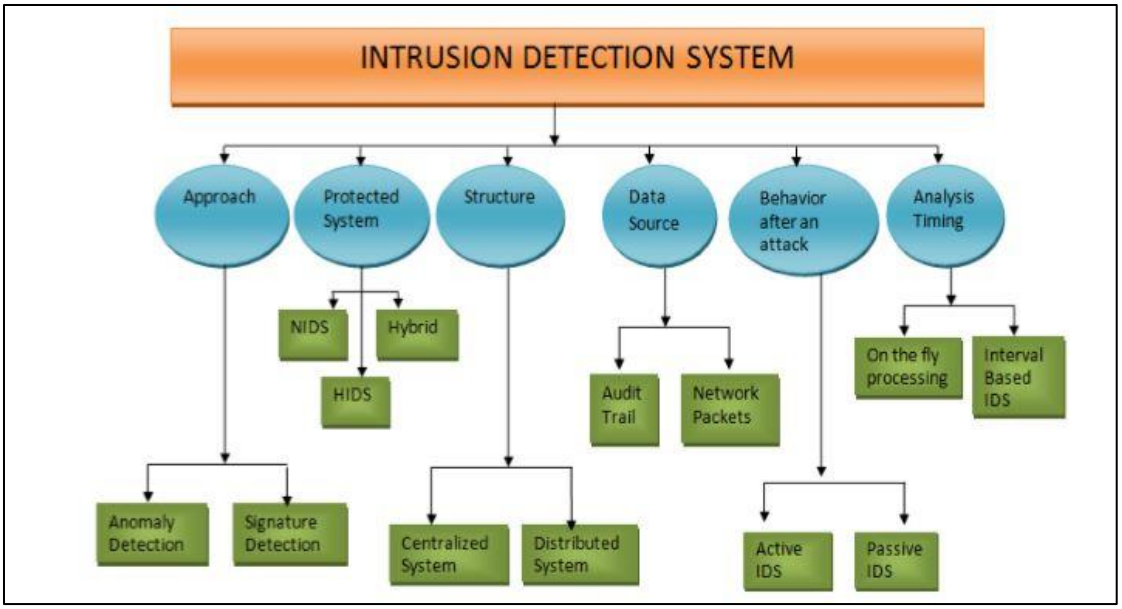

Figure 1.4: Classification of IDS [50]

c) Protected System: A protected system uses information that comes from the whole segment or a single host in that segment. IDS which collect information from a large segment are known as NIDS and the one which collects information from a single host are HIDS.

- NIDS: A network IDS collects Information regarding the local network. All the layers of OSI are under observation. Each host in the network is analyzed. A network IDS can easily be installed on active network. The figure below shows the NIDS.

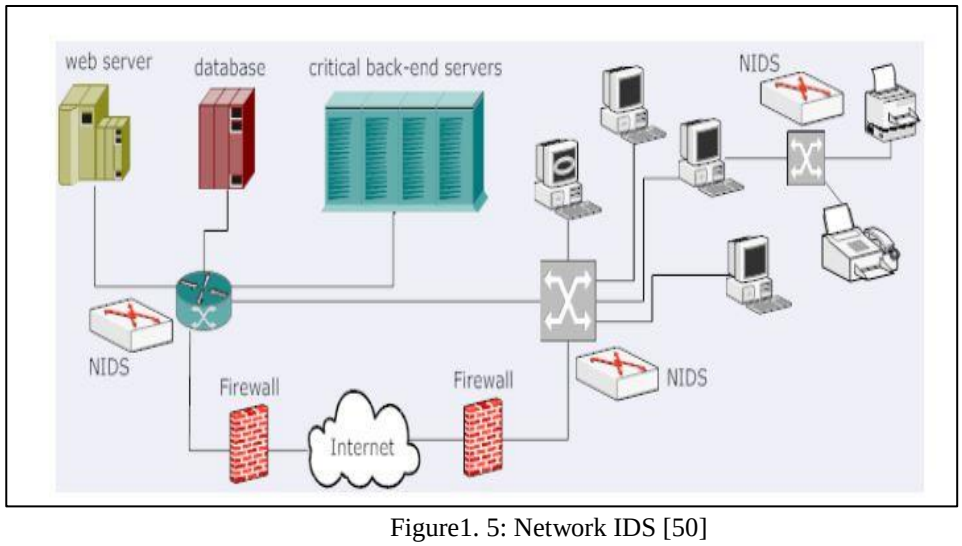

Figure1. 5: Network IDS [50]

- HIDS: It examines network packets that try to access the host. The network layer is examined of the protected host. File system integrity is maintained also, log files are examined for all activities. In case of any illogical change an alarm in the system is generated. Figure 1.7 shows HIDS.

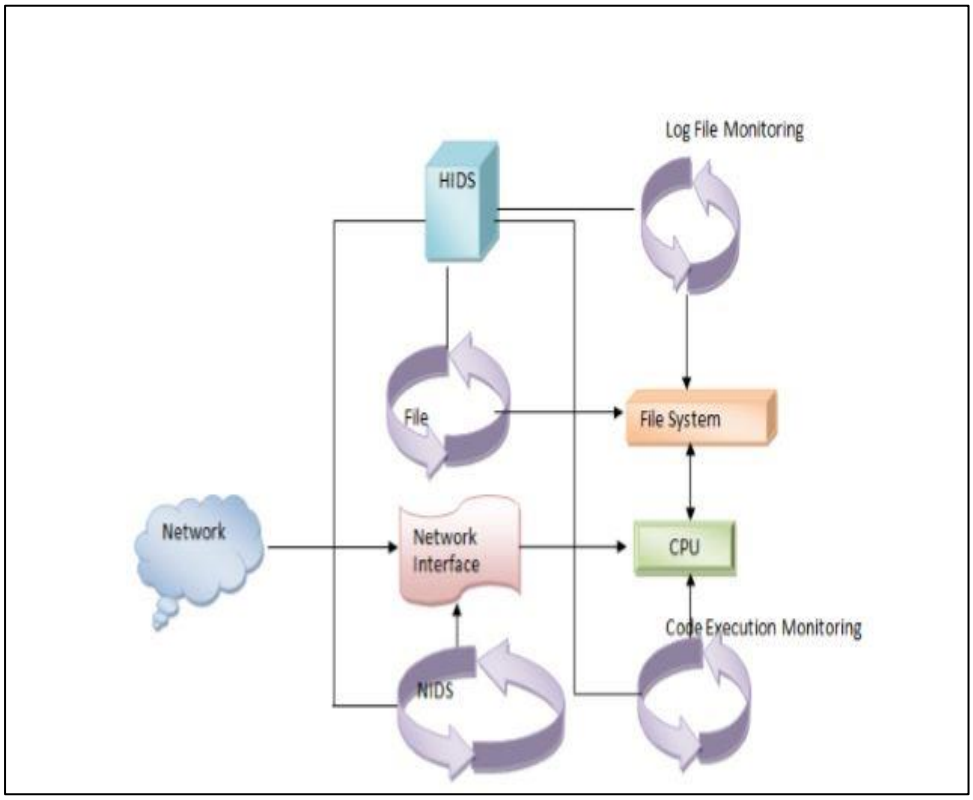

Figure 1.6: Host IDS

d) **Structure:** On the basis of structure, there are two different categories:

- Centralized System: Data is collected from single and multiple hosts. For analysis the data are transferred to the central location. Some of the examples are Bro, ARMD *etc*.
- Distributed System: Here, data is collected at each host and analysis of data is done in a distributed fashion. Some of the examples are CSM, AAFID and GRIDS.

e) **Data Source:** Based on the source of the data classification of IDS can be done in two categories namely network packets and audit trail.

- Audit Trail: It is a set of records which provides documentary proofs of the activity sequence of activity affected at any instant of time or event.
- Network Packets: A data unit which consists of user data and control information.

f) **Analysis Timing:** Depending on the analysis time, IDS can be classified into interval based IDS and fly processing IDS.

- On the fly processing: The intrusion detection system performs verification of the events and makes response simultaneously. It requires a large amount of RAM as it needs high data storage in order to trace all the packets present online.

- Interval Based IDS: A process is used to check the log files and the current status at predefined intervals.

1.3.2 Architecture of IDS

There are multiple components of Intrusion Detection System as shown in the below figure. Information Collection, Detection and Response are the major components. Each of the components are explained below:

- **Information Collection**: This component collects data from the system. It monitors the whole network regularly. Some of the inputs are log files, network packets and system logs. All the input is directed to the event generator which converts the inputs to a collection of smaller events and then further passes it to the sensors.
- **Detection**: The detection module aims to process the data which is collected by the sensors. It generates alarms on the basis of the events going on within the system. In this module the knowledge base is a system information and this information is provided by experts. There is a database present, which stores information regarding signatures and patterns. Whenever, the sensor senses some malicious activity in the

system, it matches it with the present database and reports to the respond component which is based on the detection policy.

- **Response**: The role of this component starts when intrusion is detected in the system. This can be automatic or may involve human interaction [5]. The administrator receives an email or an alarm about the intrusion in the system depending on system configuration.

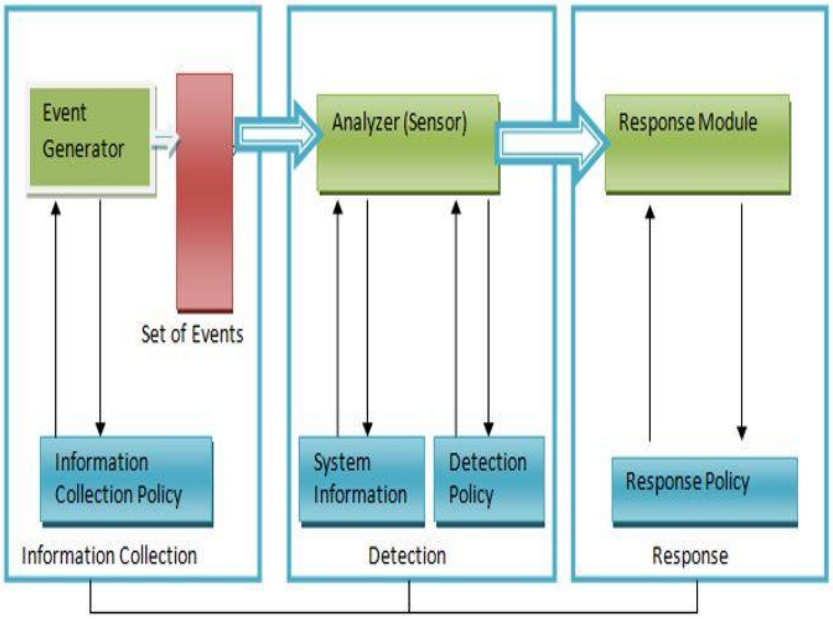

Figure 1.7: Architecture of IDS

Chapter Summary: In this chapter an introduction to WSN and Intrusion detection system is presented. This chapter gives the basic knowledge about types of intrusion detection systems.

Chapter – 2

Protocols & Attacks in WSN Network

This chapter consists of an introduction to WSN protocols and attacks. Also, AODV protocol has been discussed in detail.

2.1 Protocols in WSN networks

A routing protocol plays an important role in providing a secure communication in an adhoc network. The main aim of a routing protocol is to maintain efficient and accurate path between different nodes in the network. A number of protocols have been discovered for WSN to maintain security in the network. There are various applications of a WSN network. These applications may range from mobile and dynamic network for small and static network. There are three major branches of routing protocols: Reactive, Hybrid and Proactive.

General properties of WSN routing protocols are:

- The protocol distribution should be done in such a way that it leads to the total increase in the reliability of the network.
- The protocol should be energy efficient.
- Routing Protocol must maintain security in the network.
- A routing protocol must be designed to avoid any type of overhead in the network.
- A routing protocol must be aware of the Quality of Service (QoS).

- **Reactive Routing Protocol**

A reactive routing protocol finds a route only if it is demanded when communication between hosts on a mobile network is essential by flooding the network with RREQ packets; examples of such protocols are AODV, DSR and CBR *etc*.

- **Proactive Routing Protocol**

Proactive routing protocols maintain tables and tend to perform route discoveries periodically and automatically in order to build up a table related to network topology [10]. On every mobile node routes are discovered without the request of communication with the host. Some of the examples of proactive protocols which are table driven are DSDV, CGSR, OLSR *etc*. Due to the basic mechanism of proactive routing protocol these protocols suffer from some disadvantages like node entries are to be maintained for each node, slow recovery from failure, Overhead is involved in making routing table *etc.*

- **Hybrid Routing Protocol**

A hybrid routing protocol is a combination of the advantages of proactive and reactive routing protocol. Proactively prospected routes are initially established and further, serve the demand of activated nodes through reactive flooding. A hybrid routing protocol consists of the mechanisms of proactive and reactive routing protocols. The initial routine starts with the establishment of proactively prospected paths.

2.2 AODV

Adhoc on demand vector routing protocol is a mobile ad-hoc network protocol. It has a dynamic topology. The working of this protocol is a combination of DSR and DSDV [11]. The future of on demand route discovery and route maintenance is taken from DSR and hop-by-hop routing, usage of node sequence numbers is taken from DSDV. The unique feature of AODV is that it obtains routes purely on-demand [37]. It is a table driven protocol. It uses the routing table to store information and after a fixed interval of time a route expires if it is not used. Within a fixed interval of time a route expires. Also, AODV maintains a single route between a source-destination pair. AODV supports unicasting & broadcasting communication.

2.2.1 Message format in AODV

AODV uses four control messages, namely Hello, RREQ, RREP, Data and RERR.

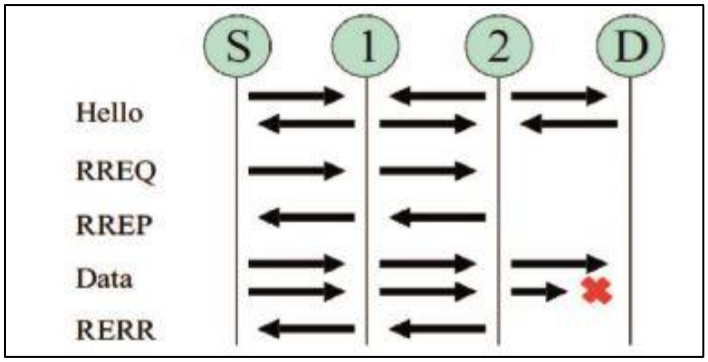

Figure 2. 1: Control message in AODV

- **Routing Request (RREQ)**

A RREQ packet is flooded by a node which needs to find out its destination in the whole network. RREQ contains values which informs that for how long it needs to be further forwarded and on every retransmission this value increases. Retransmission occurs in the case of no reply. Every node in the network maintains two counts, one is the node sequence number and the other is broadcast id. The source address represents the address of the sender. Request Id is the unique ID associated with the packet. Source sequence number is the unique number that helps in keeping a check at the number of requests already sent.

Source Address	Request ID	Source Sequence no.	Destination Address	Destination Sequence no.	Hop Count

Figure 2. 2: RREQ Format

- **Routing Reply (RREP)**

The originator of the RREQ gets its reply in the form of RREP from a node which is either the destination or the node has the valid route to the specified address. It is possible to unicast the message as every time RREQ is forwarded cache is maintained consisting of the originator details. The source address is the address of the source. The destination

address is the address where the request is to be sent. The destination sequence number helps to keep a check on the number of RREP requests. Life time is the time interval in which the request is valid.

Source Address	Destination Address	Destination Sequence no.	Hop Count	Life Time

Figure 2.3 RREP Format

- **Route Error Message (RERR)**

All the nodes observe their nearby nodes and broadcasts the messages when the nodes which is adjacent to it has a broken link or if it receives a data packet destined for a node for which it does not have an active route. The first field represents the IP address of the node to which the request could not reach and the second field represents the sequence number.

Unreachable Destination on IP Address	Unreachable Destination on Sequence Number

Figure 2.4: RERR Format

- **Hello Message**

A hello message can be used by a node to know its neighbors. These messages are never forwarded at their time to live is equal to one.

2.3 Attacks in WSN

- **Reply Attack**: In the reply attack, the attacker retransmits the information in order to infuse routing traffic in the network [12]. This attack aims to increase the traffic on the routes leading to wastage of bandwidth of the network and can also be used to undermine poorly designed security solutions.

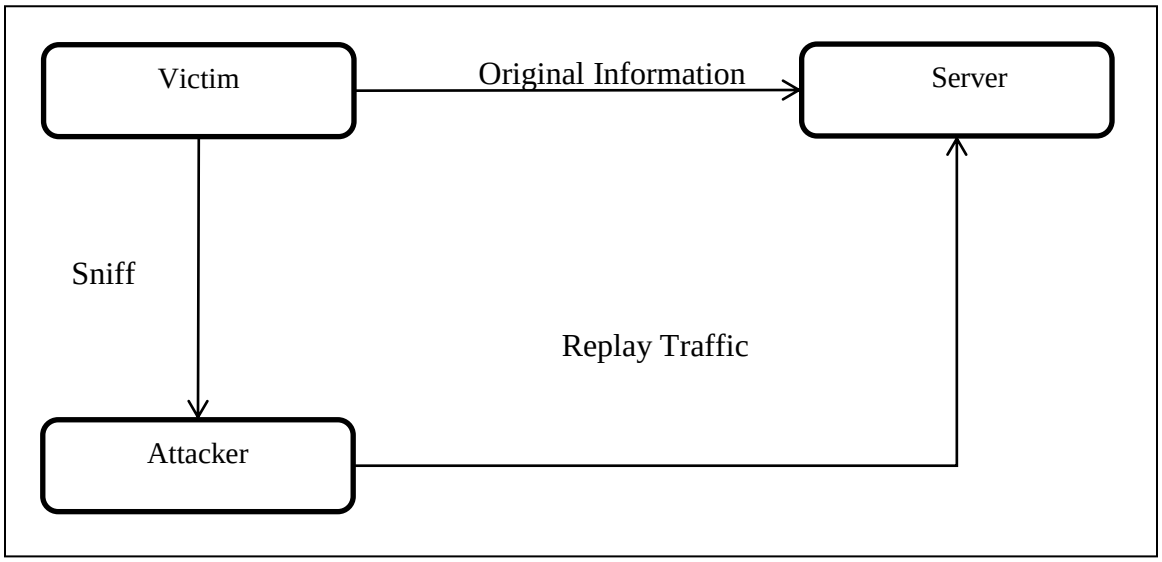

Figure 2.5 : Representation of replay attack

- **Byzantine Attack**: Here, the intruder attacks a single node or a group of nodes work together work in the collision and carry out attacks like selective dropping packets which finally leads to degradation of routing services.

- **Spoofing Attack**: In this attack a node takes up the identity of a node originally present in the network and receives information which is meant for the original node.

- **Worm hole attack**: In this attack, two attackers work simultaneously on different ends of the network. They communicate by forwarding the data they over hear and replay the packets in the network [13]. They replay valid messages to invalid locations.

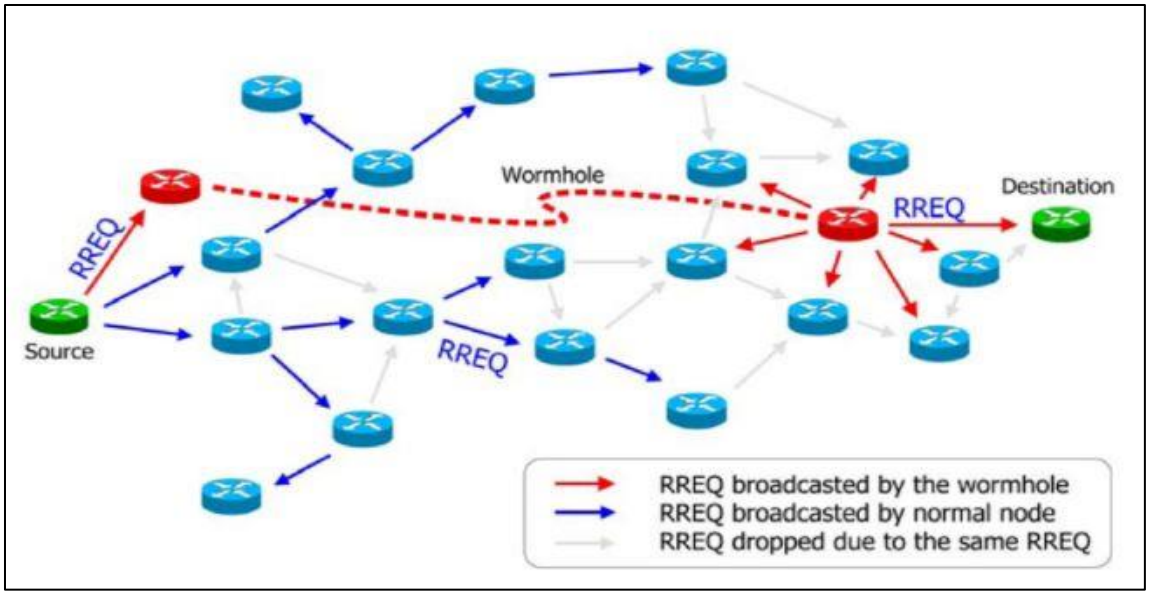

Figure 2.6: Worm hole attack [14]

- **Black hole attack**: In this attack, the intruder waits for its neighbors to initiate communication process i.e., route discovery. When the malicious node obtains the RREQ packet, it then sends a RREP packet with an increased sequence number [15]. Further, the malicious node does not allow any forwarding of packets.

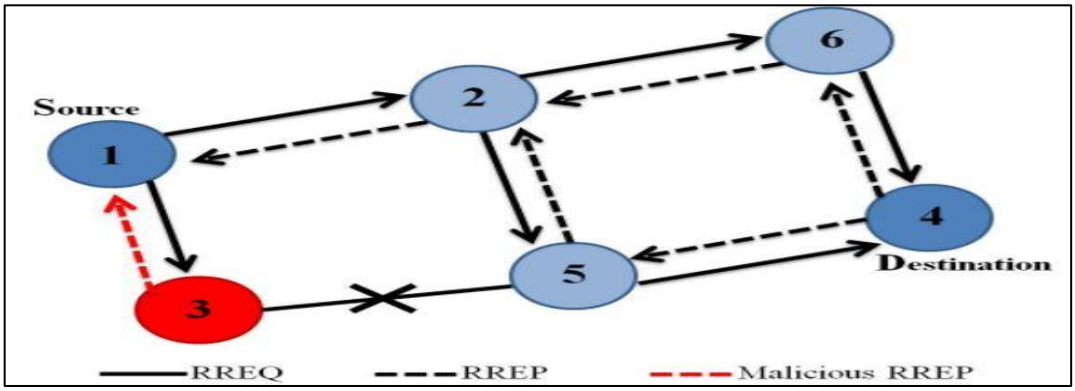

Figure 2.7: Black hole attack in AODV [33]

Chapter Summary: This chapter consists of a brief and a clear description of the protocols in WSN is given. AODV which is important protocol the WSN platform is discussed in detail. In order to understand the implementation the understanding of this chapter is necessary.

Chapter -3

Literature Survey

3.1 Overview of WSN and IDS

A Wireless Sensor Network (WSN) is made up of sensor nodes and sinks. Sensor nodes can self-organize and self-heal. Their nature is distributed and decentralized. Here, communication is dependent on intermediate multihop nodes. Sensor nodes are basically sending to collect information from the network surrounding it and give the collected information to the sinks. As security is a big concern in a WSN network, therefore several solutions have been provided regarding this. These security mechanisms can ensure the authenticity and eliminate most of the attacks [37].

An intrusion detection system is one of the most popular options to address the issue of security in a WSN network. An IDS is also known as the second line of defense. If IDS recognizes an attack, it raises an alarm and prompts the system to take some action. There are basically, two classes of IDS. The first one is the anomaly based or rule based IDS [38, 39]. Another name of a rule based is signature based. It takes the help of signatures that are already built-in. Although, the anomaly based IDS can detect new as well as known attacks, but often generate false positive as well as false negative alarms. Other than anomaly detection IDS there are IDS available which work on articular scenarios, one of the examples is the watchers [40]. These works on proactive routing protocol and detect anomalies. Further, some IDS are based on reactive routing protocols [42].

3.2 Overview of Techniques of IDS

- **Signature-Based IDS**: They are better known as rule based IDS as they have some predefined rules related to the attacks. [43] consist of a rule based IDS. Here, every node in the network has IDS within it. There are various attacks that IDS can detect one of them is sink hole attacks which is described in [44]. Also, the architecture of IDS is given in [45].

- **Anomaly Based Detection:** The main aim is to classify nodes as normal and malicious. A number of anomalies based IDS have been developed by now [46]. In [34] an unsupervised neural network is used which is used to detect unknown attacks. Further, there are several techniques related to IDS are discussed in [47] and they are independent of each other
- **Hybrid Intrusion Detection Systems**: It combines signature-based and anomaly-based approaches. In [48] a hybrid IDS is discussed using SVM algorithm to differentiate between normal and malicious node. Further, in [47] an IDS is discussed which uses stream flow to detect anomalies through hybrid IDS is discussed.

3.3 Related work of Black hole attack and Flooding Attack in WSN

Zdravko et al. [51] have presented a routing algorithm REWARD. The algorithm uses the broadcast radio to keep a check on its neighbor's behavior and detects the black hole attack within the network. Also, it creates a distributed database which records all the malicious activities.

Mohammad Wazid et al. [52] have discussed that black hole can be a great threat to a HWSN network and some measure of security need to be provided. Hence, they have proposed an efficient group based detection scheme. Black hole makes degrades the performance of the overall network.

K.Ram Venkatesh et al. [53] has suggested a trust routing plan based on active recognition and further their algorithm offers effective routing and scalability. The active trust plan that they have used rapidly notes the trust of the node and hence avoids the malicious nodes in the network.

Kumari R et al. [54] have reviewed methods to detect attacks in the network, which lead to higher energy consumption within the network. Their survey includes the vampire attack which can be fatal to network.

Saifullah et al. [55] have proposed a new protocol ARHUM and have also tested it. The protocol is capable of sensing all DOS attacks, including black hole.

Hao Chi Wong et al. have presented a scheme that can detect hello flooding attacks. The scheme proposed by them is similar to the GPS radio system.. Whenever a node receives a message which can be suspicious, it coordinates with its neighbors to find the source of the malicious packet.

Rodrigo Braga et al. have presented a lightweight method for DDoS attack detection. They have compared their results with the KDD-99 DATASET and have observed that their technique has comparatively lower overhead.

Virendra Pal Singh et al. have proposed a method to detect and also prevent hello flood attack . The process of detecting the malicious activity is based upon the strength of the hello messages received.

Table 3.1: Summary of Black hole attack and Flooding Attack in WSN

S.no	Year of Publication	Authors	Approach
1	2017	Hao Chi Wong	Based on signal strength of the sent message
2	2017	Rodrigo Braga Edjard Mota Alexandre Passito	Lightweight method for DoS attacks
3	2017	K.ram venkatesh P.v.n.n durga prasad	Active recognition algorithm
4	2017	Richa Kumari Pankaj Kumar Sharma	Survey
5	2017	Saifullah Aminl KashifSaghar I, Muhammad Burhan Tariq Abbasi Adnan Elahil	ARHUM
6	2016	Mohammad Wazid Ashok Kumar Das	Group based detection and prevention scheme
7	2015	Zdravko Karakehayov	Reward algorithm
8	2013	Shahid Raza,	SELVET IDS

9	2010	Virendra Pal Aishwarya S.	Single Streangth used to detect malicious activity.

3.4 Related work in Security of WSN

Reina et al. [16] particular have discussed WSN and adhoc networks, near field communication putting light on its connection to IoT. Though these platforms are compatible, but a lot of research work is required in this domain. Further, they have also have presented an overview of a smart environment in order to illustrate a possible IoT mode architecture.

Bellavista et al. [17] have discussed the brand new opportunities in wide-scale urban monitoring. Also, they have thrown a light on MANET and WSN convergence paves the way for the development of a brand new Internet of Things (IoT) communication platforms.

Raza et al. [49] implement and evaluate an intrusion detection system for the Internet of things. The authors explain that 6LoWPAN is an integral part of IoT and it has become important to protect the 6LoWPAN networks as they have a wide range of applications. Hence, they present SELVET, the first IDS for IoT which consist of a novel architecture and intrusion detection algorithm.

Shah et al. [18] compares the performance of DSDV, AODV and DSR routing protocols for ad hoc networks using NS-2 [5]. They have observed that poor performances of DSR are mainly attributed to aggressive use of caching [5]. On the other hand DSR's aggressive caching helps to the keep the routing load down.

Chen et al. [19] have presented simulation experiments of the AODV protocol and compared it with 802.15.4 MAC with clustered wireless settings. They investigate the basic problems of AODV and analyze the effect of incorporating multiple links. Further, they have presented multihop routing between one sensor and mobile sinks, and consider the delay*energy metric, which is a compound metric to evaluate the performance of diverse data collection schemes [6].

Shakil et al. [20] classifies data and assists the users in extracting useful information from data and also helps identifying a suitable algorithm for accurate predictive model from it. The main aim of this paper is to predict dengue disease using WEKA data mining tool [7]. The researchers here have made an important effort to extract information from a dataset elated to dengue which is a life threatening disease.

Abdelshafy et al. [21] have presented a new anti-flooding method that integrates into reactive protocol in MANETS. In the proposed methods cryptographic techniques which conserve the power and consumption of resources [8]. As an example, they integrate AODV to study the performance of the network under the absence and presence of the mechanism they have suggested.

O'Reilly et al. [22] surveys the problem of anomaly detection in wireless sensor networks in non-stationary environment. As Anomaly detection in a WSN is an important aspect of data analysis in order to identify data items that significantly differ from normal data. A characteristic of the data generated by a WSN is that the data distribution may alter over the lifetime of the network due to the changing nature of the phenomenon being observed. [9]

Fu et al. [23] have discussed anomaly mining algorithm which is developed to detect anomaly data of perception layer and also discusses an intrusion detection scheme which designed to detect anomalies.

Sedjelmaci et al. [24] proposes a lightweight anomaly detection technique based on game theory concept. With the help of Nash equilibrium, they have predicted the equilibrium state that allows the IDS agent to activate its anomaly detection technique to detect new attack's signature.

Arrington et al. [25] has proposed a method that discriminates between human (actor) activities orchestrated in a simulated environment by adaptive IDSs to detect the behavioral patterns. [12]

Chapter 4

Problem Statement

This chapter includes the problem statement of the thesis. It has also been explained as to why security has become a major concern in WSN networks.

4.1 Problem Statement

WSN has widespread applications in multiple domains. There are various challenges when a WSN network is considered. One of the major challenges is maintaining the security of the network. The domain of security has attracted attention in the recent times. As a WSN network may have multiple designs hence, it is difficult to design a single security design for each WSN network while still maintaining low overheads.

Many of WSN applications, protecting the whole data path from the device towards the remote server, which includes the mobile gateway, are definitely a main concern in WSN systems. Intrusion is a malicious activity that targets the security, confidentiality, integrity, and availability of the data flowing in the network. Potential vulnerabilities are continuously growing as we keep connecting new devices to the network. Some devices which are poorly secured at as an entry point for cyber-attacks which further allow attackers to cause malfunctions in the present network.

In this thesis the primary focus is simulating WSN networks which follow AODV routing protocol. The networks being simulated are under attacks like a black hole and flooding attack. After the simulation of networks, network traffic is captured and is analyzed through machine learning algorithms. Various classification algorithms are applied to the network traffic dataset captured. Also, the networks are analyzed under evaluation metrics like packet status, jitter and throughput.

4.2 Thesis Objectives

The work of this thesis has been done to achieve the following objectives:

- To simulate AODV networks with black hole and flooding attack.

- To analyze the network traffic using machine learning algorithms.
- To analyze the network under evaluation metrics like packet status, jitter and throughput.

Chapter – 5

Proposed Methodology and Implementation Details

In this chapter, we present the implementation work of our thesis. The solution to the problem in the previous section has been discussed below. This chapter provides the implementation details of the intrusion detection approach that we are following. The methodology used to implement the set objectives and the experiments which were performed are explained in this chapter.

5.1 Proposed Methodology and Work Flow

In this section we discuss the methodology used in this thesis work. The flowchart in figure 5.1 shows the simple steps followed. Simulation of the AODV protocol with various attack scenarios has been used to generate the dataset. The main aim is to analyze the AODV protocol under various attacks like a black hole and flooding attack.

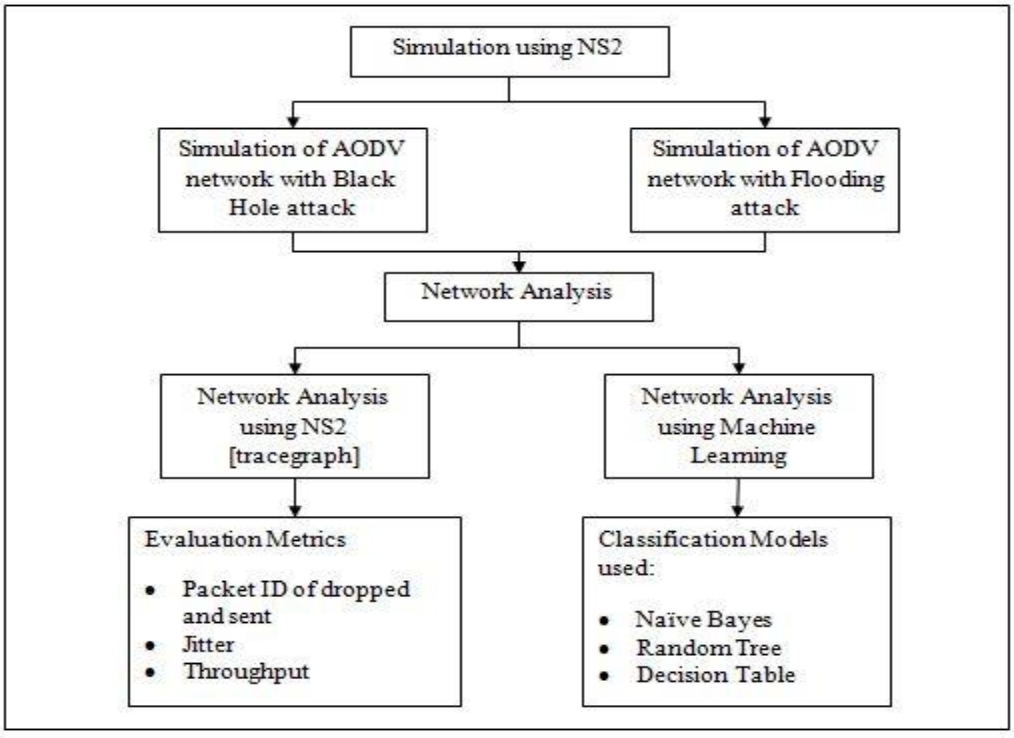

Figure 5.1: Work Flow of the thesis

The network simulated followed the AODV routing protocol. Further, the networks were accused with three different attacks: black hole and flooding attack. Once, the simulation has been done in NS2, there are two different files being generated as the result. The trace file (.tr file) and the network animator file (.nam file). Both the files are used for network analysis.

Trace graph is used to analyze the network animator file. It provides discrete event simulation targeted to network research for wired and wireless network. It is being used to plot the results of the network. Tracegraph allows its users to analyze their network from different ways. Analysis of parameters like throughput, end to end delay and jitter *etc*. can be evaluated using it. Also, graphs of various performance characteristics can be plotted in the form of 2D and 3D graphs. By interpreting various results of the tracegraph the malicious node can be identified.

5.2 The Network Simulator (NS2)

5.2.1 NS2 Overview

Network Simulator can be understood as a network driven simulator, which was developed by University of California, USA in 1989 with the help of many organizations. Presently, it is a project supported by DARPA [34]. Efforts are still being made to improve the features of NS. It is the responsibility of the users to keep a check on their work and watch for bugs. To help out the user a manual, namely NS manual is present for guidance. NS2 is implemented on Linux-based platform and is better known as an event driven simulator. In network Simulator the timing of the events is taken over by a scheduler. Multiple types of networks can be simulated using NS such as WPAN and WPAN according to the TCL scripts written. Also, several popular protocols such as UDP and TCP can be implemented using NS. Further network elements like signal strength and popular traffic models like FTP and CBR can be simulated.

NS2 uses two different languages, namely C++ and OTcl (an object oriented extension of Tcl). Simulation process is made efficient and faster with the help of C++ programming. In order to design a topology in NS2 an OTcl script must be designed by the user.

Through the script the user can define the topology of the network. Also, the output format can be set by the user. With the help of OTcl network component objects event scheduler objects are created. Once the simulation results are produced the output can be used for simulation analysis. The output can also be analyzed using the network animator or NAM.

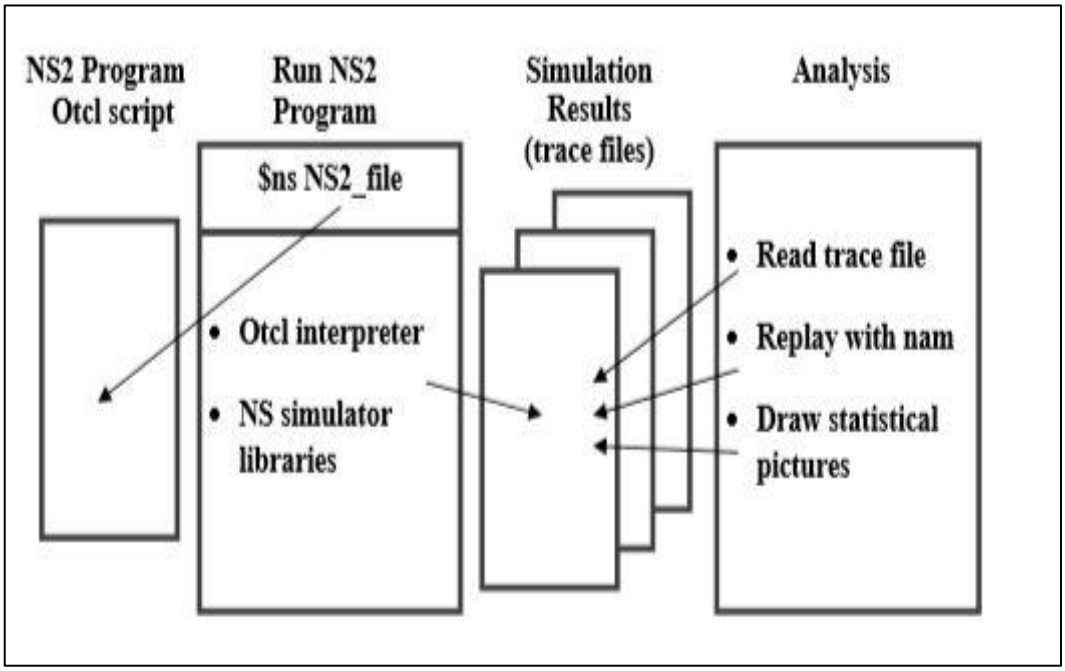

Figure 5.2 : Running program in NS2

5.2.2 Tool Command Language (Tcl)

Tool Command Language [tcl] [35] was developed by John Ouster from University of California, Berkeley. It is one of the popularly used languages. The application areas of Tcl include desktop application, testing, administration *etc*. One of the major advantages of using Tcl is that it is compatible with C and its libraries can operate directly into the C programs.

5.2.3 The Network Animation (NAM)

NAM has been implemented as an animation tool since 1990. It is used to trace data packets. The output is in the form of trace data from the network simulator. Further,

Marylou Orayani improved it. Presently, it developed by ISI under the Conser and SAMAN projects. The format of the trace file is made up of 12 fields as shown below:

Event	Time	From Node	To node	Packet Type	Packet Size	Flags	Fid	Source Address	Destination Address	Sequence Number	Packet Id

Figure 5. 3: Trace File Format

Table 5.1 represents the description of the fields of trace graph.

Table 5.1: Description of the fields of the tracegraph format

Field no.	Field	Description
1	Event	Represented by one of the four symbols from r, +, - and d, which mean received, enqueued, dequequed and dropped respectively.
2	Time	Time is the second field which explains the instant at which the event occurred.
3	From Node	Input node on the link
4	To node	Output node on the link
5	Packet Type	Packet type can be cbr or tcp which mean continuous bit rate and or transmission control protocol respectively.
6	Packet Size	Represents the size of the packet
7	Flag	Represents the flag associated with the trace file.
8	Fid	Id associated with the flag.
9	Source and Destination Address	Add. of the source and sink for the trace file.
10	Sequence Number	Represents a network layer protocol
11	Packet ID	Identification number associated with the packet

5.2.4 The Tracegraph

The results of simulation process can be analyzed using tracegraph. It can be considered as a data representation option for NS2. As it is a difficult process to understand the results of the simulation, hence tracegraph plays a useful role in this domain [36]. It provides a huge range of graphs, nearly 250 verities to analyze the result. Tracegraph has been implemented in MATLAB 6.0 and can be compiled and run on the same. Along with this the compiled versions for Linux and Windows are easily available on the Internet. Tracegraph supports multiple file formats like wireless (old and new trace), wired-cum-wireless, wired, satellite. There are multiple stages for file loading in tracegraph. The initial stage is the file format recognition phase; the second phase is the trace file parsing phase, which is used to extract important simulation data which is in the form of temporary files. The trace file consists of surplus data which is not even important to the user hence, necessary information must be extracted.

5.3 Overview of used classification techniques

- **Naïve Bayes**

It is a simple scheme for building classifiers. It is in fact a family of classifiers wherein each of the member classifiers are founded on the common principle of Bayes theorem. Here in, all member classifiers presume the value of all the attributes to be independent of each other given the class variable. For example, any record, in a collection of records of fruits, with the attribute values as red, round and 10cm in diameter is classified as an apple for the attributes of color, shape and size respectively. Any possible existence of any kind of correlation among the attributes of shape, color and size is disregarded, and are assumed to contribute independently to the probability of the particular record (fruit) being an apple. In a supervised learning setting and for some type of probability models certain naïve bayes classifiers can be trained very efficiently. The maximum likelihood method is used for parameter estimation for various Bayes models in a variety of practical applications without accepting Bayesian probability or using any Bayesian methods.

- **Decision Table**

They offer a very compact and precise way of modeling complex rule sets and their corresponding actions. Every decision in this table corresponds to a variable, relation or predicate whose value is mentioned for each of the condition alternatives. Each action corresponds to an operation to be performed, while the entries specify the particular set of actions and their particular order of execution as per the condition it corresponds to. Sometimes these tables also comprise of the don't care values that are represented using a hyphen. They can help in simplifying the decision tables, especially in a case wherein the actions are not influenced by the conditions. In some cases, conditions which were presumed to be of a lot of consequences prove to be completely irrelevant to the actions to be performed.

- **Random Tree**

In Random Tree algorithm a tree is constructed which considers K number of attributes those are chosen randomly. This process is repeated for each node. It is one of the popular classifiers used in machine learning.

5.4 Simulation in NS2

5.4.1 General workflow of the simulation in NS2

- **Generation of Tcl file**

TCL is a scripting language which is very similar to python and PERL. Within the TCL code we create nodes in the network and define the links between them. Also, we need to create the malicious nodes here. Once, the TCL code is ready. The TCL code needs to be executed in the NS2 simulator. In order to run the TCL file (black.tcl) we need to write the following on the terminal:

ns file_name.tcl

5.4.2 Simulation of AODV networks

Using the above mentioned workflow simulation of two different AODV networks has been performed:

(i) Experiment 1: **AODV network simulation in NS2 with black whole attack.**

- Simulation Information: The table below shows the simulation information about the black hole attack in AODV.

Table 5.2: Simulation information of AODV protocol under black hole attack

Simulation Information	
Simulation Length	4.989
Number of sending nodes	6
Number of receiving nodes	6
Number of dropped packets	334
Number of lost packets	328
Minimal packet size	28
Maximal packet size	1078
Number of sent packets	202138
Number of forwarded packets	44
Number of dropped bytes	170340
Packet dropping node	1

- Simulation of the black hole attack in NS2

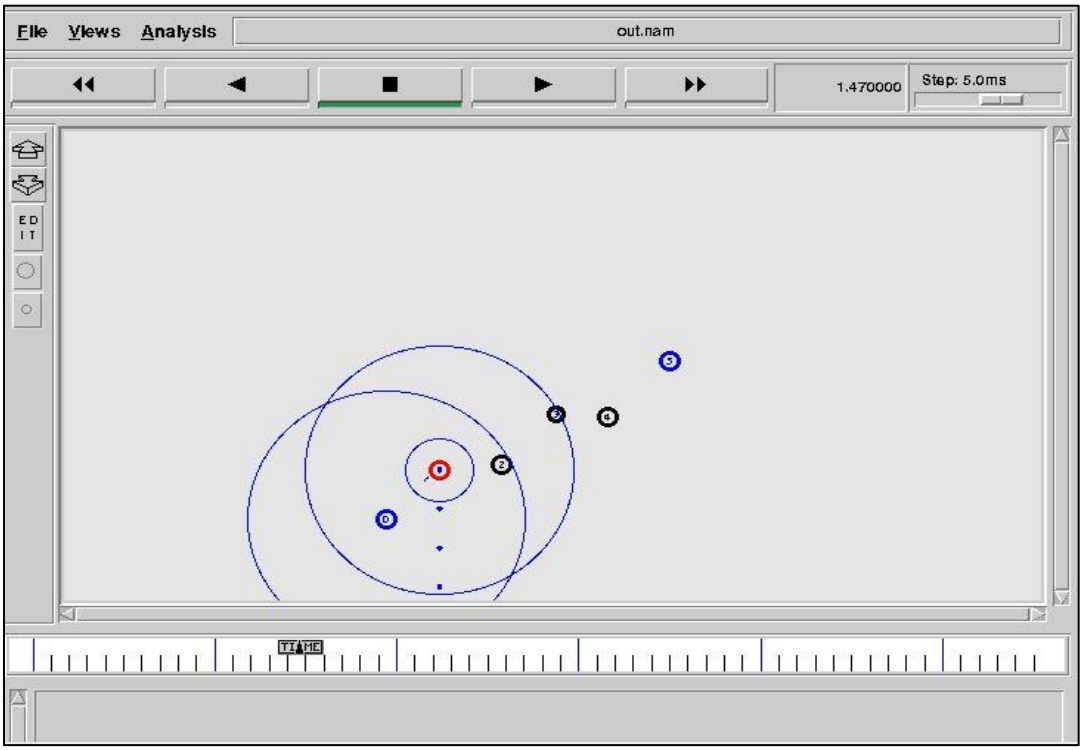

Figure 5.4: Black hole attack simulation in an AODV network using NS2

(ii) **Experiment 2**: **AODV network simulation in NS2 with flooding attack.**

- Simulation Information: The table below shows the simulation information about the black hole attack in AODV.

Table 5.3: Simulation information about flooding attack under flooding attack

Simulation Information	
Simulation Length	5.01623
Number of sending nodes	19
Number of dropped packets	191

Minimal packet size	220
Maximal packet size	640
Number of sent bytes	9240
Number of forwarded packets	6
Number of dropped bytes	72240
Packet dropping node	9,13,15

- Simulation of flooding attack in NS2

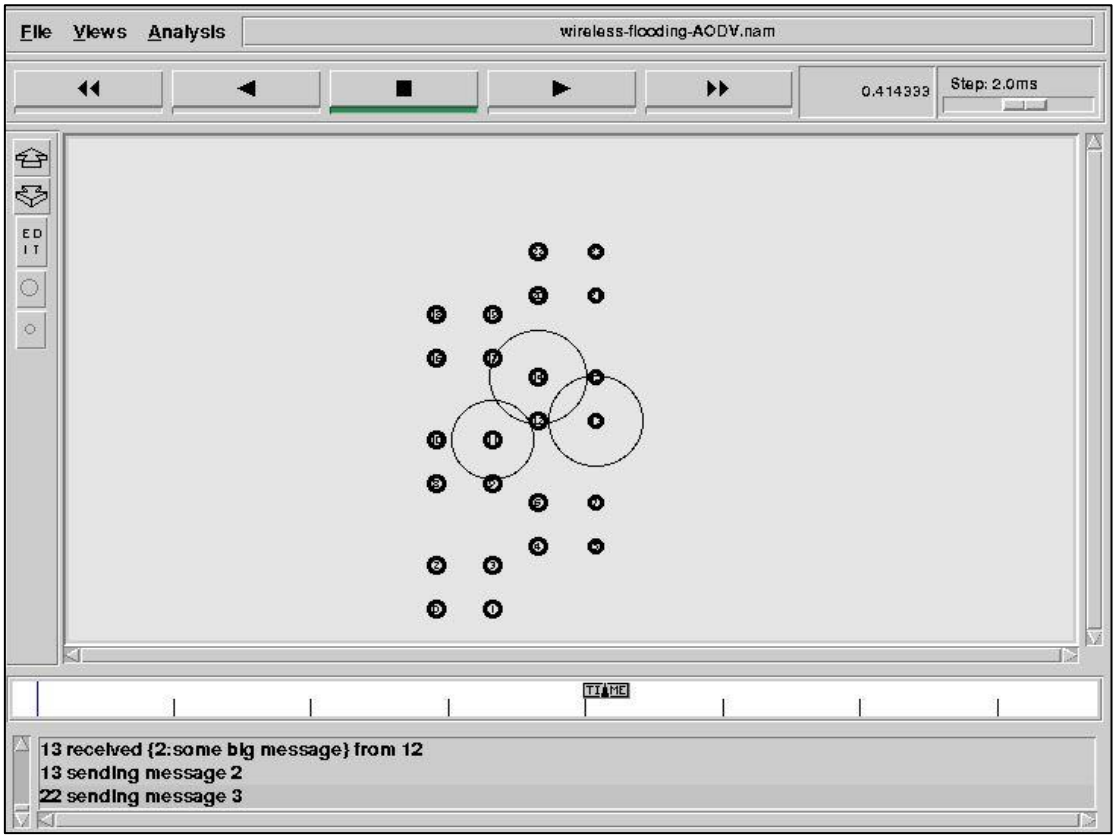

Figure 5.5: Simulation of AODV protocol under flooding attack

Chapter Summary: In this chapter we presented the NS2 simulation of two different networks which follow the AODV protocol.

Chapter – 6

Results, Evaluation and Analysis

This chapter shows the results of the simulation on performance metrics like jitter, throughput and the packet status. Simulation information of the malicious node in the network is also presented. In this chapter machine learning results are discussed as well.

6.1 Evaluation Metrics

(i) Jitter: Jitter can be defined as the delay that may occur in receiving the packets within the network. Packets are transferred in the form of streams that are continuous in nature and are evenly separated. This lag may occur due to conditions like configuration errors, congestion and improper queuing. This delay may not be constant.

(ii) Throughput: Throughput is the standard amount of data that that has moved successfully from sender to receiver in asset interval of time. It is measured in bits per second (bps), megabits per second (Mbps) or gigabits per second (Gbps).

(iii) Packet Status: Packet status is the state of the packet within the network. A packet can have four different states, namely sent, forwarded, dropped and received.

6.2 Analysis of Black hole attacks in an AODV network

The black hole attack is a kind of Denial of Service attack. During the route discovery malicious node portrays that it has the best path to the destination node. On receiving a RREQ message, it responds with a fake RREP, and further, when the malicious node receives packets from the source it drops the packets instead of forwarding it. We have simulated black hole attack in an AODV network.

- **Malicious Node Detection**: While analyzing the .tr file in tracegraph, it is possible to evaluate the simulation information of each and every node in the network. Hence, it is observed that all the nodes in the network except the malicious node has a null or a minimal count of the dropped packets. In the present network it was evaluated

that node 1 in the network is malicious the simulation information of the node is given below.

Table 6.1: Simulation information of the malicious node in Black Hole Attack

Simulation Information	
Number of received packets	346
Number of forwarded packets	0
Number of dropped packets	334
Number of dropped bytes	170340
Minimal packet size	28
Maximal packet size	1020
Average packet size	277.5

- **Packet Status**

The graph in figure 6.1 displays the information regarding dropped packet and packet drop time. The x axis represents the packet drop time and the y axis represents the id of the dropped packets. In black hole the malicious node drops the packets travelling on the network.

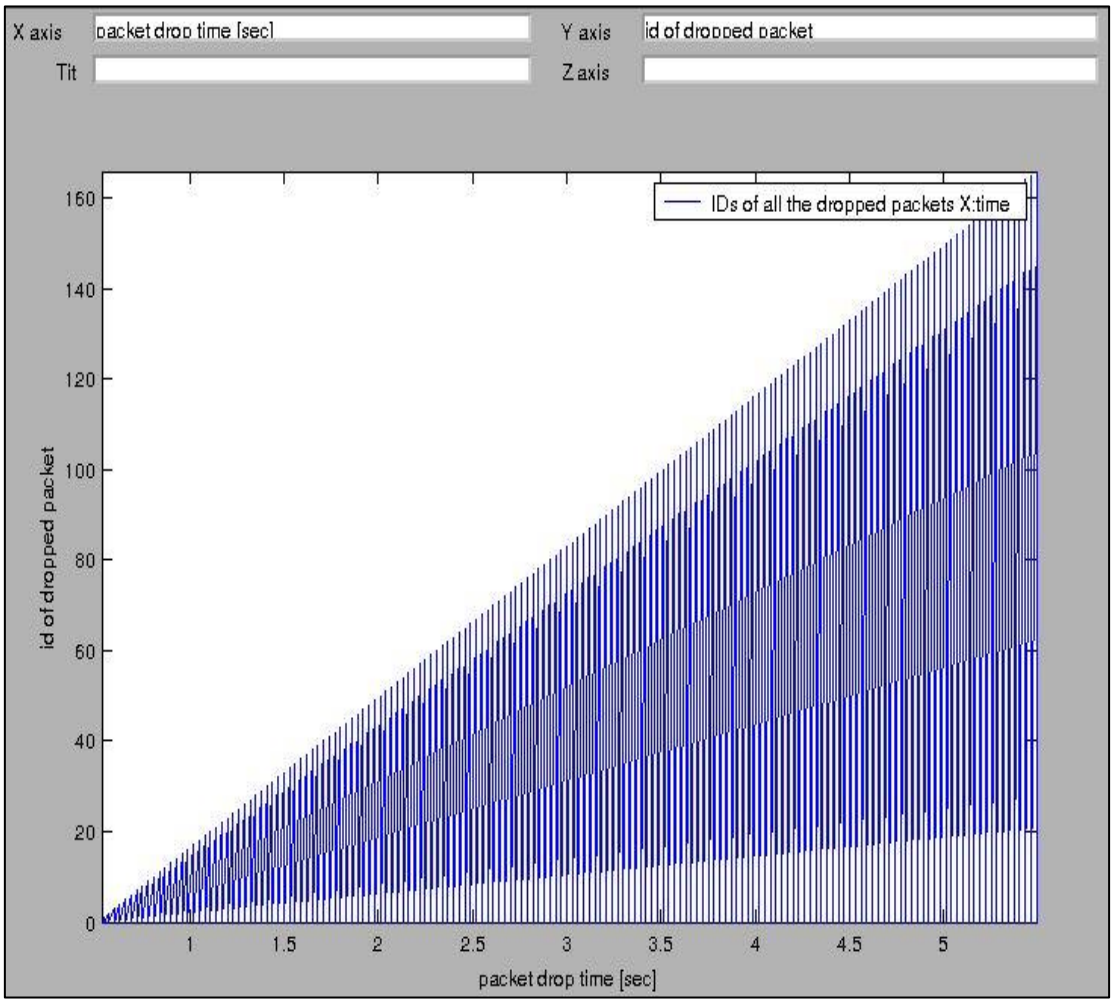

Figure 6.1 : Dropped packets in AODV network under black hole attack

- **Jitter**

In figure 6.2 y-axis represents the jitter of the dropped packet and the x-axis represents the respective sequence number. In black hole attack jitter may be caused due to dropped packets in the network. The graph represents the jitters of the dropped packets according to their respective sequence number.

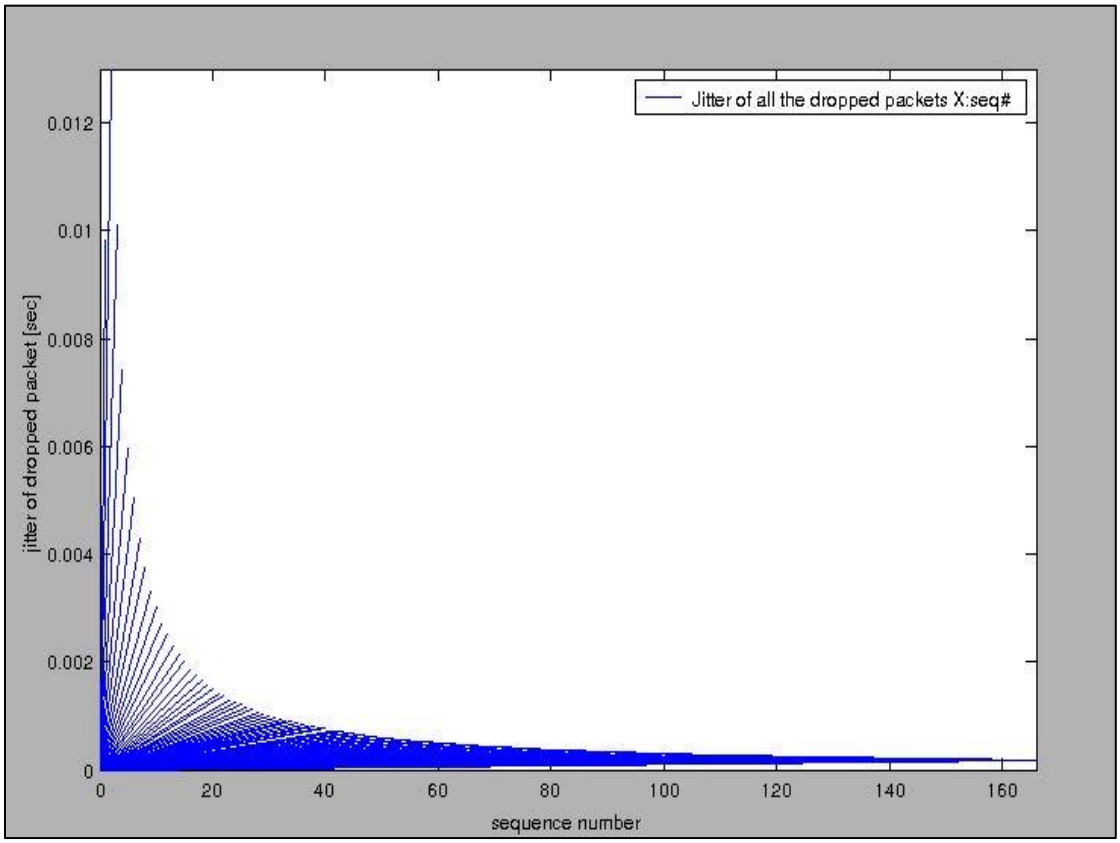

Figure 6.2: Jitter of the dropped packets in black hole attack

- **Throughput**

The graph in figure 6.3 represents simulation time on the x axis and throughput of dropped packet on the Y axis. The throughput of a network can vary from time to time. In the graph below it can be clearly observed that throughput at 1.5 sec is the highest value of throughput of the network.

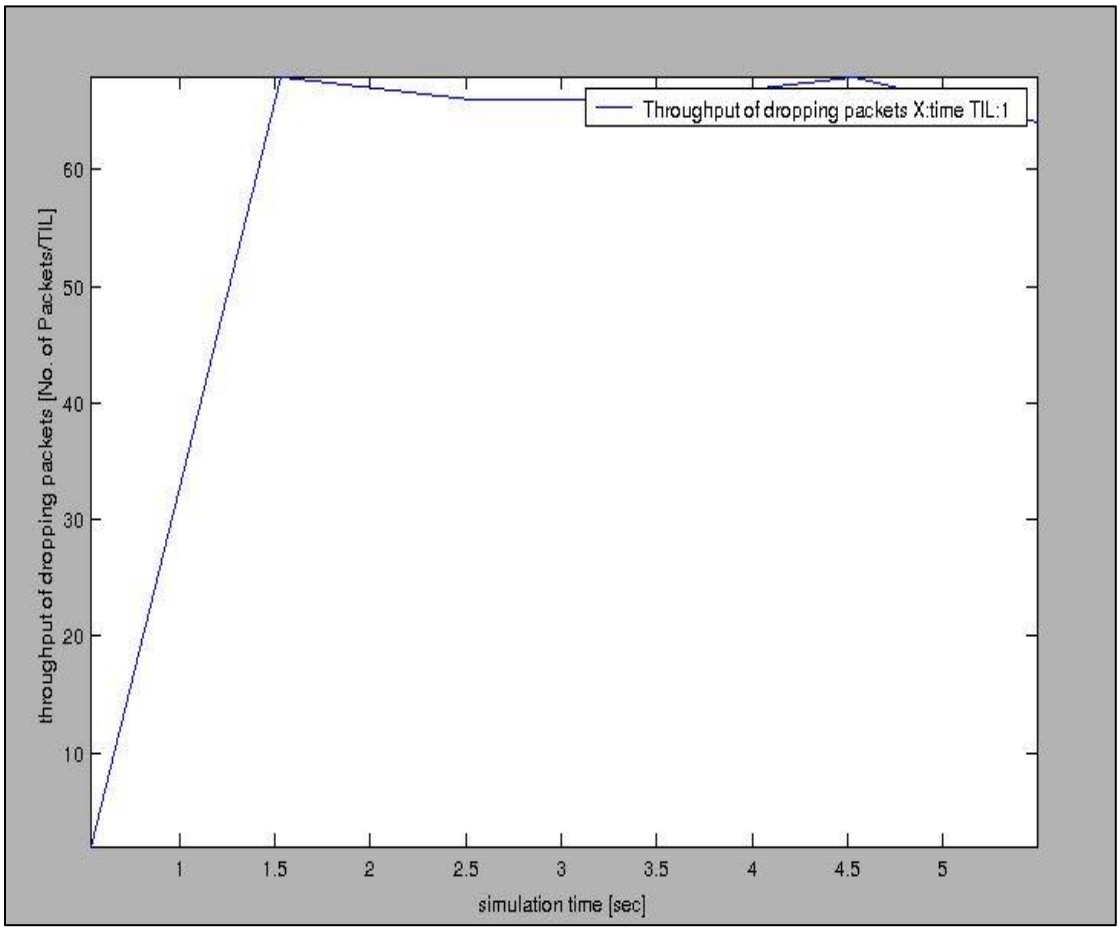

Figure 6.3: Throughput of dropping packet in AODV network.

- **Machine Learning analysis**

The below table represents the performance of the dataset related to black hole attack in AODV. The performance of the dataset was tested with three different models namely, Naïve Bayes , Decision Tree and Random Tree. It is observed that Decision Table model gives the most accurate results with almost 94.8% accuracy.

Table 6.2: Machine Learning classification analysis results for Black Hole

Model Name	Naïve Bayes	Decision Table	Random Tree
Percentage of Correctly Classified Instances	75.7895 %	98.9183%	74.7596 %
Percentage of Incorrectly Classified Instances	24.2105	1.0817 %	25.2404 %
Mean absolute error	0.1988	0.0244	0.1289
Root mean squared error	0.3126	0.0733	0.3523
Percentage of Relative absolute error	59.8341 %	7.989 %	42.1682 %
Percentage of Root relative squared error	80.1782 %	18.673 %	89.7445

6.3 Analysis of Flooding Attack in an AODV network

Flooding attack in AODV is a type of denial of service attack where the malicious nodes send a large number of SYN requests to the target system in order to consume large amount of resources which makes the rest of the network unresponsive to legitimate traffic. This phenomenon decreases the total efficiency of the network.

- **Malicious Node Detection**: While analyzing the .tr file in tracegraph, it is possible to evaluate the simulation information of each and every node in the network. Hence, it is observed that the malicious node is the node with the highest number of sending packets. In the present network it was evaluated that node 11 in the network is malicious node with the highest number of sent packet count of the simulation information of the node is given below.

Table 6.3: Simulation information of malicious node in flooding attack

Simulation Information	
Number of received packets	920
Number of sent packets	960
Number of dropped packets	6
Number of dropped bytes	1900
Minimal packet size	300
Maximal packet size	640

- **Packet Status**

The graphs below show the information regarding sent packets in the network. The x-axis represents the packet sent time and the y axis represents the id of the sent packet. In flooding attack it is observed that the node forwarding the maximum packets is the malicious node. Hence, in figure 6.4 the graph depicts the status of the sent packets.

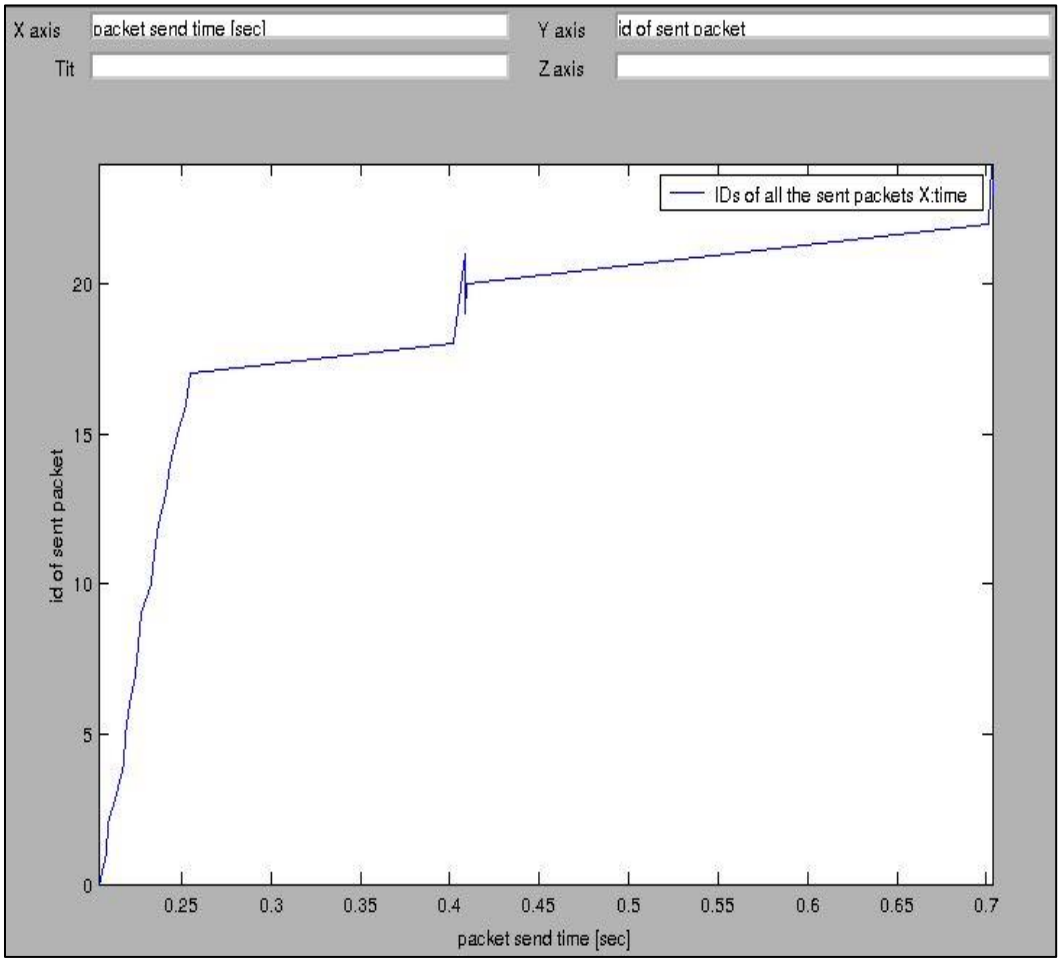

Figure 6.4: Packet status of sent packets in Flooding Attack

- **Jitter**

The graph in figure 6.5 depicts the sequence number on the x-axis and jitter of sending packets on the y axis. The cause of jitter in flooding attack can be factors like congestion due to the relative increase of traffic compared from the normal conditions**.**

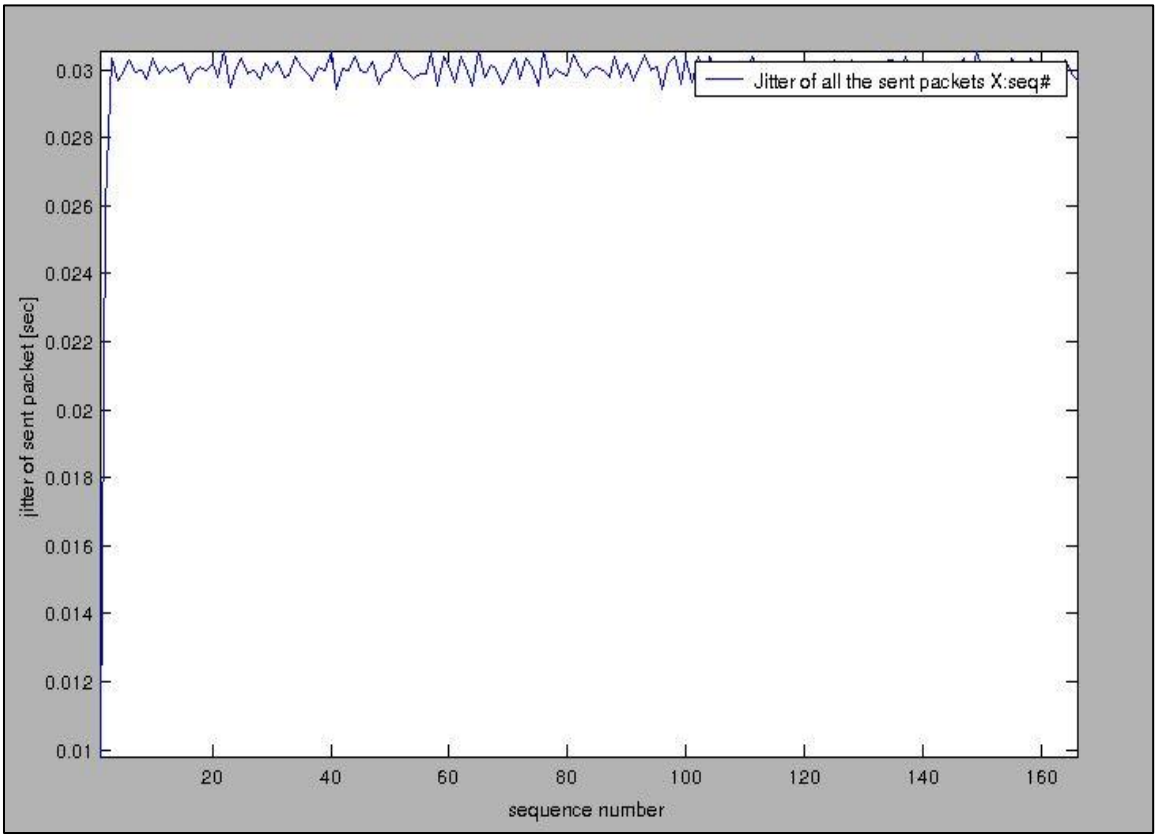

Figure 6.5: Jitter of sent packets in flooding attack

- **Throughput**

The graph in figure 6.6 represents simulation time on the x axis and throughput of dropped packet on the Y axis. Throughput of a network can vary from time to time. In the graph below it can be clearly observed that throughput at 1.5 sec is the highest value of throughput of the network.

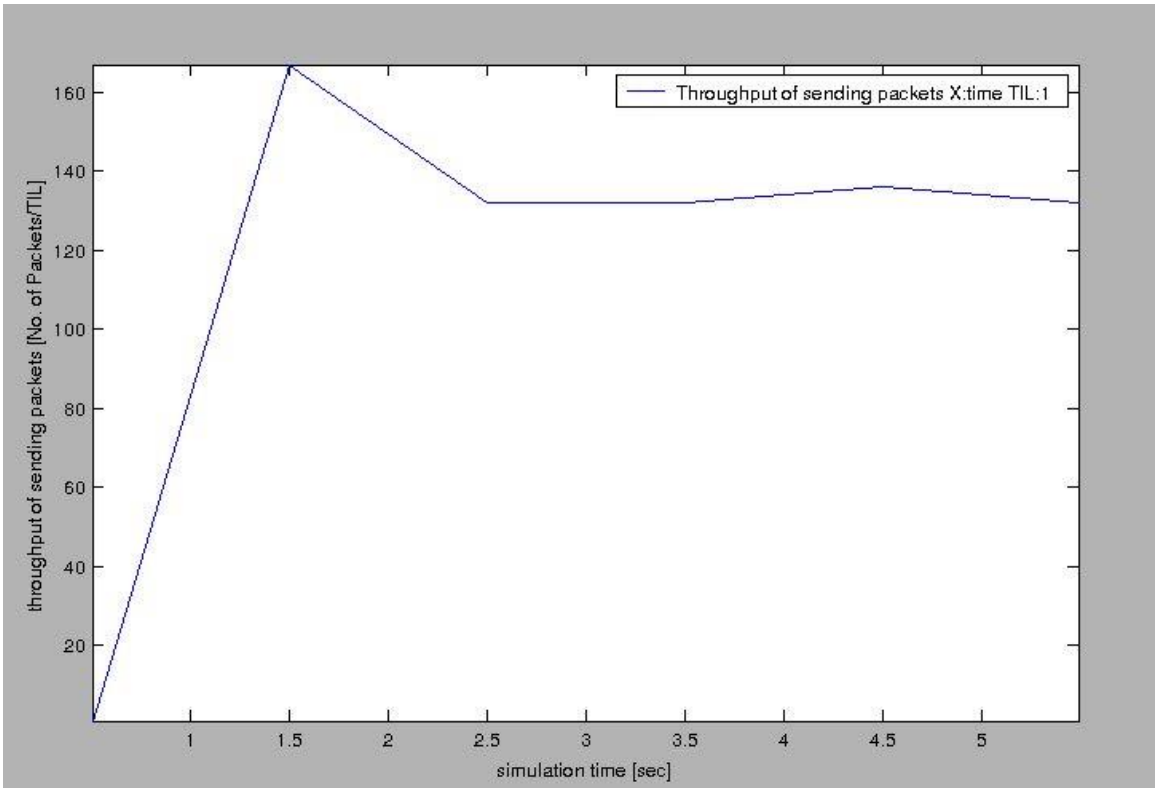

Figure 6.6: Throughput sent packets in flooding attack

- **Machine Learning analysis**

The below table represents the performance of the dataset related to worm hole attack in AODV. The performance of the dataset was tested with three different models namely, Naïve Bayes , Decision Tree and Random Tree. It is observed that Naïve Bayes model gives the most accurate results with almost 77% accuracy.

Table 6.4: Machine learning classification analysis results for Flooding Attack

Model Name	Naïve Bayes	Decision Table	Random Tree
Percentage of Correctly Classified Instances	77.381 %	72.6316 %	72.6316 %
Percentage of Incorrectly Classified Instances	22.619 %	27.3684 %	27.3684 %
Mean absolute error	0.189	0.2484	0.1671
Root mean squared error	0.3155	0.344	0.3579
Percentage of Relative absolute error	56.8819 %	74.7692 %	50.2899 %
Percentage of Root relative squared error	76.346 %	83.0301 %	86.3777 %

Chapter Summary: In this chapter the results regarding network analysis are presented. Each network has been analyzed on evaluation metrics like packet status, jitter and throughput. Also, each network is analyzed using machine learning algorithms like Naïve Bayes, Decision Tree and Random Tree.

Chapter 7

Conclusion and Future work

7.1 Conclusion

The application domain of WSN is wide and hence, security has become one of the important issues in any WSN network. Security within the network needs to be maintained for a WSN network to function smoothly but there is always a scope of a malicious node in the network which can disrupt the normal working of the network.

The research carried out in this thesis mainly focuses on identifying the malicious node in the network. Also, the networks are evaluated on performance metrics like packet status, jitter and throughput. In this thesis, we have particularly simulated two networks implementing the AODV routing protocol. Two different attacks, namely black holes, and flooding attack have been simulated. Each network has been analyzed using machine learning algorithms. Further, tracegraph has also been used to identify the exact malicious node in the network. In machine learning classification algorithms such as Naïve Bayes, Random Forest and Random Tree have been used. Machine learning is applied on the dataset generated by the simulation process [.tr file].

After the simulation process two different files are generated namely, the trace file and the network animator file. The trace file, helps generating the dataset. The network animator file helps to gather simulation information for each node in the network and also produces numerous graphical results which further helps in understanding the network.

7.2 Future Scope

In this particular thesis we aim to identify the intruding node within the network and hence, for the future scope a deeper analysis of the network can be done using other machine learning techniques. Also, different patterns and behaviors of each node can be identified in order to compare it with other nodes in the network and classify a particular

node as malicious and non-malicious. Also, an alarm or alert can be generated if there is any malicious node in the system.

References

[1] P. Singh, O. Gupta, and S. Saini, “A brief research study of wireless sensor network,” Advances in Computational Sciences and Technology, vol. 10, no. 5, pp. 733–739, 2017.

[2] Figure available on: https://www.researchgate.net/figure/259296305_fig1_Figure-1-WSN-architecture.

[3] R. Kumari and S. Dalal, “Review paper on design and simulation result analysis of data aggregation in ns2 for wsn with security,” 2017.

[4] B. Prabhu, N. Balakumar, and A. J. Antony, “Wireless sensor network based smart environment applications,” 2017.

[5] A. Lazarevic, V. Kumar, and J. Srivastava, “Intrusion detection: A survey,” in Managing Cyber Threats. Springer, 2005, pp. 19–78.

[6] Kumar, Sandeep, and H. Eugene Spafford. "A software architecture to support misuse intrusion detection." (1995).

[7] Axelsson, Stefan. “Intrusion detection systems: A survey and taxonomy”, vol. 99, 2000.

[8] S. Kumar, “Classification and detection of computer intrusions,” Ph.D. dissertation, Purdue University, 1995.

[9] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fern ´ andez, and ´ E. Vazquez, “Anomaly-based network intrusion detection: Tech- ´ niques, systems and challenges,” computers & security, vol. 28, no. 1, pp. 18–28, 2009.

[10] K. Konate and A. Gaye, “Modelling of a secure mechanism in routing protocol of manets: Application of theory of games,” International Journal of Distributed and Parallel Systems, vol. 2, no. 6, p. 335, 2011.

[11] S. Agarwal, S. Bansal, and A. S. Siddiqui, “Performance analysis of reactive, proactive and hybrid routing protocol used in petroleum tank over network control systems,” in Proceeding of International Conference on Intelligent Communication, Control and Devices. Springer, 2017, pp. 367–374

[12] U. Ghugar and J. Pradhan, “A study on black hole attack in wireless sensor networks,” IJACTA, vol. 5, no. 1, pp. 001–003, 2017.

[13] J. Kurmi, R. S. Verma, and S. Soni, “An efficient and reliable methodology for wormhole attack detection in wireless sensor network,” Advances in Computational Sciences and Technology, vol. 10, no. 5, pp. 1129–1138, 2017.

[14] S.-M. Jen, C.-S. Laih, and W.-C. Kuo, “A hop-count analysis scheme for avoiding wormhole attacks in manet,” Sensors, vol. 9, no. 6, pp. 5022–5039, 2009.

[15] I. Dhyani, N. Goel, G. Sharma, and B. Mallick, “A reliable tactic for detecting black hole attack in vehicular ad hoc networks,” in Advances in Computer and Computational Sciences. Springer, 2017, pp. 333–343

[16] D. G. Reina, S. L. Toral, F. Barrero, N. Bessis, and E. Asimakopoulou, “The role of ad hoc networks in the Internet of things: A case scenario for smart environments,” in Internet of Things and Inter-Cooperative Computational Technologies for Collective Intelligence. Springer, 2013, pp. 89–113.

[17] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, “Convergence of manet and wsn in iot urban scenarios,” IEEE Sensors Journal, vol. 13, no. 10, pp. 3558–3567, 2013

[18]S. Shah, A. Khandre, M. Shirole, and G. Bhole, “Performance evaluation of ad hoc routing protocols using ns2 simulation,” in Conf. of Mobile and Pervasive Computing, 2008.

[19] C. Chen and J. Ma, “Simulation study of aodv performance over ieee 802.15. 4 mac in wsn with mobile sinks,” in Advanced Information Networking and Applications Workshops, 2007, AINAW’07. 21st International Conference on, vol. 2. IEEE, 2007, pp. 159–164.

[20] K. A. Shakil, S. Anis, and M. Alam, “Dengue disease prediction using weka data mining tool,” arXiv preprint arXiv:1502.05167, 2015.

[21]M. A. Abdelshafy and P. King, “Resisting flooding attacks on aodv,” SECURWARE, vol. 25, 2014.

[22] C. O’Reilly, A. Gluhak, M. A. Imran, and S. Rajasegarar, “Anomaly detection in wireless sensor networks in a non-stationary environment,” IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1413–1432, 2014.

[23]R. Fu, K. Zheng, D. Zhang, and Y. Yang, “An intrusion detection scheme based on anomaly mining in Internet of things,” 2011.

[24] H. Sedjelmaci, S. M. Senouci, and M. Al-Bahri, “A lightweight anomaly detection technique for low-resource iot devices: A gametheoretic methodology,” in Communications (ICC), 2016 IEEE International Conference on. IEEE, 2016, pp. 1–6.

[25]B. Arrington, L. Barnett, R. Rufus, and A. Esterline, “Behavioral modeling intrusion detection system (bmids) using Internet of things (iot) behavior-based anomaly detection via immunity-inspired algorithms,” in Computer Communication and Networks (ICCCN), 2016 25th International Conference on. IEEE, 2016, pp. 1–6.

[26] J. Wang, S. Jiang, and A. O. Fapojuwo, “A protocol layer trust-based intrusion detection scheme for wireless sensor networks,” Sensors, vol. 17, no. 6, p. 1227, 2017.

[27]R. V. Biradar, V. Patil, S. Sawant, and R. Mudholkar, “Classification and comparison of routing protocols in wireless sensor networks,” Special Issue on Ubiquitous Computing Security Systems, vol. 4, no. 2, pp. 704–711, 2009.

[28] S. K. Singh, M. Singh, and D. Singh, “Energy-efficient homogeneous clustering algorithm for wireless sensor network,” International Journal of Wireless & Mobile Networks (IJWMN), vol. 2, no. 3, pp. 49–61, 2010.

[29] S. Manjula, C. Abhilash, K. Shaila, K. Venugopal, and L. Patnaik, “Performance of aodv routing protocol using group and entity mobility models in wireless sensor networks,” in Proceedings of the International MultiConference of Engineers and Computer Scientists, vol. 2, 2008, pp. 1212–1217.

[30] S. Mohapatra and P. Kanungo, “Performance analysis of aodv, dsr, olsr and dsdv routing protocols using

[31] S. Gowrishankar, T. Basavaraju, M. Singh, and S. K. Sarkar, “Scenario based performance analysis of aodv and olsr in mobile ad hoc networks,” in Proceedings of the 24th South East Asia Regional Computer Conference, vol. 15, no. SP4, 2007. [32] Figure available on: www.researchgate.net

[33] S. McCanne and S. Floyd. Network Simulator. http://www.isi.edu/nsnam/ns/

[34] TCL Tutorial. http://www.tcl.tk/man/tcl8.5/tutorial/tcltutorial.html

[35] Tracegraph http://www.tracegraph.com/download.html

[36] Ad hoc on-demand distance vector (AODV) routing. Available on http://www.ietf.org/rfc/rfc/rfc3561txt.

[37] H. Deng,Q. A. Zeng, and D. P. Agrawal, “SVM-basedintrusion detection system for wireless ad hoc networks,” in Proceedings of the 58th IEEE Vehicular Technology Conference(VTC’03),pp. 2147–2151,October2003.

[38] Y. Ping, J. Xinghao,W .Yue,and L. Ning,“Distributedintrusion detection for mobile ad hoc networks,” Journal of Systems EngineeringandElectronics,vol.19, no.4, pp.851–859, 2008.

[39] S. Northcuttand J. Novak, NetworkIntrusionDetection, SAMS, 3rdedition, 2002.

[40] T. M. Chen, G.-S. Kuo, Z.-P. Li, and G.-M. Zhu, "Intrusion detection in wireless mesh networks," in Security in Wireless MeshNetworks,Y.Zhang,J.Zheng,andH.Hu,Eds.,CRCPress, NewYork,NY,USA,2007.

[41] E. J. Caballero, "Vulnerabilities of intrusion detection systems in mobile ad-hoc networks—the routing problem," in TKK T110.5290SeminaronNetworkSecurity,2006.

[42] I. Krontiris , T. Dimitriou and C. Freiling, "Towards intrusion detection in wireless networks" , in Proceeding *13th European Wireless Confrence,Paris,France,April* 2007.

[43] H. Jadidoleslamy, "A hierarchical intrusion detection architecture for wireless sensor networks," International Journal of NetworkSecurity&ItsApplications,vol.3,no.5,2011.

[44] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "Intrusion detection of Sinkhole attacks in wireless sensor networks," in Algorithmic Aspects of Wireless Sensor Networks ALGOSENSORS,vol.4837ofLectureNotesinComputerScience, pp.150–161,Springer,2008.

[45] H. Jadidoleslamy, "A hierarchical intrusion detection architecture for wireless sensor networks," International Journal of NetworkSecurity&ItsApplications,vol.3,no.5,2011.

[46] M. S. Islam and S. A. Rahman, "Anomaly intrusion detection systeminwirelesssensornetworks:securitythreatsandexisting approaches," International Journal of Advanced Sciences and Technology,vol.36,pp.1–8,2011

[47] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wirelesssensornetworks,"JournalofHighSpeedNetworks,vol. 15,no.1,pp.33–51,2006.

[48] H.SedjelmaciandM.Feham,"Novelhybridintrusiondetection system for clustered wireless sensor network," International JournalofNetworkSecurity&ItsApplications,vol.3,no.4,2011.

[49] Raza, Shahid, et al. "Lithe: Lightweight secure CoAP for the Internet of things." *IEEE Sensors Journal* , 2013.

[50] R. Rajpal, R., & S. Kaur," A Hybrid Approach for Intrusion Detection using Misuse Detection and Genetic Algorithm" (Doctoral dissertation),2015.

[51] Z. Karakehayov, "Using reward to detect team black-hole attacks in wireless sensor networks," Wksp. Real-World Wireless Sensor Networks, pp. 20– 21, 2005.

[52] M. Wazid and A. K. Das, "A secure group-based blackhole node detection scheme for hierarchical wireless sensor networks," Wireless Personal Communications, vol. 94, no. 3, pp. 1165– 1191, 2017.

[53] K. R. Venkatesh and P. D. Prasad, “Dynamic conviction protected and trustable direction-finding in wireless sensor networks,” IJITR, vol. 5, no. 3, pp. 6170– 6172, 2017.

[54] R. Kumari and P. K. Sharma, “A literature survey on detection and prevention against vampire attack in wsn,” in Advances in Computer and Computational Sciences. Springer, 2017, pp. 271– 279.

[55] S. Amin, K. Saghar, M. B. T. Abbasi, and A. Elahi, “Arhum-arrive protocol with handshake utilization and management,” in Applied Sciences and Technology (IBCAST), 2017 14th International Bhurban Conference on. IEEE, 2017, pp. 401– 407.

[56] W. Pires, T. H. de Paula Figueiredo, H. C. Wong, and A. A. F. Loureiro, “Malicious node detection in wireless sensor networks,” in Parallel and Distributed Processing Symposium, 2004. Proceedings. 18th International. IEEE, 2004, p. 24.

[57] R. Braga, E. Mota, and A. Passito, “Lightweight ddos flooding attack detection using nox/openflow,” in Local Computer Networks (LCN), 2010 IEEE 35th Conference on. IEEE, 2010, pp. 408– 415.

[58] V. P. Singh, S. Jain, and J. Singhai, “Hello flood attack and its countermeasures in wireless sensor networks,” IJCSI International Journal of Computer Science Issues, vol. 7, no. 11, pp. 23– 27, 2010.

Video presentation

https://www.youtube.com/watch?v=il4I7IFDL54

Research Publication

[1] N. Girnar and S. Kaur "Design of Financial Inclusion System for Rural India", in Proceedings of IEEE International Conference on Computing Communication and Automation (ICCCA2017), Galgotia University, Noida, May 5-6, 2017.

[2] N. Girnar and S. Kaur "Intrusion Detection in Adhoc Networks in IOT", in Proceedings of IEEE International Conference on Intelligent Computing and Control System (ICICCS 2017), VCE, Madurai, June 15-16, 2017.