Security Analysis of DSR and DSDV 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 Applications

Submitted By

Kriti Taneja

(601534007)

Under the supervision of:

Dr. Sanmeet Kaur

Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

July 2017

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "Security Analysis of DSR and DSDV Protocol in Wireless Sensor Networks", in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Computer Science and Applications* 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.

Kriti Taneja

(Kriti Taneja)

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 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, 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 in the University for making provisions of infrastructure such as library facilities, computer labs equipped with Internet facility, immensely useful for the learners to equip themselves with 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.

ABSTRACT

Wireless Sensor Networks are deployed in various application areas such as healthcare, military, agriculture, home automation, etc. Security of WSNs has become crucial issue because of the transmission of sensitive data through the systems integrated with WSN architecture. Many methods has been developed to secure computer networks and communications over internet, but WSN requires different security mechanism because of its unique architecture and the constraints it faces. Intrusion detection method is one such method which has gained importance over the past few years. An Intrusion detection system gathers the information from various devices within a network and analyzes that information to identify any possible security threats.

There are different techniques of intrusion detection which are discussed in this thesis. Anomaly detection technique has been implemented in the thesis to detect intruder in the network. WSN routing protocols are classified into various types, that are, mode of function, type of network structure and participation styles of nodes. Mode of function is further classified into reactive, proactive and hybrid. DSR and DSDV routing protocols, which are reactive and proactive protocols respectively, are simulated in a network in this thesis.

The main objective of this thesis is to do a comparative study of network behavior of DSR and DSDV protocol with intrusion and without intrusion. This comparison is done because anomaly intrusion detection technique has been applied. The evaluation metrics on the basis of which performance is compared are throughput, packet ID of received data packets and cumulative sum of lost bytes. this performance evaluation is done using trace graph tool in NS-2 network simulator. Furthermore, the dataset generated after simulation is deeply analyzed on a machine learning tool, by processing the data on different classification algorithms to obtain the results.

Table of Contents

List of Figures

List of Tables

List of Screenshots

List of Algorithms

CHAPTER 1

INTRODUCTION

1.1 Wireless Sensor Network

Wireless Sensor Network (WSN) is a network which consists of distributed autonomous devices which pertain wireless connection among each other. These devices contain sensors to monitor the physical conditions or environmental conditions. Wireless sensor network have gained importance in the field of science and technology in recent years because of various features it provides such as ease of implementation, can operate in a harsh environment, ease of maintenance and provide high-level performance. The sensors in WSN are capable of automatically detecting diverse environment metrics and hence processing data and transmitting it to the base station or other nodes. This autonomous and intelligent behavior of sensors does not need manual manipulation for collecting data. In recent years, WSN has gained its prominence and has made its way to the construction of Internet of Things (IoT) systems in various fields such as Healthcare, Military, Agriculture, Manufacturing, Traffic control, supply and retail, and much more. WSNs are made up of a huge number of tiny and low-cost devices connected to each other for communicating data they collect by sensing the environment happenings.

A sensor field consists of several sensor nodes which function as transceivers having a capability of collecting data and routing it back through the sink node or a gateway to the end user. The architecture of this network contains multiple hops and has an absence of infrastructure. The sink node communicates to the end user via Internet, satellite and other wireless networks such as WiFi, WiMAX, etc. and can also be connected directly to end users in some cases (Figure 1.1). A sensor node consists of five main components:

- Microcontroller: It carries out the processing of the data by simple computations and gives the required output. It also consists of a small segment of storage memory embedded in it. It controls other components of the sensor nodes and executes the associated algorithms to produce an output.

- Transceiver: Its basic usage is communication with other nodes and other parts of the network. This communication leads to high power consumption.
- Memory: These sensor nodes consist of a temporary storage unit such as RAM, ROM, SRAM, SDRAM, etc. or external storage such as USB.
- Power: Sensor nodes get power energy from battery supplies which are rechargeable. To recharge these batteries, natural sources can be used such as solar power, kinetic energy, power from turbines, etc.
- Sensor/Actuator: Sensor is the main component of these nodes which distinguish them from other embedded devices. This component gives nodes a sensing capability from the physical environment. There are many types of sensing units categorized as temperature, humidity, moisture, light, etc. It is also composed of an Analog to Digital converter (ADC). Analog signals received from the sensor unit by sensing physical phenomenon are converted into Digital signals by ADC for further processing by the microcontroller. These sensor nodes are responsible for gathering the information from surroundings by sensing and routing the information to its neighbor nodes or to the sink. The routing decision depends on the protocol that has been applied in the network.

WSN architecture supports both, multi-hop as well as single-hop communication among nodes. When the transmission range of radio signal is large then every sensor node can communicate directly with the base station in a single hop creating a star topology but it consumes high degree of the power supply which makes it less common for usage in WSN.

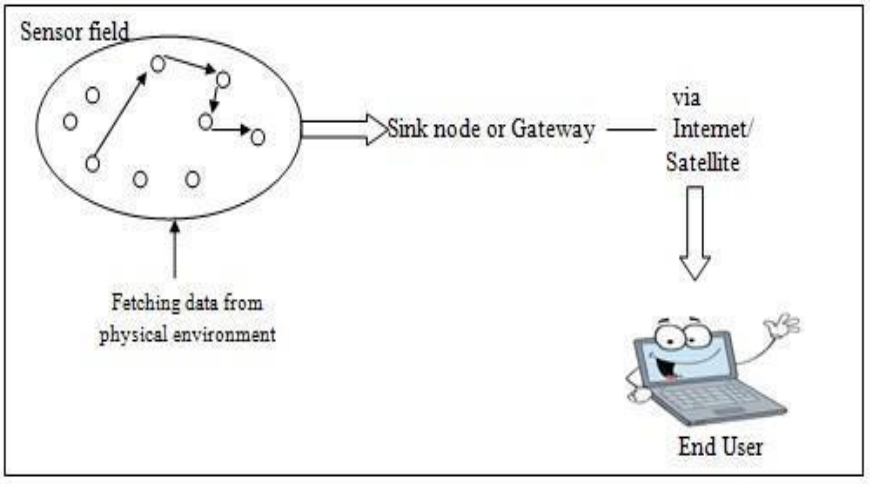


Figure 1.1: Architecture of WSN

The protocol stack architecture or layered architecture of WSN is shown in Figure 1.2. Here, physical layer is responsible for transmitting and receiving data packets among nodes in a network. This function is performed by transceivers present in the sensor nodes. This layer is also responsible for generating and selecting carrier frequency, encrypting and decrypting data transmitted and received. Medium access control layer is responsible for handling error control hence ensuring reliable communication and also manage the accessing of a channel to avoid collision with neighbor's broadcast message. Routing layer focuses on the routing mechanism i.e. selecting and generating a reliable route to transmit data from sensor node to the end user and the application layer provides an environment for deploying software for various WSN application such as military, healthcare, industrial, agriculture, etc. to translate the data in understandable format. It is also responsible for traffic management. With the help of such software, queries can be sent and answered to obtain certain information.

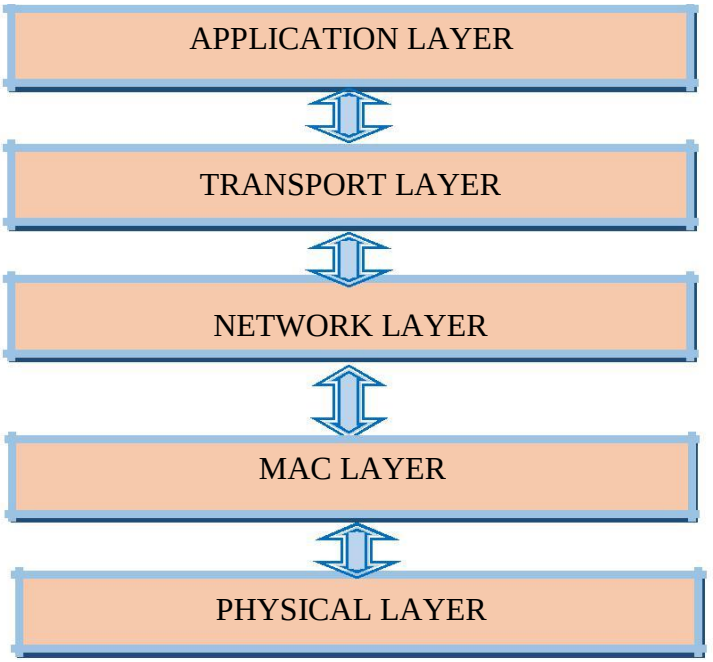


Figure 1.2: Layer stack of WSN

1.1.1 WSN Applications

Wireless sensor networks are applied in various fields mentioned below and diagrammatically represented in Figure 1.3.

- Security surveillance applications: Wireless sensor networks are used in military applications. Sensors are deployed in the battlefield to monitor the actions of the opponent by tracking their movements.
- Healthcare: Through wireless sensor networks patient's health can be monitored remotely without the need of presence of doctor physically near a patient. Different devices consisting sensors are deployed near the patient to track their medical behavior and therefore create an alert when an emergency is needed.
- Environmental monitoring: WSNs are required for sensor-based devices to communicate while monitoring the environment, it could be temperature, humidity, crops, livestock, etc. Actuators can also be attached to these networks for control systems such as irrigating crops or fertilizing crops based on sensor measurements derived.
- Smart home: Home automation is achieved by creating a home area network (HAN) in which sensors, smart devices, utilities, smart meter, etc are integrated with communication technologies within a building or residential home. All these devices communicate with each other automatically when sensing any happening in the surroundings. The smartphone can act as a remote control to manage all these devices at home. Some examples of home automation applications are smart lamp, smart bins, smart door lock, and many more.
- Industrial applications: In this domain, WSN is exploited in some industrial processes such as monitoring, manufacturing, commercial and financial transactions, security, transportation, logistics, etc. By applying sensors in logistics operations, the work of people, system, and assets can be coordinated. It is also used for monitoring the quality of some assets such as liquids, food, vegetables, etc by continuously monitoring the temperature and humidity of the container where these utilities are kept. In the automotive industry, sensors are used in traffic management and parking systems where communication is done in WSNs.

- Agriculture application: It is very common nowadays to use WSNs in the agriculture field, to reduce the manual work which leads to inaccurate measurements and predictions further causing wastage of water and deprived quality of crops or plants. Sensors based agriculture is much more accurate and has better performance compared to manual agriculture.
- Civil structure monitoring: WSNs are also used for monitoring and tracking movements inside a building or infrastructure. It is helpful for civil engineers to track assets remotely without any need for a site inspection. This also has a great advantage of receiving data at daily basis rather than weekly or monthly basis

Figure 1.3: WSN

Applications **1.1.2 WSN Challenges and Constraints**

WSN faces various unique challenges and has operational constraints. Some of these have been highlighted below.

- Sensor nodes in the sensor field requires power for fetching data from outside environment and hence work on batteries. For efficient working of the network, these sensor nodes should have sufficient amount of power to keep working. Therefore, WSN focuses on the protocols that concern power conservation rather than some performance metrics such as throughput which is focused on traditional networks.
- Node deployment is a challenge in WSNs because of the complications in the physical environment of the area where they are deployed such as in military area, area prone to disaster, an area facing harsh weather interruptions, etc. Therefore, it is necessary for these nodes to be autonomous in the direction of self-maintenance, self-repair, and self-management. The position where these sensor nodes are deployed must not be predetermined or pre-calculated to allow the random deployment of this network.
- The medium of communication among nodes and base station is wireless which implicit a challenge on designing such network for efficient communication with minimum loss rate. If the network supports multi-hop communication rather than single hop then it is energy efficient because the later one requires a large amount of transmission power. In multi-hop communication, nodes communicate among themselves to cooperate in the sensor field to find an efficient route to the sink.
- The two indispensable issues, that is privacy and security should be considered carefully while operating the entire network because sensitive data communication takes place in sensor networks. Due to some computing limitations and resource constraint, traditional security mechanism in sensor networks is difficult to apply. Therefore new security mechanism is needed for sensor networks. Some of the challenges that forbid traditional security mechanism to be applied on sensor network are as follows:
    - Due to the limitation of data storage and power in sensor nodes, sensor network becomes resource constraint.
    - Sensor network includes unreliable communication channel which makes it much more prone to physical attacks.
    - The result of unreliable communication leads to increase in lost and damaged number of packets.

- The broadcast nature of sensor network leads to unreliable communication.

- Remote management feature of sensor network excludes physical maintenance hence creating a challenge to its security.
- The networks in which systems are placed securely face network attacks only, for which security mechanisms are applied on to them which are not capable of securing sensor network where nodes are deployed in a physically harsh environment consisting both physical attacks as well as network attacks.

1.2 Security issues in WSN

WSNs are widely used in mission-critical applications, civilian's applications as well as in healthcare as discussed in previous section. Most of the applications of WSN are vulnerable to security issues because of the sensitive nature of the collected information. The basic requirements of security services are discussed in this section. The WSN suffers from many constraints which are also discussed in this section.

1.2.1 Basic Security Requirements

Effective security architecture of a network must have the following security requirements:

- Availability: The network services and resources must be available to the authorized entity of the network whenever required. The architecture of the security mechanism should be built considering such threats to provide availability in a network.
- Authentication: A security mechanism in WSN should ensure that all nodes in the network are authenticated by assuring the recipient, that it received the message from the source that claims to be from. The communication among nodes should be authenticated. The authentication mechanism should be robust so that no malicious node can surpass that and enter the network.
- Data confidentiality: Security mechanism should include data encryption for providing data confidentiality which means other than the source and destination no one can access that message and misuse it.

- Integrity: It denotes that the data sent from node X to node Y is not modified by any malicious node say Z. It assures the authenticity of the data sent from one node to other and this can be done applying an effective confidentiality mechanism.
- The freshness of data: In WSN, sensor nodes takes the measurements of different physical phenomenon related to environment and send them at a particular interval of time. A malicious node can track the old measurements and resend to them to other nodes. Therefore, a time stamp is required with every measurement data sent to other nodes or sink. This mechanism is called data freshness in WSN.
- Non-repudiation: While detecting the malicious node, an analysis of all sent and received packet logs of every node is done. What if a node denies of sending a message perhaps it did. To avoid a scenario where a node denies of sending a message perhaps it did, a mechanism should be built where the message contains its original source ID or address. This can be done using Digital Signatures.

1.2.2 Communication constraint

Sensor nodes in WSN contain some resource constraints such as storage, limited energy, processing capacity and communication bandwidth. These constraints of sensor nodes have an immense effect on security services of WSN.

- Energy: Communication is much costlier in WSN than computation as it consumes a very large amount of energy of sensor nodes. The energy is consumed in different actions of these sensors:
    - During communication among sensor nodes.
    - During computation in a microprocessor.
    - Energy used by the transducer.

  Cryptographic functions also consume a high level of energy, therefore more the level of security in WSN, more will be energy consumption.
- Computation: Embedded processors in sensor nodes do not have powerful processing feature, therefore critical cryptography algorithm is difficult to implement in Wireless Sensor Networks.
- Storage: Sensor nodes consist of two types of memories, RAM and flash memory. RAM stores sensor data, application programs, and stores

computation while flash memory is used to store downloaded application codes. In sensor nodes, there is not enough space to compute complicated algorithms.

- Communication range: Transmission range of the sensor nodes in WSN is very low compared to other devices.

1.2.3 Key management issues

Key management is a mechanism used for encryption and decryption of data for confidentiality and authentication purposes. In WSN it has some to work with.

- Pre-deployment of key: Since sensor network is infrastructure less hence topology is not predetermined, therefore, in such case pre-deployment of a key is the best option known till date, but it has some issues. Two ways of deploying keys to nodes in a network are, first, a single mission key is installed on every node of the network and second is pair-wise private keys for every single node in the network. If the former one applied then capture of any one of those nodes will bring the whole sensor network in compromised state. If the later one is used then installing a pair of keys in each and every node of the network is a very impractical method because of resource limitations. Also, pair-wise sharing of keys is not efficient since direct node to node communication is not achievable when the neighbor nodes are at a longer distance because of increase in transmission radio signals.
- Shared key discovery: When a sensor node discovers its neighbor in the range for wireless communication, they share a key to create a link between them. This mechanism from discovering neighbor to creating a link is known a shared key discovery. This approach should be programmed very carefully which should not permit any attacker to seek into the network and know the shared key between every two nodes.
- Path-key Foundation: Shared key approach is applied when nodes communicate o each other through the single hop. Now if the communication is multi-hop then a key for that path should be installed for assuring a secure communication between the source and the destination node.

1.2.4 Secure Routing

For Wireless Sensor Networks, various routing protocols with different mechanism are developed because of sensor network's different architecture from traditional networks. These routing protocols are categorized into three different types:

- Flat based routing
- Hierarchical based routing
- location based routing

The limitation of these protocols is that these are not security oriented. These protocols lack security services in their mechanism, therefore routing in WSNs is prone to different types of attacks such as Sinkhole, Sybil, Wormhole, Hello flood, Selective forwarding and much more. A deep detailing of routing protocols and attacks on sensor networks is given in Chapter 2 of this thesis.

1.3 Introduction to Intrusion Detection

The biggest concern in WSNs is its security as it has been discussed in the previous section. Therefore, it is required for secure operation of a network and to detect intrusion in minimal time before attacker can harm the network. Intrusion is an act of breaching the security policy of an information system. Intrusion detection is the act of detecting such intrusions that attempt to compromise the basic security requirements such as availability of resources, integrity, confidentiality, etc. as discussed in previous section of the thesis. Solution to the security attacks in a network exists in three terms: Prevention, Detection and Mitigation. The first step is to prevent the intrusion created by these attacks by applying a mechanism against the target attack but if the attacker manages to pass the measures taken in intrusion prevention then the second step comes on the way. Detection is the second step which will detect the compromised nodes in the network. It is a process of monitoring and analyzing the activities in a network to identify the possible incidents of violations of security policies of a network. At last intrusion mitigation will mitigate any attack from the network by removing the affected nodes to secure the network.

1.3.1 Intrusion Detection System

An Intrusion detection system (IDS) will capture various information of the intrusion affected network such as a type of attack, attack affected nodes, the location of an

intruder, intruder type (active or passive), time, etc. IDS consist of some tools, resources, and methods to identify an intrusion. It helps to deal with security attacks, however in any security system intrusions cannot be prevented totally. Due to the presence of an intrusion, confidential information of the security system such as security keys is assessed by the intruder which further results in the failure of such security system. Hence, IDS is designed to prevent intruder assessing the confidential data by revealing intrusion before any disclosure of the system resources. IDS is known as the second wall of defence in a security system.

1.3.2 Intrusion Detection System requirements

For an efficient and reliable working of IDS it should fulfil some requirements such as the ability to identify new as well as old intrusions or attacks on time. An efficient IDS avoids introducing overheads which degrades the system performance. Reliable IDS should work referring open and cooperative certified standards and should be transparent to the users. The judgement of the performance of IDS is done by calculating the rate of false positive and false negatives during detection phase, which should be minimal to be rated as an efficient IDS.

1.3.3 Intrusion Detection System classification

IDSs can be further classified as following types:

- **Intruder Type:** Intruders by attacking creates intrusion in the network. Intruders or attackers breach the security of the network in two ways, external and internal.
    i. External Intruder: An outsider attacks the network by reaching it through different means such as attacking a network through a tunnel (worm hole attack) or by attacking a internal node of the network and make it malicious.
    ii. Internal Intruder: A node which is a member of the network and has been compromised with different types of attacks to violate the security of the network. These compromised nodes can act as a selfish node, which uses all the network resources by itself rejecting other nodes request and hence saves its battery for communication. The second one is a malicious node, which causes damage to other nodes and the network by initiating Denial of Service attacks.

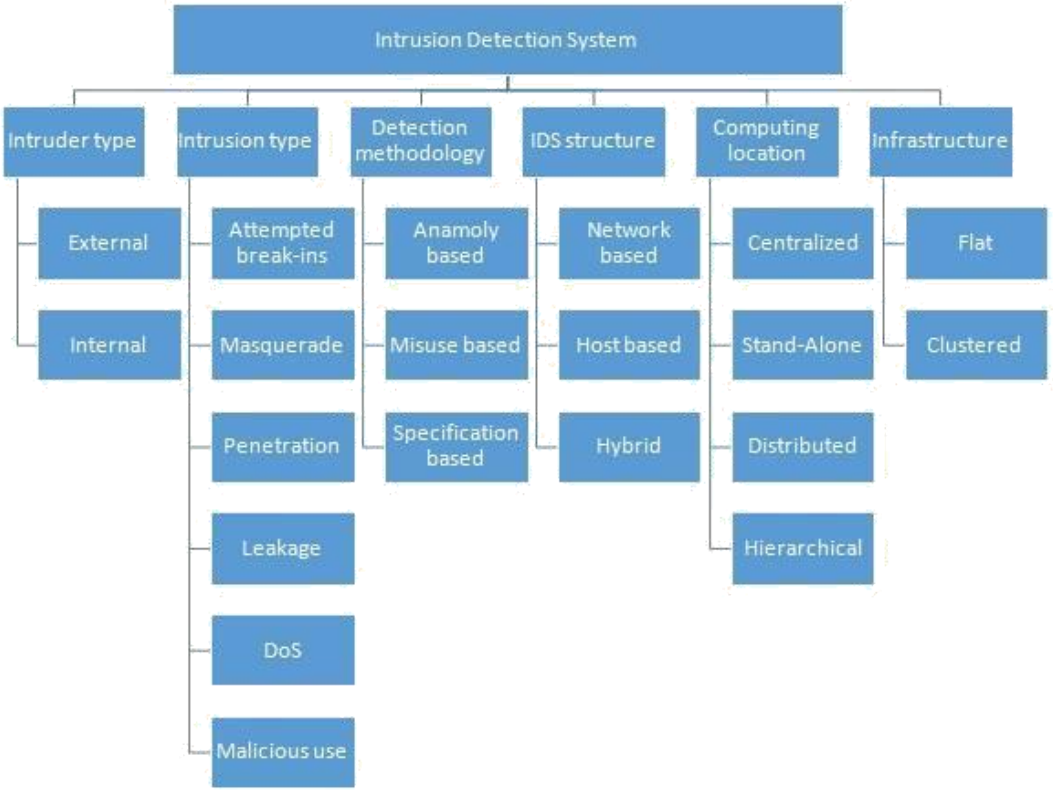


Figure 1.4: Taxonomy of IDS

Detecting internal intruder is harder than external ones because they act as an authentic member of the network and therefore have all the security keying material.

- **Intrusion Type:** In various ways, intrusion can take place in a network.
  - Penetration: By gaining an unauthorized access to the network.
  - Attempted Break-in: By attempting to break into the network through unauthorized access.
  - Masquerade: Attacker uses a fake identity to get access to the network.
  - Leakage: Flow of some information of the network to an outsider.
  - Denial of Service: Blocking the network resources for other nodes in a network which leads to congestion of the network.
  - Malicious use: By harming the network resources deliberately.

  An IDS should have capabilities to detect all the above intrusion types and related intruders.

- **Detection methods:** IDSs are categorized into three types.
  - Anomaly based detection

In this type of detection, a profile of normal activity of the network is maintained and is compared against the observed events. If significant deviations are observed then presence of an intrusion is detected. It generates many false positive which is a disadvantage of this type of detection. Another disadvantage is, a regular updation of the profile created is required because network normally changes its behavior rapidly. The advantage of using this method is that it will detect the unknown attacks which are not been encountered previously.

- Misuse/ Signature/ Rule-based detection

  In this detection method, a profile database is created of a network behavior under particular attacks. By comparing this profiled data as a reference, future attacks can be detected. The disadvantage of using this method is, that it will not be able to detect any unknown attack, whose profile is not created previously.

- Specification based detection

  In this detection method, some specifications and constraints are defined for working of a specific protocol. The execution of any program is then monitored with respect to these constraints defined to find whether a program is under attack or not. This method helps in identifying unknown attacks too and has a low false positive rate in its result. It combines the advantages of both misuse and signature based detection method. But the development of such constraints is also very time-consuming task as they are created manually.

- **IDS structure:** IDS are further classified on the basis of the location or structure where data is taken to be analyzed.

  - NIDS: (Network based IDS) are installed in the network elements which are active such as routers and hence listen all the network transmissions passing through them, captures and also examine the packets that are transmitted in a communication.

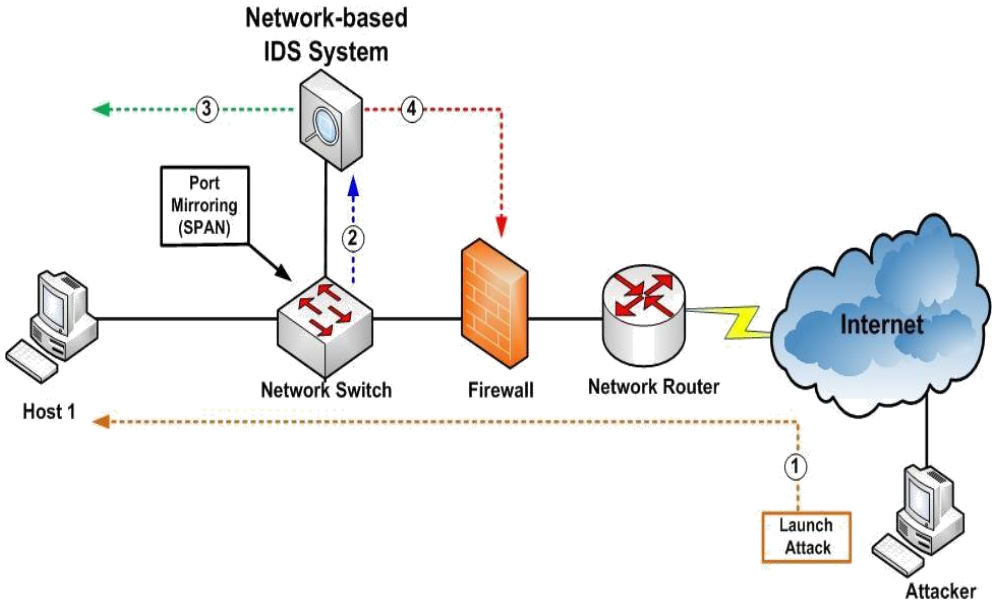


Figure 1.5: Architecture of network-based IDS [50]

I t monitors the system configuration and activities of different applications and maintains log file for all the activities happening in a system and it generates an alert if notice any undesirable deviation in the working of the system.

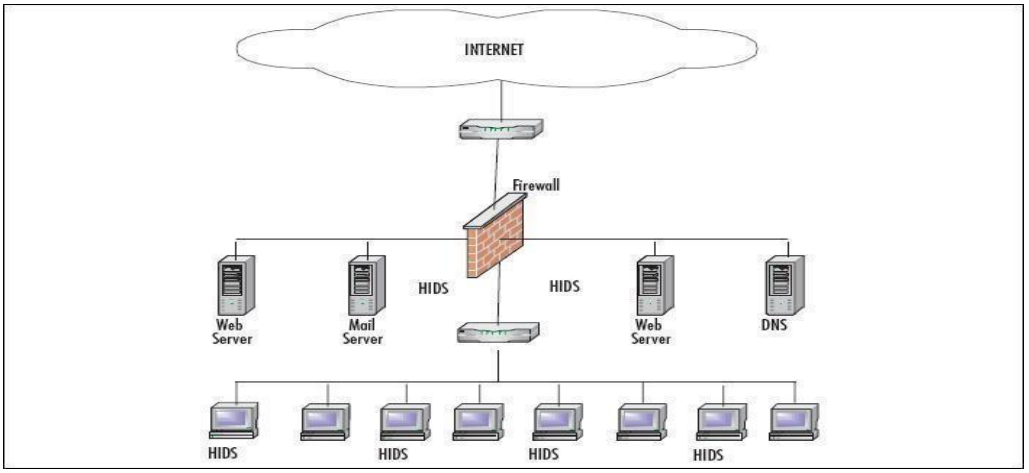


Figure 1.6: Architecture of Host based IDS [50]

- Hybrid IDS: It combines the characteristics of both HIDS and NIDS with an addition of mobile agents. These mobile agents create log files on each and every host and perform checks for these system log files.

A central agent is assigned to check all network traffic to identify any anomaly if exists.

- **Computing Location:** IDS is categorized into four categories according to the location where data is collected for analysis.
    - Centralized IDS: A centralized system is assigned to perform monitoring of the network activities and also to detect intrusions in the network by analyzing the network activity data.
    - Distributed IDS: Each and every node is installed with IDS agent in a network and hence performs Intrusion detection techniques. If any node detects an intrusion whose response is weak then it can request for global cooperative Intrusion detection but if the intrusion response is strong then it can independently declare it as an attack and alert the whole network about it.
    - Stand Alone IDS: In contrast to the cooperative IDS, stand-alone IDS installed in each and every node of the network does not share any information about the intrusions they detect among each other.
    - Hierarchical IDS: This type of IDS is proposed for clustered architecture of the network where cluster heads monitor their subsequent nodes and also performs a global Intrusion detection for decisions to make.
- **Infrastructure:** IDSs are divided into two categories on the basis of the network infrastructure.
    - Flat: In this infrastructure all nodes are considered at the same level, performing equivalent tasks such as routing. This infrastructure is suitable for a classroom or a conference networking.
    - Clustered: In this type of infrastructure all nodes are not considered as on the same level with the same functioning. Cluster heads are elected from nodes which perform the routing function and other nodes act as members of these cluster heads. These cluster heads have more powerful devices than other nodes to work with and hence have battery backups to work without any interruption.

1.3.4 Basic Architecture of IDS

The architecture of IDS consists of three main components information collection, detection and response.

- Information collection: In this module information is collected from IoT components such as sensors nodes and other smart physical objects and then transfers that information to an event generator after applying some information collection policy, which is then converted into a set of events such as network packets and then these are sent to analyzer for detecting any intrusion.

- Detection: The collected information is now analyzed using some pattern matching algorithms. In this module system information consists of information of all previously detected attacks as their signature for monitoring purpose. The two databases are created, one consists of the configuration of the IDS and other consists the signatures of previously detected attacks. By applying a detection policy on the network data, a report is sent to response component of IDS.
- Response: Response is sent when an intrusion is detected. This response can be answered in two ways, automatically or with some human intervention. The response can be sent via email to the administrator about intrusion detected.

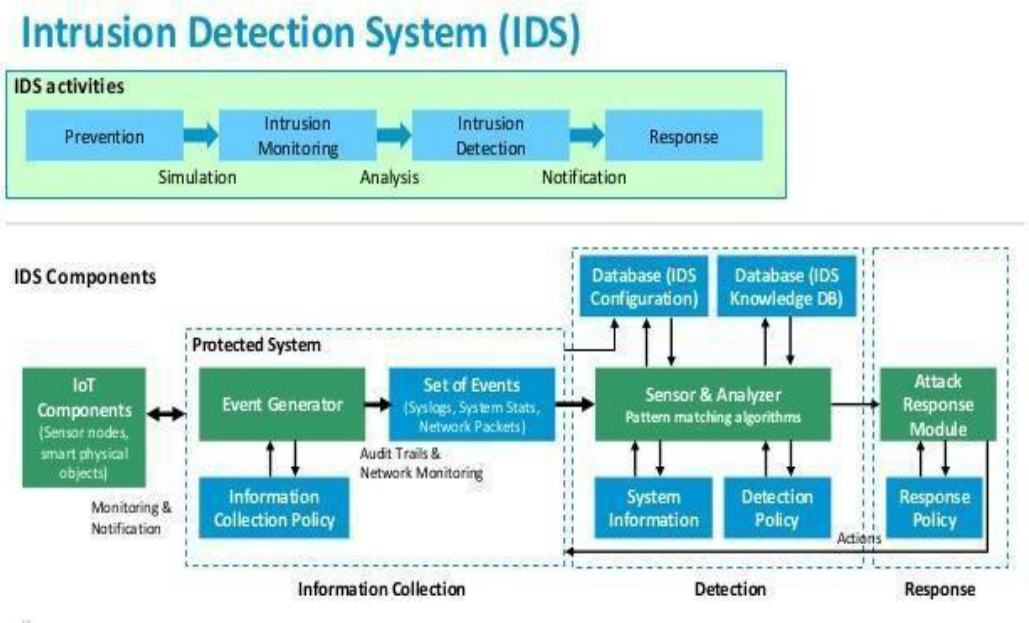


Figure 1.7: Architecture of IDS in WSN [48]

1.4 Organization of Thesis

Chapter 1 gives a brief introduction about Wireless sensor network, its challenges and constraints. Security of WSN is also discussed, which is the most critical challenge of WSN. Implementation of Intrusion Detection System in Wireless sensor network security mechanism is the topic of concern under this thesis.

Chapter 2 provides brief information about routing protocols of WSN and attacks that are faced by wireless sensor network. The thesis is concerned with DSR and DSDV protocols and Flood attack implementation on these protocols.

Chapter 3 provides the survey of Intrusion detection system on wireless sensor network. Discussion on related work on various attacks simulated in WSN architecture, WSN protocols simulation and various intrusion detection techniques is provided in this chapter of the thesis.

In Chapter 4 problem statement and objectives to carry out the thesis work is stated.

Chapter 5 includes the discussion about the procedure used to accomplish the targets of the thesis. Test setup, parameters for performing test and planning of dataset utilized is talked about in this part. The data about methodology and software tools that are utilized as a part of the presented work is also discussed in this section of thesis.

Chapter 6 presents the results and main findings of the work carried out in the thesis.

Chapter 7 contains the results of the thesis and work for future is also prescribed.

CHAPTER 2

ROUTING PROTOCOLS AND ATTACKS IN WSN

A method through which data is sent from one node to other is known as routing and to perform routing, routing protocols are used. Protocol job is to select the route from source to destination node. Sometimes source node does not have the required frequency to directly communicate with the destination, therefore intermediate nodes are needed to route the packet from source to destination, which requires a secure and reliable route from source to destination for communication. WSN has different behavior than traditional networks and due to some constraints; it has a different classification of protocols.

2.1 WSN routing protocols classification

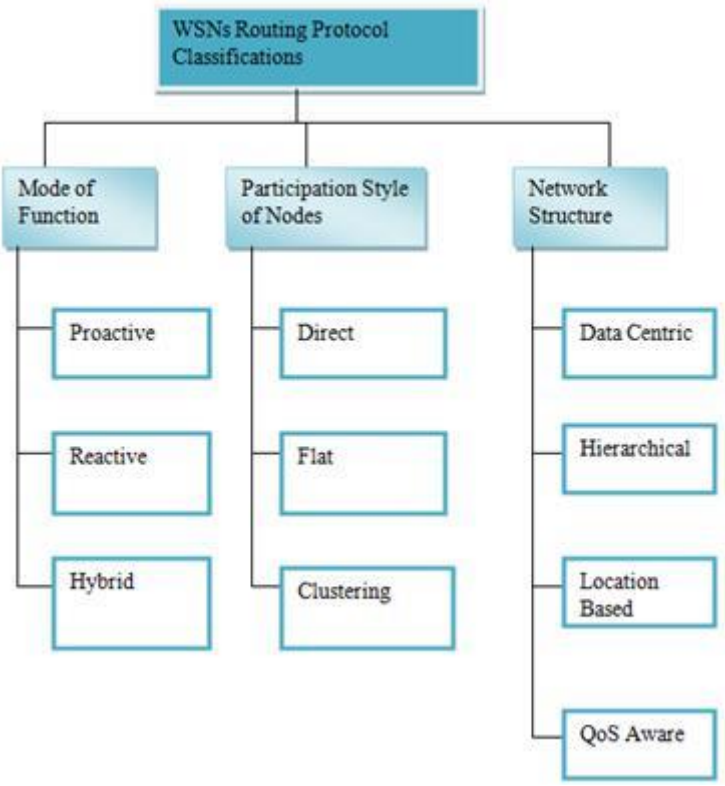


Figure 2.1: WSN routing protocols classification [54]

WSN routing protocols are classified into three categories: mode of function, participation style of nodes and network structure.

- **Participation style of nodes:** Participation style of nodes is again classified into three types: flat, direct and clustered. In the direct type, source node directly communicates with the base station and sends information directly to it. While in flat type, a route is first discovered between source and base station and through intermediate nodes information is transferred. In clustering type, nodes are grouped into different clusters and each cluster will have a cluster head which will directly communicate with other cluster's cluster head and a base station.

- **Network structure:** Network structure is further classified into four types: Data-centric, hierarchical, location based and QoS aware. In data-centric structure, the node sends a query based request to all nodes in a network, if query matches then that will revert back the data requested by the first node. This type structure eliminates redundant transmissions.

  In hierarchical based structure, protocols perform the energy based routing by selecting high energy nodes for data transmission purpose which are known as cluster heads. LEACH protocol is an example of such type of classification.

  In location-based structure, each and every node in a network calculates its position in the network and hence calculates the distance of neighbor node using GPS or through calculating signal strengths. In this type of routing, nodes maintain two types of state: active and sleep state. In an active state, node will perform all the ideal activities while in sleep state node will be at rest and does not perform any activity. This state theory is helpful for conserving energy of the node i.e. when a node is not performing any activity the it will not waste its energy by being vigorous all time.

  QoS (Quality of Service) routing focuses on some network layer requirements which provide reliability in the communication. It includes some QoS metrics such as bandwidth, delay, and energy for delivering data by a node. An example of such routing protocols is SPEED (stateless protocol for real-time communication in sensor network).

- **Mode of Function:** The three modes of such routing classification are: reactive, proactive and hybrid.

In proactive protocols, a routing table is created by every node and hence is periodically updated. Pre-decided paths are available to a node so that it does not waste time in route discovery process and immediately send data to the destination. Therefore, no delay is imposed in this type of protocols. A controlled traffic is required to regularly update the routing tables.

In reactive protocols, routing tables are not generated and hence route discovery mechanism is carried out. On demand, a route is generated by the node. At moment route discovery mechanism can cause communication delay in a network. When a node asks for a route to destination a route discovery mechanism is initiated and sent to destination and the source waits for reply of route from destination. In this type of mechanism, a node has only partial knowledge of its route to destination; it does not have any knowledge of rest of the network which is a benefit because it will save the node's energy from keeping routes for the entire network.Hybrid is combination of proactive and reactive protocols. It will compute all the routes such as proactive protocols do and then improves those at time of routing as reactive protocols do. it will help in decreasing the cost of the network.

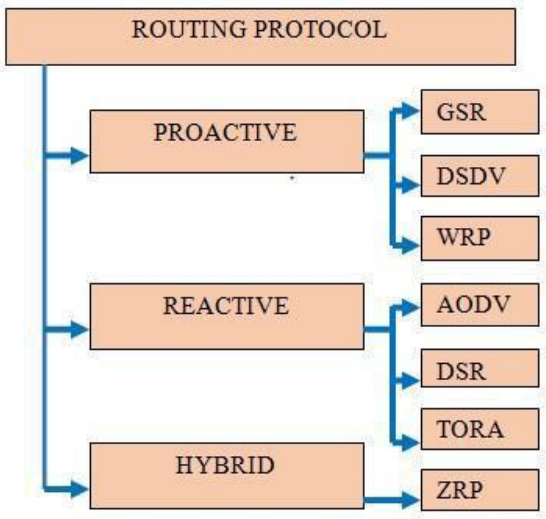


Fig 2.2: Classification of routing protocols on the basis of mode of function

Protocols under Proactive, reactive and hybrid type are illustrated in Figure 2.2. This thesis is concerned with one proactive protocol and one reactive protocol that is DSDV and DSR respectively.

2.2 DSR protocol

DSR protocol is a reactive protocol because it performs route discovery on demand when a transmitting node requests one. A message can be transferred from one node to other by two types of routing techniques - source routing and destination routing. In source routing entire route has been specified by the source node in its message header while in destination routing only destination node is specified in message header by the source. DSR protocol uses source routing instead of destination routing which requires creation of routing table at each and every intermediate node. DSR protocol makes the network self-configuring and dynamic. The two main activities carried out in DSR protocol are Route Discovery and Route Maintenance. In Route discovery, path identification from source to destination is carried out, on the other hand, Route maintenance is carried out when there is any lineage in the link or any other error found. The step by step working of Route Discovery and Route Maintenance is shown in Algorithm 2.1, 2.2.

Algorithm 2.1 Route discovery in DSR

Algorithm: Route discovery in DSR

Begin

Initialize *S, D*

Broadcast RREQ packet from S to neighbor nodes

If packet already exists **Then**

  Discard packet

Else If route found in route cache **Then**

  Send RREP to S

Else

  Append node address in packet and rebroadcast to its neighbor

End If

Algorithm 2.2 Route maintenance in DSR

Algorithm: Route maintenance in DSR

Begin

Initialize *S, D*

Start Route discovery and send RREQ packets

If link is broken **Then**

Generate RERR message

Else

Receive RREP

End If

If alternate route found in cache **Then**

Modify source route in packet

Else

Start Route discovery

End If

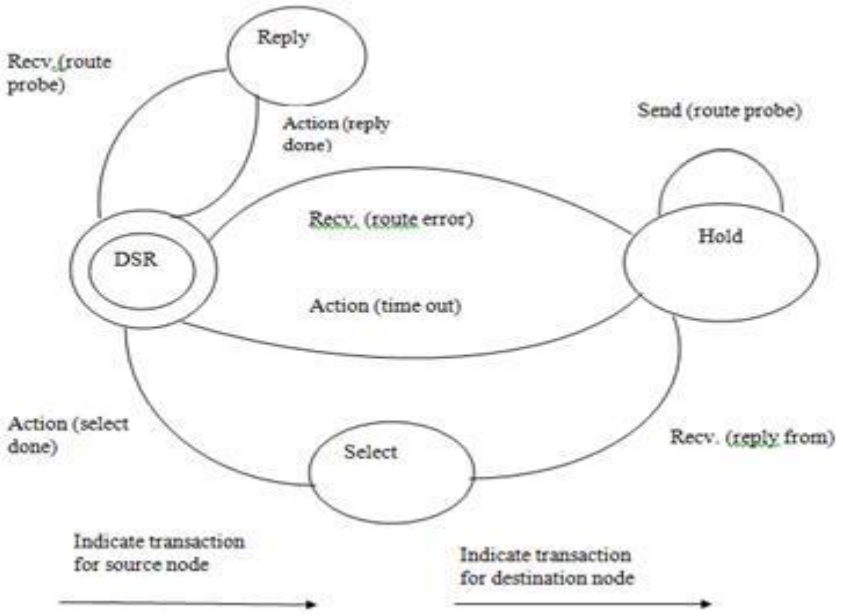


Figure 2.3: A working of DSR protocol [50]

2.3 DSDV Protocol

DSDV routing protocol is proactive in nature which implies that nodes refer the routing table for route knowledge to communicate with other nodes. This protocol mechanism is based on the Bellman-Ford algorithm. Every node maintains routing table which consists of the attributes - destination, intermediate node to reach destination, number of hops to reach destination. Every node sends this table to its neighbor node. DSDV protocol is an improvement to simple Distance Vector method by excluding loop creation and count to infinity problem of Distance Vector and this is done by adding sequence number generation attribute in routing table which is originated from destination to ensure loop-free mechanism.

Due to regular updating of routing tables, the consumption of battery power of nodes is high thus making this protocol unsuitable for large network with a large number of nodes and is also not suitable for highly dynamic networks because an urgent requirement of creation of sequence number is needed when topology of network changes.

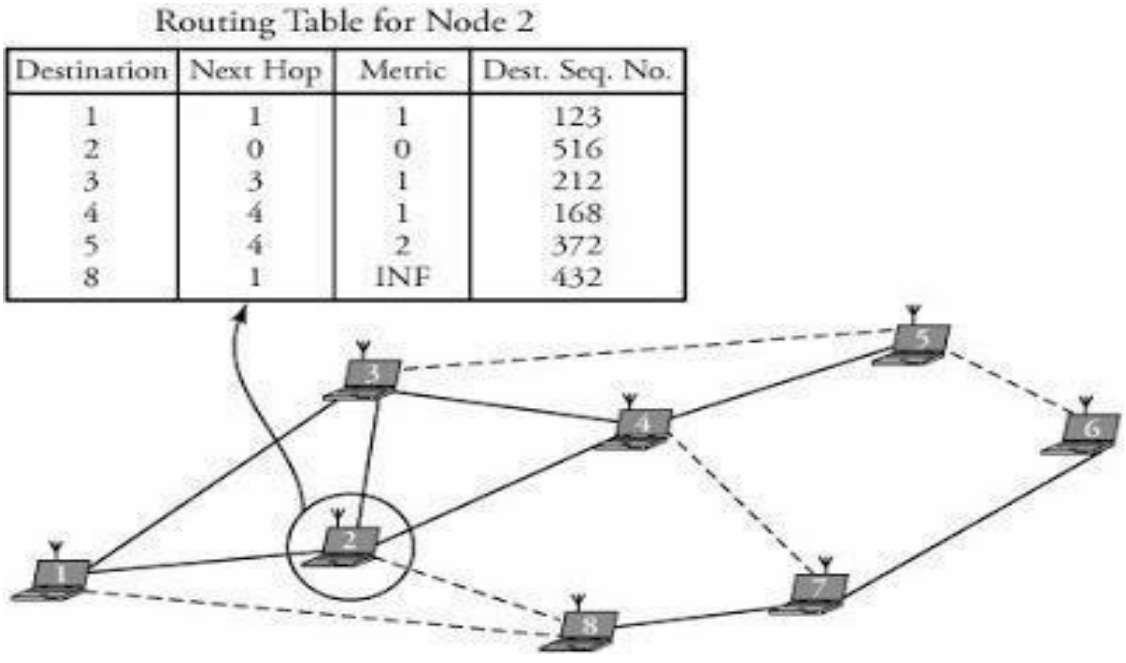


Figure 2.4: Routing table created by each node in DSDV Protocol [51]

Each node in this protocol mechanism maintains a routing table. This table consists of some routing information which is updated periodically by a node when the network topology changes. This information consists of a sequence number, destination address, a number of hops travelled to destination and destination sequence number. Here the dashed lines in Figure 2.4 represents that there is no communication between the two end nodes in the line, therefore in node 2 routing table, there is no routing information about node 8 and hence in metric section INF (infinite) is assigned corresponding to node 8 information.

2.4 Routing Attacks in WSN

WSNs are vulnerable to various types of attacks because of its various constraints and challenges as discussed in previous section. There are various types of attacks that focus on the basic security requirements of WSNs such as attacks on authenticity of the communication within WSNs, attacks on the availability of the network and attacks against integrity. The examples of attack authentication and secrecy can be eavesdropping, spoofing of packets, packet replay attacks, etc. DoS (Denial of Service) attack is referred as attack on availability of the network which can target any layer of sensor network layered architecture. Further classification of DoS attacks is represented in Figure 2.5

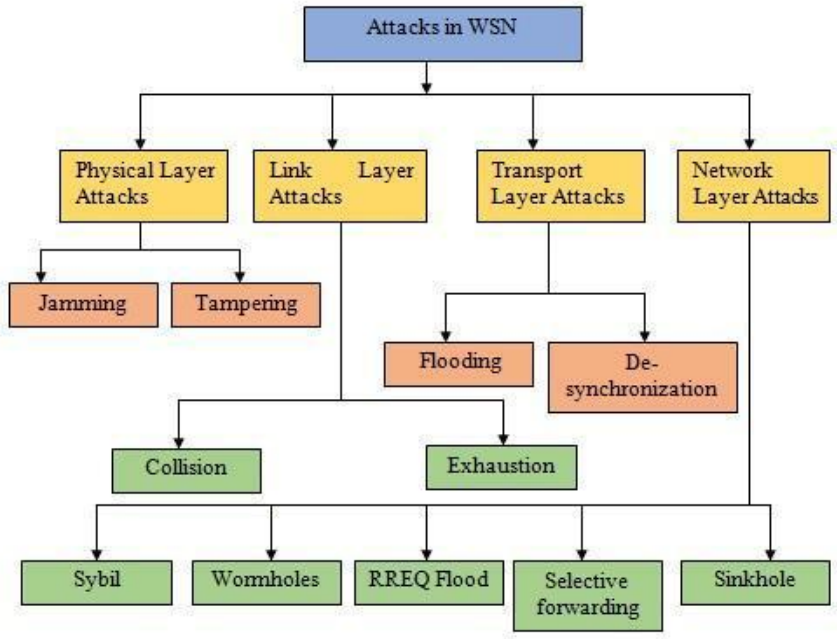


Figure 2.5: Taxonomy of Routing attacks in WSN

- **Physical Layer attacks**

  The Physical layer includes two types of attacks, Jamming and tampering.

  - Jamming: Jamming in physical layer interferes the node radio frequency in a network. It can be as much powerful as to disrupt the entire network or can be less powerful to disrupt only a section of a network.
  - Tampering: Tampering is accessing some sensitive information of a node such as cryptographic keys or some other data and altering the node on the basis of the accessed data. Replacement of a node with a compromised node can be carried out which is accessed by an attacker very easily.

- **Link Layer Attacks**

  This layer ensures connection among nodes in a communication network. The attacks that are introduced in this layer can be collision and exhaustion of resources.

  - Collisions: When two nodes transmit packet with same frequency simultaneously then a collision occurs. Packets collision results in checksum mismatch in data portion at the receiving node. Hence, the packet will become invalid and is discarded.
  - Exhaustion: If these collisions repeatedly take place in a network then it will cause resource exhaustion as the energy reserves of these transmitting nodes is continuously depleting.

- **Network Layer Attacks**

  This layer consists of following attacks:

  - Selective forwarding: In this type of attack, attacker creates an intermediate malicious node which does not forward the packets further in two ways- by dropping some of them and forwarding others or by dropping all of the packets it receives. The later one's example can be Black hole attack.
  - Sinkhole: In this attack, the attacker represents the malicious node in an attractive way by showing an incorrect routing information to other

nodes in a network. This will result in all nodes sending their packets to destination through a route which consists this malicious node as intermediate node. Through this attack, selective forwarding attack and black hole attack can be further initiated very easily.

- Sybil: In this attack, the attacker node or malicious node will send incorrect information to other nodes of the network such as its position, signal strength, frequency, etc. In this attack, a single node i.e. malicious node can take multiple identities and transmit incorrect information to other nodes.
- Wormhole: In this type of attack a tunnel is created by an attacker between two networks. The malicious node in one network retrieves all the information from other nodes and sends it to another malicious node in another network through this tunnel.
- Flood attack: Flood attack is a DoS attack under active attack. Denial of service (DoS) attack makes the network resources unavailable for nodes temporarily or indefinitely hence congesting the whole network.

- **Transport Layer attacks**
  - Flooding: In this attack, attacker will make requests for new connections repeatedly with different nodes in a network leading to flooding which in result can cause resource exhaustion too because each connection requires various resources.
  - De-synchronization: This attack will create a disruption in a connection when attacker will send spoof messages to the destination which will cause a request for retransmission of the message from the destination node. The end host that is destination node will think that it is an error and waste time and resources for solving this error which in reality does not exist.

2.5 Flood attack in WSN

The attack which is concerned in the thesis is Flood attack. The strategy and working of RREQ flood attack are explained below.

- **Attack Strategy:** Flood attack causes network congestion by repeatedly broadcasting RREQ (Route Request) messages, created by attacker,

containing the destination address of node that does not exist in the network. If RREQ message does not reach to destination node, RREP (Route Reply) message will not be generated and reverted back by destination node to allow transmission of data packets from source to destination in a network which results in clogged network. This attack is considered as DOS attack by consuming all the network resources in broadcasting RREQ messages and declining other functioning requests results in lethal impact on network performance.

To verify and determine the effect of RREQ flooding attack on DSR and DSDV protocols, four simulation experiments have been performed for comparing the network performance with and without attack which is further discussed in Chapter 5 of the thesis.

- **Attack Implementation:** A step wise description of the implementation of RREQ flood attack is given below.
    - The attacker creates an RREQ message with destination of the node that does not exist in the network.
    - Encapsulate this message and broadcast it in the network.
    - Other nodes forward this message according to the mechanism of DSR and DSDV protocols respectively in the network.
    - After sending first RREQ message, attacker creates another one, this time with different destination that also does not exist in the network.
    - Encapsulate and broadcast it.
    - Repeat steps d and e, every time pointing to a different destination node that does not exist in the network.

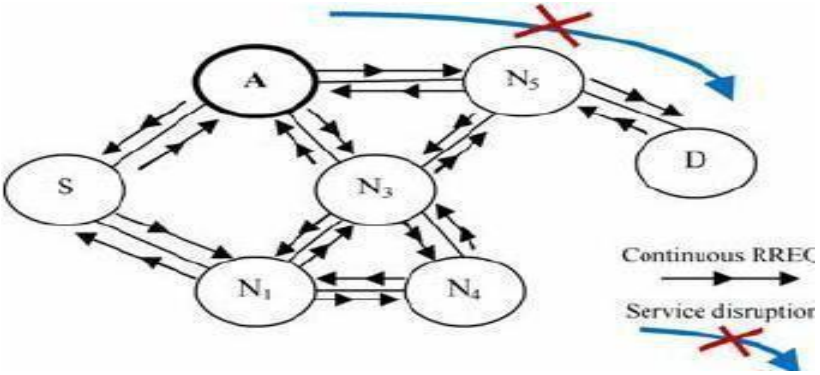


Figure 2.6: Flood attack in a network [52]

Chapter Summary

In this chapter, classification of WSN routing protocols is described on the basis of its mode of function, participation style of nodes and network structure. One reactive and one proactive protocol is concerned in this thesis that is, DSR and DSDV which are introduced in this chapter briefly. Routing attacks in Wireless sensor network classification based on layered architecture of WSN is discussed and flood attack strategy and implementation mechanism is described in this chapter.

CHAPTER 3

LITERATURE REVIEW

This chapter presents the output of literature survey of various techniques of intrusion detection in WSN, various attack simulation and WSN routing protocols. This chapter also discuss about taxonomy of IDS in WSN which is the topic of concern in this thesis.

3.1 Taxonomy of IDS in WSN

Up until this point, different sorts of security dangers in WSNs have been discussed in previous chapters. These assaults can be handled by utilizing some particular countermeasures: IDS mechanism and techniques that make utilization of various basic standards. The majority of those standards depend on the suspicion that there exists a perceptible contrast between the conduct of an attacker and the conduct of a genuine node, with the end goal that the IDS can coordinate those prearranged or learned guidelines. Following this supposition, IDSs can be characterized according to specific detection techniques i.e. anomaly, misuse and specification based techniques.

The misuse detection frameworks are utilized to distinguish known examples of interruptions while anomaly based techniques are utilized to identify new or obscure interruptions. A specification-based technique is situated in light of a few deviations from ordinary practices.

Figure 3.1 demonstrates a scientific classification of IDSs in WSN that consents to this characterization.

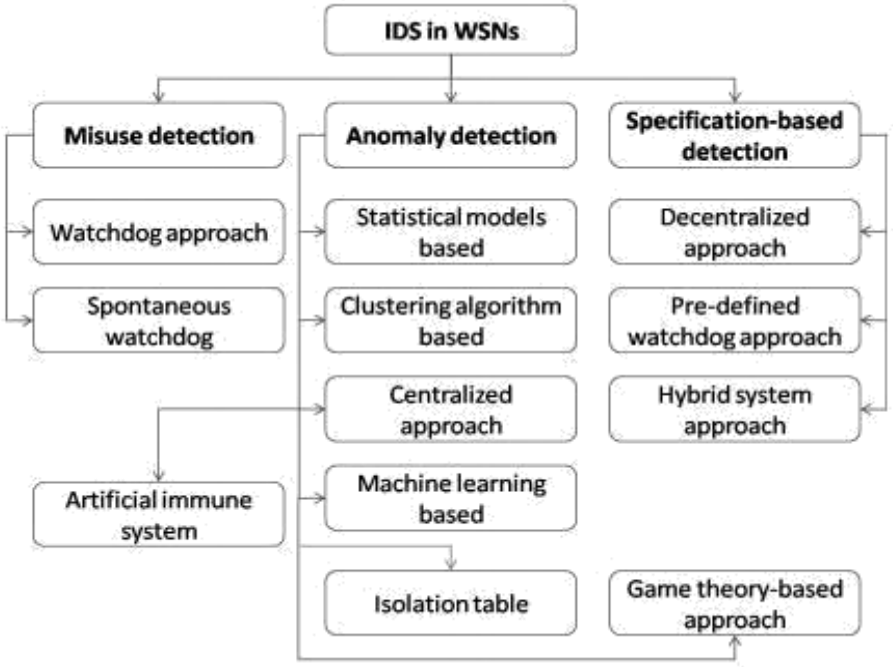


Figure 3.1: Taxonomy of IDS in WSN [51]

A. Misuse Detection Schemes:

The utilization of misuse detection methods with regards to a WSN is a mind boggling errand. The overseer of the system needs to show assault designs as per assaults that may happen in future. Also, the extreme memory requirements of WSNs make misuse detection based IDSs that need to store attack signatures generally hard to execute and more averse to be successful [1]. In this way, there are not very many papers that review abuse discovery method for WSNs. In any case, the majority of them take the watch dog approach, where packet monitoring takes to put in a few particular nodes in the system [3].

- Watchdog approach:

  This approach depends on the communicated idea of the remote interchanges and the suspicion that sensors are typically thickly conveyed. Every byte communicated in the system is received by the recipient as well as by an arrangement of neighboring nodes inside the sender's radio range. In ordinary cases, neighbor nodes should dispose of the packet, since they are not real beneficiaries, but rather for interruption location this can be utilized as a profitable review information. Thus, a node can initiate its IDS specialist and screen the packets sent by its neighbors by catching them [6].

B. Anomaly based Detection:

In WSN, numerous IDS systems use anomaly based strategies. These sorts of frameworks, as a rule, depend on examining whether the behavior of sensor nodes can be considered as should be expected or strange as indicated by specific presumptions and measurements. Most scientists have adopted this strategy as a principle technique to recognize interruptions, as they think of it as is simpler to apply than misuse or specification based recognitions [6].

- Statistical Model-Based Approach:

  Onat and Miri [7] proposed an anomaly identification based security conspire for WSNs. In their strategy, every sensor node fabricates a basic measurable model of its neighbor's conduct, and these measurements are utilized to identify different assaults.

- Clustering Algorithm-Based Approach:

  In [8], Loo et al. built up an intrusion detection technique for directing assaults that use a fixed-width clustered calculation to manufacture a model of typical conduct. The disadvantage of this technique is that the technique puts excessive calculations on sensor nodes. The creators guarantee that since the proposed IDS don't require correspondence between sensor nodes, it altogether diminishes the power utilization.

- Artificial Immune System:

  In a takeoff from anomaly detection methods, the need for Artificial Immune System (AIS) was talked about in [10]. In this work, Shaust et al. address these naturally propelled calculations as a conceivable answer for recognizing trouble making in WSNs. They deduce in the paper that AIS is really a decent decision for anomaly identification in WSNs. Actually, different scientists have utilized this approach as a component of their tests. For instance, Kim et al. [12] demonstrated the likenesses between the properties of WSNs and biological immune frameworks and presented a specific AIS, the Dendritic Cell calculation (DCA), which was utilized to recognize cache positioning assaults in coordinated dispersion routing.

- Isolation Table:

  In [17], Chen et al. proposed an anomaly recognition technique for three-level progressive WSNs (base station - primary cluster heads-secondary cluster heads) in light of a disconnection table. In this technique, the

separate table records the abnormality data and the location specialists utilize it to disengage nodes from the system.

- Machine Learning Approach:

  There are some IDSs that depend on different machine learning systems. The [15], [16], [17], and [18] present machine learning and automata-based learning approaches as an inconsistency recognition apparatus for remote sensor systems. In [15], Misra et al. utilized a learning automata based approach to identify malicious nodes. This approach depends on packet testing, where an extent of the bundles crossing the system is inspected to distinguish whether they are vindictive nodes or not. Results acquired from the analysis demonstrate that the recognition rate is high and the energy utilization is low for WSNs. The expanded adaptation of the work is displayed in [20].

- Game Theory Approach:

  Different analysts have connected Game Theory based models in intrusion recognition techniques [21], [24], [25], [26], [27], [29]. Game Theory based models can be superb answers for wired systems as far as the level of security, however, for WSNs, it is important to demonstrate their relevance: sensors are furnished with obliged vitality sources, and the execution of these models appears to diminish when the quantity of nodes is expansive.

C. Specification based approach:

Some specification-based plans have been proposed as IDS answers for WSNs. The fundamental detriment of this approach is that the advancement of attack or protocol specification is finished by individuals. For this situation, the executive or the architect of the system needs to physically define the specification that portray what a right operation is and screen any conduct as for those limitations.

- Decentralized Approach:

  One of the first works in this examination track was presented by Silva et al. in [30]. They proposed decentralized IDS depend on a few predefined rules. The technique has three stages: (i) information procurement, where packets are gathered in a wanton mode keeping in mind the end goal to filter out the vital information before putting away it, (ii) control application, where the rules are connected to the stored information, and (iii) recognition

stage, where the quantity of raised disappointments are contrasted with the normal measure of incidental disappointments that defines whether an interruption has happened or not. There are numerous different works in this subject [31], [32], [33], [34], [35], [36], [37], [38] those utilization diverse systems to determine interruption recognition examples and assault signatures.

- Predefined Watchdog Approach:

  Krontiris et al. have proposed different specification-based IDS with a specific end goal to identify blackhole [1], Selective forwarding [1], and sinkhole [39], [41] assaults in WSNs. Their approach depends on watchdogs, which have pre-defined rules for raising interruption alarms.

D. Hybrid System Approach:

The specification-based approach integrates the points of misuse and anomaly detection techniques. However, some specific IDSs enable both recognition procedures to exist together and cooperate in one single identification operator. That is, such specialists will make utilization of mechanized preparing based anomaly recognition techniques and human-made control based misuse identification procedures. These methodologies are known as hybrid frameworks.

Hai et al. [42] proposed a hybrid interruption recognition framework that incorporates both anomaly and misuse strategies. The specific objective of this strategy is to recognize directing attacks in WSNs. For vitality efficiency, they utilize various leveled WSNs. In the misuse recognition module, the creators utilize pre-defined guidelines, for example, packet interim rule, integrity govern, packet delay rule, and radio transmission rule.

The broadened adaptations of the above work have been distributed by the same leading author (alongside others) in [43], [44] and [45].

Many other authors have likewise taken part in Intrusion Detection method area of WSN as follows:

Sun et al. (2007), performed a survey on the security of mobile ad hoc network and WSN. MANETs and WSN are used in so many applications and some of them are deployed in a hostile or insecure environment, therefore security is a big concern.

Intrusion detection techniques have been discussed and challenges faced to build an Intrusion detection technique is also explained in detail [13].

Rajasegarar et al. (2008), has provided an overview of some anomaly detection techniques in WSN. Author has focused on some specific characteristics of anomaly detection algorithms such as, an algorithm should be feasible to conserve the node energy and keep the network lifetime longer and also these detectors should not hinder the normal working of the network [14].

Wazid et al. (2016), proposed a technique for detecting the intrusion for a hybrid anomaly, which consists of multiple attacks such as black hole, worm hole, sink hole, etc. The hybrid anomaly is very difficult to detect as it's difficult to find out which attack mode or type is present in a network. The author proposed an algorithm which uses the concept of K-means clustering to detect such intrusion in which intrusion patterns are created before handed over training data using K-means technique. The data set is created using Opnet Modeler to evaluate the presented approach. The proposed technique detects black hole and misdirection attacks in a network and hence achieves 98.6% detection rate and 1.2% false positive rate [19].

Hidoussi et al. (2015), proposed a new centralized Intrusion detection system to detect black hole and selective forwarding attacks in a cluster-based architecture of WSN. The system is designed by keeping in mind the basic and essential characteristics of a WSN, that is, energy efficient and vulnerability to different types of attacks. For future, some more attacks will be included for detection with the proposed system such as Sybil attack and hello flood attack [23].

Bosman et al. (2016), proposed a new technique for anomaly detection using sensor's neighborhood information as a key characteristic. Traditional anomaly detection techniques were operated as centralized, which demands the measurement data of nodes calculated from a central location which is a limitation of WSNs because it adds up high data communication cost. Therefore, the author has proposed a new technique which involves decentralized anomaly detection, based on machine learning concept. This technique reduces the energy and spectrum consumption of network which seems to be the main concern of the paper [63].

Roman et al. (2006), proposed a technique to keep a watch on the communication of sensors with its neighbor sensors known as watchdog technique. Guidelines to apply IDS on static sensor networks are also introduced in this paper. They have also concluded that IDS architecture which is applied on ad hoc network cannot be applied to sensor networks. They have not performed any simulation and implementation of the proposed technique and IDS architecture on a particular group of protocols [2].

Table 3.1: Related work on intrusion detection

S.No.	**Year of Publication**	**Authors**	**Technique used**
1.	2007	Sun et al.	Survey on ID techniques.
2.	2008	Rajasegarar et al.	Anomaly detection technique
3.	2016	Wazid et al.	Hybrid anomaly detection + K-means clustering.
4.	2015	Hidoussi et al.	Proposed a new centralized Intrusion detection system to detect black hole and selective forwarding attacks in cluster-based architecture WSN.
5.	2016	Bosman et al.	Decentralizedanomaly detection technique + machine learning concept
6.	2006	Roman et al.	Watchdog technique

3.2 Various attack simulation on WSN routing protocols

Dubey et al. (2016), performed a simulation of flood attack on AODV protocol in MANET infrastructure using NS-3 network simulator. Observation is done by changing malicious nodes number and position. After implementing the project with experiments, the author has concluded that due to presence of flood attack in MANET average packet loss rate and delay time for delivery increases which results decrease in throughput [4].

Pai et al. (2013), performed a simulation of black hole and gray hole attack in AODV protocol. Simulation is carried out in NS-2 network simulator. Performance metric used to calculate the effectiveness of these DOS attacks is lost packet rate and hence author has concluded that a number of attackers are directly proportional to data packet loss rate [5].

Kothari et al. (2013), proposed a different mechanism in original DSR protocol with the motive to reduce communication overhead and negative effect of malicious nodes. Simulation of DSR and black hole attack on DSR is carried out with variation in a number of nodes in a network- 10,20,30,40, 50 and is carried out in NS-2 network simulator. The metrics at which these two network scenarios are compared are throughput, end to end delay and packet delivery ratio. The results show that if in DSR network the number of nodes increases then end to end delay decreases while in DSR with black hole, end to end delay increases because of number of malicious nodes increases [22].

Jiwen et al. (2009), performed a comparative study of various attacks simulation on DSR protocol. The attacks simulated are RREQ flooding attack, Black hole attack and active black hole attack. The simulation is carried out using NS-2 network simulator. A new attack method is also been pointed out in this paper, that is, active black hole attack which attracts a large number of packets than the traditional black hole attack. The results of the implementation conclude that RREQ flooding attack is much more destructive to network than both types of black hole attacks, active and passive [40].

Table 3.2 Related work summary on attack simulation

S.No.	**Year of Publication**	**Authors**	**Attack simulated**
1.	2016	Dubey et al.	Flood attack simulation
2.	2013	Pai et al.	Black hole + gray hole attack Simulation
3.	2013	Kothari et al.	DSR + black hole attack simulation comparison.

4.	2009	Jiwen et al.	RREQ flood + active black hole + passive black hole attack simulation comparison.

3.3 Routing protocols of WSN

Tripathi et al. (2010), performed a simulation in NS-2 network simulator to analyze the performance of DSDV protocol in two different network scenarios, one where source and sink nodes are static and other where source and sink nodes are dynamic. They have concluded that, end to end delay and an average number of dropped packets in static scenario is greater than that of dynamic scenario [9].

Singh et al. (2010), prepared a literature survey on routing protocols of WSN, describing their strengths and limitations by giving a detailed information about their characteristics. WSNs have different architecture than traditional networks, therefore its routing protocols consist of some different characteristics and have different mechanism compared to other protocols [11].

Arya et al. (2014), done a comparative study of AODV, DSR and DSDV protocols of WSN using NS-2 network simulator. The results are analyzed through metrics such as throughput, packet delivery ratio and end to end delay and hence conclusions are made that AODV is better protocol for WSN than DSR and DSDV when considered overall [28].

Table 3.3 Related work on routing protocols simulation

S.No.	**Year of Publication**	**Authors**	**Routing protocols simulated**
1.	2010	Tripathi et al.	DSDV with static nodes + DSDV with mobile nodes simulation comparison.
2.	2010	Singh et al.	Survey on WSN protocols.
3.	2014	Arya et al.	DSR + AODV + DSDV simulation comparison.

Chapter Summary

In this chapter, the work related to this thesis done by other authors is mentioned in brief. The related work done is sub divided into different sections, as, IDS techniques in WSN, routing protocols of WSN, and various attacks of WSN. Various authors contribution to the related area is discussed in brief in this chapter.

CHAPTER 4

PROBLEM STATEMENT

The extent of WSN is far reaching in numerous application areas, due to its wide utilization, it faces many difficulties and security is one its key test. WSN arrange outlines are not quite the same as the customary systems that were utilized, therefore, the conventional security components don't work for WSNs. Consequently, security is a critical area in WSN.

One of the sub-domain and major concern in security of WSN is intrusion which is a malicious activity affecting the integrity, security, confidentiality and availability of the data which flows in the network. To detect various types of intrusions, IDS (Intrusion Detection System) mechanism is applied on WSNs.

The essential concentration of the proposition is to contemplate different Intrusion Detection procedures that can be implemented on WSN and apply one of those strategies to recognize interruption in DSR and DSDV routing protocols of WSN. Distinctive trials have been carried on DSR and DSDV routing protocols networks and anomaly detection technique is applied to identify attack in these system situations.

4.1 Thesis Objectives

- To study various routing protocols of WSN.
- To study the behavior of DSR and DSDV routing protocols by simulating them in NS-2 network simulator environment.
- To study the behavior of DSR and DSDV routing protocols in presence of flood attack through simulation.
- To apply anomaly based Intrusion Detection technique to detect the presence of intrusion in the network.
- To compare the performance of DSR and DSDV routing protocols in presence of flood attack with DSR and DSDV routing protocols in absence of flood attack on the basis of some parameters.
- To analyze the results using machine learning algorithms.

CHAPTER 5

METHODOLOGY AND IMPLEMENTATION

In this section we show the methodology used in this thesis. The answer for the issue in the past area has been talked about beneath. This part gives the execution points of the intrusion detection approach that is followed. The approach used to execute the set targets and the experimentations which were performed are clarified in this section.

5.1 Proposed Methodology

In this area of the theory the proposed methodology of the system is talked about in the organization of flowchart in Figure 5.1. The strategy taken after by the framework proposed in this thesis in Figure 5.1 incorporates four fundamental parts which are simulation of the system, dataset readiness, Intrusion Detection procedure taken after under which machine learning based approach is connected to examine the network traffic information. The network simulation took under the DSR and DSDV routing protocols. Further, the systems were denounced with an attack, that is, flooding attack.

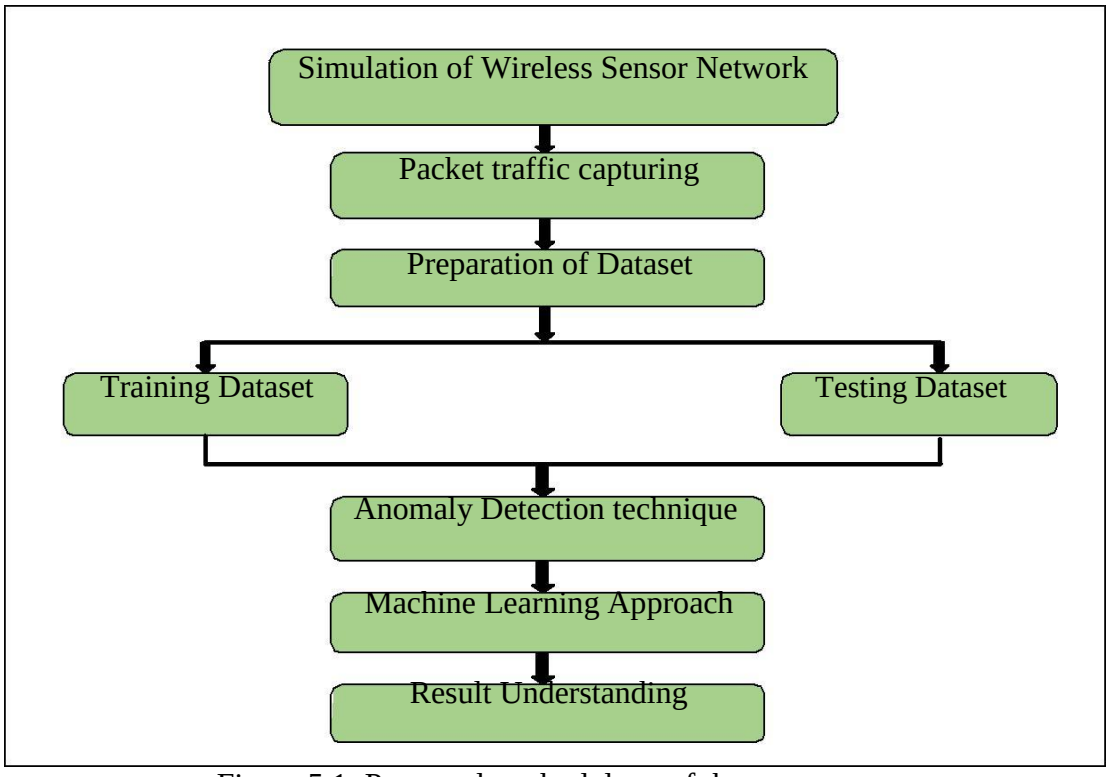


Figure 5.1: Proposed methodology of the system

5.2 System Workflow

A diagram of how the execution of the system, presented in this proposal is shown as a flowchart in Figure5.2.

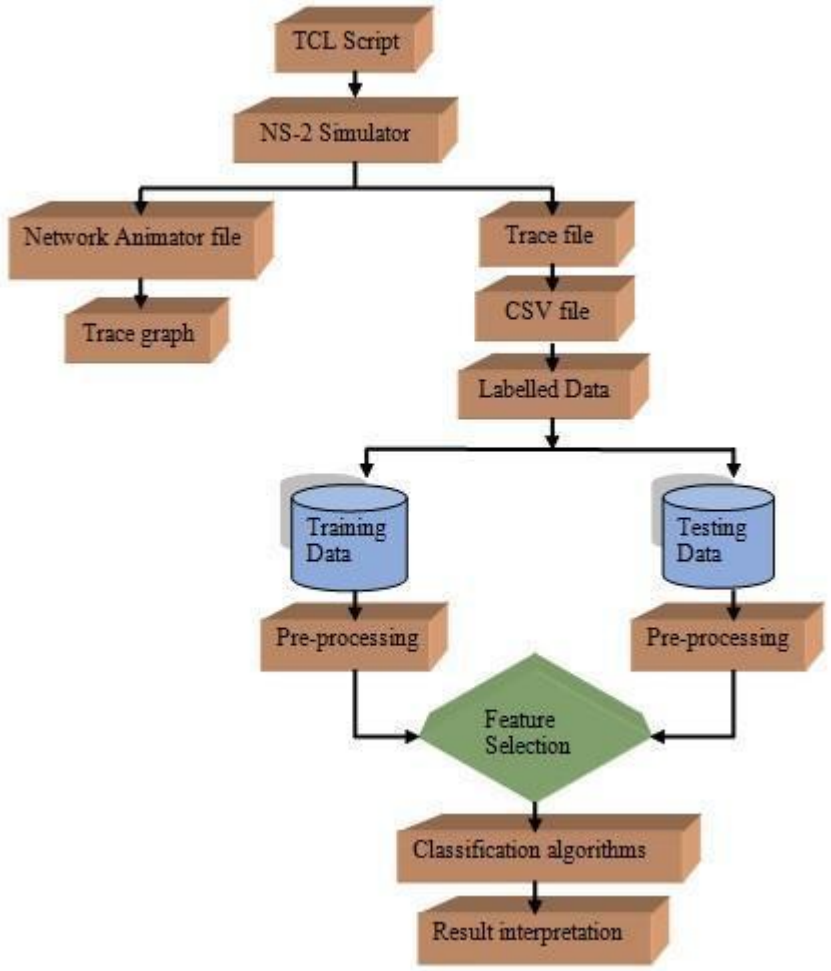


Figure 5.2: System workflow

At first level, a TCL script has been made for actualizing a system and is executed. Execution of TCL script in NS-2 results in generation of nam file and a trace file. Execution of nam file will graphically speak to the system simulation on nam window, while trace record contains the data of the system correspondence, for example, packet status, communication protocol, the size of a packet, length of bytes, nodes position, time stamp, and so on. At next level, the trace file captured is converted over to CSV organization and labeling of information is done as such as to test on machine learning tool for profound investigation of the system data. Some piece of the information got from trace file is set as training information and remaining is testing information. The trait chosen for arrangement of information is

packet status. In Final level, distinctive machine learning algorithms are applied on the information got from simulation. Anomaly based intrusion detection technique has been applied to detect any type of abnormal behavior by monitoring the system activity and comparing it with the normal behavior of the network. In Figure 5.2 system workflow applied to accomplish the research is floated.

5.3 Software tool used

In this segment of theory, the software tools or programming utilized for actualizing simulation tests in this thesis are portrayed in detail and furthermore the characteristics of the information recovered from the trials has additionally been talked about.

5.3.1 NS-2

NS-2 stands for Network Simulator Version 2. It is an open source software used for event driven simulation developed at UC Berkely and is written in OTcl and C++ languages. This is very helpful for research in communication networking field. Endeavors are as yet being made to enhance the elements of NS. It is the obligation of the clients to keep a beware of their work and look for bugs. To assist the client a manual in particular NS manual is available for direction. NS2 is actualized on Linux-based stage and is also called an occasion driven test system. In Network Simulator the planning of the occasions is assumed to control by a scheduler. Numerous sorts of systems can be reproduced utilizing NS, for example, WPAN and WPAN as indicated by the TCL scripts composed. Additionally, a few prominent conventions, for example, UDP and TCP can be actualized utilizing NS. Additionally arrange components like flag quality and prominent activity models like FTP and CBR can be mimicked. It is used for simulating both wired as well as wireless network. It is a UNIX-based software, is not supported by Windows or any other Operating System. Tcl language is used for scripting programs for simulation of a network. The basic architecture of NS-2 is shown below in Figure 5.3.

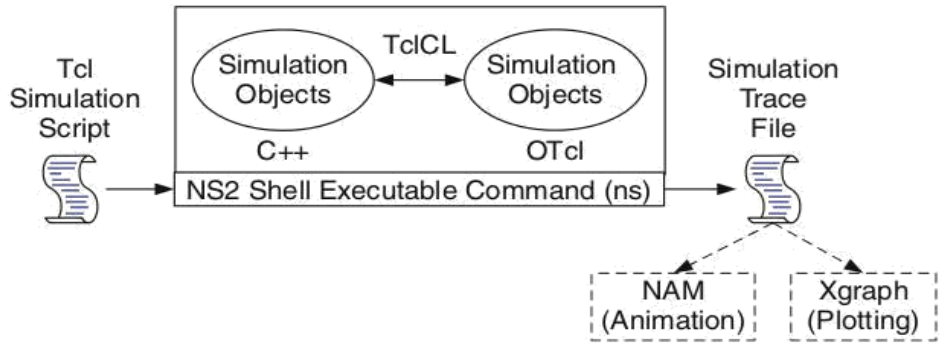


Figure 5.3: Basic architecture of network simulator [53]

5.3.2 NAM: Network Animator is an animation tool in NS-2 used to view the network simulation traces and the packet traces in a network. NAM file is executed with the help of following command on terminal.

nam <nam_file>

Where nam_file is an animator file generated after executing the Tcl script for the network by Network simulator. It is used for visualizing the working of network such as node movement, packet traces, topology, etc. A nam window is demonstrated in Figure 5.4.

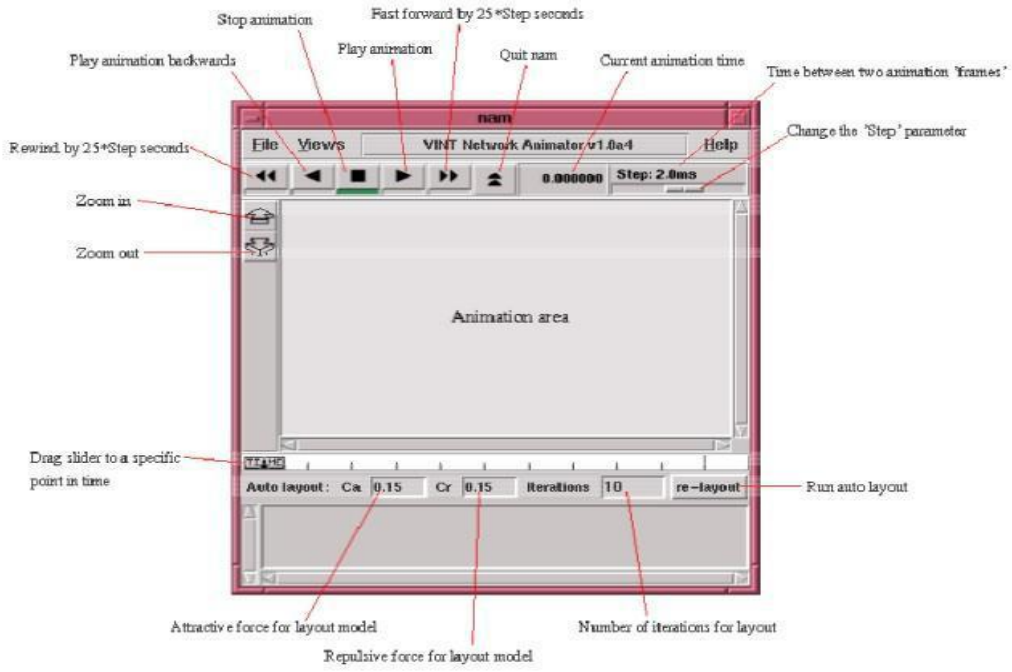
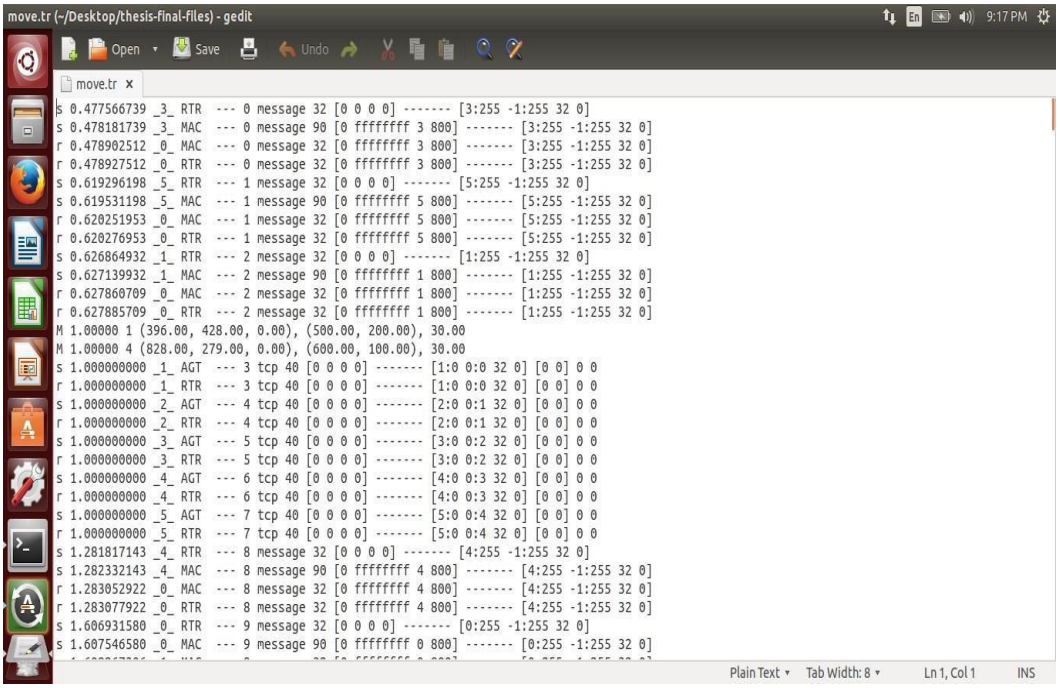


Figure 5.4: NAM window

5.3.3 Trace file: The record composed by an application (or by the Coverage Server) to store general system data in NS2 is called as Trace File. Keeping in mind the end goal to produce a trace record we need to make a trace record in Otcl script.



Screenshot 5.1: Trace file screenshot

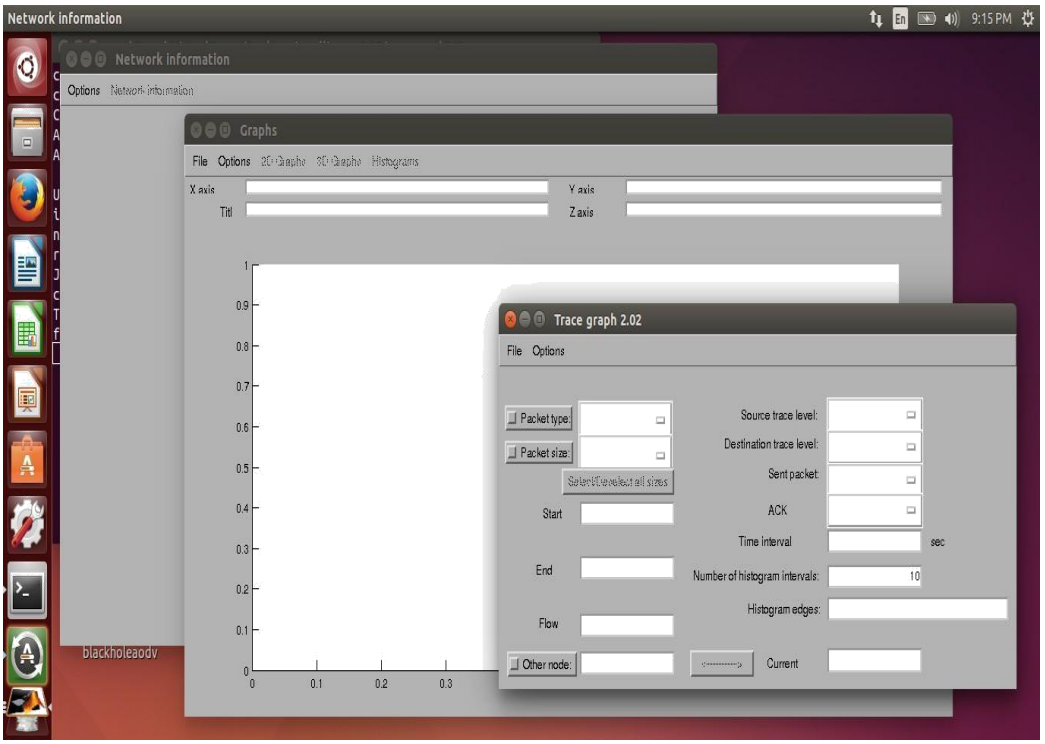
5.3.4 Trace graph: Trace graph is a third party software used to plot graphs of the trace file from NS-2. It is supported by LINUX as well as Windows Operating System. A screenshot of the same is shown in Screenshot 5.2.

It consists of three windows:

i. The first window is used to select the trace file of which trace graph you want to create.

ii. The second window is the main window that creates the graph (2D, 3D, histograms).

iii. The third window will display all the simulation information such as packet delivery ratio, lost packets, received packets, dropped packets, an end to end delay, also provide information of the source and destination nodes and also intermediate nodes information.



Screenshot 5.2: Trace graph windows screenshot

5.4 Simulation Details

This simulation is done by executing TCL scripts on NS-2 arrange test system over LINUX (Ubuntu) Operating system. Four TCL scripts are executed to comprehend the working of the routing protocols in the presence and absence of intrusion by executing the scripts on NS-2 to speak to the system situation outwardly through NAM Illustrator window.

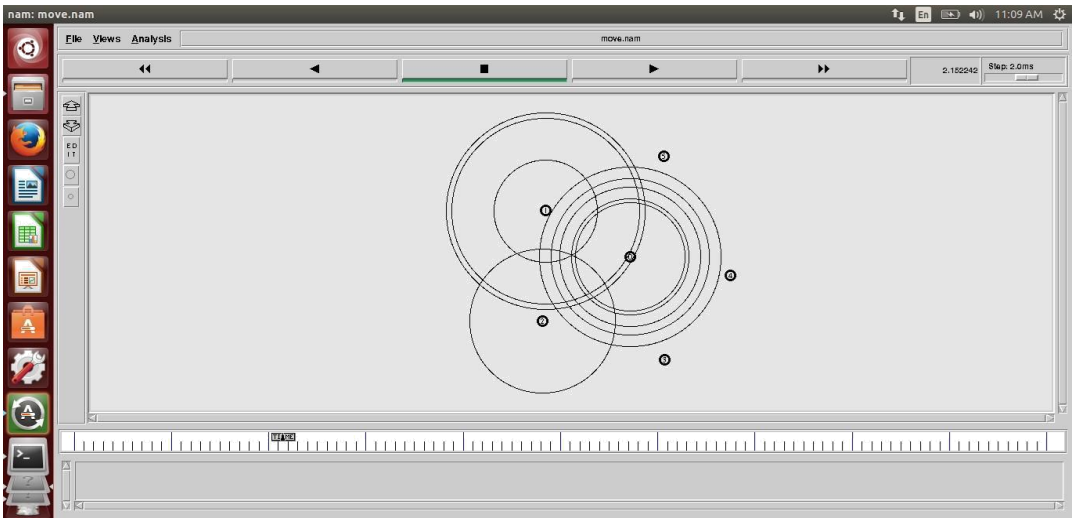
The trial has been completed with the essential intention of applying Anomaly-based Intrusion Detection Technique to recognize the likelihood of the presence of interruption in the system. The analysis on NS-2 test system has been performed for four arbitrary system topologies whose screenshots are taken in Screenshot 5.3, 5.4, 5.5, 5.6 for DSR protocol, DSDV protocol, DSR with flood attack, DSDV with flood attack consisting 6, 6, 24, 24 number of nodes respectively. In a topology with DSR protocol, every one of the 6 nodes are portable while in DSDV arrange topology, just source and sink nodes are versatile rest are static and topologies with intrusion comprise of every single static node.

Experiment 1: DSDV Network Simulation without flood attack

Table 5.1 shows the simulation information of DSDV protocol without flood attack implementation and Screenshot 5.3 displays the network scenario for the same.

Table 5.1 Simulation Information of DSDV protocol without Flood Attack

Simulation	
Simulation Length	3.810
Number of sending nodes	6
Number of receiving nodes	6
Number of dropped packets	15
Number of lost packets	0
Minimal packet size	28
Maximal packet size	1618
Number of sent packets	1333
Number of forwarded packets	144
Number of dropped bytes	1072



Screenshot 5.3: Network scenario of DSDV protocol without flood attack

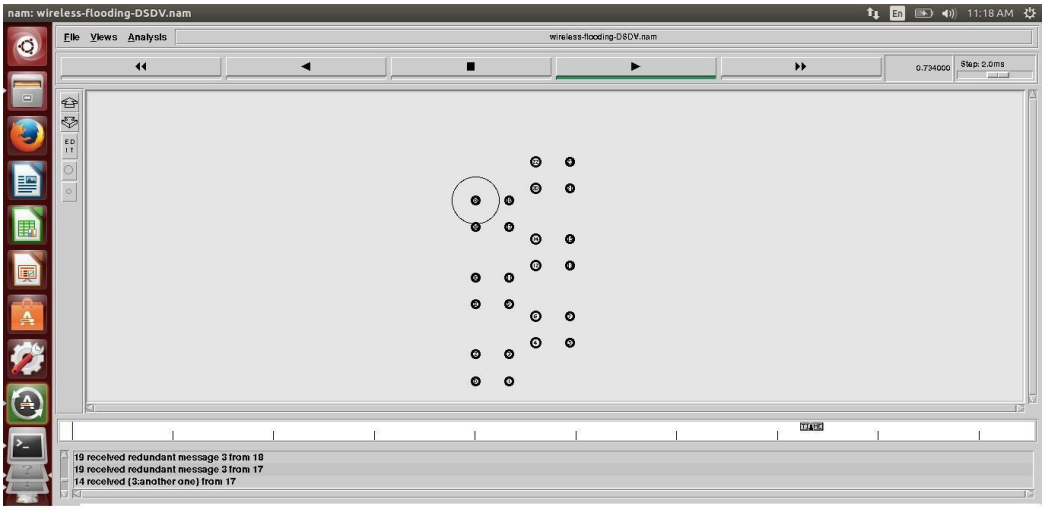
Experiment 2: DSDV Network Simulation with Flood Attack

Table 5.2 shows the simulation information of DSDV protocol with flood attack implementation and Screenshot 5.4 displays the network scenario for the same.

Table 5.2 Simulation Information of DSDV protocol with Flood Attack

Simulation Information	
Simulation Length	5.886
Number of sending nodes	24
Number of receiving nodes	0
Number of lost packets	620
Minimal packet size	32
Maximal packet size	680
Number of sent packets	738

Number of forwarded packets	0
Packet dropping node	3,4,6,10,11



Screenshot 5.4: Network scenario of DSDV protocol with flood attack

Experiment 3: DSR Network Simulation without Flood Attack

Table 5.3 shows the simulation information of DSR protocol without flood attack implementation and Screenshot 5.5 displays the network scenario for the same.

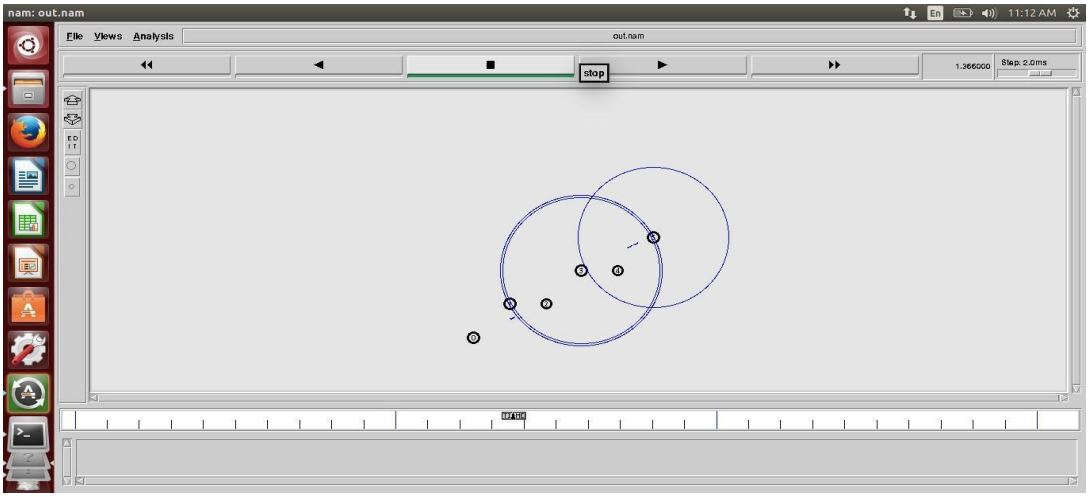


Table 5.3 Simulation Information of DSR protocol without Flood Attack

Simulation Information	
Simulation Length	4.786
Number of sending nodes	6
Number of receiving nodes	6
Number of lost packets	24
Minimal packet size	28
Maximal packet size	1618
Number of sent packets	381
Number of dropped packets	0

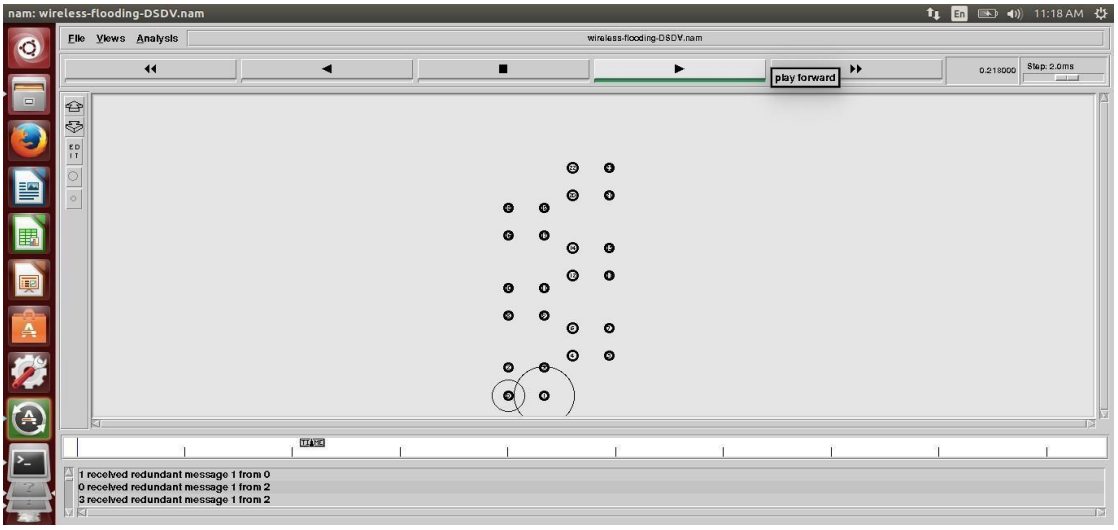
Experiment 4: DSR Network Simulation with Flood Attack

Table 5.4 shows the simulation information of DSR protocol with flood attack implementation and Screenshot 5.6 displays the network scenario for the same.

Table 5.4 Simulation Information of DSR protocol with Flood Attack

Simulation Information	
Simulation Length	4.565

Number of sending nodes	10
Number of receiving nodes	3
Number of lost packets	95
Minimal packet size	32
Maximal packet size	44
Number of sent packets	200
Number of dropped packets	65
Nodes dropping packets	2,4,5,9



Screenshot 5.6: Network scenario of DSR protocol with flood attack

Simulation parameters information that are applied in these networks is provided in Table 5.5.

Table 5.5: Simulation parameters

Parameters	**Parameter value for network 1**	**Parameter value for network 2**	**Parameter value for network 3**	**Parameter value for network 4**
Maximum simulation time	10	10	10	10
Routing Protocol	DSR	DSDV	DSR with flood attack	DSDV with flood attack
Propagation Model	Two ray ground propagation	Two ray ground propagation	Two ray ground propagation	Two ray ground propagation
MAC layer Protocol	IEEE 802.11	IEEE 802.11	IEEE 802.11	IEEE 802.11
Node placement	Mobile	Mobile	Static	Static
Number of Nodes	6	6	24	24

5.5 Dataset preparation

Trace record contains the system data in the raw format, determined subsequent to the simulation of the system. This unknown configuration is then changed over into a comprehensible arrangement and consequently, the properties of the dataset are depicted beneath in Table 5.6 and Table 5.7.

Table 5.6: Dataset description for DSR and DSDV protocol without Flood Attack

Attributes	**Description**
Status	Packet status (r, d, s)
Timestamp	Current time of the event
Hs	ID for this node
Hd	ID for next hop towards the destination
Ni	Node ID
Nx	Node's x-coordinate
Ny	Node's y-coordinate
Nz	Node's z-coordinate
Ne	Node energy level
Nl	Trace level such as AGT, RTR, MAC
Information	Packet information at IP level, MAC level, and Application level

Table 5.7: Dataset description for DSR and DSDV protocol with Flood Attack

Attributes	**Description**
Pkt status	Packet status (r, d, s)
Timestamp	Current time of the event
Node ID	Unique identification of every node in a network
Layer	Layer responsible for moving data packets (MAC, RTR, IFQ)
Pkt ID	Unique identification of packets

Pkt Type	Type of packet (cbr, DSR, RTS, ARP)
Pkt Size	Size of packet
Transmission time	Time took for transmitting packet
Sender_Mac ID	Mac ID of sender node
Receiver_Mac ID	Mac ID of receiving node
Mac_type	Mactype (800: IP header:0x0800, ETHERTYPE_ARP is 0x0806)
Information	DSR details (route error, link break, route request, etc)

5.6 Classification Details

The data produced by simulation of a network with attack and without attack have been analyzed and classified using different machine learning models. A brief description of these models is given in this section.

1. Naive Bayes

Naive Bayes is a measurable order strategy and depends on the Bayesian hypothesis. It accepts that each element is autonomous of each other and henceforth ascertains the outcome. It also accepts that properties don't interface with each other. It is an order calculation for double and multi-class characterization issues. Naive Bayes display is fabricated quicker than different models i.e. training is faster on the grounds that it requires less measure of training information to gauge come about. It is a basic plan for building classifiers. It is in certainty a group of classifiers wherein each of the part classifiers is established on the basic rule of Bayes hypothesis. Herein, all part classifiers assume the estimation of the considerable number of ascribes to be free of each other given the class variable. For instance, any record, in an accumulation of records of natural products, with the characteristic esteems as red, round and 10cm in width is named an Apple for the traits of shading, shape, and size separately. Any conceivable presence of any sort of relationship among the qualities of shape, shading, and size is slighted, and are accepted to contribute freely to the likelihood of the specific record (organic product) being an apple. In a directed getting the hang of

setting and for some kind of likelihood models, certain credulous Bayes classifiers can be prepared effectively. The greatest probability strategy is utilized for parameter estimation for different Bayes models in an assortment of practical applications without tolerating Bayesian likelihood or utilizing any Bayesian strategies.

2. J48

J48 utilizes decision tree for classification by creating a parallel tree for each tuple in the database to group the entire dataset. It overlooks the missing esteems in a dataset and predicts them on the premise of known estimations of the quality in a record.

3. Random Forest

Random Forest is a classifier which comprises of numerous choice trees and by figuring a normal number of votes of all trees, a yield is anticipated. This calculation runs productively on extensive datasets as it can deal with an expansive number of information factors by maintaining a strategic distance from variable cancellation. The forest created in past for a few information can be reused in future for another information.

Chapter Summary

This chapter examines the philosophy used to perform tests completed in this postulation. Exploratory setup, programming apparatuses portrayal is displayed in this section. Simulation details in the postulation are portrayed and classification details are likewise described. The screenshots of the tests done are given and subtle elements of the determined dataset are additionally depicted in this part.

CHAPTER 6

RESULTS AND DISCUSSION

In this section, consequences of the experiments that are discussed in previous chapter are appeared. The results of the system reproduced utilizing NS-2 have been talked about. The network working under a few conventions have been examined and contrasted with the network that contains an interruption. Furthermore, information caught from simulation has been examined utilizing Anomaly Detection approach that aides in identifying an interruption and its conduct in the system. Results of the simulation appear on execution measurements like cumulative sum of lost bytes, throughput, and the packet status. Simulation data of the malicious node in the system is likewise exhibited. In this chapter, machine learning results are talked about too.

6.1 Analysis of DSDV and DSR Network without attack

The after effect of the recreation performed without any attack utilizing DSR and DSDV protocol can be examined utilizing distinctive assessment measurements and we have focused on the throughput of the receiving packets and the cumulative sum of lost bytes measurements individually.

- **Throughput**

  The graph in Figure 6.1 and Figure 6.2 represents the throughput of receiving packet represented on X-axis increases as simulation time on Y-axis comes to an end hence receiving maximum of data packets to the destination.

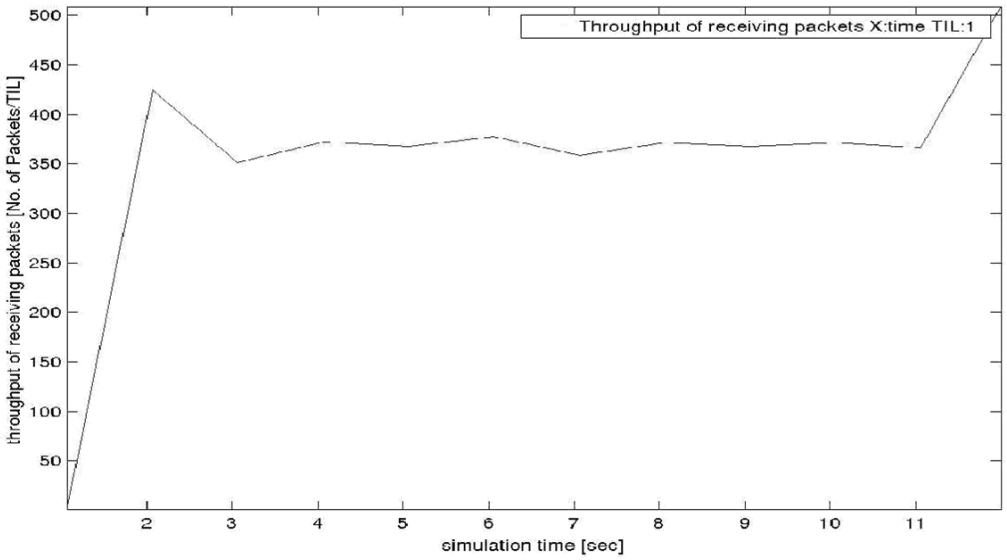


Figure 6.1: Throughput of receiving packets versus Time for DSR without flood attack scenario

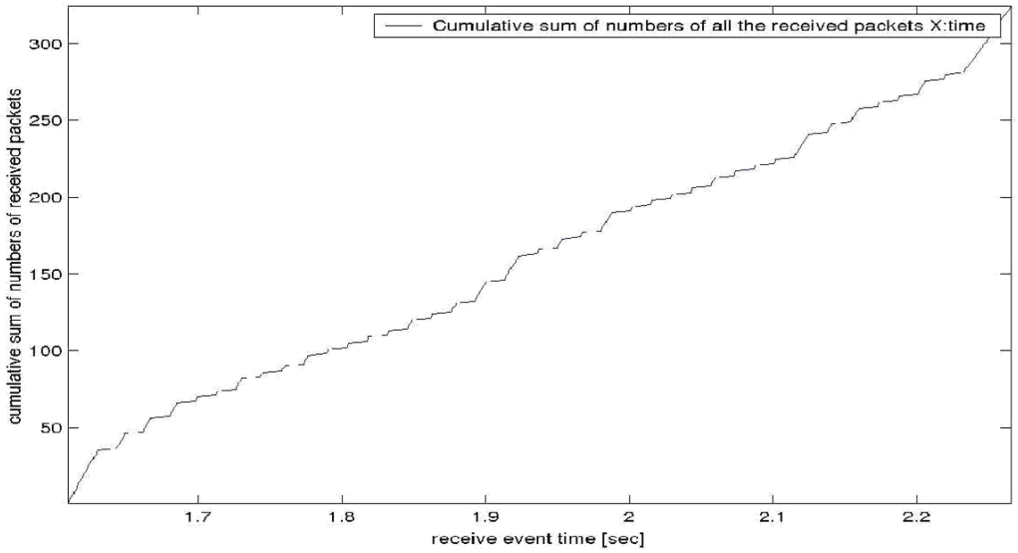


Figure 6.2: Throughput of receiving packets versus Time for DSDV without flood attack scenario

- **Packet Status**

The graphs shown in Figure 6.3 and Figure 6.4 represents packet IDs of the received data packets in the network as an evaluation metric for the network behavior for both DSR and DSDV protocols respectively. The X axis represents packet receive time and Y axis represents the ID of received packets.

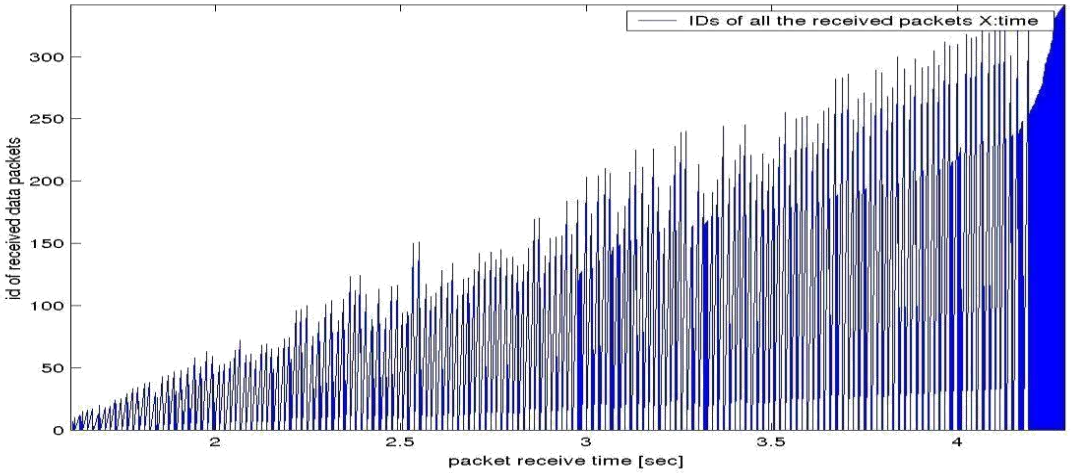


Figure 6.3: Received data packets in DSDV protocol without intrusion

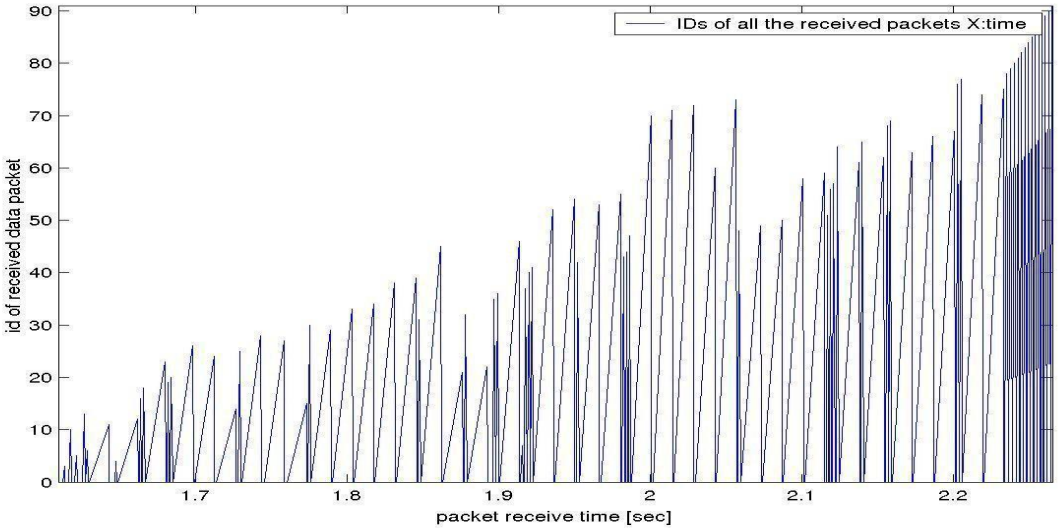


Figure 6.4: Received data packets in DSR protocol without intrusion

- **Machine learning results**

  Table 6.1 represents the performance of the dataset related to DSR and DSDV network without flood attack. The performance of the dataset was tested with three different models namely, Naïve Bayes , J-48 and Random Forest. It is observed that Random Forest model gives the most accurate results of DSR network with almost 96.61% accuracy and J48 gives the most accurate results of DSDV network with almost 93.21% accuracy.

Table 6.1: Machine Learning classification analysis results for DSR and DSDV Network

Algorithm	Dataset	Time is taken to build model	Currently classified instances % accuracy	Incorrectly classified instances % accuracy	Mean absolute error	ROC area
Naive Bayes	DSDV	0.1	73.8120	26.188	0.1532	0.680
	DSR	0.05	61.7209	38.2231	0.2681	0.774
J48	DSDV	0.05	93.2153	6.7856	0.1025	0.991
	DSR	0.02	75.1212	24.8788	0.1856	0.660
Random Forest	DSDV	0.28	66.4561	33.5439	0.2297	0.789
	DSR	0.94	96.6198	6.3814	0.1347	0.989

6.2 Analysis of Flood attack in DSR Network

- **Throughput**

  Figure 6.5 speaks to throughput for receiving packet versus time chart for DSR protocol where a straight line at 0 amid the entire simulation demonstrates no information bytes have been received by any node because of inhabitance of system resources due to the presence of flood attack.

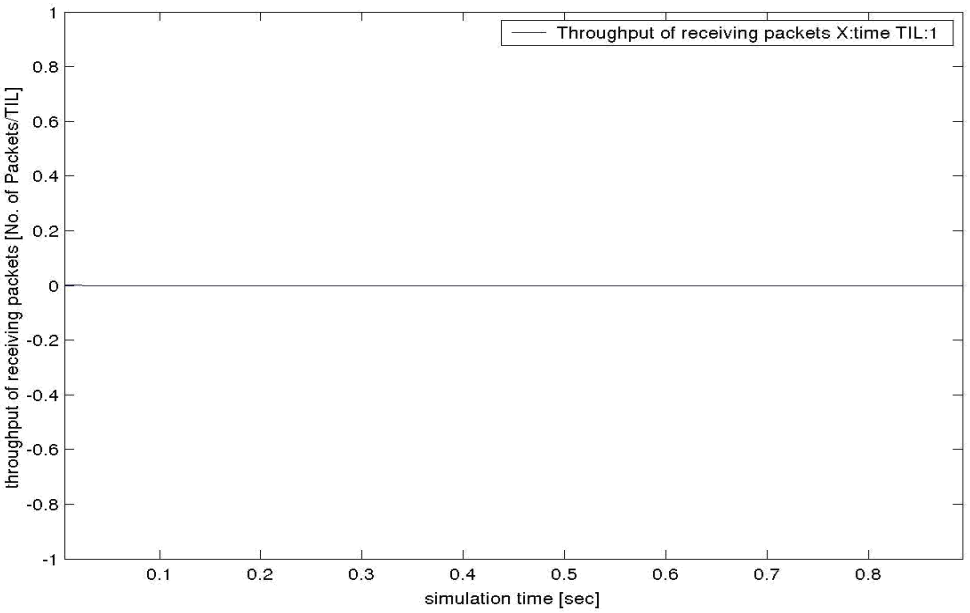


Figure 6.5 Throughput of receiving packets versus Time for DSR in the presence of flood attack.

- **Cumulative sum of lost bytes**

  Figure 6.6 demonstrates the increase in the cumulative sum of lost bytes while simulating the system that contains flood attack malicious nodes. This increase in lost bytes tends to decreased correctness and completeness of the routing protocol in the system. It can be reasoned that DSR does not include any mechanism for shielding the system from malicious node making flood attack.

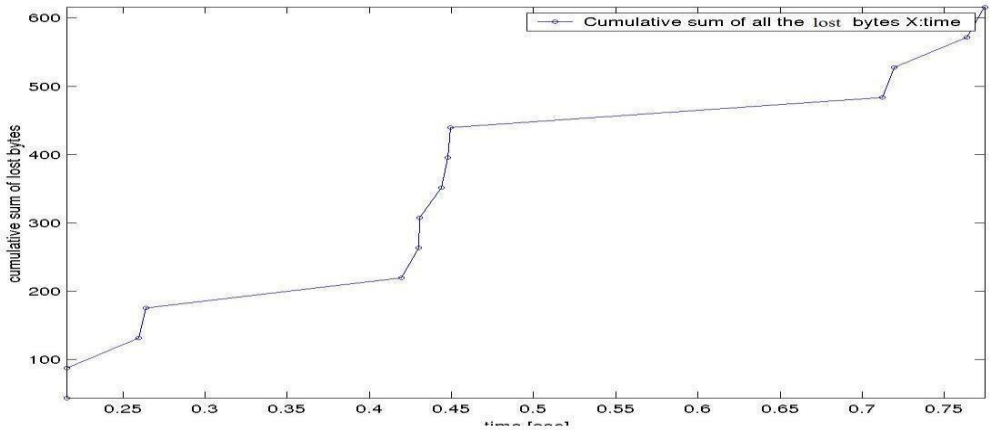


Figure 6.6: Cumulative sum of lost bytes versus time under DSR flooding attack.

- **Machine learning results**

  Table 6.2 represents the performance of the dataset related to flood attack in DSR. The performance of the dataset was tested with three different models namely, Naïve Bayes , J-48 and Random Forest. It is observed that Random Forest model gives the most accurate results with almost 71.21% accuracy.

Table 6.2: Machine Learning classification analysis results for DSR with Flood

Algorithm	**Time is taken to build model**	**Currently classified instances % accuracy**	**Incorrectly classified instances % accuracy**	**Mean absolute error**	**ROC area**
Naive Bayes	0.01	70.4545	29.5455	0.2802	0.758
J48	0.01	66.6667	33.3333	0.3638	0.500
Random Forest	0.11	71.2121	28.7879	0.2224	0.850

6.3 Analysis of Flood attack in DSDV Network

- **Throughput**

  Figure 6.7 represents throughput for receiving packet versus time graph for DSDV protocol where a straight line at 0 amid the entire simulation demonstrates no information bytes have been received by any node because of occupancy of system resources due to the presence of flood attack.

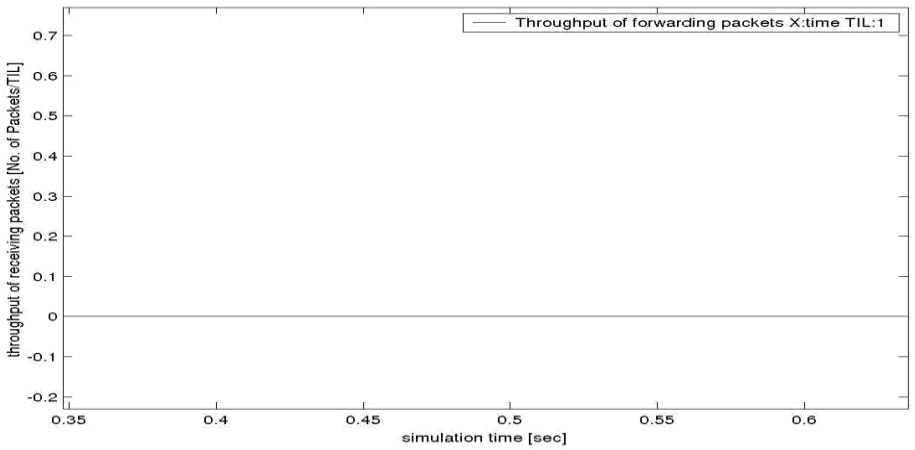


Figure 6.7: Throughput of receiving packets versus Time for DSDV in the presence of flood attack.

- **Cumulative sum of lost bytes**

  Figure 6.8 demonstrates the increase in the cumulative sum of lost bytes while simulating the system that contains flood attack malicious nodes. This expansion in lost bytes demonstrates the decreased correctness and completeness of the routing protocol in the system. It can be concluded that DSDV does not include any mechanism for shielding the system from malicious node initiating flood attack.

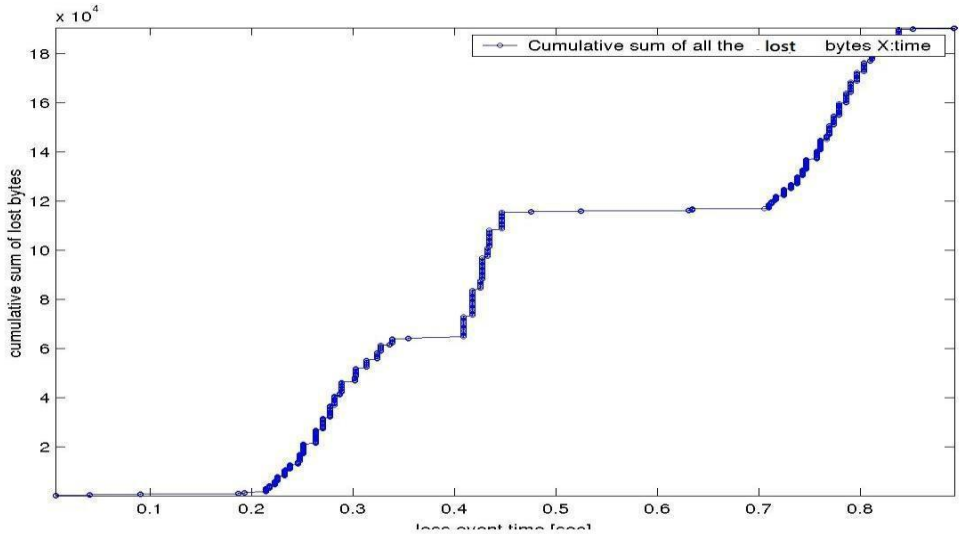


Figure 6.8: Cumulative sum of lost bytes versus time under DSDV flooding attack.

- **Machine learning results**

  Table 6.3 represents the performance of the dataset related to flood attack in DSDV. The performance of the dataset was tested with three different models namely, Naïve Bayes , J-48 and Random Forest. It is observed that J-48 model gives the most accurate results with almost 88.56% accuracy.

Table 6.3: Machine Learning classification analysis results for DSDV Flood attack

Algorithm	**Time is taken to build model**	**Currently classified instances % accuracy**	**Incorrectly classified instances % accuracy**	**Mean absolute error**	**ROC area**
Naive Bayes	0.03	75.5208	24.4792	0.1425	0.926
J-48	0.13	88.5625	11.4375	0.1744	0.805
Random Forest	4.04	74.4792	25.5208	0.1994	0.945

Chapter Summary

In this section, the outcomes with respect to the network analysis are exhibited. Each system has been investigated by assessment measurements like packet status, cumulative sum of lost bytes and throughput. Likewise, each system is investigated utilizing machine learning calculations like Naive Bayes, J48, and Random Forest.

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 Conclusion

WSN has a system design which gives the capacity to sensor nodes gather information from the physical condition and transmit it further to different nodes. This correspondence among nodes ought to be exceptionally all around secured and to guarantee that a security mechanism is required. In many sorts of research we have found regardless of applying those security systems, attacks get to the nodes making them malicious and crushing the system.

The experiments were done in this theory essentially concentrates on recognizing the malicious node in the system. Additionally, the systems are assessed on execution measurements like packet status, cumulative sum, and throughput. In this thesis, we have simulated four systems actualizing the DSR and DSDV routing protocols. Flood attack on these protocols has been simulated. Each system has been broke down utilizing machine learning algorithms. Further, trace graph has likewise been utilized to distinguish the correct noxious node in the system. Machine learning classification algorithms, for example, Naïve Bayes, Random Forest, and J48 have been utilized.

After the simulation procedure, two distinct documents are produced to be specific, the trace file and the network animator document. The trace document, helps creating the dataset. The network animator document accumulates simulation data for every node in the system and furthermore delivers various graphical outcomes which additionally helps in understanding the system.

7.2 Future Scope

In this specific proposal we mean to distinguish the attack in node inside the system and subsequently, for the future degree, a more profound investigation of the system should be possible utilizing other machine learning techniques. Likewise, different patterns and practices of every node can be recognized so as to contrast it with different nodes in the system and characterize a specific node as noxious and non-vindictive.

REFERENCES

[1] I. Krontiris et al., "Intrusion Detection in Wireless Sensor Networks," in 1*3th European Wireless Conference,* Paris, France, 2007.

[2] R. Roman et al., "Applying Intrusion Detection Systems to Wireless Sensor Networks," in *IEEE Consumer Communications & Networking Conference (CCNC 2006),* 2006.

[3] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad hoc Networks," in *MobiCom'00,* 2000, pp. 255265.

[4] S. Dubey et al., "Analysis of Effect of Flooding on Performance of Ad hoc Network," *International Journal Of Engineering And Computer Science ISSN,* vol. 5, pp. 19230-19236 , 2016.

[5] B. H. K. Pai et al., "Detection and performance analysis of various DOS attacks under collaborative environment," in *elsevier, emerging research in computing, information communication and application* , 2013.

[6] M.S. Islam, and S. AshiqurRahman, "Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches," in I*nt. J. Advanced Science and Technology*, vol. 36, November 2011.

[7] I. Onat and A. Miri, "An Intrusion Detection System for Wireless Sensor Networks, Wireless and Mobile Computing," *Networking And Communications*, vol. 3, 2005, pp. 253-259.

[8] CE. Loo et al., "Intrusion Detection for Routing Attacks in Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 2, pp. 313-332, 2006.

[9] S. K. Singh, "Routing Protocols in Wireless Sensor Networks – A Survey," *International Journal of Computer Science & Engineering Survey (IJCSES)* , vol.

1, 2010.

[10] S. Shaust and H. Szczerbicka, "Misbehavior Detection for Wireless Sensor Networks – Necessary or Not?," in *6th Fachgesprach Drahtlose Sensornetze der GI/ITG-Fachgruppe Kommunikation und Verteilte Systeme*, Germany, 2007, pp. 51-54.

[11] B. S. A. L. Osborne et al., "INTRUSION DETECTION TECHNIQUES INMOBILE AD HOC AND WIRELESS SENSOR NETWORKS," in *IEEE wireless communiations*, 2007.

[12] J. Kim et al., "Danger is Ubiquitous: Detecting Malicious Activities in Sensor Networks using the Dendritic Cell Algorithm," in *ICARIS*, LNCS 4163, 2006.

[13] A. Abduvaliyev, "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks," *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, vol. 15, 2013.

[14] A. Nadeem, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks," *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, vol. 15, 2013.

[15] S. Misra et al., "LAID: a Learning Automata-based Scheme for Intrusion Detection in Wireless Sensor Networks," *Security and Communication Networks*, vol. 2, pp. 105-115, 2008.

[16] Z. Yu and J. Tsai, "A Framework of Machine Learning Based Intrusion Detection for Wireless Sensor Networks," in *SUTC'08*, 2008, pp. 272279.

[17] S. Doumit and D. P. Agrawal, "Self-organized Criticality and Stochastic Learning based Intrusion Detection System for Wireless Sensor Network," in *MILCOM 2003*, pp. 609-614.

[18] S. Banerjee et al., "Intrusion Detection on Sensor Networks Using Emotional Ants," *Int'l J. of Applied Science and Computations*, vol. 12, no. 3, pp. 152-173, 2005.

[19] F. Hidoussi, "Centralized IDS Based on Misuse Detection for ClusterBased Wireless Sensors Networks," in *springer*, 2015.

[20] S. Misra et al., "A Simple Learning Automata-based Solution for Intrusion Detection in Wireless Sensor Networks," *Wireless Communications and Mobile Computing, Special Issue on Architectures and Protocols for Wireless Mesh, Ad Hoc, and Sensor Networks,* vol. 11, no. 3, 2011, pp. 426-441.

[21] A. Agah et al., "Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach," in *3rd IEEE International Symposium on Network Computing and Applications*, September. 2004, pp. 343-346.

[22] R. Kothari, "Implementation of Black Hole Security Attack using Malicious Node for Enhanced - DSR Routing Protocol of MANET," *International Journal of Computer Applications* , vol. 64, 2013.

[23] A. Milenkoski, "Evaluating Computer Intrusion Detection Systems: A Survey of Common Practices," *ACM Computing Surveys,* vol. 8, 2015.

[24] Y. Maet al., "The Intrusion Detection Method based on Game Theory in Wireless Sensor Network," in *IEEE Ubi-Media Computing*, 2008, pp. 326-331.

[25] A. Agah and S.K. Das, "Preventing DoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach," *International Journal of Network Security (IJNS)*, vol. 5, no. 2, pp.145-153, 2006.

[26] M. Krishnan, "Intrusion Detection in Wireless Sensor Networks," Project Paper, *University of California at Berkeley*, Unpublished.

[27] Yenumula B. Reddy, "A Game Theory Approach to Detect Malicious Nodes in Wireless Sensor Networks," in *SENSORCOMM'09*, Greece, 2009.

[28] N. A. Alrajeh, "Intrusion Detection Systems in Wireless Sensor Networks: A Review," *InternationalJournalofDistributedSensorNetworks*, 2013.

[29] Yenumula B. Reddy and S. Srivathsan, "Game Theory Model for Selective Forward Attacks in Wireless Sensor Networks," in *17th Mediterranean*

Conference on Control and Automat, 2009.

[30] A.P.R. da Silva et al., "Decentralized Intrusion Detection in Wireless Sensor Networks," in *1st ACM International Workshop on Quality of service and security in wireless and mobile networks*, Montreal, Quebec, Canada, October 2005.

[31] L. Mostarda, and A. Navarra, "Distributed Intrusion Detection Systems for Enhancing Security in Mobile Wireless Sensor Networks," *International Journal ofDistributed Sensor Networks*, vol. 4, no. 2, pp. 83-109, 2008.

[32] Y. Wang et al., "Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks," *IEEE Trans. Mobile Computing*, vol. 8, no. 6, pp. 698-711, 2008.

[33] L. Guorui et al., "Group-based Intrusion Detection System in Wireless Sensor Networks," *Computer Communications*, vol. 32, no. 18, pp. 4324-4332, 2008.

[34] M.V. de Sousa Lemos et al., "A New Collaborative Approach for Intrusion Detection System on Wireless SensorNetworks," in *Novel Algorithms and Techniques*, Springer, 2010.

[35] S. Shin et al., "An Experimental Study ofHierarchical Intrusion Detection forWireless Industrial Sensor Networks," in *IEEE Trans. Ind. Informat*, vol. 6, no. 4, 2010, pp. 744-757.

[36] T.M. Mubarak et al., "A Collaborative, Secure and Energy Efficient Intrusion Detection Method for Homogeneous WSN," in *International Conference on Advances in Computing and Communications (ACC-2011)*, Springer, 2011.

[37] S.K. Singh et al., "Intrusion Detection based Security Solution for Cluster-based Wireless Sensor Networks," in *Int. J. Advanced Science and Technology*, vol. 30, May 2011.

[38] H. Jadidoleslamy, "A High-Level Architecture for Intrusion Detection on Heterogeneous Wireless Sensor Networks: Hierarchical, Scalable and Dynamic Reconfigurable," in *Wireless Sensor Network*, vol. 3, 2011, pp. 241-261.

[39] I. Krontiris et al., "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks," *LNCS*, vol. 4837, pp. 150-161, 2008.

[40] J. CAI et al., "The Simulation and Comparison of Routing Attacks on DSR Protocol," in *IEEE*, 2009.

[41] I. Krontiris et al., "LIDeA: a Distributed Lightweight Intrusion Detection Architecture for Sensor Networks," in *4th International Conference on Security and Privacy in Communication Networks*, Istanbul, Turkey, 2008.

[42] T.H. Hai et al., "Hybrid Intrusion Detection System for Wireless Sensor Networks," in *ICCSA 2007, LNCS 4706*, pp. 383396, 2007.

[43] T.H. Hai and E.N. Huh, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge," in *7th IEEE International Symposium on Network Computing and Applications*, 2008, pp. 325-331.

[44] T.H. Hai et al., "A Lightweight Intrusion Detection Framework for Wireless Sensor Networks," *Wireless Communications and Mobile Computing*, vol. 10, no. 4, April, 2009.

[45] E.N. Huh, and T.H. Hai, "Lightweight Intrusion Detection for Wireless Sensor Networks, in Intrusion Detection Systems," Pawel Skrobanek (Ed.), *InTech*, 2011.

[46] "DSR routing protocol simulation," https://ns2projects.org/networking-projects.html

[47] Nader F. Mir, “Mobile Ad-Hoc Networks,” in Computer and Communication Networks, *Prentice Hall*, 2006, ch. 19, sec. 19.3.

[48] "Flood attack in a network," https://www.researchgate.net/publication/257353025_ The_Impact_of_Resource_Consumption_Attack_on_Mobile_Ad-hoc_Network_Routing.

[49] "NS-2 working," http://www.ns2blogger.in/p/n.html.

[50] Raja Waseem Anwar et al., "A Survey of Wireless Sensor Network Security and Routing Techniques," *Research journal of Applied Science, Engineering and Technology*, 2015.

LIST OF PUBLICATIONS

- Kriti Taneja and Sanmeet Bhatia, "Automatic Irrigation System using Arduino UNO" *International Conference on Intelligent Computing and Control Systems ICICCS*, 2017. (Published)

- Kriti Taneja and Sanmeet Bhatia, "Intrusion Detection System in WSN" *ACM Compute,* 2017. (Communicated)

VIDEO LINK

- https://youtu.be/meH_F2px41Y