5.1. FLOW DIAGRAM FOR HETEROGENEOUS WSNs

Fig. 5.1: Flow Diagram for Heterogeneous WSNs
5.2. FLOW DIAGRAM FOR HOMOGENEOUS WSNs

![Flow Diagram for Homogeneous WSNs]

Fig. 5.2: Flow Diagram for Homogeneous WSNs

5.3. UML DIAGRAMS FOR INTERFERENCE DETECTION

5.3.1. Unified Modeling Language

The Unified Modeling Language allows the software engineer to express an analysis model using the modeling notation that is governed by a set of syntactic semantic and pragmatic rules.

A UML system is represented using five different views that describe the system from distinctly different perspectives. Each view is defined by a set of diagrams, which is as follows.

- **User Model View**
  
  i. This view represents the system from the users perspective.
  
  ii. The analysis representation describes a usage
scenario from the end-users perspective.

- **Structural model view**
  
  i. In this model the data and functionality are arrived from inside the system.
  
  ii. This model view models the static structures.

- **Behavioral Model View**
  
  It represents the dynamic of behavioral as parts of the system, depicting the interactions of collection between various structural elements described in the user model and structural model view.

- **Implementation Model View**
  
  In this the structural and behavioral as parts of the system are represented as they are to be built.

- **Environmental Model View**
  
  In this the structural and behavioral aspects of the environment in which the system is to be implemented are represented.

UML is specifically constructed through two different domains they are:

✓ UML Analysis modeling, this focuses on the user model and structural model views of the system.

✓ UML design modeling, which focuses on the behavioral modeling, implementation modeling and environmental model views.
Use case Diagrams represent the functionality of the system from a user's point of view. Use cases are used during requirements elicitation and analysis to represent the functionality of the system. Use cases focus on the behavior of the system from external point of view.

Actors are external entities that interact with the system. Examples of actors include users like administrator, bank customer etc., or another system like central database.

5.3.2. Use-case Diagram

![Use Case Diagram for Interference Detection](image)

Fig. 5.3: Use Case Diagram for Interference Detection
5.3.3. Activity Diagrams for Interference Detection

Fig. 5.4: Activity Diagram for Module 1

Fig. 5.5: Activity Diagram for Module 2
Fig. 5.6: Activity Diagram for Module 3
if the received packet from other than port

it will be filtered

Discard

Valid packets send to destination

destination

Fig. 5.7: Activity Diagram for Module 4
5.3.4. Sequence Diagrams for Interference Detection

Fig. 5.8: Sequence Diagram for Module 1

Fig. 5.9: Sequence Diagram for Module 2
1: connected()
2: check whether the port is authorized or unauthorized
3: authorized path then send to valid destination
4: not valid, path is discarded

Fig. 5.10: Sequence Diagram for Module3

1: connected()
2: if received path from other than port connected to filter
3: Valid send to destination
4: not valid, discarded

Fig. 5.11: Sequence Diagram for Module4
5.4. IMPLEMENTATION FOR INTERFERENCE DETECTION

5.4.1. Modules

The present study is divided into the following modules

1. Constructing Sensor Network
2. Packet Creation
3. Find authorized and un authorized port
4. Constructing Inter-Domain Packet Filters
5. Receiving the valid packet

5.4.2. Modules Descriptions

Module-1

In this module, we are going to connect the network. Each node is connected the neighboring node and it is independently deployed in network area. And also deploy the each port no is authorized in a node.

Module-2

In this module, browse and select the source file. And selected data is converted into fixed size of packets. And the packet is send from source to detector.

Module-3

The intrusion detection is defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. In this module check whether the path is authorized or unauthorized. If path is authorized the packet is
send to valid destination. Otherwise the packet will be deleted. According port no only we are going to find the path is authorized or Unauthorized.

**Module-4**

If the packet is received from other than the port no it will be filtered and discarded. This filter only removes the unauthorized packets and authorized packets send to destination.

**Module-5**

In this module, after filtering the invalid packets all the valid Packets will reach the destination.
5.4.3. Front End Interface Designs
// Received...
Packet 140 Source->D3-----------------------------
Packet 141 Source->D3-----------------------------
public static void main Received...
Packet 142 Source->D3n(String[] args)
{
    Detector r1=new Detector(); Received...
Packet 143 Source->D3;
    while (true)
    {
        r1.send();
    }
}
// Received...
Packet 144 Source->D3End of Testing =
}
Received...
5.4.4. Front End Interface Designs for Multiple Sensor Screens
Sink2

**********THIS IS FROM PORT R_102**********

Sink3

**********THIS IS FROM PORT R_106**********