Chapter 2

Selective Forwarding Attack

2.1 INTRODUCTION

In a wireless sensor network, the node uses multi-hop transmission to deliver the packet from source to destination. An adversary can compromise some of the internal nodes and cause misbehavior while routing the packets in the network. Selective Forwarding Attack (Brown and Xiaojiang 2008) is one of the routing attacks which intentionally drop some of the packets passing through them without delivering to the destination. It is very harmful for critical applications and can damage the network communication.

The drawbacks of the existing detection schemes are:

1. Requirement of more storage space due to one-way hash key chains for authentication.
2. Possibility to suspect the nodes available in the forward routing path only.
3. Nodes are loosely time synchronized.
4. Static network topology.
5. Lack of Energy measurements.
The proposed scheme is discussed with the different phases as shown below:

2.2.1 Detection Phases

detected as malicious node. Retains the same identification for longer time duration, then the node is detected as malicious node. Each node monitors each other ID number. In case the node number matches the ID number, according to their placements. After mobility, base station provides an ID malicious node based on the respective node ID. Base station provides an ID malicious node in the forward routing path. This scheme also detects the malicious nodes that are not present in the data received by the malicious nodes. The acknowledged packets are forwarded from the check points to the base station. If there is a malicious acknowledgment through the check points, the acknowledged packets are retransmitted to the data receivers. The nodes provide acknowledgment if they receive the data.

2.2 PROPOSED SCHEME-1: CHEAD BASED

Results of the simulation are discussed. Divisions of this chapter give the simulation details of the schemes and the acknowledgment and energy based schemes are proposed. The sub- acknowledgment and energy based schemes are analyzed. To achieve the above targets, Chebyshev and Cumulative

analyze the performance of the proposed scheme.

This chapter proposes malicious node detection schemes for selective forwarding attack in the mobile wireless sensor network and to overcome due to redundant transmissions.

4. Overhead due to redundant transmissions.

5. Few schemes detect only one malicious node in the forward.

6.
a trap message after the successful receipt of the packet. In the forward path randomly. In the downstream link, check point generates base station/destination node assigns the nodes to be the checkpoint.

Checkpoint Selection Phase

Selected based on the DSR protocol (Bahl et al. and Shamyegam 2009). Forward path through which the data is to be transmitted. Forward path is selected based on the route reply packet with the selected node/base station. If responds to the route reply packet with the selected node, source node sends the route request packet to the destination.

Forward Route Selection Phase

Network and stores the next hop neighbor ID for identifying the topology of the network. After receiving the node ID, the node identifies its neighbor node.
Detection Process

Successfully transmitted from the source to the destination message generated by the last checkpoint. It shows that the data has been to its next node in the forward path. If the destination receives the trap cumulative acknowledgment packet, it generates the trap message and sends acknowledgment packets are cumulated. Once the check point receives the
Step 6: Source node sends the data packet to the next node which lies in the forward path. Upon receiving the data, the node sends the acknowledgement packet and the receiving node sends its acknowledgement packet along with the data packet and thus frames the cumulative acknowledgement (CACK).

Step 7: Once the check point receives the cumulative acknowledgement, it generates the trap message and it is forwarded along with the data to the next check point.

Step 8: Upon receiving the cumulative acknowledgement packet and the trap message, the base station detects the exact malicious node in the forward path based on the negative acknowledgement (NACK). If any node holds its ID after a predetermined time interval of the window, that node is suspected as malicious and is illustrated in the algorithm.

Step 9: Once the malicious node is detected, it is removed from the network and the packet is forwarded through the alternate path.
**Input:**

CAKP : A cumulative packet received

\[ \{ Data_n, ACK_0, ACK_1, \ldots, ACK_n \} \]

n: Total # of ACKs in CAKP

m: Total # of nodes in the forwarding path

RDS: Receive Data Successfully

CKPID: Check Point ID

NID: Node ID

**Trap :** \{ CKPID, RDS, NID of NACK \}

1. create a list of responses [] and traps[] of length m

2. for i=0,\ldots,n-1

   responses [n-1] <- ACK \_n-i remove ACK \_n-i from CAKP

   if ACK \_n-i == n then

      return \{ RDS=1 \}

   else \{ RDS=0 \}

   return CKPID

   endif

3. for i=0,\ldots,n-1

   traps [n-i] < NIDs(NACK)

   remove and CKPID and RDS from trap[]

4. for i=0,\ldots,n-1

   if CKPID [trap] != CKPID i+1 then

   if (trap[RDS]==1) then

      return CKPID’s

   else

      return the NIDs(NACK)

   end if

5. return \{ NIDs(NACK) \}

**Figure 2.1 Algorithm of the CHEAD Scheme**
Figure 2.2 Node-ID Detection
2.2.2 Detection Analysis

The proposed detection scheme has been analyzed based on the following scenarios.

Scenario 1: Based on node ID

If any node holds the ID after the timer expires, that node is suspected to be malicious. The value of the timer depends on the number of hops in the forward routing path and a maximum time of transmission delay. Packet delivery ratio, and throughput are further analyzed to confirm the node to be a malicious node. In Figure 2.2, the node ID’s of window A and window B are different except the node IDs such as 45, 15 and 21. They are treated as malicious nodes.
Scenario 2: Checkpoint detection

The checkpoints are randomly selected, if the base station/destination selects the malicious node as checkpoints that generate acknowledgement and trap message on its own and forward the packet to its neighbor node. In that case, detection of malicious node may be suspected based on the node ID and packet delivery ratio. The checkpoint ID is valid until the window expires. In Figure 2.3 Node 13 and 63 are source nodes and base station is treated as destination node and forward paths are 13-8-11-21-25-83-89-86-BS and 63-91-68-16-94-BS respectively.

The checkpoints are 21, 16 and 83. The forward path from the source 63 to base station does not contain any malicious nodes. But the forward path from 13 to the base station contains 21 as check point but it is also a malicious node. In this case, a checkpoint is a malicious node and it is detected based on node ID and packet drop ratio.

Scenario 3: Source node detection

The base station broadcasts the request to nodes, and the malicious node responds to the base station with the route request packet station to gather the routing information and misguide the route in the network. Figure 2.4 shows that the malicious node 15 voluntarily responds to the base station after receiving the route request and misguides the route. The actual forward path is 15-62-69-95-86-BS and malicious node suggests the route as 15-68-16-94-86-BS. The node is detected based on the packet drop ratio and based on the cumulative acknowledgement packet.
Figure 2.4 Source Node Detection

Scenario 4: Node can be a malicious node

The existing methods such as CHEMAS and CADE; detect any two nodes in the selective forward path as malicious node. In CHEMAS, malicious node lies within the range of check points. In CADE, the detection scheme is used to identify the two malicious nodes in the forward path.

The proposed scheme detects the exact malicious nodes. The checkpoint generates a trap message and forwards it to the next check point stating that packet drop does not exist up to that checkpoint. Between the two checkpoints, acknowledgement of each node is cumulated if the data has been transmitted successfully. Once the check point receives the cumulative acknowledgement successfully, then it generates the trap message. If any
node between the check points fail to forward the data packet, cumulative acknowledgment and trap message, then the node is suspected to be malicious node. In mobile nodes, the cumulative acknowledgment packet can also get dropped due to the collision and timer expiry as the nodes are mobile nodes. Overlapping of the window causes the packet drop in the network. Checkpoint should not misjudge a normal node to be a malicious node.

Figure 2.5 Normal Node as Malicious Node

In Figure 2.5 Node 5 drops the cumulative acknowledgement packet and it is treated as malicious node. Based on the negative acknowledgement, the malicious node is identified.

**Packet format of the Cumulative Acknowledgement**

<table>
<thead>
<tr>
<th>Data</th>
<th>Ack0</th>
<th>Ack1</th>
<th>…</th>
<th>Ack N</th>
<th>NACK</th>
</tr>
</thead>
</table>

**Packet Format of the Trap message**

<table>
<thead>
<tr>
<th>Checkpoint Node ID</th>
<th>RDS</th>
<th>Node IDs of NACK</th>
</tr>
</thead>
</table>

Figure 2.6 Packet format of the cumulative acknowledgement and trap message
The packet format of Cumulative acknowledgement and trap message is shown in Figure 2.6. If NACK is set to 0, it denotes that it is a negative acknowledgement of the data packet and if it’s set to 1, it denotes that it is a negative acknowledgement of the route, and if the node has not seen the route a packet sent by the base station/destination. Received Data Successfully (RDS=1) denotes that data is received up to the particular check point indicated by its node ID. Once the destination/base station identifies the malicious nodes, the destination broadcasts the node ID of NACK packet. Source requests the destination to send the alternate forward path.

2.2.3 Performance Analysis

The performance of the proposed scheme is analyzed using Network Simulator (NS-2). The factors that influence the detection accuracy are network throughput and packet delivery ratio.

2.2.3.1 Simulation parameters

The parameters assigned for simulations are given in Table 2.1. Malicious nodes are randomly located on the forward paths of source and base station. Node IDs, check points, source, and destination are assigned before the transmission starts.
Table 2.1 Simulation Parameters of CHEAD Scheme

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field Size ((\text{m}^2))</td>
<td>1000 X1000</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>50</td>
</tr>
<tr>
<td>Packet Size ((\text{bytes}))</td>
<td>512</td>
</tr>
<tr>
<td>Transmission range ((dBm))</td>
<td>15.0</td>
</tr>
<tr>
<td>Receiving range ((dBm))</td>
<td>-91.0</td>
</tr>
<tr>
<td>Transmission Protocol</td>
<td>UDP</td>
</tr>
<tr>
<td>Traffic</td>
<td>CBR</td>
</tr>
<tr>
<td>Data Rate ((Mbps))</td>
<td>10</td>
</tr>
<tr>
<td>Pause Time((s))</td>
<td>24.0</td>
</tr>
<tr>
<td>Simulation Time((s))</td>
<td>100</td>
</tr>
<tr>
<td>Propagation Model</td>
<td>Two ray ground model</td>
</tr>
<tr>
<td>Mobility Model</td>
<td>Random Waypoint model</td>
</tr>
<tr>
<td>Number of Malicious Nodes</td>
<td>20</td>
</tr>
<tr>
<td>Type of attack</td>
<td>SFA</td>
</tr>
<tr>
<td>Examined Routing Protocol</td>
<td>DSR</td>
</tr>
<tr>
<td>Mobility ((m/s))</td>
<td>0-10</td>
</tr>
<tr>
<td>No. of Packets sent per Second</td>
<td>168</td>
</tr>
<tr>
<td>Packet Loss((\text{pkt/sec}))</td>
<td>66</td>
</tr>
<tr>
<td>Detection of Malicious Node((ms))</td>
<td>200</td>
</tr>
</tbody>
</table>

1.2.3.2. Simulation outputs

The simulation topology is shown in Figure 2.7. It contains the check points, source node and destination nodes with their ID. The nodes 2, 11, 13, 23 are the checkpoints.
Few packet drops have occurred during the data transmission Phase which is indicated in Figure 2.8.
During the data transmission, malicious nodes are detected. Node 2 is a check point node and malicious node. The other malicious nodes are 7, 14 and 41 as shown in Figure 2.9.

![Figure 2.9 Detection of Malicious Nodes](image)

In the simulation, different types of field configurations are used including the forward path nodes which are moving randomly, pausing for a fixed time of 24.0 seconds and moving randomly in a 1000m x 1000m area. The simulation time is 100 seconds and results are taken after 50 simulation runs. The Constant Bit Rate (CBR) traffic is introduced while the data transmission is carried out to check the detection accuracy.

The performance of the proposed scheme is evaluated with following metrics.
- Packet Delivery Ratio.
- Throughput.
- Packet Drop Ratio.
- Energy Consumption.
- Latency.

### 2.2.3.3 Packet delivery ratio

It is observed from the simulation results, that the packet delivery ratio of the network increases until the packet drop ratio of the network is considerably less and decreases as the packet drop ratio of the network is high. Since the accuracy of the detection scheme is improved according to the detection methodology, the proposed scheme yields better network performance. There is also for the possibility of undetected malicious node in the network if the packet drop is less and it is due to the CBR traffic and overlapping of the window.

Figure 2.10 shows the packet delivery of normal nodes. It is inferred that the packet delivery rate of nodes 0, 12 and 23 are above 80% and nodes 1 and 21 are from 30% to 50%. During the time interval from 30 seconds to 40 seconds and from 95 seconds to 99 seconds, the packet delivery ratio is only 20%. Hence it is inferred that, even the normal nodes could be predicted as a malicious node.
Figure 2.10 Packet Delivery of Normal Nodes

Figure 2.11 Packet Delivery of Checkpoint Node
Figure 2.11 depicts the packet delivery ratio of checkpoint node, normal node, and malicious node. It is observed that node 2 is a checkpoint and is detected as malicious node. The packet delivery ratio is 80 like normal nodes. The proposed scheme detects the checkpoint based on node ID. The timer of that particular node holds above the maximum time. Further, it is observed that timer of normal node ID is 40 seconds but the timer of checkpoint is 120 seconds for an observed window. Node 14 is a malicious node and its packet delivery ratio is 0. The packet delivery ratio of normal nodes 17 and 12 are above 200. The packet delivery ratio of the node 8 is 160.

2.2.3.4 Throughput

Throughput denotes that the transmission of packets has been done successfully. Figure 2.12 shows the throughput of the malicious nodes and normal nodes. The throughput of the malicious nodes 2 and 14 are very less when compared to other nodes 17 and 6.
Figure 2.13 Throughput of the Network

It is observed from Figure 2.13 that the throughput of the network decreases when the presence of malicious nodes in the network increases and thus degrades the overall performance of the system.

Figure 2.14 Packet Drop Ratio
The packet drop ratio is defined as the fraction of packet lost per node. It invites the retransmission of packets to recover from the packet loss. The packet drop ratio of the normal nodes is significantly different from that of the malicious node. From the Figure 2.14, it is observed that the packet drop ratio of the network increases with the increase in number of malicious nodes. The performance of the network is said to be good if the network has less packet drop ratio and more packet delivery ratio.

2.2.3.5 Energy consumption

Though the cumulative acknowledgement is transmitted up to the check point, it reduces the communication overhead in the forward path. Since the proposed detection scheme uses control packets to detect the malicious node, it consumes more energy.

2.2.3.6 Latency

The average latency of the network is 38 seconds after the detection of malicious node and 50 seconds before the detection of malicious nodes.

2.3 PROPOSED SCHEME –II ENERGY BASED DETECTION

The existing detection schemes consist of inclusion of packets such as cumulative acknowledgement, event packet, acknowledgement packets, control packets and alert packets for detecting the malicious node. With the inclusion of packets for detections, communication overhead will be more. The proposed detection scheme identifies the malicious node based on the energy value of the node. The network is divided into virtual grids in order to reduce the energy consumption. The forwarding path is identified by DSR
protocol. This scheme also detects more than one malicious node in the network.

2.3.1 Assumptions

The detection scheme is proposed with six assumptions. Firstly, assumption, nodes are mobile and located in the specific terrain range. Secondly, is the grid head which is laid in the specific grid until the data packets are sent from the grid head to the base station. Third, the base station is kept stationary and located in the first grid. Fourth, energy is allotted to all nodes initially. Fifthly, forward routing path is selected by DSR protocol and the node is assumed to be maintained by the neighbor routing table. Finally, the messages are authenticated using one-way hash chains.

2.3.2 Detection Phases

The different phases of the proposed scheme are as follows:

- Grid Formation and Grid Head assignment
- Energy allocation
- Forward route selection path
- Data transmission
- Detection of malicious node

Grid Formation

Firstly, the sensor nodes are divided into virtual girds with the specific terrain range. Since the nodes are scattered and are also mobile, control packets are required to identify the adjacent nodes and to identify the forward routing path. Nodes which are located far away from the base station
consumes large amount of energy. The major part of node’s energy is lost due to communication and reduces node’s life time. The virtual grids are framed to increase the node’s life time. The total terrain range which is in a square with size "dxd" is divided equally to form the grids. Grids are formed based on x and y coordinates assigned. Figure 2.15 represents that the base station is located at the first grid.

![Grid Formation](image)

**Figure 2.15 Grid Formation**

The base station is stationary but all the other nodes and grid heads are mobile nodes. The size of each grid is 159m. The terrain of first grid starts from (0, 0) and ends with (159,159). For 500 nodes, there are 63 grids. Each
grid consists of grid head. Equation (2.1) is used to identify the location of the node in a particular which grid.

\[ lX = \frac{x}{d} \text{ and } lY = \frac{y}{d} \]  

(2.1)

Where,
\[ d \] is the grid size

\([LX,LY]\) is the grid ID and assigned in the matrix form.

Grid head Assignment

Role of grid head is necessary to propagate the information data packets to its neighbor nodes. Grid head is responsible for routing the packets and improving the quality of the routes. The grid head is assumed as the node with the largest residual energy in each grid and is randomly assigned. If the same nodes are acting as grid head for a long time, then the life of the nodes is reduced. A random algorithm is used for selecting the grid head. i.e, grid head is randomly assigned and it is changed frequently. The selection factors of the grid are information that can be transferred from the nodes and to the base station, communication cost, energy consumed to detect the malicious node and the energy of the node. If the grid head is located near the base station and with the adjacent grid head, then the communication cost is reduced. The problem is how to formulate the criteria to select the grid head to select the nodes that provide satisfied data from source node to the base station. The combinative measurement for node \(i\) is denoted as \(\beta \alpha\) and it is defined in Equation (2.2).

\[ \lambda_i = \alpha \phi(u_i) - \beta C(gh, \hat{i}) + \gamma e(\hat{i}) - \delta m(i) \]  

(2.2)
Where $\varphi(i)$ is the information utility of the node $i$; $C(gh, i)$ represents the communication cost between the gridhead $gh$ and node $i$. $\varepsilon(i)$ reflects the current energy level in node $i$, $i$, $m(i)$ is the energy consumed for detecting the malicious node. When node $i$ is selected frequently, the energy of the node decreases because grid head acts as a gateway of the grid and can lead to the degradation of the performance of the network. Since the nodes are mobile, the coefficients $\alpha, \beta, \gamma, \delta$ are adaptive and it should be flexible with respect to grid size, noise model, receiver sensitivity and movement of sensors. Grid head is the node which has maximum $\lambda$ for detecting the malicious nodes.

Where $N$ is the set of remaining nodes to which the grid head sends querying requests for detecting the malicious nodes. 

$$N_{ut} = \sum \lambda_i$$

In Equation (2.3), $N_{ut}$ is the node utility at time $t$ and it is defined as the sum of all the combinative measurements of sensor node. Before allocating the grid head and distribution of node energy in order to identify the malicious node, the nodes have the capability of self optimization and the co-efficient’s should satisfy $\alpha + \beta + \gamma + \delta \leq 100$ units of energy. It is critical to choose the appropriate values for them at run time. For specific task, a set of thresholds and corresponding values of $\alpha, \beta, \gamma$ are predefined. If the value of $N_{ut}$ is small or below a certain threshold, it indicates that the energy of the grid head decreases, and $y$ should be assigned a larger value compared to $\alpha, \beta, \gamma, \delta$. In this case, grid head tends to select the nodes with more energy to act as a grid head. This increases the node life time and reduces the communication cost between the node and grid head.
Energy Allocation

Initially, energy is allocated to all the nodes in the network by the base station. The energy value of each node is defined as \( k \). During energy distribution \( k \) value is equal to 100 units. This energy can consume 20 units for transmission, 20 units for reception, 20 units for computing grid formation, route selection path and checking the node energy. The 30 units are allocated for packet drop and collision, and 10 units for connection establishment. In the 30 units of packet drop and collision 10 units are consumed for the collision and the remaining 20 units are considered as essential energy (ESS). If the value of \( k \) is less than the ESS then it is suspected as a malicious node where ESS is an essential energy and is assumed to be 20. These values are assigned for the simulation purpose and it is subject to change practically with respect to grid size, noise model, receiver sensitivity, and movement of sensors.

Forward Route Selection Path

Routing between the source node and the grid head is done by using DSR protocol. Each grid head first identifies the source node located in that particular grid. Then, the grid head sends the request to the adjacent grid head. After the identification of the source node, it sends the route request packet to the destination node/base station. It responds the route reply packet with the selected forward routing path through which data is transmitted.
Data Transmission

First the data is transmitted from the base station to the grid head of the virtual grid and then the grid head is checked for the node which needs to transmit the data from the base station. If the source is not located in the specific grid, then the request is transmitted to the next grid head and it continues the process of checking the nodes in that grid and then transfers it to the particular node.

Figure 2.16 Data Transmission

Figure 2.16 depicts the transmission of data between the grids. The base station is represented by the triangle symbol, grid head is represented by an ash color circle and the ordinary nodes are represented by a black color circle. Data packet to be transmitted is represented using a colored circle.
Transmission of packets from base station to the node is represented by the arrowheads clearly.

The data transmission phase is as follows:

- The base station sends a request to the grid heads in the corresponding grids.
- The grid heads deliver the request to all the nodes located in that grid for identifying the source. If the source is not located in the grid then the request is transferred to the next grid.
- After the identification of the source, it sends the route request packet to the base station, and then, the base station replies the route selection path to transmit the data.
- Route identification and data transmission is done by using the control packets in the dynamic source routing protocol.
- The nodes send an acknowledgement to the grid head.
- In turn the grid head sends the acknowledgement to the base station.

Detection of malicious node

The detection phase is mainly based on the acknowledgement packets of routing algorithm from the grid head to the base station and to the energy level of each node. If the base station gets the proper acknowledgement for each transmission, it means that there might be no malicious nodes in the transmission path. If the base station fails to get the acknowledgement packets within the time period, it means that it will check the energy level of each node in the grid using grid head. The node which has
the energy level lower than its essential level drops its acknowledgment packets and is detected as the malicious node by the base station. After detecting the malicious node, it is removed from the network to maintain the proper transmission of data. The packet is forwarded to the destination or base station by choosing the next alternate path. Packet drop may occur due to lack of receiver sensitivity and collision since nodes are mobile nodes, in the same way there is a chance of identifying the normal node as malicious node.

![Figure 2.17 Detection of Malicious Node](image.png)

**Figure 2.17 Detection of Malicious Node**

The transmission of data packets in the grids and the transmission of acknowledgement packets is shown in Figure 2.17 and its flow chart is depicted in Figure 2.18.
Energy distribution for detection (k is the node energy)
20 units for transmission
20 units for reception
20 units for grid formation
30 units for packet drop and collision (PC) - (20 units of PC is initialized as ESS)
10 units for connection establishment

Selection of Forward Routing path

k < ESS

Malicious node is detected and it is removed from the network

Packet is forwarded through alternate path
2.3.3 Detection Analysis

The proposed detection scheme has been analyzed based on following contexts.

Scenario 1: Grid head detection

The grid heads are mobile and randomly selected; it will search whether the nodes of the forwarding path be in the specific grid or in adjacent grid. Since only 30 units of energy are allocated for the packet drop and collision, there is a chance of assuming the malicious node as grid head based on the initial energy. In that case, grid head is identified as malicious node if it drops any route acknowledgement packet and further confirmation is done by considering its collision rate and packet delivery ratio.

Scenario 2: Source node detection

The base station broadcasts the request to the nodes and malicious node may respond to the base station with route request packet which gather the routing information and misguide the route in the network. In this case the malicious node is identified by the grid head based on energy level allotted for packet delivery and collision.

Scenario 3: Node may be malicious node

Any node which lies in the forward path may be malicious node and grid head checks for the energy level of each node. If the energy level is less than the essential energy after considering the drop ratio, the node is suspected as malicious node.
2.3.4 Performance Evaluation

The performance of the proposed scheme is evaluated through glomosim simulator. Detection accuracy, energy consumption, byte overhead, throughput, packet delivery ratio, success rate, false positive ratio, and false negative ratio are observed. The proposed detection scheme is implemented with mobile sensors which are uniformly placed in the grid. The simulation parameters are shown in Table 2.2.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Nodes</td>
<td>500 nodes</td>
</tr>
<tr>
<td>No. of Grids</td>
<td>63</td>
</tr>
<tr>
<td>No. of Grid Heads</td>
<td>63</td>
</tr>
<tr>
<td>Transmitting range (dBm)</td>
<td>15.0</td>
</tr>
<tr>
<td>Receiving range (sensitivity dBm)</td>
<td>-91.0</td>
</tr>
<tr>
<td>Max. No. of Control Packets</td>
<td>6</td>
</tr>
<tr>
<td>Field Size ($m^2$)</td>
<td>2000 X 2000</td>
</tr>
<tr>
<td>Mobility Model</td>
<td>Random way point</td>
</tr>
<tr>
<td>Mobility ($m/s$)</td>
<td>0-10</td>
</tr>
<tr>
<td>Maximum Speed ($s$)</td>
<td>10</td>
</tr>
<tr>
<td>Propagation Model</td>
<td>Two ray ground model</td>
</tr>
<tr>
<td>No. of Malicious Node</td>
<td>255</td>
</tr>
<tr>
<td>Simulation Time ($s$)</td>
<td>900</td>
</tr>
<tr>
<td>Packet Size ($bytes$)</td>
<td>1460</td>
</tr>
<tr>
<td>Pause Time ($s$)</td>
<td>30</td>
</tr>
<tr>
<td>No. of Packets per Second</td>
<td>148</td>
</tr>
<tr>
<td>Data Rate ($Mbps$)</td>
<td>5</td>
</tr>
<tr>
<td>Packet Loss ($pkt/sec$)</td>
<td>80</td>
</tr>
<tr>
<td>Detection of Malicious Node ($ms$)</td>
<td>500</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>DSR</td>
</tr>
<tr>
<td>Type of attack</td>
<td>SFA</td>
</tr>
</tbody>
</table>
2.3.4.1 Energy level of the nodes

Sensors are randomly selected as a malicious node that will selectively drop the forwarding packets. Based on the energy level of the node, malicious nodes are detected.

![Energy Levels of the Node](image)

**Figure 2.19 Energy Levels of the Node.**

Figure 2.19 represents the energy level of grid head (GH), ordinary node (ON) and malicious nodes (MAL) after the transmission and reception of packets in the network. It has been observed that the energy level of grid head is in the range of 80% and above. The energy level of ordinary node is in the range of 70% and above. But the energy level of malicious node reduces abnormally. This indicates that the malicious node selectively drops the packets.
2.3.4.2 Packet drop ratio

The delivery ratio of the network is less when more malicious nodes are present in the network. The number of packets sent and throughput are varied due to the presence of malicious nodes. In Figure 2.20, the malicious nodes increase the packet drop ratio and decrease the delivery ratio of the network, the presence of malicious nodes affect the performance of the network. The packet drop rate of the normal node is significantly different from the malicious node.

![Figure 2.20 Packet Drop Ratio](image)

2.3.4.3 Throughput

Figure 2.21 represents the throughput of various scenarios. If the network does not consist of malicious nodes, then its throughput is certainly high. If the network consists of malicious nodes in the network without the detection process, the throughput is low, after the detection process throughput of the network is increased. If there is a less number of malicious
nodes, throughput of the network is low when compared to the network that does not contain any malicious nodes. If there are more malicious nodes in the network, then the throughput of the network is very low.

![Figure 2.21 Throughput Analysis of the Network](image)

### 2.3.4.4 Byte overhead

The proposed scheme does not use any control packets for detection. The acknowledgement packet of DSR protocol is used for detection. Along with the detection scheme, it is observed that bytes overhead is less. It is inferred that the detection scheme does not contain any additional control packets for detection. The overhead of the proposed detection scheme is less when compared to the existing detection schemes.
2.3.4.5 Accuracy of detection scheme

This simulation model investigates the accuracy on malicious node.

![Accuracy of detection scheme](image)

**Figure 2.22 Success Rate in Malicious Node Identification**

Figure 2.22 depicts the success rate of malicious nodes. The success rate is 80% whereas the drop rate is 0.9.

![Success Rate in Malicious Node Identification](image)

**Figure 2.23 False Positive Rates in Malicious Node Identification**

Figure 2.23 shows the false positive rates with a drop rate of 0.9.
Figure 2.24 False Negative Rates in Malicious Node Identification

Figure 2.23 and Figure 2.24 show the false positive rate and false negative rate in detecting malicious node respectively. The simulation result indicates that the false positive error rate is very low. This is because the energy of the grid head is less than the essential energy. The grid head can be assumed as malicious node. Packet drop and collision may occur due to the node mobility, i.e., the node may not lie within the range of the receiver’s sensitivity and packet drop may also be occurring due to the timer expiry. In this case, grid head may wrongly identify the malicious node based on the energy consumption for packet drop and collision of the particular node. The false negative error rate is very low, if there is more number of malicious nodes in the network which may not be detected because the energy consumed for the packet drop and collision of the normal node and the malicious node is lesser than the essential value.
2.3.4.6 Energy consumption

Figure 2.25 shows the energy consumption rate of the nodes. Small percentage of energy is essential to frame the grids. The normalized energy is calculated as the ratio of the total current energy of all nodes to the total energy of all nodes at the start of the simulation. Since the scheme is based on the grid, the normalized energy of the network is less. The energy consumption for the formation of the grids also depends upon the width of the grid and the receiver sensitivity. The total energy consumed by the proposed scheme is only 20% of the initial energy assigned to the node.

When compared to the bytes overhead, a major part of the energy is consumed in a grid formation and forward path identification since the nodes are mobile nodes. Detection scheme consumes less energy. This is because the detection scheme is basically dependent on the energy of the node rather than the control packets like acknowledgment packets.
2.4 COMPARISON OF THE PROPOSED SCHEMES WITH THE EXISTING SCHEMES

The comparison of the proposed schemes with the previous schemes is given in Table 2.3. The existing detection schemes are based on static wireless sensor networks. In multihop acknowledgement scheme, communication and complexity of the detection are high. It does not require time synchronization, acknowledgement packets, and authentication schemes. It generates duplicate packets due to packet loss in the network.

In CHEMAS, detection accuracy is high and overheads like communication is high. It requires authentication protocol and generates control packets for detection. In MDT, detection accuracy is not analyzed. It does not require time synchronization. It also defends against sinkhole attack. It does not use any control packets for detection. In CADE, The network performance metrics such as detection accuracy, energy consumption etc are not analyzed. The detection scheme is complex. It needs authentication mechanism for packets to be transmitted.

In the game theory model, detection accuracy depends upon the channel rate and the packet drop ratio. It does not include base station for detection. It is a complex detection scheme and different approach to detect the malicious node. Time synchronization is required.

In the proposed schemes, network performance metrics are analyzed. The proposed schemes improve the performance of the network. The proposed schemes immediately react after the detection of malicious nodes without any further delay. The proposed schemes are simulated in a mobile environment.
Table 2.3 Comparison of the proposed schemes with the existing Schemes

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Multi-hop Acknowledgement</th>
<th>CHEMAS</th>
<th>MDT</th>
<th>CADE</th>
<th>Game theory Model</th>
<th>CHEAD</th>
<th>EBD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection rate</td>
<td>95% when channel error rate is 15%</td>
<td>High</td>
<td>Not analyzed</td>
<td>Not analyzed</td>
<td>Channel rate and dropping rate</td>
<td>90%</td>
<td>80%</td>
</tr>
<tr>
<td>Communication overhead</td>
<td>high</td>
<td>Reasonable</td>
<td>Acceptable but still reduced further by improving routing mechanisms or deploying additional sensors.</td>
<td>Not analyzed</td>
<td>Not analyzed</td>
<td>Significant</td>
<td>Less</td>
</tr>
<tr>
<td>Includes base station for detection</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Time synchronization</td>
<td>Not required</td>
<td>Yes</td>
<td>Not required</td>
<td>Not required</td>
<td>Yes</td>
<td>Yes</td>
<td>Not required</td>
</tr>
<tr>
<td>Identifies the original reason for packet loss</td>
<td>yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Not analyzed</td>
<td>No</td>
<td>yes</td>
</tr>
<tr>
<td>Security against sinkhole attack</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>yes</td>
</tr>
<tr>
<td>One-way key chains</td>
<td>Not required</td>
<td>Required</td>
<td>Not required</td>
<td>Not required</td>
<td>No</td>
<td>required</td>
<td>required</td>
</tr>
</tbody>
</table>
Table 2.3 (Continued…)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Multi-hop Acknowledgement</th>
<th>CHEMAS</th>
<th>MDT</th>
<th>CADE</th>
<th>Game theory Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplicate packet</td>
<td>Data packet</td>
<td>None</td>
<td>No</td>
<td>Data-reply packet is dropped</td>
<td>No</td>
</tr>
<tr>
<td>ACK generation</td>
<td>none</td>
<td>Always</td>
<td>none</td>
<td>packet is dropped</td>
<td>None</td>
</tr>
<tr>
<td>Energy Consumption</td>
<td>Not analyzed</td>
<td>Not analyzed</td>
<td>Not analyzed</td>
<td>Not analyzed</td>
<td>Not analyzed</td>
</tr>
<tr>
<td>Nodes</td>
<td>stationary</td>
<td>Stationary</td>
<td>Stationary</td>
<td>Stationary</td>
<td>Stationary</td>
</tr>
<tr>
<td>Authentication</td>
<td>Not required</td>
<td>µTELSA required</td>
<td>required</td>
<td>required</td>
<td>Not required</td>
</tr>
<tr>
<td>Node life time</td>
<td>exhaust</td>
<td>Decreased</td>
<td>decreased</td>
<td>exhaust</td>
<td>Not analyzed</td>
</tr>
<tr>
<td>Immediate reaction</td>
<td>No</td>
<td>No</td>
<td>Base station can react immediately without any unnecessary delay.</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Detection Complexity</td>
<td>Complex</td>
<td>Light weight</td>
<td>Light weight and simple</td>
<td>Complex</td>
<td>Complex</td>
</tr>
</tbody>
</table>
2.5 SUMMARY

The detection schemes of SFA for wireless sensor nodes have been proposed. The simulation result shows that the proposed scheme detects the malicious nodes with an accuracy of 80%. The existing schemes like CHEMAS, CADE introduces control packets to detect the malicious node in static WSN. The energy consumption of the existing detection scheme is considerably high and thus reduces the node lifetime.

The modified DSR routing protocol is proposed using CHEAD scheme and it consumes more energy. The packet delivery ratio, network throughput, and latency of the detection scheme are improved. EBD scheme is based on energy allocation without altering the existing routing protocol and yields less overhead. It consumes less energy and accuracy of the detection is improved. The performances of the proposed schemes are analyzed through simulations and it is improved when compared to the existing schemes. The detection schemes have been found suitable for mobile environment.