CHAPTER 6
CLUSTERING AND SECURITY IN WSN

6.1 Introduction

In the fields of surveillance and monitoring through WSN clustering play a major role to enhance the lifetime of the network and scalability. Many researchers have done the work on selection of clusters but these strategies lacks in data recovery. The developed methods consider the heterogeneity in power and maintain groups of vice-cluster heads that can become cluster head in future when the current cluster head come to end. The headship rotates among the vice-cluster heads. Security of WSN is an important issue due to the unattended nature of wireless sensor networks. The sensor nodes inside the WSN send the sensed data towards the base station so the traffic near the base station/ sink increase. The attacker can conceal the anonymity of sink by just performing the traffic analysis inside the wireless sensor network. So a methodology is required to preserve the anonymity of sink. In this chapter the methodologies are developed to remove these problems from wireless sensor networks.

6.2 Material and Methodology

In this section, the methodologies for formation of cluster inside the WSN and security against sink location privacy are discussed.

6.2.1 Formation of Cluster

In this section network system model and the different algorithms for selecting the different leader nodes will be presented.

a) Network system model

Network consists of many clusters as $C=\{c_1, c_2, c_3, \ldots c_n\}$, where $n$ represents the number of clusters present. Each cluster contains some nodes as $S=\{s_1, s_2, s_3, \ldots s_m\}$, where $m$ gives total number of sensor nodes present in a cluster. Each cluster contains a head node that collects the data from each sensor nodes present in the cluster and forward the whole data to base station. Each cluster also contains some vice-cluster heads (VCHs). The VCHs reside near the cluster heads, these VCHs are selected on the basis of randomness as given in equation.
6.1. The task inside the cluster is distributed by cluster head (CH). CH divides the task (T) in parts \( t_1, t_2, t_3, \ldots t_r \) and assigns the tasks \( t_i, i = 1, 2, 3, \ldots r \) to VCHs. VCHs assigns the task to other nodes, present in the lower levels. The nodes at level \( i \) assign some part of the task to itself except node at level 1 and forward the residual task to the nodes at level \( i - 1 \), the nodes at level \( i - 1 \) handles some part of the task itself and forward residual task to the nodes at level \( i - 2 \) and so on the task is distributed towards the depth of the DAG. The tasks are assigned to the node on the basis of the performance of the node. The VCHs can work as CH in future when CH comes to end. Before coming to end, CH maintains a set of the VCHs and assigns the charge of CH to VCH that comes first in the set. The Remaining VCHs can work as the nodes for recovery also. Figure 6.1 shows the network system model which contains 1 cluster, 1 CH and 5 VCHs.

The randomness and deviation are measured as per the equation (6.1) and (6.2) as follows.

\[
\text{Randomness} = \sum_{i=1}^{m} P_i \log P_i \quad (6.1)
\]

\[
\text{Deviation} = \sum_{i=1}^{m} P_i \log P_i - P_i \quad (6.2)
\]

![Fig. 6.1 Network System Model](image)

**b) Result Collection Model**

The collection of result starts from the leaf node of the DAG. The leaf nodes send the data to its parent nodes, parent nodes aggregate the data and send the aggregated data to its parent in this way the data comes at the VCH nodes. The VCH nodes collect the data, aggregate it,
forward it to CH and maintain a log for data. When CH comes to end it nominate one VCH node as CH. The nominated CH gets the data from the logs (present at VCHs) which have been loosed due to the depletion of CH. Now the CH node sends the data to base station. The figure 6.2 shows the procedure for result collection. It contains one CH and three VCHs and some nodes connected to VCHs.

![Result Collection Model](image)

**Fig. 6.2 Result Collection Model**

c) **Cluster Head Selection**

The cluster head selection process comprises of three phases:

- Setup Phase
- (Vice-Cluster- Head) VCH selection Phase
- (Cluster Head) CH selection Phase

Now each phase is elaborated by algorithms as given in the further texts.

```
Begin(Setup phase)
    BS maintains a record of nodes location and power.
    for each cluster C
    Repeat
        for i=1 to m
```
Repeat
    Calculate the randomness
    If (-2.04383 <= Randomness <= 2.839258)
    Select the node i as the CH.
    Exit
End
BS sends the DB entries for the cluster C to the CH.
End
End

Begin (VCH selection phase)
    for each cluster C
    Repeat
        for each node i=1 to m
            Repeat
                If (Node i=CH)
                    Call slect_VCH()
                    Count_CH++;
                End
            If (Count_CH != 1) then
                Call the procedure for setup phase for the cluster C
        End
    End
End

Begin (select_VCH)
    CH broadcast the request for getting the power and location value of one hop distance nodes.
    CH maintains a record for reply from the one hop distance nodes.
    for each one hop distance node
        Repeat
            Calculate the randomness of the node
            If (-2.04383 <= Randomness <= 2.839258) then
Select the node as VCH. Put in a list.

Else

Node work as simple node

End

End

Begin (CH selection)

CH gets the power signal

if (power < Threshold) then

CH selects the first VCH (VCH₁) from the list.
Broadcast the message as VCH₁ becomes CH
CH sends the required data to VCH₁
End

Now VCH₁ works as the cluster head.

End

d) Working of Different Category of Sensor nodes

This section discusses the works performed by different types of nodes present in the network. The procedure for each node is presented by algorithms as follows.

i) VCH Node

Start(VCH)
Read the packet from the QUEUE
Switch(packet Type)

Case VCH_REQ:
Create the log entry for the node and send the reply to the requesting node.

Case FLUSH_LOG:
Append the log entries in the created log of the node.

Case VCH_DESTR:
Remove the entry of the log from the VCH for the sender node
Case COMMIT:
    Remove the log entry from the VCH with the positive response to the sender.

Case REP_NODE:
    Send the reply to the node if it is chosen for recovery.

ii) Node at level 2

Begin(Node at level 2)
    if(new task assigned )
    Begin
        Assign the part of the task to itself
        Assign the TID to it.
        Request for log entry in the parent VCH.
    End
for i=3 to DEPTH of the DAG
    REPEAT
Read the packet from QUEUE
Switch(Packet type)
    Case NODE_REQ:
        Assign a ID to the task and assign the partial task to the lower level nodes. Put this ID into the set of pending tasks.
    Case ABORT:
        Reassign the task to other child nodes. Readjust the entry of the task in the pending list.
    Case REPLY:
        Get the reply of the node from lower level.
    Case REQ_ACK:
        Send acknowledge to the sender nodes.
    Case REQ_TASK:
        Create the part of the task and assign the task to the lower level nodes.
e) **Recovery Mechanism**

This module is used to recover the data when any node crashed abruptly. In wireless sensor network the node crashed often due to its deployment conditions.

```
Begin (recovery mechanism)
   Broadcast the crash information of the node or CH.
   Select new CH from the VCHs.
   Get the log entries from the remaining VCHs.
   Get the database items and the instruction set of the node or CH.
   Analyze the log and redo the updates
   Begin
      Redo the changes in the data items and remove the uncommitted task’s values.
   End
Now the VCH work as the CH with the state of the old CH.
End
```

### 6.3 Hiding of Sink Location

Before discussing the developed methodology this section needs to discuss the network and attacker model considered for analysis of the methodology.

a) **Network and Attacker model**

The network and attacker model consists of some sensor nodes and an attacker. The sensor nodes \( \{s_1, s_2, s_3, \ldots s_n\} \) can communicate with each other. The sensing range of each sensor node is fixed. The sensor nodes form some clusters \( \{c_1, c_2, c_3, \ldots c_n\} \) inside the region and a group of sensor nodes belongs to some cluster. The attacker inside the region is a passive attacker which can only eavesdrops the messages. The network consists of a sink node which gathers the information from the region. The attacker does not have control of any sensor node and it cannot distinguish the real and fake message, due to the encryption of messages by shared key. The attacker can only find the location of sink on the basis of traffic analysis inside the network. The network and attacker model is shown in figure 6.3.
b) Developed Strategy

The developed scheme works in two phases:

- Route Discovery Phase
- Data Gathering Phase

i) Route Discovery Phase

Route discovery phase works in two levels

- Cluster Head Level
- Sink Level

- Cluster Head Level Route Discovery

The cluster head sends the DIS_ROUTE message encrypted with a shared key to the sensor nodes coming in its communication range. Inside the cluster, selective forwarding is used to send the messages; it means only one copy of the message is forwarded to other sensor nodes. The sensor nodes that receive the DIS_ROUTE message generate a fake message (FDIS_ROUTE) of the same size and send this message (encrypted with a shared key) to the cluster head. The sensor nodes that receive the DIS_ROUTE message forward the message appended with its ID to its neighbors that come in communication range and also send the FDIS_ROUTE message to its sender nodes. The process of route discovery is shown in figure 6.4.
• **Sink Level Route Discovery**

At the Sink level route discovery, the sink node sends the DIS_ROUTE message appended with its ID to the cluster head. The cluster head receives the message and generates a FDIS_ROUTE message of same size as DIS_ROUTE, send this FDIS_ROUTE message to sink. The cluster heads that receive the DIS_ROUTE message selectively forward it to other cluster heads. Other cluster heads receive DIS_ROUTE and generates FDIS_ROUTE message and send it to its sender nodes. The process is shown in figure 6.5.
ii) **Data Gathering Phase**

After route discovery, this phase works which gathers the information from the network. This phase also works in two levels.

- **Cluster Head Level Data Gathering**
- **Sink Level Data Gathering**
- **Cluster Head Level Data Gathering**

The cluster head receives the data from the sensor nodes present in its own cluster and send this data to sink. Since the traffic near cluster head becomes more so the point near to cluster head can also be focused by attacker. To overcome this situation, in this level data gathering the nodes send the data towards the one hop neighbors (OHN) of cluster head and OHN nodes circulates the data among themselves. As shown in the figure 6.6, sensor nodes 1, 2, 3, 4, 5, 6, 7 are work as OHN nodes. These nodes get the data from lower level nodes and send the aggregated data to other nodes present in same ring. The OHN node that receives the data, aggregate its data and forward it towards other OHN node in the same ring. The node that receives the data from its neighbor OHN nodes before sending becomes the communicator node (CN). CN append its data and sends the data to cluster head. The role of communicator node rotates among the OHN nodes.

![Fig. 6.6 Cluster Head Level data gathering](image)

**Sink Level Data Gathering**

The Cluster heads that can directly communicate with sink forms a ring around the sink. As shown in figure 6.7 cluster heads H1, H2, H3, H4, H5, H6 and H7 can directly communicate with sink node. The cluster head nodes circulate the data among themselves after some fix periodic time. As shown in the figure 6.7 cluster head H1 sends the data to H2, H2 collect the data from H1, aggregate the data with its own data and forward the data to cluster head H3,
Cluster head $H_3$ collects the data from cluster heads $H_2$ and $H_4$, cluster head $H_3$ becomes the Communicating master node (CMN) for the sink and send the aggregated data of $H_1$, $H_2$, $H_4$ and itself to sink.

![Fig. 6.7 Sink Level Data Gathering](image)

6.4 Performance Results

This section discusses the results that are obtained after the application of developed methodologies.

6.4.1 Results of Formation of Cluster

To evaluate the performance of the method used for clustering, throughput (work done per unit time) is taken as the parameter. The Simulation Scenario is created in OPNET which contains 20 sensor nodes with two clusters. The scenario is executed for 600 seconds, 1200 seconds, 10800 seconds and 18000 seconds. The method is compared with random method in which the developed method in not applied. Table 6.1 gives the different simulation parameters that are applied in design of the scenario and table 6.2 shows the comparative results of the developed method.
Table 6.1 Simulation Parameters

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Area</td>
<td>1x1 km (Fix)</td>
</tr>
<tr>
<td>2</td>
<td>Network size</td>
<td>20 nodes</td>
</tr>
<tr>
<td>3</td>
<td>Topologies</td>
<td>2 Cluster Head</td>
</tr>
<tr>
<td>4</td>
<td>Simulation Time</td>
<td>600/ 1200 seconds</td>
</tr>
<tr>
<td>5</td>
<td>Packet Size</td>
<td>1500 bits</td>
</tr>
<tr>
<td>6</td>
<td>Packet Inter-Arrival Time (sec)</td>
<td>Constant (1)</td>
</tr>
<tr>
<td>7</td>
<td>CSMA/CA Parameters</td>
<td>Default</td>
</tr>
<tr>
<td>8</td>
<td>Sensing duration (sec)</td>
<td>0.1</td>
</tr>
<tr>
<td>9</td>
<td>Physical Layer Parameters</td>
<td>Default</td>
</tr>
</tbody>
</table>

Table 6.2 Comparative Results

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Time for Simulation (Seconds)</th>
<th>Throughput (bits per seconds) (Random)</th>
<th>Throughput (bits per seconds) (Developed method)</th>
<th>Improvement (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>600</td>
<td>1666.99</td>
<td>2223.86</td>
<td>33.41</td>
</tr>
<tr>
<td>2</td>
<td>1200</td>
<td>1336.074</td>
<td>2117.739</td>
<td>58.504</td>
</tr>
<tr>
<td>2</td>
<td>10800</td>
<td>1042.496</td>
<td>1549.497</td>
<td>48.63</td>
</tr>
<tr>
<td>4</td>
<td>18000</td>
<td>1531.229</td>
<td>2007.304</td>
<td>31.09</td>
</tr>
</tbody>
</table>

6.4.2 Results of Hiding of Sink Location

To evaluate the performance of hiding sink location methodology, first the mathematical analysis is given to find the total traffic generated inside the network and power requirement. Further simulation results are given.

i) Mathematical Analysis

Let, Total \( n \) sensor nodes are deployed in the cluster and each sensor node generate \( p \) messages except the sensor at one hop distance from the cluster head. FDIS_ROUTE
message is taken at the time of route discovery because the attacker can set up its position at the time of route discovery by getting the location of sink by traffic analysis.

- Traffic Analysis

The sensor nodes at one-hop distance from the cluster head generate \( q \) messages. Each message has the same length as \( L \) bits. Suppose, \( R_k = kR_1 \) is the radius of \( k \)-hops coverage area of one sensor node. The area of 1-hop coverage (\( A_1 \)) by a sensor node is \( \pi R_1^2 \). Let the total area of the cluster is \( S \), since the total number of sensor nodes present in the cluster are \( n \), so the number of nodes per unit area is given as \( n/S \) and the number of nodes present in \( k \)-hop distance (\( N_k \)) of one sensor node are \( n \* \pi R_k^2 / S = n \* \pi k^2 R_1^2 / S \). The area of \( k \)-hop ring (\( A_k \)) (shown by yellow color in Figure 5.8) is given as

\[
A_k = \pi(k^2 R_1^2 - (k-1)^2 R_1^2) = \pi R_1^2(k^2 - k^2 - 1 + 2k) = \pi R_1^2(2k-1) = (2k-1)A_1.
\]

Suppose the maximum hop count in a cluster is \( h \) then the area from the \( k \)-hop ring to the \( h \)-hop ring (\( A_{k-h} \)) is

\[
\sum_{i=k}^{h} A_i = \sum_{i=1}^{h} A_i - \sum_{i=1}^{k-1} A_i = \sum_{i=1}^{h} (2i - 1)A_1 - \sum_{i=1}^{k-1} (2i - 1)A_1
\]

\[
= A_1\left(\sum_{i=1}^{h} (2i - 1) - \sum_{i=1}^{k-1} (2i - 1)\right) = A_1\left((1 + 3 + 5 + 7 + 9 \ldots + 2h - 1) - (1 + 3 + 5 + 7 + 9 \ldots + 2(k - 1) - 1)\right)
\]

\[
= A_1\left(\frac{h}{2}(2 \times 1 + (h - 1) \times 2) - \frac{k-1}{2}(2 \times 1 + (k - 1) \times 2)\right) = A_1(h^2 - (k - 1)^2)
\]

The traffic (\( \text{TRAF\_GEN}_k \)) generated by each node present in the \( k \)-hop ring can be calculated as (The nodes in the \( k \)-hop ring forward the message of outer rings and generate the message itself).

\[
\text{TRAF\_GEN}_k = A_{k-h} \times \frac{n}{S} \times p \times L = A_1(h^2 - (k - 1)^2) \times \frac{n}{S} \times p \times L
\]

Traffic generated by each 1-hop distance node is given as

\[
\text{TRAF\_GEN}_1 = A_{1-h} \times \frac{n}{S} \times q \times L = A_1(h^2 - (1 - 1)^2) \times \frac{n}{S} \times q \times L
\]

\[
= A_1(h^2) \times \frac{n}{S} \times q \times L
\]

Traffic generated by each 2-hop distance node is given as

\[
A_{2-h} \times \frac{n}{S} \times p \times L = A_1(h^2 - (2 - 1)^2) \times \frac{n}{S} \times p \times L
\]
So the total number of messages generated by 1-hop ring is given as
\[ A_1(h^2 - 1) \times \frac{n}{S} \times p \times L \]

\[ = A_1(h^2 - 1) \times \frac{n}{S} \times q \times L - A_2(h^2 - 1) \times \frac{n}{S} \times p \times L \]

\[ = A_1(h^2) \times \frac{n}{S} \times q \times L - A_4 \times \frac{n}{S} \times p \times L \]

\[ = A_1 \times \frac{n}{S} \times L(h^2q - h^2p + p) \]

\[ = A_1 \times \frac{n}{S} \times L(h^2(q - p) + p) \]

Probability Mass function (P (CN=k)) for r nodes to be selected as communicator node (CN) in a cluster is given as: Suppose the probability for a node in 1-hop distance to be selected as communicator node as x, so the probability to become a normal node will be 1-x.

\[ P(CN = r) = C_r \times \frac{n!}{(n-r)!} \times x^r (1-x)^{n-r} \]

Fig. 6.8 message generated in k-hop ring

Fig. 6.9 Message generated in 1-hop distance
Suppose, each cluster head generates the message of length Y and the number of cluster heads inside the network are given as N, the whole area of the region is R, then we can say N/R cluster heads (CHs) are present per unit area. Let the radius of 1-hop distance CHs is r₁. Let, rₖ = j₁, the radius of the j-hop distance CHs, Area of 1-hop coverage is A₁ = πr₁². Let the number of messages generated by CHs are u except the 1-hop distance CHs and the hop count for the network is H. The messages generated by 1-hop distance CHs are v. Then the traffic generated (TRAFFIC_GENᵢ) by j-hop ring is given by:

\[ \text{TRAFFIC}_\text{GEN}_j = A_{1-h} \times \frac{N}{R} \times u \times Y = A_1 (H^2 - (j - 1)^2) \times \frac{N}{R} \times u \times Y \]  \hspace{1cm} (6.5)

Traffic generated by each 1-hop cluster head is calculated as

\[ \text{TRAFFIC}_\text{GEN}_1 = A_1 (H^2) \times \frac{N}{R} \times v \times Y \]

Traffic generated by each 2-hop cluster head is given as

\[ \text{TRAFFIC}_\text{GEN}_2 = A_1 (H^2 - 1) \times \frac{N}{R} \times u \times Y \]

So the total number of messages generated by 1-hop ring is given as

\[ \text{TRAFFIC}_\text{GEN}_1 \cdot \text{TRAFFIC}_\text{GEN}_2 = A_{1-h} \times \frac{N}{R} \times v \times Y - A_{2-h} \times \frac{N}{R} \times u \times Y \]

\[ = A_1 (H^2) \times \frac{N}{R} \times v \times Y - A_1 (H^2 - 1) \times \frac{N}{R} \times u \times Y \]

\[ = A_1 \times \frac{N}{R} \times Y (H^2 v - H^2 u + u) \]

\[ = A_1 \times \frac{N}{R} \times Y (H^2 (v - u) + u) \]

Refer to Equation (6.3) for A₁_h and A₂_h.

- **Power Analysis**

Consider model shown in figure 5.19 for power analysis. The power requirement for transmitting the data is E_t and for receiving the data is E_r. Energy for aggregating the data is E_a and energy for amplification is E_{amp}. So the power requirement for transmitting the L bits for distance, d is given as E_t[L, d] = E_t × E_{amp} × L × d². Power requirement for receiving a message of L bits is given as E_r[L, d] = E_r × L.

**Energy requirement among the nodes and Cluster heads**

Let the total hop count for a cluster is h, n number of nodes present in the cluster. Assume that equal numbers of nodes n/h are present in each ring. Then the total cost for data transmission is given as.
\[ \text{Total}_{\text{Trans\_cost}} = \frac{n}{H} \left( \sum_{k=1}^{h} \text{TRAFFIC\_GEN}_k \times (E_t[L, d] + E_r[L, d]) \right) \]

Refer to Equation (6.4) for TRAF\_GEN\_k.

Let, each sensor node communicate with \( t \) sensor nodes in its range, then the cost of Route discovery can be given as

\[ \text{Total}_{\text{Route\_cost}} = n \times t \times (E_t[L, d] + E_r[L, d]) \]

Total energy cost for a cluster is given as:

\[ E_{\text{cluster}} = \text{Total}_{\text{Trans\_cost}} + \text{Total}_{\text{Route\_cost}} \] (6.6)

**Energy requirement among the Cluster heads and Sink**

Let the hop count for the network is \( H \), \( N \) number of cluster heads are present in the network, Assume equal number of cluster heads are present in each ring as \( N/H \). so the total cost for data transmission is given as

\[ \text{Total}_{\text{Trans\_cost\_sink}} = \frac{N}{H} \left( \sum_{j=1}^{H} \text{TRAFFIC\_GEN}_j \times (E_t[L, d] + E_r[L, d]) \right) \]

Refer to Equation (6.5) for TRAF\_GEN\_j.

Suppose each cluster head node communicates with \( T \) cluster head nodes in its range, then the cost of Route discovery can be given as:

\[ \text{Total}_{\text{Route\_cost\_sink}} = N \times T \times (E_t[L, d] + E_r[L, d]) \]

Total energy cost between cluster head nodes and sink is:

\[ E_{\text{Sink}} = \text{Total}_{\text{Trans\_cost\_sink}} + \text{Total}_{\text{Route\_cost\_sink}} \] (6.7)

The Total energy cost of the network is calculated as:

\[ E_{\text{Total}} = E_{\text{cluster}} + E_{\text{sink}} \] (6.8)

**ii) Simulation Results**

To evaluate the performance simulation scenarios are created in OPNET which contains 1 sink, 4 cluster heads and 40 sensor nodes. The table 6.3 gives the simulation parameters. Two scenarios are created, scenario 2 gives the results when the developed method is not applied (random) and scenario 3 provides the results when developed method is applied. The parameters that are considered to evaluate the performance are throughput, end to end delay, traffic received and traffic send. To show the results for security at cluster head level and sink level these parameters are evaluated at cluster head and sink. Figure 6.10 shows the results for sink level security and figure 6.11 and 6.12 show the cluster head level security. The summary of the results are given in table 6.4.
Table 6.3 Simulation Parameters

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Number of Clusters</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>Network Area</td>
<td>500*500 Square meter</td>
</tr>
<tr>
<td>3</td>
<td>Number of Sensor Nodes</td>
<td>40</td>
</tr>
<tr>
<td>4</td>
<td>Number of Routers/Cluster Head</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>Base Station (Sink)</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>Packet Size (Bytes)</td>
<td>1024</td>
</tr>
<tr>
<td>7</td>
<td>Packet Interval Time (Seconds)</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>Sensing Duration (Seconds)</td>
<td>0.1</td>
</tr>
<tr>
<td>9</td>
<td>Packet Reception Power Threshold (dB)</td>
<td>-85</td>
</tr>
<tr>
<td>10</td>
<td>Transmission Power (Watt)</td>
<td>0.05</td>
</tr>
</tbody>
</table>

Fig. 6.10 Performance Parameters under attack and under developed method for Sink
Fig. 6.11 Performance Parameters under attack and under developed method for Cluster Head
Fig. 6.12 Performance Parameters under attack and under developed method for Cluster Head 2

**Table 6.4 Summary of Results**

<table>
<thead>
<tr>
<th>Node</th>
<th>Method</th>
<th>Throughput (bits/seconds)</th>
<th>End to End Delay (seconds)</th>
<th>Traffic Received (bits/seconds)</th>
<th>Traffic Send (bits/seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sink</td>
<td>Under Attack</td>
<td>9907.27</td>
<td>0.027847</td>
<td>836.27</td>
<td>1018.31</td>
</tr>
<tr>
<td></td>
<td>Under developed Method</td>
<td>6209.84</td>
<td>0.009986</td>
<td>1632.14</td>
<td>1012.62</td>
</tr>
<tr>
<td>Cluster Head 1</td>
<td>Under Attack</td>
<td>2386.64</td>
<td>0.03965</td>
<td>562.06</td>
<td>1018.31</td>
</tr>
<tr>
<td></td>
<td>Under developed Method</td>
<td>1271.51</td>
<td>0.019818</td>
<td>1137.78</td>
<td>1012.62</td>
</tr>
<tr>
<td>Cluster Head 2</td>
<td>Under Attack</td>
<td>5926.37</td>
<td>0.024012</td>
<td>4463.79</td>
<td>1018.31</td>
</tr>
<tr>
<td></td>
<td>Under developed Method</td>
<td>4378.56</td>
<td>0.020071</td>
<td>3918.79</td>
<td>1012.62</td>
</tr>
</tbody>
</table>
6.5 Conclusion

The chapter provides methodologies for cluster head selection and security in WSN. Since, WSNs are applied in such environment where it becomes vulnerable to security threats. The cluster head inside the cluster in WSN can provides balancing of energy and task among the nodes in the cluster. The methodology for cluster head provides improvement in throughput in the situation where the role of cluster head can rotates among the sensor nodes. Due to the application area of WSN the sensor nodes inside the WSN crashed frequently, the developed methodology provides a recovery strategy to overcome this problem. The chapter gives a methodology for hiding the location of sink from attacker. It performs efficiently and improves the throughput by 62.68%, decreases the delay 64.14% at the sink and provides the traffic received at sink 95.17%.