CHAPTER 3

AN ENERGY EFFICIENT CLUSTER DEPENDENT LEADER ELECTION IN MANETS

3.1 INTRODUCTION

One of the primary concerns related to Mobile ad hoc networks is to provide low energy consumption and secure communication among mobile nodes. Since the nodes in MANET perform all its activities by themselves and the network activities are carried out by nodes cooperation, energy consumption and security pose a serious issue. Unlike traditional networks, it is not possible to have centralized ID to monitor the network. In most of the cases, the size of the network could not be predicted. To overcome these issues the common approach followed is to divide the network into a set of one hop or multihop clusters where each node in the network belongs to at least one cluster. Nodes in the cluster elect a leader which acts as the IDS for the cluster. The leader node election can either be random-based given by Huang & Lee (2003) or connectivity based given by Kachirski & Guha (2002). Both the methods have the drawback of letting some nodes to die earlier than others. Unfortunately, these methods fail to balance the remaining resources during the election process due to false information about nodes. Though energy is considered as the private information, nodes which utilize the service of the other nodes (cluster head) lie about their resource level with the selfish intention of not to offer service to others. Thus, the nodes have to be motivated to render truthful information and to avoid selfish behaviour.
3.2 CLUSTERING

The characteristic of each cluster may vary due to nodes mobility. The clustered ad hoc network maintains relatively a stable topology and supports in making the route search process more efficient. The cluster topology guarantees less flooding and easy discovery of optimal routes between source and destination. A cluster structure is illustrated in Figure 3.1. Under a cluster structure, mobile nodes may be assigned a different status or function, such as Cluster Head (CH), Cluster Gateway (CG), or Cluster Member (CM). A CH normally serves as a local coordinator for its cluster members, performing intra-cluster transmission, data forwarding and monitoring. A CG is a non-CH node with inter-cluster links, so it can access neighbouring clusters and forward information between clusters. A CM is an ordinary node, which is a non-CH node without any inter-cluster links.

![Figure 3.1 Cluster structure](image)
3.3 SYSTEM MODEL

Since energy is one of the prime factors, every node tries to conserve its own energy to prolong its lifetime in the network. This makes the node to behave selfish and non-cooperative with its neighbours. Hence, to motivate nodes to truthfully participate in the network activities, in this chapter a new Secure Cluster Dependent Leader Election (S-CDLE) mechanism is proposed to optimize the energy utilization among nodes in the cluster and to encourage the cluster members to reveal the truth by means of incentives during the election process. To conserve energy, mobility is considered as one of the parameters in the leader election process. This is done, so as to eliminate the frequent leader election process that happens in the case of the CH moving out of the cluster.

In S-CDLE the nodes in the network are grouped as clusters by the grid-based approach, where it reduces the processing time while rearranging the clusters. We also address the identity delegation attack caused by selfish nodes. The nodes are motivated to follow truth telling strategy with the help of incentive payment. The incentives are given to nodes to reveal their private information as given by Mas-Colell et al. (1995). The Vickrey, Clarke, and Groves (VCG) approach guarantees that the nodes follow truth telling strategy. Moreover, the efficient election mechanism to identify selfish nodes reduces the overhead on the network compared to static (IDS).

3.4 IDENTITY DELEGATION ATTACK

Owing to the dynamic topology and absence of centralized management, MANETs are more vulnerable to threats from compromised nodes. The attacks can be classified into two types: external and internal attacks. External attacks are carried out by nodes that do not belong to the network. They cause congestion, false routing information or cause
unavailability of services whereas the latter is injected by compromised nodes that are part of the network. In internal attacks the malicious node from the network gains unauthorized access and impersonates as a genuine node. A selfish node in a network is a node which portrays itself as a legitimate node depleting the network resources. Any network with selfish nodes is easily susceptible to intrusion and identity delegation attack. An identity delegation attack, according to Alex & Ashwin (2013), is an internal attack where two malicious nodes which are part of the network are used by the attacker to drop the packet. One node is spatially close to the sender. The other node is the next hop from the sender. Consider the scenario illustrated in Figure 3.2 where node $S$ sends a packet to the malicious node $M_2$ to be relayed to node $T$. The attacker delegates the identity and credentials of the compromised node $M_2$ to a colluding node $M_1$ close to sender $S$. After $S$ sends the packet to node $M_2$, $M_1$ uses the delegated identity of $M_2$ and transmits the packet. The intended next hop of $M_2(T)$ will not get the packet since it is not in the range of $M_1$. In case of cluster topology, the CM can exhibit selfish behaviour of stealing the identity of other CM nodes in the cluster for performing malicious activity.

![Figure 3.2 Identity delegation attack](image)

Figure 3.2 Identity delegation attack
3.5 SYSTEM OVERVIEW

S-CDLE mechanism requires clusters with initial head elected based on the distance and mobility of the node. During the election process the nodes broadcast their cost within the cluster. Based on the cost, nodes cooperate to elect a leader node after which the leader distributes the incentives (a form of reputation) to the nodes voted for it. The secure leader election is ensured by encryption of the incentive packet distributed by the leader. The mechanism based design model is adopted for designing incentives in the form of reputation to encourage nodes to honestly participate in the election scheme by revealing their cost. To motivate the nodes to behave truthfully in every election round, we relate the amount of services provided by the CH to its members according to the node’s reputation value. Besides, this reputation value is used to give routing priority and build a trust environment. The nodes are rewarded in the form of incentives for their legitimate activities; the nodes can acquire an incentive when they actively participate in the network activities. The nodes which conserve their energy or refuses to participate in the regular network activities cannot earn the incentive. At the same time, when a node misbehaves by transmitting unnecessary packets to earn incentive it will be monitored by cluster head. Thus, the mechanism helps to identify and prevent selfish nodes.

3.5.1 Cluster Formation

The goal of cluster formation is to impose a structure or hierarchy in the MANET. Clustering reduces the traffic by limiting the packet transmission during head election process. Based on the grid-based approach the clusters are formed and the network is divided into grids. The division of the network topology into grids is done taking into account the transmission
range of each node. The size of the grid depends upon the number of nodes in 
the networks. If the number of nodes in a particular grid is more than a certain 
threshold value, the grid is further divided into smaller grids. This approach 
has the advantage of reduced computational complexity, mainly for the 
clusters with a large number of nodes. As grid-based algorithm has the 
coverage of lower data transmission range, less energy is utilized for 
transmission. This reduces traffic overhead for a single CH to manage a large 
amount of CM information.

The clusters are formed by calculating relative distance of the node 
from their neighbour nodes. The distance vector consisting of the relative 
distance values is constructed for every node in the network. From the 
distance vector value of every node the maximum value is identified which 
denotes the maximum reachability of the node. From this set of maximum 
values, the node with less mobility is chosen as CH to ensure stability of the 
cluster for a longer period of time. The reason for choosing a less mobile node 
as CH can be justified by the amount of energy dissipation involved in the 
activities of a cluster. Since CH is responsible for monitoring activities of the 
cluster, it requires more energy to manage member information and for 
communicating to the other CHs. Thus, the initial cluster formation is 
efficient as it selects the less mobile node as CH. The algorithm for cluster 
formation is given in Algorithm 3.1.

**Algorithm-3.1. Initial Leader Election**

```plaintext
begin
    /*compute mobility vector for each node*/
    if(NodeID != NodeID_{neighbour})
        /* Compute relative distance of node_i(x_i, y_i)
        from each of its neighbour node_j(x_j ,y_j)*/
```
\begin{align*}
    \text{dist\_vector}[i] &= \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2} \\
    \text{Mob\_vector}[i] &= \text{dist\_vector}[i](T_2 - T_1) /*for each node i*/ \\
    \text{Max\_dist}[i] &= \text{Max}(\text{Mob\_vector}[i]) \\
    \text{CH\_ID} &= \text{min}(\text{Max\_dist}[i])
\end{align*}

3.5.2 Leader Election

The proposed S-CDLE mechanism imposes that every node in the cluster must reveal its own private information (cost) based on the node type. This works under the principle of game theory. The type of the player (node) is known from each player available type set defined as normal and selfish. Each player selects his own strategy according to how much the node values the outcome. If the players’ strategy is normal, then the node reveals the true cost. The leader election algorithm is individually invoked in every cluster without disturbing the entire network. The election process consists of four phases that include cost calculation, voting, payment, and incentive distribution. The election mechanism is invoked when:

i. A new node enters/leaves the cluster

ii. The energy level of the CH falls below the threshold value

iii. The node stays as CH for a longer period of time

3.5.2.1 Cost calculation

Cost function is designed by considering two properties: privacy and stability. The former is to avoid the depletion of resource level by selfish nodes, which is considered as the most sensitive information. On the other hand, the latter is to avoid frequent head elections resulting in depletion of
network resources. The cost determines the node to be elected as the leader. Factors to be considered in the calculation of cost function are discussed below.

(a) Mobility

In MANET, the time that the node remains bound to a cluster also depends upon the mobility of the node which is calculated as relative distance per unit time. The selection of mobility parameter in cost calculation can be justified as the node which has less mobility stays as CH for a longer period of time avoiding frequent election. The election mechanism can be executed only when it is needed, thus conserving network resources. Therefore, less mobile nodes are considered as potential candidates for leadership. Thus, mobility of the node is an important factor and the cost is directly proportional to mobility. The mobility of a node can be expressed as

\[
M_i = \frac{\text{Relative Distance}}{\text{Time Taken}}
\]

\[
M_i = \frac{\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}}{(y_2 - y_1)}
\]

(3.1)

where \(M_i\) is the mobility of node, \((x_1, y_1)\) is the initial position of the node at time \(T_1\), \((x_2, y_2)\) is the final position of the node at time \(T_2\) and \((T_2 - T_1)\) is the time interval.

(b) Reputation

The reputation reveals the degree of legitimate behaviour of the node. The leader must have higher reputation as it is entrusted with the responsibility of monitoring member nodes. The relative reputation is calculated for each node with respect to the cluster to which it belongs. A
node with high reputation is essentially a potential candidate for election. The relative reputation value of \( node_i \) in each cluster \( C_j \) is calculated as

\[
Rep_i = \frac{R_i}{\sum_{i=0}^{n} R_i}
\]

where \( Rep_i \) is the relative reputation of the \( node_i \) in cluster \( C_j \), \( j \in C \), \( R_i \) is the reputation value of \( node_i \), \( n \) is the total number of nodes in cluster \( C_j \) and \( C \) is the total number of clusters.

(c) Energy Level

A leader node requires more energy compared to the other member nodes for monitoring and performing cluster services. If a lesser energy node is elected as a leader, the energy will dissipate in a short time resulting in re-election, which leads to the ease of leader’s service. Thus, a higher energy node is considered as potential candidate for election.

\[
Cost = \text{Relative reputation} \times \frac{\text{Mobility of the node}}{\text{Energy per unit time}}
\]

\[
= \left( \frac{R_i}{\sum R_i} \right) \times \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2} \frac{\text{power}_i}{\text{power}_i}
\]

Thus, the cost function can be expressed as:

\[
Cost_i = Rep_i \times \frac{D_i}{\text{power}_i}
\]  \hspace{1cm} (3.2)

where \( cost_i \) is the cost value of \( node_i \), \( Rep_i \) is the relative reputation value of \( node_i \), \( D_i \) is the relative distance value of \( node_i \) and \( \text{Power}_i \) is the energy of \( node_i \).
3.5.3 Voting and Election

During election, every node broadcasts its cost to the other nodes within the cluster. The cost decreases with increased energy as given in Equation (3.2). Based on the minimum cost, the nodes vote to elect a leader. The node which has received the maximum number of votes becomes the leader for the cluster. The leader then distributes incentives to the nodes that have voted for it to encourage the nodes to participate honestly in the further election rounds. The design of incentives is based on a classical mechanism design model VCG. To motivate the nodes to behave truthfully in every election, we relate the amount of services provided by the CH to the nodes’ reputation. According to Cluster-Based Routing Protocol (CBRP), all inter-cluster communication is done through CH. The node with the highest reputation is considered as the most trusted node and is given priority for routing by CH. If two nodes A and B, belonging to the same cluster, request their CH at the same time to transmit packet to their respective destination nodes in other clusters, then the CH can accept only one request for packet transmission at a particular instant and the node with higher reputation is given priority. Thus, each node is motivated to truthfully participate in every election for increasing their reputation. The Algorithm 3.2 describes the leader election process.

Algorithm-3.2. Leader election

begin
/*n is the number of nodes in a cluster*/

\[ R_i = R_{INITIAL} \quad /* R\text{INITIAL takes a value of 5, at the start */} \]

/*calculate relative reputation of a node in each cluster*/

for all node \(i \) in cluster

\[ \text{Rep}_i = R_i / \sum_{i=0}^{n} R_i \]

/*calculate cost for each node*/

\[ \text{Cost}_i = \text{Rep}_i \times D_i / \sum_{i=0}^{n} R_i \times \text{Power}_i \]

/*on receiving hello all nodes reply with their cost*/
if(received hello from all neighbours)
    Begin_Election
    Broadcast_Cost(NodeIDᵢ, Costᵢ)
else
    if(neighbour(i) = 0)
        Stateᵢ = CH
        isleader(i) = TRUE
    endif
endif
endfor
end

3.5.4 Incentive and Payment

The secure leader election is ensured by encryption of the incentive distributed by the leader. RSA algorithm is used for securely transmitting the incentive from CH to member nodes. A selfish node will lose its conserved energy if elected as a leader; thereby it refrains from participating in the election mechanism. If it fails to participate, it will not receive the incentive that the leader distributes to the nodes that have voted for it. The only way it can refrain from participating in the election and yet receive the incentive is by stealing the identity of the other node that has participated in election. Algorithm 3.3 depicts how the payment and incentives are calculated. The aim is to conserve the identity of the node by encrypting the incentive and maintain a public-private key pair for each node. The leader node distributes the incentive encrypted by the node’s public key. The node decrypts the message with the help of its private key (known only to the node), which prevents the identity delegation attack and thus ensures secure leader election. The secure incentive distribution by the leader can be expressed as:

\[ Send\_incentive \left( Encrypt \left( Pb_{CM}, Incentive_{CM} \right) \right) \]

\[ Receive\_incentive \left( Decrypt \left( Pr_{CM}, Incentive_{CM} \right) \right) \]
where $Incentive_{CM}$ is the incentive given by CH to CM, $Pb_{CM}$ is the public key of the CM and $Pr_{CM}$ is the private key of CM. Each cluster is assigned equal Budget (B) for every election process. The incentive to be distributed by CH to its members depends on the number of votes that the elected node has received and the budget as shown in Equation (3.3). The node that does not cast any vote will not receive any incentive from CH. The incentive given to each node depends on the nodes’ relative reputation within the cluster. Hence, any node will strive to increase its reputation in order to receive more services from the leader. The payment to CH can be expressed as:

$$P_{ch} = \sum_{i=0}^{n} vote_{ch}(i, Cost_i) \times B$$ (3.3)

where $P_{ch}$ is the payment given to CH, $vote_{ch}(i, Cost_i)$ is a Boolean value which is true if $node_i$ has voted for CH and B is the total budget value for a cluster.

![Figure 3.3 Election of CH in the presence of selfish nodes](image-url)
Algorithm-3.3. Incentive and Payment

begin

/*Every node $i$ votes for node $k$ within the cluster $C_j$ */

$i; k \in n; j \in C$

if(there exists a node $i$ such that cost$_i < $ cost$_k$)

leader$_n$ode$(i) = i$

isleader$(i) = TRUE$

state$_i = CH$

if(isleader$(i) = TRUE) )$

Send Join$_req$(NodeID$_{CH}$, NodeID$_{CM}$)

Update node details

/*Calculate payment for CH of each cluster*/

$P_{ch} = \sum_{i=0}^{n} vote_{ch}(i, Cost_i) * B$

/*Send payment for each node*/

Send_incentive (Encrypt (Pb$_{CM}$, Incentive$_{CM}$)

end if

else

Send_vote(NodeID$_k$, NodeID$_b$, cost$_k$)

leader$_n$ode$(k) = i$

isleader$(k) = FALSE$

state$_k = CM$

Receive Join$_Ack$(NodeID$_k$, NodeID$_{CH}$)

Receive_incentive (Decrypt (Pr$_{CM}$, Incentive$_{CM}$)

endif

end
Table 3.1 Costs of nodes in cluster 1

<table>
<thead>
<tr>
<th>Node ID</th>
<th>Cost</th>
<th>Reputation-I</th>
<th>Reputation-II</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>8.1</td>
<td>10</td>
<td>15</td>
</tr>
<tr>
<td>13</td>
<td>12.5</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>11</td>
<td>8.9</td>
<td>9</td>
<td>11</td>
</tr>
<tr>
<td>4</td>
<td>10.6</td>
<td>10</td>
<td>12</td>
</tr>
<tr>
<td>16</td>
<td>9.8</td>
<td>8</td>
<td>11</td>
</tr>
</tbody>
</table>

Figure 3.3 represents the topology of MANETs with 18 nodes divided into 4 clusters using grid-based approach, where the relative distances of every node from the neighbour nodes are computed from the distance Equation (3.1). Every node broadcasts its cost to the every other node within the cluster. For example in cluster 1, node 9 has the least cost compared to other nodes within the cluster and is elected as the leader. Table 3.1 presents the cost of nodes in cluster 1. Node 9 distributes the incentive to its members, after it has been elected, based on the reputation of CMs. Nodes with higher reputation receive more incentive.

The reputation of node increases with every round as a portion of the incentive is added to the node’s current reputation. Reputation I and Reputation II in Table 3.1 denote the reputation value of nodes in subsequent election rounds. Identity delegation attack is created by node 13 in cluster 1 by stealing the identity of node 11. The probability of node 11 receiving the incentive is less than 1 as the two nodes (11 and 13) are waiting to receive their incentive. Node 13 attempts to decrypt the incentive packet with its own private key resulting in unsuccessful decryption. A node being identified as selfish does not receive any incentive from the leader and hence its reputation remains the same. In Figure 3.3, node 13 is identified as a selfish node, stealing the identity of node 11 since it has the same reputation value as that
of the previous round. But other nodes in the cluster have increased their reputation. Thus, secure incentive payment is ensured. Figure 3.4 shows the message broadcasts between CH, legitimate node, and selfish node.

3.6 MATHEMATICAL PROOF

Let $N$ be the number of nodes that try to receive the incentive, $N_s$ be the number of nodes that are successful in stealing and $R_i$ be the relative reputation of the node with respect to its cluster $C_j$. For each node $N_i$ in $N_s$, if encryption is successful $R_i = R_i + \text{Incentive}_i$, else $R_i = R_i$. Number of nodes that cast vote to the $CH = N - N_s$. Let $P'_i$, be the probability of a node $n$ not receiving the incentive and $N - N_s$ denotes the number of legitimate nodes waiting to receive the incentive. Let $X$ be the number of iterations. Let $A_1$ be the product of probability of a legitimate node not receiving the incentive in $n$ iterations of CILE mechanism, and $A_2$ be the product of probability of a legitimate node not receiving the incentive in $n$ iterations of S-CDLE mechanism.

\[
P'_n = 1/(N - N_s)
\]

\[
A_1 = \prod_{i=0}^{X} P'^i_n
\]

\[
A_2 = \prod_{j=0}^{X} P'^j_n
\]

In the existing Cluster Independent Leader Election (CILE) mechanism, $N_s \rightarrow N - 1$, there is at least one legitimate node whose identity can be stolen by the other nodes in the cluster. The nodes can successfully steal the incentive of the legitimate nodes due to the absence of secure encryption mechanism. Thus, the product of probability of the legitimate node not receiving the incentive tends to 1 in each iteration. In S-CDLE mechanism, $N_s < N - 1$ as the secure encryption mechanism identifies the selfish nodes and prevents
them from receiving the incentive. In the existing Cluster Independent Leader Election (CILE) mechanism, $N_s \rightarrow N - 1$, there is at least one legitimate node whose identity can be stolen by the other nodes in the cluster. The nodes can successfully steal the incentive of the legitimate nodes due to the absence of secure encryption mechanism. Thus, the product of probability of the legitimate node not receiving the incentive tends to 1 after every iteration. In S-CDLE mechanism, $N_s < N - 1$ as the secure encryption mechanism identifies the selfish nodes and prevents them from receiving the incentive. In S-CDLE approach the product of probability of the legitimate node not receiving the incentive will always be less than 1 as the nodes identified as selfish do not have increased reputation value in subsequent elections. In CILE mechanism, $N_s \rightarrow N - 1$, $\lim_{N_s \rightarrow N-1} N - N_s \Rightarrow N - (N - 1) = 1$. 

**Figure 3.4 Message broadcast in a cluster**
From Equation (3.4) $P'_n \to 1$. Therefore in CILE, the probability of a legitimate node not receiving the incentive is 1. In S-CDLE mechanism, $N_2 < N - 1 = N - N_s > 1$. From Equation (3.4), $1/(N - N_2) < 1$ is obtained. Thus, $P'_n < 1$. Therefore, in S-CDLE mechanism, the probability of a legitimate node not receiving the incentive is less than 1. Thus, $A_2 \leq A_1$.

### 3.7 SIMULATION RESULTS

S-CDLE leader election mechanism is simulated using NS2. The comparative results show the performance analysis of the CILE by Mohammed et al. (2011) and S-CDLE payment design. In the existing approach, CILE overcomes all the other traditional methods like weight-based, connectivity-based and random-based approaches but the proposed S-CDLE incorporates the grid-based and load balancing methods to overcome CILE. Thus, stability is maintained in S-CDLE over CILE.

#### 3.7.1 Simulation Environment

The simulation environment consists of nodes with maximum transmission range of 250m. The clusters are formed using the grid-based approach where each node belongs to one cluster. In the case of overlapping clusters, the node is assigned to one of the clusters based on the closeness of the node to the CH. The energy model in NS2 is used to measure the energy dissipation of nodes using four metrics namely idle power, sleep power, transmission power and reception power. Initially, 100 joules of energy is assigned for each of the nodes. The lifetime of the node is calculated by constantly measuring the energy and mobility of each node. The algorithm is tested for 20, 30 and 40 nodes to measure the performance of the S-CDLE mechanism. The simulation parameters are summarized in Table 3.2.
3.7.2 Performance Analysis

The objective of performance analysis is to study the performance and to compare the stability of CH with respect to CILE and S-CDLE mechanisms in the presence of identity delegation attack. As the algorithm runs in separate clusters under three conditions specified in Section 3.5.2.1, the network overhead is reduced by avoiding frequent head elections, thereby increasing the stability factor. For larger networks, frequent head elections may become a constraint on the information management and network resources. The CILE mechanism undergoes frequent CH changes in each iteration to ensure the property of fairness. The rate of change of CH in S-CDLE is less compared to CILE mechanism as shown in Figure 3.5, Figure 3.6 and Figure 3.7 for 20, 30 and 40 nodes, respectively.

Table 3.2 Simulation parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation time</td>
<td>200 seconds</td>
</tr>
<tr>
<td>Movement model</td>
<td>Random waypoint model</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>20, 30, 40</td>
</tr>
<tr>
<td>Transmission range</td>
<td>250m</td>
</tr>
<tr>
<td>Traffic type</td>
<td>CBR/UDP</td>
</tr>
</tbody>
</table>

The X-axis indicates the Cluster ID and the Y-axis indicates the cluster ID of every cluster. The values are represented for 4 iterations of the algorithm. S-CDLE ensures that the rate of change of CH is less, thus providing stability. The reputation value of the nodes is regarded as a parameter to analyze the effect of identity delegation attack by the selfish nodes.
The node need not express its selfish behavior by dropping the packets. All selfish nodes may not be malicious and the motive of such nodes may be to conserve energy. Selfish behavior of the nodes may lead to malicious activities. The identification of the selfish behavior by S-CDLE mechanism is to prevent the future malicious activities of the node. In the election of CH, S-CDLE mechanism does not allow the reputation of suspected nodes to increase in further iterations, whereas the reputation of the nodes in CILE mechanism keeps increasing till they are identified as malicious. The results are shown in Figure 3.8.

The energy of the node denotes their lifetime which is considered as the most important factor in MANET. Any mechanism proposed for MANET should handle the resources with less depletion of energy. If energy depletes at a faster rate, the nodes die and IDS present in the nodes cease to function. Energy plays a crucial role in IDS-based applications. The election scheme consumes energy of the nodes, hence frequent elections may cause considerable amount of energy to be utilized for electing CH rather than for managing cluster activities and routing.
Figure 3.6 Rate of change of CH for 30 nodes

Figure 3.7 Rate of change of CH for 40 nodes

Figure 3.8 Reputation value of S-CDLE and CILE mechanism
The comparative analysis of remaining energy of the nodes in CILE and S-CDLE election mechanism is depicted in Figure 3.9, Figure 3.10 and Figure 3.11 for 20, 30 and 40 nodes, respectively. As CH election algorithm is invoked in individual clusters independently, the lifetime of the cluster is increased by avoiding frequent CH elections, which proves to be highly beneficial for larger networks with more number of clusters. Table 3.3 represents comparison of the average remaining energy of the nodes in each cluster for CILE and S-CDLE mechanism. In this proposed work, the change of cluster head and comparison of energy values between CILE and S-CDLE is analyzed. The computation cost of the nodes and energy value is shown in, Table 3.1 and 3.3 respectively.

Table 3.3 Comparison of energy values in joules

<table>
<thead>
<tr>
<th>Cluster ID</th>
<th>S-CDLE</th>
<th>CILE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster 1</td>
<td>99.785</td>
<td>99.102</td>
</tr>
<tr>
<td>Cluster 2</td>
<td>99.786</td>
<td>99.178</td>
</tr>
<tr>
<td>Cluster 3</td>
<td>99.738</td>
<td>99.302</td>
</tr>
<tr>
<td>Cluster 4</td>
<td>99.697</td>
<td>99.303</td>
</tr>
<tr>
<td>Cluster 5</td>
<td>99.724</td>
<td>99.354</td>
</tr>
<tr>
<td>Cluster 6</td>
<td>99.790</td>
<td>99.076</td>
</tr>
<tr>
<td>Cluster 7</td>
<td>99.738</td>
<td>99.093</td>
</tr>
</tbody>
</table>
Figure 3.9 Percentage of remaining energy for 20 nodes

Figure 3.10 Percentage of remaining energy for 30 nodes
3.8 CONCLUSION

The proposed S-CDLE mechanism for cluster-based network provides an efficient solution for the detection of selfish nodes in MANET. The mechanism focuses on prolonging the lifetime of CH in a cluster and limited use of cluster resources for leader head election. The solution motivates the node to truthfully elect the most cost-efficient leaders. The encryption of the incentive by the leader node strengthens the mechanism to prevent the selfish behaviour of the nodes. To achieve the normal behaviour of nodes, incentives are given in the form of reputations to encourage the nodes in revealing their costs truthfully. To prevent identity delegation attack, incentives are encrypted using secure private-public key pair. Even in the presence of selfish nodes, it is demonstrated that S-CDLE mechanism reduces the number of clusters, single node clusters and the network information overhead, when compared to the existing cluster-based election models.

Figure 3.11 Percentage of remaining energy for 40 nodes